НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НДІ ТЕЛЕКОМУНІКАЦІЙ

Дванадцята міжнародна науково-технічна конференція

"ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ"

і

Десята міжнародна науково-технічна конференція студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ»

Присвячено Дню науки та Всесвітньому Дню телекомунікацій

16–20 квітня 2018 року

Матеріали конференції

м. Київ

NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE”

INSTITUTE OF TELECOMMUNICATION SYSTEMS
RESEARCH INSTITUTE OF TELECOMMUNICATIONS

Twelfth International Scientific Conference
"MODERN CHALLENGES IN TELECOMMUNICATIONS"

and

Tenth International Scientific Conference of
undergraduate and graduate students "PROSPECTS FOR DEVELOPMENT OF INFORMATION-TELECOMMUNICATION TECHNOLOGIES AND SYSTEMS"

Dedicated to the Science Day and the International Day of Telecommunication

April 16-20, 2018

Conference materials

Kyiv

XII Міжнародна науково-технічна конференція "Проблеми телекомунікацій" ПТ-2018: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2018. – 500 с.

X Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2018: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2018.

Збірник містить матеріали пленарних і секційних доповідей, представлених на Дванадцятій міжнародній науково-технічній конференції "Проблеми телекомунікацій" (ПТ 2018) та Десятій міжнародній науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС 2018), які проводяться 16–20 квітня 2018 р. в м. Києві

Електрона версія Збірника матеріалів Міжнародної науково-технічної конференції "Проблеми телекомунікацій" (кожна стаття має свою URL-адресу) на http://journals.uran.ua/ за посиланням:
http://conferenc.its.kpi.ua/proc/issue/archive.

Робочими мовами конференцій є українська, російська та англійська.

У збірник включені матеріали конференції за такими секціями:

1. Достовірне передавання інформації в телекомунікаційних системах.
2. Кабельні та оптоволоконні системи і технології.
3. Технології транспортних телекомунікаційних систем та мережні технології.
4. Безпроводові телекомунікаційні системи та технології, системи 5G.
5. Інформаційні технології в телекомунікаціях.
6. Сенсорні мережі та прикладні аспекти застосування телекомунікаційних технологій.
7. Апаратно-програмні засоби та пристрої телекомунікацій.
8. Технічна творчість радіоконструкторів України.

Семінар: Modern information and telecommunication trends.
ВИСТАВКА: Технічна творчість радіоконструкторів України.

Вчений секретар конференції
БУНІН С.Г., д.т.н., проф. ІТС КПІ ім. Ігоря Сікорського.
E-mail: sgbunin@ukr.net

Секретар оргкомітету конференції
Іванова Т.Л.
р. тел/факс. (044)204-98-21.
E-mail: conf@its.kpi.ua

Співголови конференції "Проблеми телекомунікацій":

ІЛЬЧЕНКО М.Ю. – науковий керівник Інституту телекомунікаційних систем, проректор з наукової роботи Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», академік НАНУ, д.т.н., професор;

БАРАНОВ О.А. – керівник Центру теоретико-правових проблем інформаційної сфери Науково-дослідного інституту інформатики и права при Національній академії правових наук України, д.ю.н., професор.

Організатори конференції:

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», ІТС, НДІТ;
Міжнародний науково-технічний журнал «TELECOMMUNICATION SCIENCES» ISSN: 2312-4121.

Спонсори конференції:

Організації та підприємства, які беруть участь в науково-інноваційній діяльності та в працевлаштуванні випускників ІТС, а також всі бажаючі.

Координатор Програмного комітету:

КРАВЧУК С.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ,
e-mail: sakravchuk@ukr.net

Члени Програмного комітету "Проблеми телекомунікацій":

БОГУШ В. М. - к.т.н., доц., НАУ, Київ;
БУНІН С.Г. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ГЛОБА Л.С. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ГУДИМЕНКО І.А. - Dr.-Eng. at T-Systems MSC, Дрезден, Німеччина;
ДОРОГАН Валерьян - Prof. Dr. Technical University of Moldova, Кишинів, Молдова;
ЖУК С.Я. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ЗАВИСЛЯК І.В. - д.ф.м.н., проф., КНУ ім. Т. Шевченко, Київ;

КАПШТИК С.В. . - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
КАТОК В.Б. - к.т.н., проф., ПАТ «Укртелеком», Київ;
КИСЕЛЬОВ Стів - PhD St. of Friedrich-Alexander-University, Нюрнберг, Німеччина;
КОЗЕЛКОВ С.В. - д.т.н., проф. ДУТ, Київ;
КОТ Т.М. - Dr.-Eng., Solutions Architect, NVision Czech Republic, Прага, Чехія;
ЛЕМЕШКО О.В. - д.т.н., проф., ХНУРЕ, Харків;
ЛИСЕНКО О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ЛУНТОВСЬКИЙ А.О. - Prof. at BA Dresden University, Дрезден, Німеччина;
МАКСИМОВ В.В. - к.т.н., доц. КПІ ім. Ігоря Сікорського, Київ;
МОШИНСЬКА А.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
НАЗАРЕНКО О.І. – факультет лінгвістики КПІ ім. Ігоря Сікорського, м. Київ;
НАРИТНИК Т.М. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ПОПОВ В.І. - д.м.-ф.н., проф., РТУ, м. Рига, Латвія;
ПРАВИЛО В.В. – к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
РОМАНОВ О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
РОМАНЮК В.А. - д.т.н., проф. ВІТІ, Київ;
СЕРГІЄНКО М.І. – к.т.н., доц. каф. ІЕ, ІЕЕ, КПІ ім. Ігоря Сікорського, Київ;
СКУЛИШ М.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
СТРИЖАК О.Є. - к.т.н., НЦ «Мала АНУ», Київ;
ТЕНШИ Хара - Dr.-Eng. Technical University of Dresden, Дрезден, Німеччина;
ТОЛЮПА С.В. – д.т.н., проф., НУ ім. Т.Г.Щевченка, Київ;
ТРУБІН О.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
УРИВСЬКИЙ Л.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ФЕЛЬДМАНН Маріус - Dr.-Eng. Technical University of Dresden, Дрезден, Німеччина;
ЧЕЧЕЛЬНИЦЬКИЙ В.Я. - д.т.н., проф., ОНПУ, Одеса;
ЧУМАЧЕНКО С.М. - д.т.н., с.н.с., УНДІЦЗ, Київ;
ШЕЛКОВНІКОВ Б.М. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ШПІЛЬНЕР Йозеф - Dr. at ZHAW School of Engineering, Цюріх, Вінтертур, Швейцарія;
ЯВІСЯ В.С. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ЯКОРНОВ Є.А. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ.

Технічний комітет:

1. Слюсар В.С. – транспорт, поселення, т. 204-98-21.
2. Дуля Ю.А. – головний бухгалтер НДІ ТК, т. 236-95-04.
3. Березовська О.В. – реєстрація, забезпечення документообігу, т. 204-98-21.
4. Мікляєв О.В. – технічне обслуговування електронної техніки, т. 204-98-21.
5. Мазанка Р.М. – оформлення конференції на сайті ІТС, т. 204-98-91.

Адреса для листування, телефони, e-mail:

03056, г. Київ, провулок Індустріальний, 2, корпус 30, секретарю оргкомітету конференції «ПТ» Івановій Т.Л., тел/факс. (044)204-98-21, conf@its.kpi.ua.

Адреса проведення конференції:

03056, г. Київ, провулок Індустріальний, 2, корпус № 30 КПІ ім. Ігоря Сікорського, 4 поверх.

ЗМІСТ

Пленарні доповіді

Доповідачі:

Палагін О.В., Романов В.О., Галелюка І.Б., Вороненко О.В., Груша В.М., Ковирьова О.В., Антонова Г.В., Лаврентьєв В.М., Брайко Ю.О., Імамутдінова Р.Г.
"Розумні" сенсорні мережі: від ідеї до ринку.....18

Volkmar Brückner. Dispersion management in single-mode fibers. 21

Ільченко М.Ю., Кайденко М.М., Кравчук С.О. Структурно-функціональні принципи побудови системи управління та зв'язку бортового і наземної обладнання телекомунікаційної Мережі на основі аероплатформ.....26

Мошинська А.В., Уривський Л.О. Декомпозиція процесів переходу від сценарію до стратегії передачі інформації у мультисервісній системі. 30

Казанцев Олександр. Мультифункціональна програма MixW4 для проведення цифрових видів радіозв'язку. .....*

Джулай В.М. Новітні технології зв'язку на базі SDR комплексів. .....*

Романюк В.А., Лысенко А.И., Степаненко Е.А., Романюк А.В., Жук А.В. Алгоритм принятия решений по управлению тактической беспроводной сенсорной сетью 33

Gvozdetska N.A., Globa L.S. Energy efficiency and performance improving in data center with predefined load types.....36

Новогрудська Р.Л., Юшко Н.А. Методи пошуку даних на порталі національного антарктичного наукового центру України.....39

Sulima S.V. Model for allocation of network slices in heterogeneous environment.....42

* - статті до збірника не входять.

Секція 1. Достовірне передавання інформації в телекомунікаційних системах

Співголови:
д.т.н., проф. Уривський Л.О., к.т.н., доц. Максимов В.В., к.т.н., доц. Мошинська А.В.

Доповідачі:

Грицко А.В., Гаттуров В.К. Огляд основних факторів, що впливають на якість передачі даних в мережах LTE 45

Уривський Л.О., Шевченко М.В. Особливості передачі мультисервісних потоків в стандарті DVB-T2 ТА використання їх у дуплексній лінії зв'язку 48

Яровий О.В., Пархомей І.Р. Енергетичний потенціал атмосферних оптичних систем передачі 51

Парфенюк В.Г., Сабадаш С.С. Оптимальний некогерентний демодулятор ВФМ-2 сигналів із манчестерським кодуванням модулюючого сигналу 54

Максимов В.В. Покращення технології локалізації протоколу OLSR 58

Воронюк М.М., Гаттуров В.К. Переваги використання та методи підвищення економічних показників системи моніторингу nagios для оператору зв'язку 61

Мокій А.В., Горицький В.М. Дослідження методів обробки ризиків в системі управління інформаційною безпекою 64

Павленко В.В., Горицький В.М. Основи проведення аудиту системи управління інформаційної безпеки 67

Цвілій О.О., Некраш І.І. Оціночні стандарти у сфері інформаційної безпеки 70

Секція 2. Кабельні та оптоволоконні системи і технології

Співголови: к.т.н., проф. Якорнов Є.А., к.т.н., проф. Каток В.Б.

Доповідачі:

Романишин В.С., Бердников О.М. Нарощування пропускної спроможності телекомунікаційних транспортних систем 74

Щирий А.В., Бердников О.М. Порівняння шляхів підвищення пропускної спроможності лінійних трактів телекомунікаційних транспортних систем 77

Носков В.І., Большаков Ю.Є. Дослідження впливу параметрів кабельного середовища на роботу цифрових систем передачі за XDSL технологією 80

Григоренко О.Г., Савченко П.П. Переваги використання пасивних оптичних мереж 83

Варваринець С.В., Правило В.В. Забезпечення безпеки передачі інформації в LTE 86

Секція 3. Технології транспортних телекомунікаційних систем та мережні технології

Співголови: д.т.н., проф. Романов О.І., д.т.н., проф. Лемешко О.В.

Доповідачі:

Лемешко О.В., Євдокименко М.О. Тензорна модель забезпечення якості сприймання користувачами мультимедійного потоку 89

Романов А.І., Федюшина Д.М., Донг Т.Т. Використання технології VLC для побудови мереж LI-FI та принцип її практичної реалізації 92

Нестеренко М.М., Верес Л.А. Взаємодія різних видів телефонних мереж із сучасними мережами передачі даних на базі платформи IMS 95

Світанько Н.В., Веревкін Л.Л., Хрипко С.Л. Принцип побудови телекомунікаційної системи з використанням оптичного підсилювача (EDFA) на базі технології LI-FI 98

Триска Н.Р. Синхронизация в телекоммуникациях нового поколения: обзор технологий и стандартов 101

Наритник Т.М., Єрмаков А.В., Постернак Б.С., Клин І.М., Сарапулов С.В. Використання LI-FI для передачі даних за допомогою видимого світла 104

Якимчук Н.М., Олянський В.В. Характеристика системи тактової мережевої синхронізації для оцінки часу затримки мережі 107

Лемешко О.В., Єременко О.С. Тензорна модель відмовостійкої QoS маршрутизації в інфокомунікаційній мережі 110

Полякова А.С., Сбоєв Р.Ю., Єрохін В.Ф. Асимптотичний аналіз протоколу випадкового множинного доступу «Ненаполегливий МДКН-ВК» при розв’язанні парних конфліктів на фізичному рівні 113

Верес Л.А., Омельченко Р.Ю. Аналіз архітектурних особливостей віртуалізації та переваги віртуальних контейнерів 116

Письменний І.С., Романов А.О. Мережа підприємства з програмним забезпеченням ASTERISK PBX на основі технології PLC 119

Єрмаков А.В., Постернак Б.С., Сарапулов С.В. Захист персональних даних в WI-FI мережі стандарту 802.11 122

Макарова Д.О., Лопата Д.Г., Ільницький А.І. Проблемна ситуація радіомоніторингу та напрямки її вирішення 125

Бірюков М.Л., Тріска Н.Р. Моделювання затримок пакетів точного часу 128

Романов О.І., Осокін М.Г. Аналіз рівня безпеки мереж сигналізації SS7 131

Наритник Т.М., Бондарчук С.О., Вальчук Д.С., Єрмаков А.В. Аналіз структури субгармонічних змішувачів для радіоліній терагерцового діапазону 134

Мєлєхова М.О., Носков В.І. Забезпечення QoS в TCP/IP мережах..... 137

Романишин В.С., Бердников О.М. Аналіз впливу хроматичної дисперсії в оптичних трактах на функціонування телекомунікаційних систем 140

Нестеренко М.М., Денисюк С.В. Модель оптимізації управління трафіком в мережах MPLS 143

Роговий В.П. Загрози безпеці у SDN середовищах..... 146

Полонський А.М., Міночкін Д.А. Аналіз існуючих алгоритмів розподілу навантаження на мобільні мережі на основі хмарних інфраструктур 149

Міночкін Д.А., Сушин І.О. Застосування LTE-R технології в телекомунікаційних системах залізниці 152

Секція 4. Безпроводові телекомунікаційні технології, системи 5G

Співголови: д.т.н., проф. Кравчук С.О., к.т.н., доц. Міночкін Д.А.

Доповідачі:

Лящук А.А. Дослідження використання OPEN VIRTUAL SWITCH в мережах SDN 155

Харченко Т.П., Правило В.В. Якість обслуговування (QOS) В LTE..... 158

Кравчук С.О. Ймовірність переривання зв'язку в когнітивній телекомунікаційній системі на базі аероплатформи 161

Кибенко А.В. Проблеми використання сервісу LBAAS в OPENSTACK для балансування навантаження..... 165

Авдєєнко Г. Л., Бунін С. Г., Наритник Т. М. Схемотехнічне моделювання генераторів UWB сигналів для безпроводових телекомунікаційних систем..... 168

Журавель А.С., Кравчук С.О. Динамічний доступ до спектру в мережах когнітивного радіо: підхід, що використовує теорію ігор 171

Адаменко І.О., Губар В.Г. Система для визначення концентрації домішок у дисперсному середовищі 174

Кравчук С.О., Кравчук І.М. Реалізація мімо-системи для ТСВА шляхом формування віртуальної антенної решітки 177

Кибенко А.В., Лящук А.А. Рекомендації для підвищення рівня безпеки хмарних систем на прикладі OPENSTACK 181

Заболотна А.Ю., Гаттуров В.К. Дослідження конвергенції мереж 2G та 3G на базі вузла IMS 184

Кравчук С.О., Афанасьєва Л.О., Кравчук І.М. Ієрархічна система управління і телеметрії для інтелектуальних безпілотних літальних апаратів 187

Кременецька Я.А., Морозова С.В., Андреєва Н.О. Підходи до фізичного моделювання радіоканалів зв'язку міліметрового діапазону хвиль 191

Кравчук С.О., Кравчук І.М. Ймовірність переривання зв'язку в телекомунікаційній системі на базі аероплатформи із задіянням міжплатформенного оптичного каналу у вільному просторі 194

Кайденко М.М. Роскошний Д.В. Архітектура програмно-визначуваних радіосистем для розробки радіообладнання 198

Кравчук С.О., Афанасьєва Л.О. Розподіл ресурсів з підтримкою заданої якості обслуговування для телекомунікаційної системи на основі аероплатформ 201

Кайденко Н.Н., Роскошный Д.В. Архитектура и выбор компонентов для приложений SDR 205

Макаренко А.О. Синтез OFDM-алгоритму безпроводових телекомунікаційних систем 208

Афанасьєва Л. О., Кравчук С.О., Шевченко І.І., Рисцова К.І. Схема кодованої кооперації 211

Малецький Д.В., Міночкін Д.А. Кодоване кешування 214

Шнурков В.О., Міночкін Д.А. Перспективы развития INTERNET OF THINGS с использованием сетей 5G 217

Казачінер К.А., Кравчук С.О. Технології віртуальних стільників у мережах п'ятого покоління 5G 220

Ильченко М.Е., Нарытник Т.Н., Рассамакин Б.М., Присяжный В.И., Капштык С.В. Концепция создания архитектуры «Распределенного спутника» для низкоорбитальных информационных и телекоммуникационных систем на основе группировки микро- и нано-спутников 223

Немченко К.В., Міночкін Д.А. Покращений алгоритм вертикальної синхронізації між WIMAX та WIFI 227

Секція 5. Інформаційні технології в телекомунікаціях

Співголови: д.т.н., проф. Глоба Л.С., к.т.н. Стрижак О.Є.,
к.т.н., доц. Скулиш М.А.

Доповідачі:

Пустовий Б.Л., Князєва Н.О. Автоматизація формування рівняння балансу марківського процесу 230

Радівілова Т.А., Тавалбех М.Х. Метод розшифровки трафіку TLS для виявлення прихованих загроз 233

Зайченко Ю.П., Васильев В.И., Вишталь Д.М., Любашенко Н.Д. Точные и граничные оценки стационарной вероятности доступности сетевой услуги 236

Могильний С.Б., Котик І.В. Аналіз методів паралельної обробки даних 239

Правило В.В., Белоха Д.К. Восстановление передаваемых сообщений на основе анализа сетевого трафика 242

Колюкаєва В.О., Новогрудська Р.Л. Метод композиції ВЕБ-сервісів 245

Кущ В.С., Штогріна О.С. Підхід до обробки та зберігання результатів оцінки психофізіологічного стану людини 248

Ряба Н.М., Правило В.В. Забезпечення виконання заданих показників якості обслуговування в мережах SDN..... 251

Давидюк А.М., Курдеча В.В. Виклики та проблематика в промисловому «Інтернеті речей» 254

Вергун А.І., Курдеча В.В. Безпека IoT систем за допомогою технології блокчейн 257

Коваленко В. Ю. Новогрудська Р.Л. Порівняльний аналіз підходів до побудови онтологічних моделей та баз даних 260

Прокопець В.А., Глоба Л.С. Експериментальне дослідження енергоефективності обробки даних в розподіленому ДАТА центрі 263

Запорожец Д.Б., Скулиш М.А. Анализ методов прогнозирования с использованием нейронной сети 266

Чічіков А.О., Штогріна О.С. Впровадження освітніх електронних застосувань в навчальний процес 269

Чиж В.В. , Скулиш М.А. Впровадження віртуалізації мережевих функцій на мережі платформи передачі SMS – повідомлень..... 272

Новогрудська Р. Л., Миніч М. А. Основні характеристики систем Internet of Things 276

Белокур Б.В., Скулиш М.А. Планування ресурсів гетерогенного 279

телекомунікаційного середовища на базі аналізу статистичних даних .....

Дуля О.О., Міночкін Д.А. Порівняльне дослідження архітектурних рішень для побудови масштабованих програмних продуктів 282

Остапенко М.С., Штогріна О.С. Підхід до маркування зображень 285

Лісковський І.О., Кулик М.В. Реалізація стеганографічної системи для відео з використанням сингулярного розкладання 288

Мындру М.А., Курдеча В.В. Особенности внедрения технологии WI-FI на основе стандарта 802.11AX 291

Філімонов М. Ф. Онтологічна модель моделюючого комплексу для ідентифікації морських об'єктів 294

Пльотка Б.С., Курдеча В.В. Система раннього реагування з хмарним сховищем даних 298

Бугаєнко Ю.М., Курдеча В.В. Вибір алгоритму машинного навчання для застосування при обробці даних в підмережі IoT 301

Новогрудская Р.Л., Добров Ю.А. Сравнительный анализ производительности нереляционных и реляционных систем управления базами данных 304

Шемшур Я. С., Штогріна О.С. Підхід до синхронізації даних користувачів, що взаємодіють у реальному часі 307

Запорожец Д.Б., Скулиш М.А. Сравнительный анализ методов краткосрочного прогнозирования сетевого трафика 310

Нездвецький В.С., Скулиш М.А. Аналіз засобів моделювання для мережевої СМО із динамічно змінюваними параметрами вузлів обслуговування 313

Секція 6. Сенсорні мережі та прикладні аспекти застосування телекомунікаційних технологій

Співголови:
д.т.н., проф. Лисенко О.І., д.т.н., проф. Романюк В.А, д.т.н., проф. Жук С.Я.

Доповідачі:

Новіков В.І., Алєксєєва І.В., Лисенко О.І. Процедура побудови енергозберігаючої топології безпроводової сенсорної мережі моніторингу цілей 316

Прищепа Т.А., Лисенко А.И. Исследование мобильности в беспроводных сенсорных сетях 320

Товкач И.О., Жук С.Я. Анализ влияния конфигурации сенсорной сети на точность определения местоположения источника радиоизлучения при комплексном использовании TDOA- и RSS- измерений 323

Zhivkov A., Zazerin A., Shevtsov K., Krylach O. Bandpass microwave filters on the basis of material cells 326

Stankevich S.A., Lubskyi M.S. Application of visible and nir remote sensing data for deriving of earth's surface thermal fields of high spatial resolution 329

Ходнев Т.А., Варфоломеев А.Ю. Оценка эффективности использования тракта связи протоколами RTSP-видеовещания в задачах передачи видеопоследовательностей реального времени 332

Piestova I.A. Multispectral remote sensing imagery superresolution: after resampling 336

Степанов М.М., Ткаленко О.М. Особливості застосування безпроводових сенсорних мереж 339

Верес Л.А., Фесьоха Н.О. Перспективи розвитку технологій віртуалізації 342

Марціленко С.В., Правило В.В. Проектування системи моніторингу на небезпечних хімічних підприємствах з використанням технології інтернету речей 345

Вовк А.В. Атака «ЧОРНА ДІРА» в мережах MANET 349

Богданова В.А. Бездротовий контроль та моніторинг енергоємності споживання на основі технології ZIGBEE 352

Лейко А.О. Аналіз протоколів маршрутизації в сенсорних мережах 355

Якорнов Є.А., Цуканов О.Ф. Визначення ефективності протоколів маршрутизації бездротової сенсорної мережі 358

Якорнов Є.А., Цуканов О.Ф. Визначення координат сенсорів бездротової сенсорної мережі 361

Ковальський В.І. Метод розміщення променів зондування при рейтрейсинговій аберометрії 364

Прищепа Т.О., Валуйський С.В., Дакаєв О.В. Захищена безпроводова мережа для моніторингу параметрів навколишнього середовища з мобільними сенсорами 368

Брицун А. В., Петрова В.Н. Синхронизация с использованием временных меток часов в беспроводных сенсорных сетях 371

Афанасьєв Я.Р., Новіков В.І. Методи підвищення безпеки в безпроводових сенсорних мережах 374

Гиенко О.П, Прищепа Т.А. Развитие способов применения беспроводных сенсорных сетей для контроля транспортных средств 377

Шпанчук О.О., Лисенко О.І. Підхід до аналізу споживання енергоресурсів вузлом бездротової сенсорної мережі 380

Туранська О. С., Петрова В.М. Керівні принципи та підходи до захисту інформації у безпроводових сенсорних мережах 383

Явіся В.С. Метод скорочення часових затримок сигналів геостаціонарних систем супутникового зв'язку 386

Явіся В.С. Регіональна система супутникового зв'язку..... 389

Явіся В.С. Наносупутникові навігаційні системи..... 392

Ярмола И.А., Петрова В.Н. Оптимизированное отслеживание и обнаружение целевых узлов в беспроводных сенсорных сетях..... 396

Stepanov M. N. The solution of the problem with elektromagnitnoi compatibility radochina means of mobile communication systems in the standards for 4G and 5G..... 399

Романюк А.В. Сбор информации мониторинга в беспроводных сенсорных сетях с БПЛА 402

Турейчук А.М., Лисенко О.І. Використання безпровідних сенсорних мереж для контролю пересування об'єктів на контрольованих територіях..... 405

Зубик С.О., Лисенко О.І. Шифрування даних в сенсорній мережі, на прикладі ZIGBEE..... 408

Бондарук О.А., Лисенко О.І. Алгоритм самопозиціювання вузла безпроводової сенсорної мережі..... 411

Секція 7. Апаратно-програмні засоби та пристрої телекомунікацій.

Співголови:
д.т.н., проф. Трубін О.О., к.т.н., доц. Шелковніков Б.М.

Доповідачі:

Авдеенко Г.Л., Трофименко В.В. Макет системы трансляции сигналов цифрового телевизионного вещания для учебного процесса 414

Гончаренко О.М., Авдєєнко Г.Л. Приймач сигналів супутникової навігації GPS 417

Кунєва Н. В. Необхідність використання стільникових базових станцій на сонячній енергії 420

Карнаух В.Я., Мартынюк Я.В. Входное сопротивление элементарного пьезоэлектрического излучателя 423

Trubin A. A. Coupling coefficients of different spherical dielectric microresonators 426

Trubin A. A. Bandpass filters on different spherical dielectric microresonators 429

Секція 8. Технічна творчість радіоконструкторів України

Співголови:
д.т.н., проф. Бунін С.Г.,
к.т.н., доц. Сергієнко М.І. (керівник клубу Політехнік "UT7UZA").

Доповідачі:

Антонов Олександр. Аналізатори RigExpert - надійний інструмент для виміру параметрів і налаштування антен, фільтрів та коаксіальних ліній . *

Чліянц Г.А. Виникнення і етапи розвитку радіоаматорського конструювання в Україні ..... *

Бунін С.Г. Вклад самодіяльної творчості в розвиток науки і техніки зв'язку ..... *

Сергієнко М.І., Соколенко Д.О. Технічна творчість конструкторів радіотехнічного клубу “Політехнік” UT7UZA КПІ. Минуле і сьогодення, 1924 – 2018 432

Радкевич О.І. Новітні розробки в галузі мікроелектроніки – засоби зв’язку високочастотних трактів засобів передач ..... *

Великанов М.В., Бобров В.Л. Новітні технології та засоби зв’язку в міжнародних змаганнях радіоаматорів у світі ..... *

Єрмачков С.І. Розвиток систем зв’язку в сучасних військових силах ..... *

* - статті до збірника не входять.

SEMINAR
Modern information and telecommunication trends

Співголови: д.т.н., проф. Бунін С.Г., Назаренко О.І.,
д.т.н., проф. Уривський Л.О.

Доповідачі:

Sergey Bunin. Antenna based UWB reception and transmission 435

Naritnik T.M., Ermakov A.V., Posternak B.S., Onisko O.O. Technical character of terahertz and laser waves in satellite telecommunications 439

Chernyavsky A. A. Performance analysis of carrier-aggregated multi-antenna 4×4 MIMO LTE A fronthaul 442

Solianikova V.Y. Influence of fadings on the communication channel and methods of resisting them in the multiplayer system of DVB-T2 standard 445

Martynova K.G., Fedorova L.B. Correctness of researshing signal spectrums with nonmonotonic basis function 448

Noskova D., Kvitka A., Osypchuk S. Modern wireless infocommunication technologies and infrastructure analysis for IoT implementations in scope of SMART home and SMART city concepts 451

Drobina O.S. Cognitive architecture of the 5G system based on the interaction of terrestrial and satellite components 454

Pavlenko V.M. Mapreduce calculating model on mobile devices 457

Yarosh B.Y. LTE technology for SMART GRID communication with QoS support 460

Kurdecha V.V., Trokhymenko D.V. Challenges of processing Internet of things DATA 463

Chekunov M., Osypchuk I., Kyrashchuk V., Osypchuk S. Theoretical research and practical design of IoT testbed solution based on ESP8266 SOC and blank components 466

Kurdecha V.V., Kuzimovych M.M. Clustering method modification for continuous monitoring in wireless sensor networks 469

Baria A.D., Globa L.S. USE of machine learning to solve the problem of customer churn 472

Pasichnyk O.V. Thread and data security analysis in SIP Network 475

Kurdecha V.V., Ishchenko I.O., Zakharchuk A.G. Kunieva N.V. Fuzzy logic usage for the DATA processing in the internet of things Networks 479

Десята Міжнародна науково-технічна конференція студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ»

Співголови:

ЯКОРНОВ Є.А. – заступник директора Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського, к.т.н., професор;

ГАВРИЛЮК В.В. – голова студентської ради Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського.

Доповідачі:

Ткаченко Н.К. Огляд перспективних технологій формування сигналів для підвищення пропускної здатності каналів систем супутникового телевізійного мовлення 484

Куклина А.С. Система внутреннего позиционирования, как LOCATION- BASED SERVICE 485

Прокопець В.А. Експериментальне дослідження енергоефективності обробки даних в розподіленому ДАТА центрі 486

Gritsko A.V. Overview on the main factors, which have impact on data transfer quality IN LTE networks 486

Bilokha D.K. Restoring transfer messages based on NETWORK traffic analysis 487

Лебеденко Т.Н. Динамическая модель управления очередями основанная на распределении сетевого ресурса 488

Давидюк А.М. Обмеження для існуючих рішень систем промислового «Інтернету речей» 489

Шевченко Д.В. Дослідження безпечного мережевого доступу на базі платформи CISCO IDENTITY SERVICES ENGINE 489

Пасічник О.В. Аналіз загроз та методів захисту інформації в мережі SIP телефонії 490

Полтавська С.Р. Підвищення дальності передачі інформації по ВОЛЗ шляхом застосування солітонів 491

Бурлака Г.Ю. Перспективи розвитку і переваги побудови мереж операторського класу на основі технології CARRIER ETHERNET 491

Власенко В.В. Дослідження особливостей основних протоколів при побудові сучасних захищених VPN мереж 492

Петренко О.В. Побудова оптичних транспортних мереж на базі обладнання CISCO 493

Корнійчук Ю.В. Реалізація моделі мережі передачі контенту 494

Бикова А.О. Сценарна модель і мова опису знань для оцінки і прогнозування ситуацій 495

Поліщук І.С. Інтернет речей на основі програмно-конфігурованих мереж: проблеми та виклики 496

Максимчук М.Р. Розробка циклу лабораторних робіт з дослідження параметрів безпроводових засобів зв’язку CAMBIUM 497

Грищенко О.С. Розробка циклу лабораторних робіт з дослідження параметрів безпроводових засобів зв’язку MIKROTIK 498

Тригубенко Д.О. Методи масштабування систем в архітектурі «Клієнт-Сервер» 499

Буфін Г.Г. Аналіз безсерверних хмарних технологій і шляхи подальшого їх розвитку 499

Корсун Н.А. Анализ оттока клиентов в мобильных телекоммуникациях . 500

УДК 004.75

"РОЗУМНІ" СЕНСОРНІ МЕРЕЖІ: ВІД ІДЕЇ ДО РИНКУ

Палагін О.В., Романов В.О., Галелюка І.Б., Вороненко О.В., Груша В.М., Ковирьова О.В., Антонова Г.В., Лаврентьєв В.М., Брайко Ю.О., Імамутдінова Р.Г.

Інститут кібернетики імені В.М. Глушкова НАН України, Україна

E-mail: kovyrova.oleksandra@gmail.com

Smart sensor networks: from idea to market

Development of low-cost wireless smart biosensors for express-diagnostics of plant state and creating the proper software and methodical support for integration of these biosensors into wireless sensor network for estimating plant state on agricultural large territories are considered. Sensor network configuration is showed.

Однією з основних задач у сучасному промисловому землеробстві та екологічному моніторингу є експресне оцінювання стану рослин в умовах дії стресових факторів, їх стійкості до несприятливих умов навколишнього природного середовища. Це дає змогу своєчасно вжити необхідні агротехнічні заходи для збереження врожаю або зелених насаджень.

Найбільш вірогідне оцінювання стійкості рослин до стресових факторів як природного, так і техногенного походження дає прямий метод, який застосовується у польових умовах. Але у польових умовах, як правило, неможливо відтворити стресові фактори навантаження на рослину, які рік у рік носять змінний характер. Тому розробка універсальних експресних методів оцінювання стану рослин в умовах дії стресових факторів є важливою задачею як промислового землеробства, так і захисту довкілля.

Одним з таких методів оцінювання стану живої рослини є метод індукції флуоресценції хлорофілу (ІФХ) [1]. До цього часу метод ІФХ використовувався в автономних приладах, так званих флуорометрах, для оцінювання стану рослин переважно у лабораторних умовах або на невеликих ділянках у полі. Прикладом такого флуорометру є розроблений в Інституті кібернетики і доведений до серійного виробництва портативний комп’ютерний прилад «Флоратест» [2].

Доведені до серійного виробництва бездротові біосенсори для реєстрації ІФХ, об’єднані у мережі, на відміну від автономних флуорометрів, здатні оцінювати стан рослин на великих територіях. Розроблена бездротова мережа (рис. 1) призначена для використання у промисловому землеробстві та екологічному моніторингу [3, 4] і являє собою мережу бездротових біосенсорів, які об'єднані між собою радіоканалом [5].

Для організації біосенсорів у мережу використовується координатор, основними функціями якого є: об'єднання бездротових біосенсорів у мережу, підтримання працездатності мережі, діагностика стану окремих біосенсорів та мережі в цілому, виявлення позаштатних ситуацій та інформування про це

користувача; збирання даних вимірювання від усіх бездротових біосенсорів, зберігання отриманої інформації; керування процесом вимірювання усіх або вибраних біосенсорів відповідно до програми користувача.

Концентратор мережі біосенсорів, являє собою спеціалізований комп'ютер і використовується у польових умовах для збору даних з координаторів мережі.

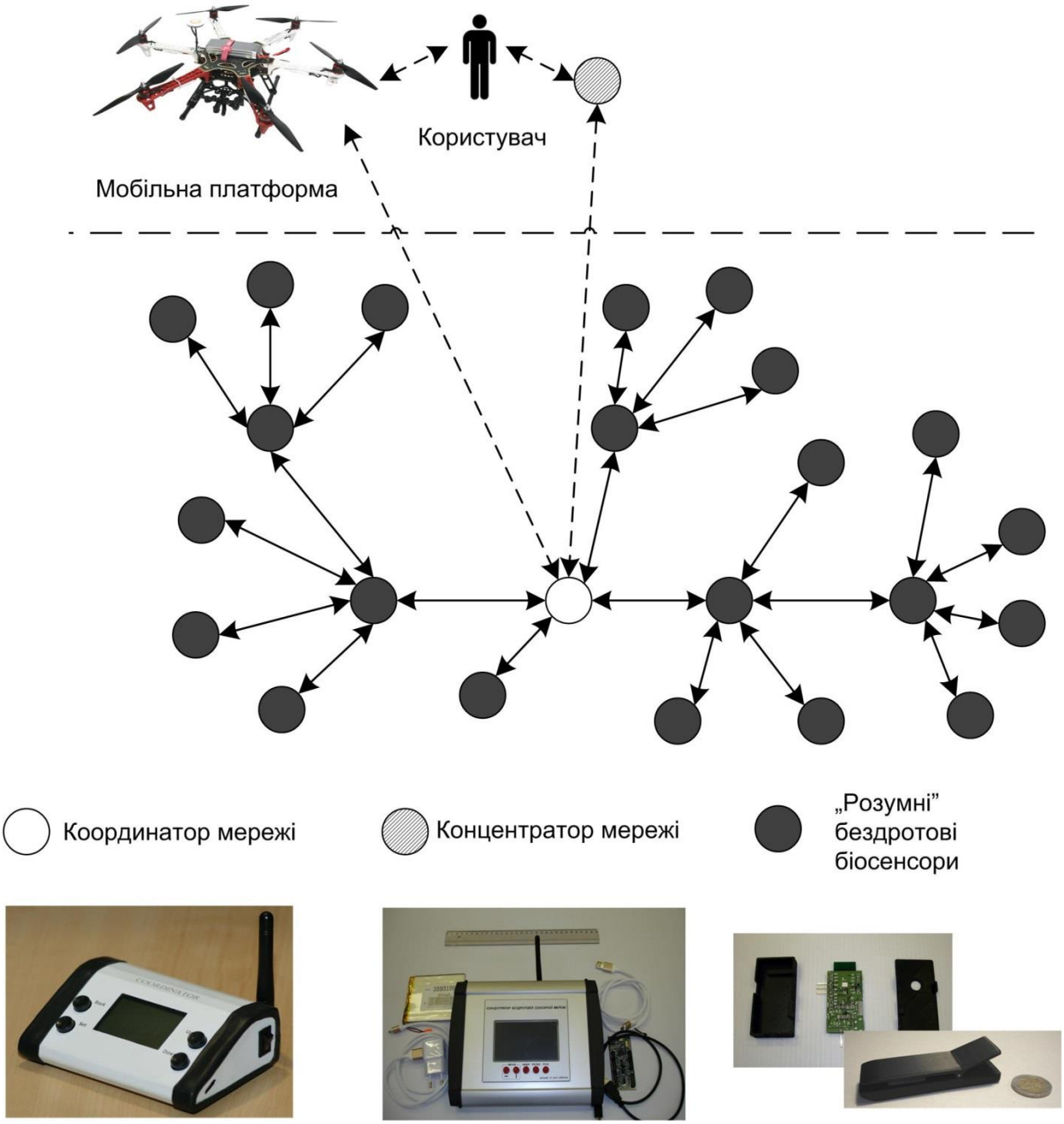


Рис. 1. Структура мережі бездротових біосенсорів

Призначенням безпілотної мобільної платформи (в нашому випадку мультикоптера) є наступне: налаштування та програмування польотного контролера мультикоптера у комплекті з GPS-модулем та застосування модуля бездротового отримання даних, рис. 2, з координатора мережі.

В основу випробувань розробленої мережі бездротових біосенсорів покладено польовий однофакторний експеримент, за результатами якого

визначено чутливість біосенсорів до впливу стресових факторів різної природи на дослідні групи рослини.

Отримані результати [1] свідчать про те, що біосенсори з високою чутливістю реагують на зміни стану рослин, тобто за розробленою методикою оцінюється не тільки поточний стан рослин, але їх стійкість до посухи, реакцію на внесення гербіцидів та добрив, що дозволяє успішно використовувати розроблені біосенсори і біосенсорні мережі у промисловому землеробстві.

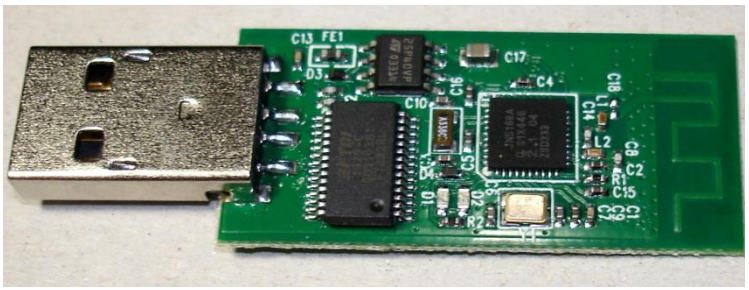


Рис. 2. Модуль бездротового отримання даних

Висновки:

1. Розроблена нова мультисенсорна інформаційна технологія для експрес-діагностики стану рослин на великих територіях сільськогосподарських угідь.

2. Розроблена і доведена до серійного виробництва мережа бездротових біосенсорів, яка включає біосенсори з радіоканалом, координатор і концентратор мережі.

3. Розроблено безпілотну мобільну платформу для зняття даних з мережі бездротових біосенсорів.

4. Розроблено методичне забезпечення для використання мережі бездротових біосенсорів у промисловому землеробстві.

Література

1. Oleksandr Palagin, Volodymyr Grusha, Hanna Antonova, Oleksandra Kovyrova, Vasyl Lavrentyev. Application of biosensors for plants monitoring // Information theories and applications, Vol. 24, Number 2, 2017 – P. 115-126, ISSN 1310-0513 (printed), ISSN 1313-0463 (online).
2. dasd.com.ua
3. Oleksandr Palagin, Volodymyr Romanov, Igor Galelyuka, Oleksandr Voronenko, Yuriy Brayko, Roza Imamutdinova . Wireless sensor network for precision farming and environmental protection// Information theories and applications, Vol. 24, Number 1, 2017 – P. 19-34, ISSN 1310-0513 (printed), ISSN 1313-0463 (online).
4. Романов В.О., Галелюка І.Б., Груша В.М Нова інформаційна технологія експрес-оцінювання стану рослин в умовах дії стресових факторів. // Комп’ютерні засоби, мережі та системи. – 2016, №15, с. 94-101.
5. Palagin O, Romanov V., Galelyuka I., Hrusha V., Voronenko O. Wireless smart biosensor for sensor networks in ecological monitoring// Proceeding of the 9th IEEE International conference on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications", IDAACS'2017, September 21–23, 2017. Bucharest, Romania – P. 679-683.

UDC 621.39

DISPERSION MANAGEMENT IN SINGLE-MODE FIBERS

Volkmar Brückner
Herder Foundation, Werl, Germany

1. Introduction

Transfer of digital data packets in optical fibers is performed by propagation of digital signals at high bit rates. In reality Gaussian shaped pulses of duration τ_B are used. Bit rate B relates to the bit sequence or time distance Δt_B between neighboring bits. For example, a bit rate of B = 1 Gbps results in $\Delta t_B = 1/B = 10^{-9}$ s = 1000 ps. In accordance with the recommendations of ITU-T a high-quality transmission can be achieved only if the bit prolongation during propagation in the fiber is no more than $\Delta t_B/10$; it means in case of 1 Gbps transmission bit duration should be no longer than 100 ps. Note that at very high bit rates (B ≥ 1 Gbps) we find only Gaussian shaped pulse in the fiber. In the following we will consider the reasons of pulse prolongation. We will present studies on the influence of chromatic dispersion (CD) as well as polarization mode dispersion (PMD) to the bit rate and its influence on the maximum transmission length in Standard Single-Mode Fibers (SSMF). Nature of CD and PMD is described elsewhere [1].

2. Basics for calculations

2.1. Standard single-mode fibers (SSMF)

We used standard single-mode fibers for calculations with the following set of parameters:

- Core diameter d = 8.5 µm
- Core material: 96% SiO_2 + 4% GeO_2, the refractive index is $n_2(\lambda) = n_{core}(\lambda)$.
- Cladding material: 98% SiO_2 + 1% GeO_2, the refractive index is $n_1(\lambda) = n_{clad}(\lambda) < n_2(\lambda)$.

Based on 3-term Sellmeier equation [2] for these core and cladding materials one can calculated the wavelength dependence of core (n_2) and cladding indexes (n_1) as well as its derivatives and the corresponding group indexes (n_{g2} and n_{g1}).

2.2. Dispersion in SSMF

The following kinds of dispersion are discussed:

- *Material dispersion* results from the line width (spectral broadening) of the light source, here in semiconductor lasers. Material dispersion parameter D_{Mat} can be calculated by $D_{Mat} = -\frac{\lambda}{c_0}\frac{d^2n}{d\lambda^2}$, where c_0 is the speed of light. Material dispersion parameter is mostly identical for core and cladding.

- *Waveguide dispersion* considers the influence of field strength in core and cladding. Thus we get an effective index n_{eff} and an effective group index $n_{g,eff}$. A waveguide dispersion parameter D_{WG} is used.

- *Chromatic dispersion* is the sum of material and waveguide dispersions. The corresponding parameter D_{Chrom} is given by

$$D_{Chrom} = \frac{1}{c_0}\frac{dn_{g,eff}}{d\lambda} = -\frac{\lambda}{c_0}\frac{d^2n_{eff}}{d\lambda^2} = D_{Mat} + D_{WG}$$

Polarization dispersion results from different propagation speed of light with different polarization. In this case one gets instead of a pulse prolongation a splitting of the pulse.

2.3. Power spectrum of bits

To perform simulation, we use the spectral shape of light at high bit rates B. Spectral shape (power spectrum) P(λ) of with Gaussian shaped laser pulses (= bits) with the central wavelength λ_0 and Δλ the line width. Minimum line width of about $\Delta\lambda = 10^{-4}$ nm at about λ_0 = 1500 nm can be found in commercially used Distributed FeedBack (DFB) lasers. Now we assume that the

carrier frequency f_L is modulated with a modulation frequency Δf_M. Mathematically modulation of light waves with modulation frequency Δf_M can be described as modulation of the carrier frequency f_L. It results in generation of side-bands $f_L \pm \Delta f_M$. The modulation frequency Δf_M (e.g. GHz) roughly corresponds to the bit rate B (e.g. Gbps), i.e. $\Delta f_M \approx B$; than we get the total line width as:

$$\Delta\lambda_{total} = \Delta\lambda_L + \left|\frac{\lambda_L^2}{c_0}\right| \cdot \Delta f_M \approx \Delta\lambda_L + \left|\frac{\lambda_L^2}{c_0}\right| \cdot B$$

If $\Delta\lambda_L >> |\lambda_L^2/c_0| \cdot B$ the laser line width dominates; otherwise (at $\Delta\lambda_L << |\lambda_L^2/c_0| \cdot B$) modulation dominates and one gets $\Delta\lambda_{total} \approx |\lambda_L^2/c_0| \cdot B$. Calculations of total laser line width are presented in Tab. **1**.

Tab. 1 Estimations of total line width (at λ_L = 1.5 µm)

$\Delta\lambda_L$ (nm)	1	10^{-4}	10^{-4}	10^{-4}
B (Gbps)	1,10 or 40	1	10	40
$\Delta\lambda_{total}$ (nm)	1	0.0076	0.076	0.300

3. Bit prolongation by chromatic dispersion

3.1. Standard calculations

The often used way is to assume a rectangular spectral shape with a line width $\Delta\lambda_{total}$ and to calculate bit prolongation per kilometer fiber length. To this end we can use the product of dispersion parameter D_{Chrom} and spectral line width $\Delta\lambda_{total}$:

$$\frac{\Delta\tau_B}{L} = D_{Chrom} \cdot \Delta\lambda_{total} .$$

For example, with $\Delta\lambda_{total}$ = 0.0076 nm (for B = 1 Gbps, see Table) and $D_{Chrom} = 16 \frac{ps}{km \cdot nm}$ we get:

$$\frac{\Delta\tau_B}{L} = 0.12 \frac{ps}{km} .$$

That means the maximum permitted bit duration τ_{max} = 100 ps will be reached after L = 822 km.

3.2. Exact calculation

For exact calculations it is much better to use a Gaussian spectral shape. For modelling we assume that power spectrum consists of partial wave groups with slightly different wavelength λ_k. The wavelength difference between neighboring wave groups is $\Delta = \lambda_k - \lambda_{k-1}$, each wave group has identical line width $\Delta\lambda_k << \Delta\lambda_{total}$. All partial wave groups together cover the spectrum *inside* the Gaussian envelope. For each partial wave we can assume again a Gaussian shape with the line width $\Delta\lambda_k$, where k denotes the "number" of wave group in the interval –k … 0 … +k. The term e^{-k^2} describes a Gaussian shaped envelope of wave group number k. Selecting k as an odd number with $\Delta = \lambda_k - \lambda_{k-1} = \frac{\Delta\lambda_{total}}{k+1}$ one can cover the line width of the spectrum.

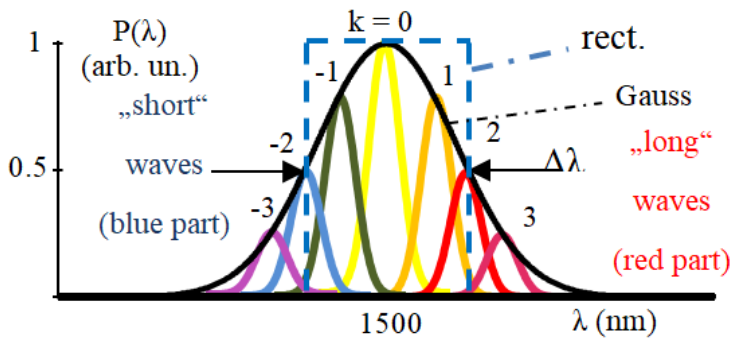


Fig. 1 Rectangular (rect) and Gaussian spectrum (Gauss) with partial waves ("rainbow colors")

For illustration we selected k = 3, i.e. k = -3 … 0 … +3. As one can see in Fig. 1 we have 2k+1 = 7 partial waves. If the total line width is $\Delta\lambda_{total}$ = 0.0076 nm (i.e. for 1 Gbps bit rate) the distance of two neighboring partial wave groups is $\Delta = \frac{\Delta\lambda_{total}}{k+1}$ = 0.0019 nm. The line widths of each partial wavelengths in Fig. 1 is $\Delta\lambda_k = \frac{\Delta\lambda}{2k+1} = 0.00109\ nm$ i.e. the whole spectrum is covered by these 2k+1 partial wave groups. Because we find in Fig. 1the "rainbow colors" from violet via blue, green, yellow, orange till red – that is why often the terms "blue part" (for shorter wavelengths) and "red part" (for longer wavelengths) are used.

Modelling of bits prolonged by chromatic dispersion means we have to consider the *temporal shape* (time-dependent power) P (t) of laser pulses (= bits) which is given by a Gaussian shaped envelope with bit duration τ_B and central time t_0. Now we will use this model to describe bit prolongation by chromatic dispersion. Without any influences (e.g. dispersion) *all* Gaussian spectral shaped partial wavelengths λ_k coincide in time (it corresponds to the situation at the beginning of the fiber, L = 0). It means all wavelengths contribute to the pulse with a certain weight. Partial waves propagate with different group indexes ($n_{g,eff}^{blue} < n_{g,eff}^{red}$) and group speeds – blue part propagates faster than red part $\left(v_{g,eff}^{blue} > v_{g,eff}^{red}\right)$. That means after a certain fiber length we can expect a picture like sketched in the next Figure (b) with time duration of envelope $\tau_L > \tau_B$; the temporal shift of partial waves results in a broadening of the bit (Figure (c)). Note that in real calculations we used much higher values of k (typically k = 499). For a Standard Single-Mode Fibers (SSMF) we used $D_{Chrom} = 15.9 \frac{ps}{km \cdot nm}$ (at λ = 1.5 μm). At the same conditions as before ($\Delta\lambda_{total}$ = 0.0076 nm and k = 499) we get $\Delta = \frac{\Delta\lambda_{total}}{k+1} = 1.52 \cdot 10^{-5}\ nm$ the time delay between partial wavelengths as $\frac{\Delta\tau_B}{L} = D_{Chrom} \cdot \Delta = 2.42 \cdot 10^{-4} \frac{ps}{km}$. Now one can perform simulation of chromatic dispersion and corresponding limits of transmission length. One has to know the following parameters (with examples):

- Central wavelength λ_0 = 1500 nm and line width Δλ = 0.0076, 0.076 or 0.304 nm (corresponding to a modulation of B = 1, 10 or 40 Gbps, see Tab. 1);
- Chromatic dispersion parameter is D_{Chrom} = 15.9 ps/km·nm;
- k_0 = 499, number of partial wave group ($-k_0$ … -1,0, +1 … k_0) resulting in $2k_0$+1 partial wave groups;
- initial bit duration τ_0 = 10, 5 or 1 ps;
- fiber length L.

Results of calculations are presented in Fig. **2**. The prolongation of the initially 10 ps bit is sketched for increasing fiber lengths L. At L = 440 km we get a 100 ps (FWHM) bit. That means the limit for a high-quality transmission at 1 Gbps bit rate is 440 km.

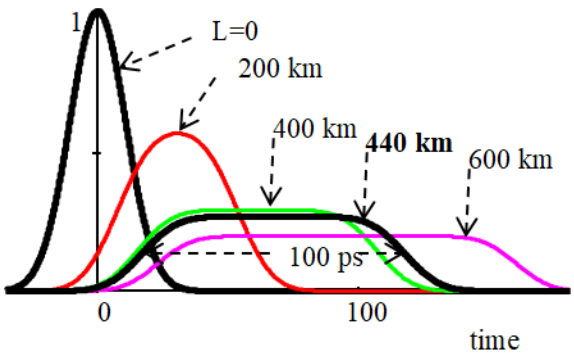


Fig. 2 Bit prolongation by chromatic dispersion for increasing fiber lengths L

The same procedure was performed at higher bit rates. For B = 10 Gbps the initial bit duration τ_0 = 5 ps is prolonged till the maximum permitted duration τ_{max} = 10 ps at fiber length L = 4.4 km; for B = 40 Gbps prolongation from τ_0 = 1 ps to τ_{max} = 2.5 ps we get at L = 0.28 km.

Calculation results of chromatic dispersion limited fiber length for high-quality transmission in spectrum with rectangular and Gaussian spectral shapes are presented in Tab. 2.

Considering real spectral shape (Gaussian) of modulated laser light we obtained shorter fiber length for high-quality transmission.

Tab. 2. Comparison of maximum fiber length for high-quality transmission in spectrum with rectangular and Gaussian spectral shapes

Spectral shape	L_{max} (km) at B = 1 Gbps	L_{max} (km) at B = 10 Gbps	L_{max} (km) at B = 40 Gbps
Rectangular	822	8.2	0.52
Gaussian	440	4.4	0.28

For dense wavelength division multiplexing (DWDM) one can transfer the bitrate 40 Gbps in 40 channels with 1 Gbps per channel over 440 km fiber length, which is much better than transfer of 40 Gbps in one single channel over 280 m only.

4. Modelling of polarization mode dispersion

Polarization mode dispersion becomes important if we can compensate chromatic dispersion in the fiber, e.g. by a dispersion-compensating fiber (DCF).

4.1. Standard calculation

Like for chromatic dispersion one can calculate maximum transmission length L_{max} assuming a rectangular time shape with a bit duration τ_{max} given by the bit rate B $\left(\tau_{\max} = \frac{1}{10 \cdot B}\right)$.

To this end we can use the product of dispersion parameter D_{PMD} and square root of maximum fiber length $\sqrt{L_{max}}$:

$$\Delta\tau_{\max} = D_{PMD} \cdot \sqrt{L_{\max}} = \frac{1}{10 \cdot B}.$$

For example, for B = 10 Gbps and $D_{PMD} = 0.103 \frac{ps}{\sqrt{km}}$ we get:

$$L_{\max} = \frac{1}{100 \cdot B^2 \cdot D_{PMD}^2} = 10000\text{km}.$$

That means the maximum permitted bit duration τ_{max} = 10 ps will be reached after L = 10000 km.

4.2. Exact calculation

For PMD one has to calculate the superposition of *two* orthogonally polarized parts of the bit. With increasing fiber length L one can find prolongation and even “splitting in time” of these two differently polarized bits (

Fig.). With the measured value of D_{PMD} = 0.103 ps/√km after L = 215 km the initial τ_0 = 1 ps bit (L = 0 km) is splited into two bits with a total bit duration of τ_{215} = 2.5 ps. This is the maximum bit duration permitted at B = 40 GBps bit rate (corresponding to a time between two neighboring bits of Δt_B = 1/B = 25 ps and a maximum permitted bit prolongation of $\Delta t_B/10 = \tau_{max} = \tau_{215}$ = 2.5 ps).

In this case we get the following picture of two neighboring bits in a 40 Gbps transmission line (Fig. 3). With D_{PMD} = 0.103 ps/√km one gets τ_{215} = 2.5 ps after 215 km.

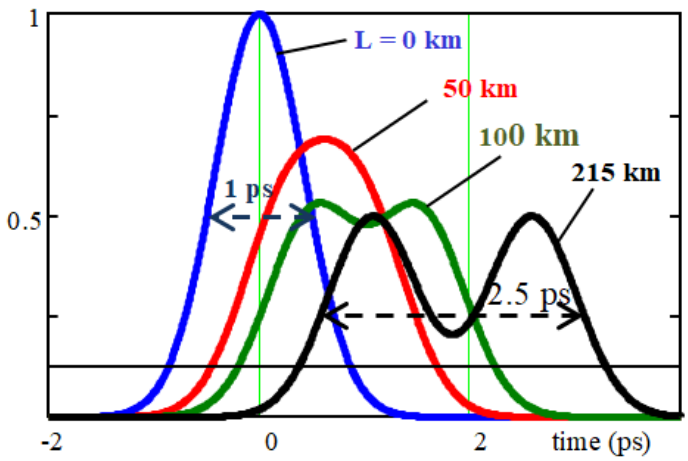


Fig. 3. Influence of PMD after fiber length L for D_{PMD} = 0.103 ps/√km

With increasing bit rate to be transferred one gets a decreasing maximum fiber length. We performed similar calculations as before for other bit rates and found the following:

- For B = 10 Gbps (Δt_B = 100 ps) a bit prolongation from 5 ps to 10 ps is reached after 2700 km fiber length;
- For 40 Gbps (Δt_B = 25 ps) bit prolongation from 1 ps to 2.5 ps is reached after a fiber length of 240 km
- For 80 Gbps (Δt_B = 12.5 ps) bit prolongation from 0.5 ps to 1.25 ps is reached after a fiber length of 52 km
- PMD limited transmission length depends on the duration of initial bits: The lower the initial bit duration the longer is the maximum transmission length. In case of $\tau_0 \rightarrow 0$ we get the values of rectangular pulse shape.

Results of calculations of PMD-limited transmission length are summarized in Tab. **2**.

Tab. 2 Comparison of maximum fiber length for high-quality transmission with rectangular and Gaussian temporal shapes

Time shape	L_{max} (km) at B = 10 Gbps	L_{max} (km) at B = 40 Gbps	L_{max} (km) at B = 80 Gbps
Rectangular	10000	625	156
Initial bit duration τ_0 (ps)	5	1	0.5
Gaussian	2700	215	52

References

1. V. Brückner: Elements of Optical Networking. Vieweg+Teubner, Springer Fachmedien Wiesbaden 2011.
2. V. Brückner: To the use of Sellmeier formula (2012, unpublished).
   Available at Springer website: To the use of Sellmeier formula - Springer and at Researchgate:
   To the use of Sellmeier formula
   https://www.researchgate.net/profile/Volkmar_Brueckner2/contributions

УДК 621.396.1

СТРУКТУРНО-ФУНКЦІОНАЛЬНІ ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ТА ЗВ'ЯЗКУ БОРТОВОГО І НАЗЕМНОЇ ОБЛАДНАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ АЕРОПЛАТФОРМ

Ільченко М.Ю., Кайденко М.М., Кравчук С.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: sakravchuk@ukr.net

Structural-functional principles of management and communication systems for border and landscape equipment of the telecommunication network on the basic of aeroplatform

Structurally functional principles of construction of the on-board control system and communication system are proposed, taking into account the necessity of the system in ensuring continuous data exchange on the control channel and telemetry with high reliability, as well as continuous data transmission over the data transmission channel towards a ground-based system with guaranteed quality.

Подальший розвиток телекомунікаційних систем на базі висотних аероплатформ (ТСВА) неможливий без розвитку структурно-функціональних принципів побудови обладнання бортової і наземної підсистем, особливо, в частині управління і каналу трафіка [1-5]. Найбільше поширення на даний час в якості аероплатформ для ТСВА знайшли безпілотні літальні апарати (БПЛА), які і стали головним об'єктом нашого дослідження.

Пропоновані структурно функціональні принципи побудови бортової системи управління та зв'язку враховують те, що система повинна забезпечувати безперервний обмін даними по каналу управління та телеметрії з високою достовірністю, а також безперервну передачу даних по каналу передачі даних в напрямку до наземної системи з гарантованою якістю.

Загальна структура бортової системи управління та зв'язку БПЛА показана на рисунку 1.

До складу системи входять: канал управління та телеметрії з антенною відповідного типу; канали передачі даних; антенна система з функціями автоматичного супроводження; бортовий процесор управління та обробки даних; блок комутації та маршрутизації; набір камер для відеоспостереження та управління польотом; засоби управління польотом та визначення орієнтації БПЛА у просторі.

Канал управління та телеметрії використовується для передачі даних управління БПЛА від наземної станції та даних телеметрії з борту літального апарату до наземної станції. Для забезпечення безперервності управління літальним апаратом на всіх стадіях польоту використовуються антени з круговою діаграмою спрямованості. Для каналу управління може бути використаний діапазон частот 30…470 (510) МГц. Швидкість передачі даних

в каналі 19,2…38,4 кбіт/с і може бути збільшена за необхідності до 100 кбіт/с. Забезпечення завадостійкості та захисту від навмисних завад здійснюється використанням технології розширення спектру: для цивільного використання пряме розширення спектру – DSSS (Direct Sequence Spread Spectrum); для військового використання – FHSS (Frequency-Hopping Spread Spectrum). Модуляція ФМ4, завадостійке кодування – каскадний код, чи блоковий турбокод зі змінною швидкістю кодування. Допустимі затримки передачі даних в каналі визначаються призначенням БПЛА і швидкістю його переміщення, відповідно і необхідним часом реакції на команду управління і складає від до 10 до 200 мсек.

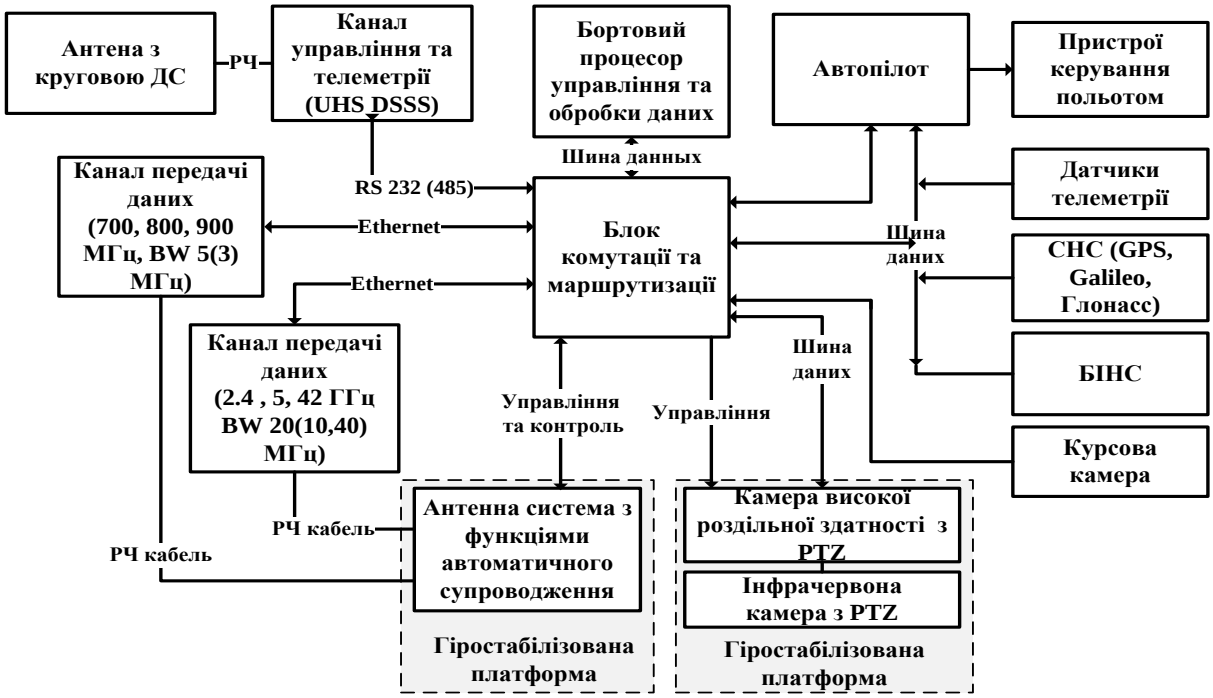


Рис. 1. Загальна структура бортової системи управління та зв’язку БПЛА

Для передачі даних використовуються канали в більш високих діапазонах частот 700, 800, 900 МГц, 2,4, 5,8, 27, 42 ГГц. При цьому для забезпечення гарантованої якості передачі даних в умовах навмисних завад одночасно можуть бути використані два канали в двох різних діапазонах. Канали передачі даних є несиметричними з часовим дуплексом, канал по напрямку до наземної станції є високошвидкісним, співвідношення лінія-вниз/лінія-вверх може складати 8/1, 16/1. Модуляція в каналах передачі – багатопозиційна ФМ2, ФМ4, КАМ 16, КАМ 64, КАМ 256. Завадостійке кодування – каскадний код, блоковий турбокод чи LDPC код зі змінною швидкістю кодування. Для забезпечення боротьби з ненавмисними завадами використовується адаптивна модуляція та кодування. В силу того, що канали передачі даних є високошвидкісними і в них застосовується механізм боротьби з навмисними завадами, ці канали можуть використовуються додатково як дублюючі для каналу управління та телеметрії, або для передачі даних управління та телеметрії одночасно по трьом різним маршрутам.

Для передачі даних використовується антенна система з направленими антенами: набір планарних антен, або дзеркальна антена з декількома діапазонними опромінювачами. Антенна система включає в себе додаткові елементи для управління поворотом антен в двох азимутальних площинах для забезпечення роботи в режимі автоматичного супроводження напрямку на наземні станцію. Для забезпечення незмінності позиції антен відносно землі вона розміщуються на гіростабілізованій платформі. Функції гідростабілізації забезпечуються додатковим поворотним механізмом (третя площина для компенсації крену платформи) та системою з трьох координатних датчиків MEMS.

Структурно функціональні принципи побудови наземної системи управління та зв'язку враховують призначення БПЛА, структуру побудови бортової системи управління та зв'язку та необхідність забезпечення живучості БПЛА в умовах виникнення різного виду завад.

Загальна структура наземної системи управління та зв'язку БПЛА показана на рис. 2.

Рис. 2. Загальна структура наземної системи управління та зв'язку БПЛА

До складу системи входять: канал управління та телеметрії з антенною відповідного типу; канали передачі даних; антенна система автоматичного супроводження БПЛА; бортовий процесор управління та обробки даних; блок комутації та маршрутизації; система відображення з камер відео спостереження; засоби управління польотом та відображення з курсової камери, а також система визначення координат наземної станції.

Канали зв'язку наземної системи мають відповідні до каналів зв'язку БПЛА параметри. В якості антени каналу управління та телеметрії може бути

використано хвильовий канал (логоперіодичну антену) чи антену з круговою діаграмою спрямованості, вона кріпиться на антенній системі каналів передачі даних з автоматичним супроводженням БПЛА. В якості антен використовуються дзеркальні антени з декількома діапазонними опромінювачами. Діаметр дзеркал визначається тактичним призначенням БПЛА і максимальною дальністю польоту. Антенна система повинна забезпечувати автоматичне супроводження БПЛА на протязі всього польоту.

Функції та структура процесору управління та обробки даних, блоку комутації та маршрутизації аналогічні до тих, які встановлюються на БПЛА. Процесор управління та обробки даних додатково виконує обрахунки для антенної системи автоматичного супроводження, обрахунки траєкторії польоту БПЛА, визначення необхідних поправок, ведення логу (документування) процесу польоту та обміну даними з БПЛА.

Для керування польотом БПЛА використовується пульт управління польотом разом з пристроєм ручного керування. Зображення з курсової камери відображаються на моніторі управляння польотом разом з іншою інформацією, яка необхідна для моніторингу польоту та управління ним.

Таким чином, запропоновано структурно функціональні принципи побудови бортової системи управління та зв’язку, що враховують необхідність системи у забезпеченні безперервного обміну даними по каналу управління та телеметрії з високою достовірністю, а також безперервну передачу даних по каналу передачі даних в напрямку до наземної системи з гарантованою якістю. Запропоновано структурно функціональні принципи побудови наземної системи управління та зв’язку, що враховують призначення БПЛА, структуру побудови бортової системи управління та зв’язку та необхідність забезпечення живучості БПЛА в умовах виникнення різного виду завад.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Prospects of using of aerial stratospheric telecommunication systems / M. Zgurovsky, M. Ilchenko, S. Kravchuk, V. Kotovskyi, T. Narytnik, L. Cybulskyi // Proceedings of the 2016 IEEE International Scientific Conference "RadioElectronics & InfoCommunications" (UkrMiCo’2016), 11-16 September 2016, Kyiv, Ukraine. IEEE Conference Publications, 2016. – P. 20-23.
3. Kravchuk S., Kaidenko M. Features of creation of modem equipment for the new generation compact troposcatter stations // Proceedings of the International Scientific Conference "RadioElectronics & InfoCommunications" (UkrMiCo’2016), 11-16 September 2016, Kyiv, Ukraine. – IEEE Conference Publications (IEEE Xplore Digital Library, DOI: 10.1109/UkrMiCo.2016.7739634), 2016.– P. 365-368.
4. Kravchuk S.O., Kaidenko M.M. Modem equipment for the new generation compact troposcatter stations // Information and telecommunication sciences. – 2016. – Vol. 7. – Nu. 1. – P. 5–12.
5. Ільченко М.Ю., Кайденко М.М., Кравчук С.О. Модемне обладнання на основі SDR-технології для тропосферних станцій нового покоління // Наукові вісті НТУУ "КПІ". – 2016. – № 5. – С. 7–16.

УДК 621.396

ДЕКОМПОЗИЦІЯ ПРОЦЕСІВ ПЕРЕХОДУ ВІД СЦЕНАРІЮ ДО СТРАТЕГІЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ У МУЛЬТИСЕРВІСНІЙ СИСТЕМІ

Мошинська А.В., Уривський Л.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: avmoshinskaya@gmail.com, leonid_uic@ukr.net

Decomposition of transition processes from Scenario to the information transmission Strategy in the multiservice system

In the paper established system correspondence between growing information needs (Scenarios) and limited resources of telecommunication technologies (Strategies) on the basic of the categories of applied theory of information for telecommunicaton.

Потреби прогнозування шляхів створення і розвитку ефективних мультисервісних систем обумовлюють необхідність розробки нових наукових методів кількісного аналізу продуктивності телекомунікаційних каналів. Такий підхід вимагає доцільного об’єднання рівнів моделі OSI при адекватному описі процесів транспортування інформації.

Сукупність використовуваних послуг одного користувача, групи користувачів, спільноти або суспільства визначає сценарій передачі інформації.

Сценарій - це сукупність інформаційних послуг, які визначаються користувачем (найчастіше без урахування реальних можливостей інформаційної спільноти щодо їх задоволення).

Імплементація Сценаріїв можлива при використанні сучасних телекомунікаційних технологій, пов'язаних з передачею інформації за допомогою електричних, оптичних, електромагнітних сигналів.

Сукупність подібних технологій поєднує в собі всі необхідні умови імплементації сценаріїв і надалі визначається, як Стратегії передачі інформації.

Під Стратегією слід розуміти сукупність способів передачі інформації (співвіднесені з Сценарієм), що використовує обґрунтоване поєднання протоколів передачі та засобів перенесення електричних сигналів.

Декомпозицію процесів переходу від сформульованого Сценарію до його реалізації на основі синтезованої Стратегії можна представити у вигляді послідовності переходів, представленої на рис. 1. Сукупність Сценаріїв і Сценарних концепцій відповідають 7-ому (Прикладному) рівню моделі OSI.

На малюнку потреби користувача в певних послугах (телефонна розмова, чат, передача даних, он-лайн аудіо та відео та ін.) Представлені у вигляді окремих сценаріїв передачі інформації (Сценарій A, B ... Z).

Змістовний сенс завдань цього рівня відображений категорією «I want…» – «Бажаю…».

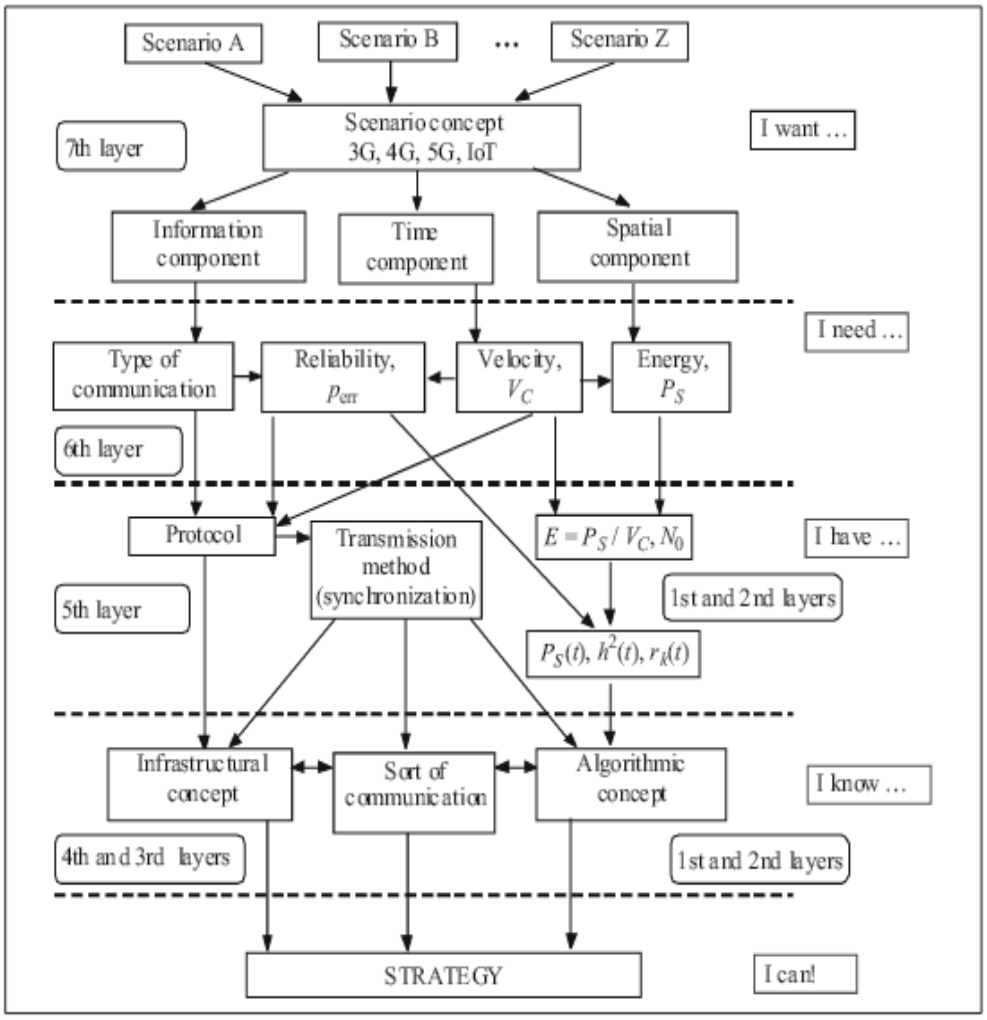


Рис. 1. Алгоритм реалізації процесу Сценарій-Стратегія

Гранична парадигма ідеального Сценарію - надання будь-якої сукупності послуг в будь-якій точці простору в будь-який момент часу в необмеженому обсязі. Сценарна концепція - набір сценаріїв, які пропонуються користувачеві в рамках наявних, реальних ресурсних можливостей.

У відповідність з логікою побудови моделі OSI наступним кроком після формулювання інформаційної завдання на вищому (7-м, Прикладному) рівні є формалізація цього завдання в поняттях транспортної (телекомунікаційної) системи на більш низькому, 6-м рівні (Відображення).

На цьому рівні виникає задача визначення такого обсягу ресурсів, який необхідний для передачі інформації відповідно до необхідних умов реалізації сценарних концепцій, а саме:

- Інформаційна компонента визначає вид зв'язку (мовний зв'язок, телевізійне мовлення, Інтернет і відповідні їм засоби реєстрації інформаційних об'єктів) і достовірність прийому інформації;

- Часова компонента визначає швидкість передачі інформації;

- Просторова компонента визначає енергетику, необхідну для перенесення сигналів у просторі.

У свою чергу, показники достовірності інформації, швидкості передачі символів і енергетики лінії телекомунікацій пов'язані між собою.

Таким чином, сукупність компонент і необхідних ресурсів для реалізації сценаріїв відповідають 6-ому рівню (Відображення) моделі OSI, змістовний сенс завдань якого відображений категорією «I need ...» - «Мені необхідно ...».

Вид зв'язку, достовірність і швидкість передачі символів визначають, з одного боку, протокол і тимчасові параметри передачі інформації, що відносяться до завдань 5-го (Сеансового) рівня моделі OSI, з іншого боку, ці ж показники безпосередньо пов'язані з енергетикою ліній зв'язку на передавальній та приймаючій стороні. Цей етап трансформації Сценарної концепції в Стратегію відображений категорією «I have» - «Я маю».

В рамках 4-го (Транспортного) і 3-го (Мережевого) рівнів вибір Стратегії передачі інформації визначають знання і можливість використання Інфраструктурної концепції, а також певного Рода зв'язку.

Інфраструктурна концепція визначає, яка мережа використовується для передачі інформації: транспортна (WAN), регіональна (MAN) або локальна (LAN). Так, наприклад, для передачі інформації за допомогою безпроводових технологій (як приклада Рода зв'язку) Інфраструктурна концепція містить знання про кількість зон обслуговування і їх розміри.

Алгоритмічна концепція містить знання про ті технології, які використовують розподіл телекомунікаційного ресурсу. Наприклад, в технології стільникового зв'язку 2-го покоління GSM використовується множинний доступ з частотним і часовим поділом каналів (FDMA, TDMA). В технології стільникового зв'язку 4-го покоління LTE технології OFDMA і MIMO допомагають розподіляти і заощаджувати ресурс.

Даний етап переходу до шуканої Стратегії визначено категорією «I know» - «Я знаю», а підсумкова Стратегія передачі інформації, яка випливає з усіх попередніх кроків, відповідно до заданої Сценарної концепцією відображена категорією «I can!» - «Я можу!».

Література

1. Ильченко М.Е. Формирование телекоммуникационных Стратегий на основе Сценариев в информационном сообществе / М.Е. Ильченко, Л.А. Урывский, А.В. Мошинская // Кибернетика и системный анализ, К. – 2017., № 53., с. 96-106.
2. Мошинская А.В. Синтез методика оценки качества цифрового сигнала // А.В. Мошинская, Д.А. Георгин // «Проблеми телекомунікації»: десята міжнародна науково-технічна конференція, присвячена дню науки в Україні (ПТ-16) 19-22 квітня 2016 р., К.: с. 62…64.

УДК 621.396.4

АЛГОРИТМ ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ТАКТИЧЕСКОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТЬЮ

Романюк В.А.[1], Лысенко А.И.[2], Степаненко Е.А.[1], Жук А.В.[1], Романюк А.В.[2]

1. Военный институт телекоммуникаций и информатизации, Украина
2. Институт телекоммуникационных систем КПИ им. Игоря Сикорского
E-mail: romval2016@gmail.com

Algorithm of decision-making management of the tactical wireless sensors network

A new approach and algorithm of decision-making for tactical wireless sensor network management are proposed, which taking into account the features of its construction and functioning.

Тактические беспроводные сенсорные сети (ТБСС) предназначены для сбора информации о состоянии войск противника и своих войск (их обнаружение, идентификация, определение координат и траекторий перемещения военнослужащих и техники и т.п.) в реальном масштабе времени. ТБСС состоят из сенсорных узлов с интегрированными функциями мониторинга определенных параметров внешней среды, их обработки и передачи данных должностным лицам пунктов управления [1]. Сенсорный узел состоит из набора датчиков параметров внешней среды (акустических, температурных, оптических, магнитных и т.д.), микропроцессора, батареи и приемопередатчика с функциями маршрутизатора (возможно наличие системы позиционирования). ТБСС относятся к классу самоорганизующихся радиосетей [2] и характеризуются: ограниченностью ресурсов узлов сети (по памяти, производительности процессора, мощности передатчика, энергии батарей), ограниченной дальностью и пропускной способностью каналов радиосвязи, динамичной топологий, концентрацией трафика вокруг шлюза и т.д. Тип узлов (стационарный, подвижной), параметры мониторинга, размерность сети, тип трафика, организация управления (децентрализованная, централизованная) зависит от назначения ТБСС и предполагаемых боевых задач.

Сенсорные узлы должны адаптироваться к частым изменениям топологии сети, трафика и эффективно использовать ограниченные сетевые ресурсы. В таких условиях обеспечить покрытие узлами необходимой площади, ее мониторинг и передачу данных с заданным качеством невозможно без эффективной системы управления (СУ) [3]. К СУ предъявляются следующие основные требования: обеспечение адаптивного и распределенного функционирования сети; оптимизация характеристик сети; обеспечение принятия решений в реальном масштабе времени; максимальная автоматизация процессов управления; безопасность передачи и т.д.

Определены основные принципы функционирования СУ ТБСС: адаптивность, функциональность, иерархичность, распределенность, координация взаимодействия, оптимальность.

Функционирование сети включает следующие этапы: планирование, развертывание (восстановление поврежденных участков) и оперативное управление. Основными функциями управления ТБСС являются: построение и поддержание покрытия, мониторинга, топологии сети, маршрутов передачи данных заданного качества при полученной топологии, обеспечение процесса передачи данных мониторинга с заданным качеством, увеличение времени функционирования сети.

Исходными данными для процесса принятия решений по управлению ТБСС являются:

1. Размеры и характеристики территории покрытия.

2. Предполагаемые параметры объектов мониторинга – тип объектов противника и их количество, возможные точки входа в зоны мониторинга и т.д.

3. Ресурсы сети: количество, типы сенсорных узлов (стационарные, мобильные); характеристики сенсорных узлов (количество и тип сенсоров в узле, модели наблюдения, параметры приемопередатчика, имеющая энергия батарей, производительность процессора, величины расхода энергии батарей при различных режимах работы, множество заложенных алгоритмов управления, протоколов информационного обмена на различных уровнях OSI и т.п.); способы (случайный, детерминированный) и средства развертывания; множество реализованных в СУ методов управления сетью и т.д.

4. Директивные требования к качеству функционирования сети по: покрытию, мониторингу и передаче данных, временам функционирования, развертывания и восстановления.

Необходимо синтезировать ТБСС, обеспечивающую заданные: качество покрытия определенной территории, качество мониторинга объектов на ней, качество передачи данных мониторинга к шлюзу, время функционирования при имеющихся ресурсах и информации о противнике.

Алгоритм принятия решений по управлению сетью содержит следующие шаги.

I. На этапе планирования (развертывания, восстановления):

1. Определить необходимый тип сенсорных узлов (количество параметров мониторинга) в зависимости от параметров объекта наблюдения.

2. Определить способ развертывания (случайный, детерминированный) в зависимости от оперативной обстановки и имеющихся средств доставки.

3. Определить тип покрытия (зоновый, целей, барьерный) и модели покрытия (дисковая, секторная и др.) в зависимости от параметров объектов противника.

4. Рассчитать необходимое количество сенсорных узлов для обеспечения заданного качества покрытия (целевые функции – минимум используемых узлов, минимум непокрытых зон, целей, барьеров, обеспечение k-покрытия и др.) на заданный интервал времени. При детерминированном (случайном) способе покрытия рассчитать координаты (области) их размещения (доставки).

5. Разместить (доставить) узлы сенсорной сети и инициализировать сеть.

II. На этапе оперативного управления:

1. Сбор информации (периодический, по событиям, по требованиям) о параметрах состояния элементов всей сети или определенных фрагментов сети.

2. Анализ информации состояния – определяются: уровень выполнения сетью своих функций, необходимость управляющего воздействия, определяются цели управления с дальнейшей детализацией их на подцели.

3. Принятие решения по управлению в виде решения задач по функциям СУ и уровням эталонной модели OSI.

Задача принятия решения по управлению ТБСС сведена к задаче многокритериальной оптимизации для заданных целей и альтернатив, представленных в виде дерева "цели – подцели (задачи управления) –алгоритмы управления – управляющие воздействия".

Задача расчета, формирования и восстановления покрытия заданного качества (в виде зон, целей, барьеров) определенной территории. Например, для максимизации времени функционирования сети $T_ф$ рассчитать максимальное количество независимых множеств покрывающих активных узлов, обеспечивающих покрытие территории с заданным качеством.

Задача мониторинга объектов з заданным качеством – определение узлов мониторинга, узлов-ретрансляторов, параметров мониторинга и интенсивности трафика узлами-мониторинга и т.п.

Задача связности и оптимизации топологии сети (сетевой уровень OSI). Для каждого полученного независимого множества активного покрытия определить связную топологию, провести ее оптимизацию в зависимости от заданных целевых функций.

Задача маршрутизации. Построить дерево маршрутов передачи заданного качества от узлов-мониторинга до шлюза по заданным целевым функциям.

Задача обеспечения QoS качества передачи данных на всех уровнях OSI.

Задача минимизации расхода энергии батарей при реализации всех процессов функционирования сети (а также по всем уровням OSI) для максимизации $T_ф$. Например, построить план последовательного использования (переключения) активных подграфов сети (активные узлы-мониторинга в покрытии + активные узлы дерева маршрутизации) для максимизации $T_ф$.

4. Выдать управляющие воздействия рассылкой служебной информации и установить режимы работы узлов (активный, пассивный; узел-мониторинга или только узел-ретранслятор; установить мощности передатчиков и т.п.), сети.

Таким образом, предложены новые подходи и алгоритм принятия решений по управлению тактической беспроводной сенсорной сетью, учитывающие особенности ее построения и функционирования.

Литература

1. Міночкін А.І. Методологія управління тактичними сенсорними мережами / А.І. Міночкін, В.А. Романюк // Збірник праць науково-технічної конференції. – К.: ВІТІ НТУУ “КПІ”. – 2008. – С. 15 – 26.
2. Бунин С.Г. Самоорганизующиеся радиосети со сверхширокополосными сигналами / С.Г. Бунин, А.П. Войтер, М.Е. Ильченко, В.А. Романюк. – К.: Наукова думка, 2012.
3. Романюк В.А Система управління неоднорідними безпроводовими сенсорними мережами / В.А. Романюк, О.І. Лисенко, А.В.Романюк, В.І., Новіков / XI Міжнародна науково-технічна конференція "Проблеми телекомунікацій -2017" . – С. 28 – 32.

UDC 621.391

ENERGY EFFICIENCY AND PERFORMANCE IMPROVING IN DATA CENTER WITH PREDEFINED LOAD TYPES

Gvozdetska N.A., Globa L.S.
Institute of Telecommunications of National Technical University of Ukraine Igor Sikorsky KPI, Ukraine
E-mail: n.gvozdetska@gmail.com

ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА ПРОДУКТИВНОСТІ РОБОТИ ЦЕНТРУ ОБРОБКИ ДАНИХ З ПЕРЕДБАЧУВАНИМ НАВАНТАЖЕННЯМ

Запропоновано концепцію ефективного комбінування енергоефективного підходу до планування задач у серверному кластері центру обробки даних PCPB та стратегії пакування задач Backfill. Запропонована концепція дозволяє підвищити енергоефективність обробки даних, розподіляти задачі різної розрахункової складності на сервери із відповідними розрахунковими можливостями і при цьому використовувати апаратне забезпечення якомога ефективніше.

Digital connected world is a concept of our future. In digital world the amount of data that needs to be processed is growing every day. Meanwhile, the requirements for computing rates and quality of provided services are also increasing. To deal with these new challenges large-scale data centers are developed. However, with the growth of data centers' computing power, the amount of electric energy consumed by servers is also increasing.

The structural unit of a modern data center environment is a server cluster. Clusters of servers are used for many purposes, including high availability, load balancing, and increased computational power. Let's consider the server cluster to be the main object of the proposed concept implementation with opportunity of its scaling to the data center environment.

In [1, 2] PCPB (Power Consumption and Performance Balance) scheduling algorithm is described. Its main principle is to schedule the tasks within the server cluster considering individual power consumption functions $P = f(CPU)$, – where *CPU* (Central Processing Unit) is the load of central processor in percent – and performance of each cluster node. $P = f(CPU)$ function is defined experimentally and can vary from node to node. According to PCPB approach, each node should be preliminary attested. Within the process of preliminary attestation, the individual power consumption functions $P = f(CPU)$ of each node are defined. Within the following process of tasks scheduling, the expected total power consumption of the cluster is counted according to the $P = f(CPU)$ functions of each node (in case of current task in queue allocation to each node alternately). The nodes are further sorted by their contribution to the total power consumption and their performance as well. The nodes are marked according to gotten values and that node which has the best sum of marks for power consumption and performance is chosen to process the current task in scheduling queue. The PCPB algorithm allowed reaching up to 10% energy efficiency gain and up to 49% of

performance gain in heterogenous cluster consisting of 20 nodes.

However, the problem is that the cluster nodes using PCPB are not fully loaded by tasks – some resources are idle because of the fact that the next scheduled task is too big to be processed by corresponding node until it becomes free. It is possible to solve this problem using Backfill approach in addition to PCPB using.

According to [3], Backfill is a scheduling optimization strategy which allows a scheduler to make better use of available resources by running jobs out of order.

The input information for Backfill is:

1. the time moments, when the most priority job will be able to start;
2. the requirements for this job to be processed.

Backfill output – the jobs with lower priority, that can be started before, so they do not delay the highest priority job. For the moment when the most prioritized job is able to start the resources are anyway reserved for it. It means that only those jobs, that do not interfere with this reservation, can be started before.

In [4] a modification for Backfill algorithm is proposed. Authors consider, that traditional Backfill main disadvantage is that it schedules small jobs first, which causes fragmentation. The new proposed approach is called IBA (Improved Backfill Algorithm) and it uses BS (balanced spiral) strategy additionally. To improve Backfill algorithm authors of [4] propose to take into account the consistency of free resources volume and tasks volume (requirements), not only starting scheduling from the smallest one.

In our research it is proposed to combine Backfill algorithm and PCPB scheduling methods to schedule tasks with the highest energy efficiency and use hardware as efficient as possible.

Concept description:

Tasks, that come to the server cluster of N nodes with different physical characteristics. Tasks are organized in a queue. Each task is characterized by its computational complexity (the number of floating point operations) and its requirements for the processing system *Vreq* – the minimal volume of RAM that is needed for task processing, *kcore_req* – number of cores that are going to be reserved by the task, *tmax* – maximum time of task processing (the processing is terminated, if exceeded).

Stage I. Tasks classification and PCPB scheduling

1. According to the modified PCPB approach, tasks are classified into groups according to their computation complexity (two groups of “hard” tasks and “simple” tasks, as for the simplest example). The threshold defining problem is solved for each particular situation and based on statistics data.

2. For “hard” tasks the pool of the most energy efficient servers is allocated, the pool of the least energy efficient servers is allocated for “simple” tasks as well.

3. Tasks are distributed among the servers in each servers’ pool respectively using the PCPB scheduling approach. Thus, the tasks are scheduled to the most energy efficient nodes with the best performance first (Fig.1).

Stage II. Backfill using for better hardware utilization

4. In case there is no place in server pool for the next task in queue, the

Backfill approach is used. Thus, the small tasks are extracted from the queue and "backfilled" to the first server which has free resources for it.

The Backfill is used for group of energy efficient servers first. In case of the lack of resources in the pool of energy efficient servers, Backfill algorithm is used for the group of less efficient servers.

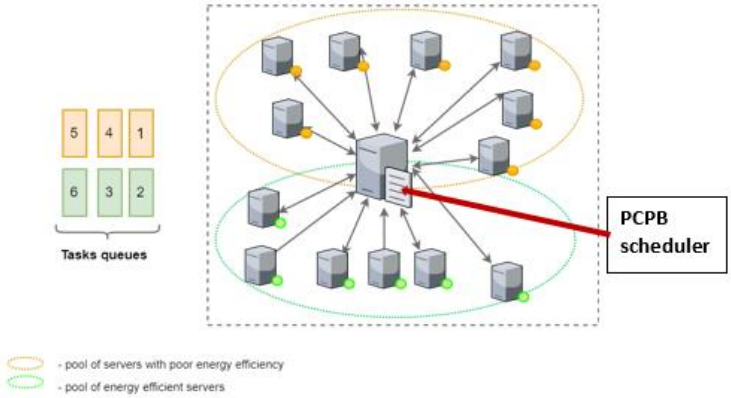


Fig. 1. PCPB scheduling according to the modified algorithm
(for two types of tasks and servers respectively)

Thus, the following goals are achieved:

- More energy efficient servers are fully loaded with the tasks – the hardware is used more efficiently;
- Servers with poor energy efficiency are loaded with those tasks that do not require high performance;
- The tasks processing performance is improved by packing tasks densely.

The proposed approach allows increasing tasks processing performance as well as energy efficiency in server cluster by using PCPB energy aware scheduling algorithm and Backfill strategy to improve hardware efficiency.

References

1. Gvozdetska N.A., Stepurin O.V., Globa L.S., "Experimental Analysis of PCPB Scheduling Algorithm" // CADSM 2017, 21-25 February, 2017, Polyana-Svalyava (Zakarpattya), UKRAINE.
2. Schill A., Globa L., Stepurin O., Gvozdetska N., Prokopets V., Power Consumption and Performance Balance (PCPB) scheduling algorithm for computer cluster // UkrMiCo 2017, Odesa, Ukraine, pp.1-8. Available online: http://ieeexplore.ieee.org/document/8095365/.
3. Suresh A., Vijayakarthick P., Improving scheduling of backfill algorithms using balanced spiral method for cloud metascheduler // Information Technology, Kalasalingam University Krishnankoil, Srivilliputtur, India.
4. Barry G. Lawson, Evgenia Smirni, Daniela Puiu, "Self-adapting backfilling scheduling for parallel systems".
5. Ahuva W. Mu'alem and Dror G. Feitelson," Utilization, predictability, workloads, and user runtime estimates in scheduling the ibm sp2 with backfilling", "IEEE transactions on Parallel and Distributed Systems,Vol. 12, no. 6, June 2001.
6. Mishra A.K., Hellerstein J.L., Cirne W. and Das C.R. (2010) Towards characterizing cloud backend workloads: insights from Google compute clusters. ACM SIGMETRICS Perform. Eval. Rev. 37, 34–41.
7. UCB/EECS-2009-28 (2010) Analysis and Lessons from a Publicly Available Google Cluster Trace . University of California at Berkeley, Berkeley, USA.

УДК 004.62

МЕТОДИ ПОШУКУ ДАНИХ НА ПОРТАЛІ НАЦІОНАЛЬНОГО АНТАРКТИЧНОГО НАУКОВОГО ЦЕНТРУ УКРАЇНИ

Новогрудська Р.Л., Юшко Н.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: rinan@ukr.net, natalia.yushko@outlook.com

DATA SEARCH METHODS ON THE NATIONAL ANTARCTIC SCIENTIFIC CENTER OF UKRAINE

The relevance of the work is to resolve the problem of organizing an effective search for a large number of poorly structured and heterogeneous information in the National Antarctic Data Center (NADC). The development and implementation of the right search method can improve the efficiency and speed of the system. On this basis, the aim of the work is to increase the efficiency and speed of the search for Antarctic research results stored in the National Antarctic Data Center. When selecting the method of searching, it is necessary to take into account the specificity of the data formats of the Antarctic researches located in the NADC, as well as their structuring and type.

Щорічно науковці ДУ НАНЦ проводять наукові експедиції на станцію Академік Вернадський. З кожної поїздки науковці антарктичного центру привозять 1000 – 2000 Гб необроблених даних. В свою чергу оброблені дані займають ще 200 – 300 Мб. Крім щорічних поїздок на рік, існують також і зимові поїздки на три місяці. В результаті таких зимівок дослідниками також збирається певний об’єм інформації [1]. Задача ускладняється тим, що співробітники працюють з даними різної форми (текст, медіа-, відеофайли, файли інших розширень). Тому, для того, щоб оптимально вирішити задачу зберігання інформації, необхідно підібрати відповідний метод пошуку інформації для підвищення ефективності роботи з порталом НЦАД. З цією метою необхідно розглянути поняття пошук інформації.

Інформаційний пошук (ІП) – процес пошуку неструктурованої документальної інформації, що задовольняє інформаційні потреби, та наука про пошук неструктурованої документальної інформації. Особливо це відноситься до пошуку інформації в документах, пошук самих документів, здобуття метаданих з документів, пошуку тексту, зображень, відео та звуку у локальних реляційних базах даних, у гіпертекстових базах даних таких, як Інтернет та локальні Інтранет, на веб-ресурсах та у електронних каталогах даних[2]. Пошук інформації являє собою процес виявлення в деякій множині документів (текстів) всіх тих, які присвячені зазначеної теми (предмету), задовольняють заздалегідь визначеним умовам пошуку (запиту) або містять необхідні (відповідні інформаційної потреби) факти, відомості, дані. Процес пошуку включає послідовність операцій, спрямованих на збір, обробку та надання інформації. У загальному випадку пошук інформації складається з чотирьох етапів: визначення (уточнення) інформаційної потреби і формулювання інформаційного запиту; визначення сукупності можливих власників інформаційних масивів (джерел); вилучення інформації з виявлених інформаційних масивів; ознайомлення з отриманою інформацією і оцінка результатів пошуку. На даний момент часу розрізняють такі типи інформаційного пошуку як повнотекстовий пошук, пошук по метаданим, пошук по зображенням.

Повнотекстовий пошук - автоматизований пошук документів, при якому пошук ведеться не по іменах документів, а по їх вмісту, всьому документу або по його частині [3]. Режим повнотекстового пошуку дозволяє ввести в пошуковий рядок одне слово, а пошук тексту буде здійснюватися по всіх його словоформам. Задля того, щоб забезпечити найбільшу продуктивність системи, необхідно ввести поняття індекс пошуку. Повнотекстовий індекс - словник, в якому перераховані всі слова наявні у даній системі чи документі, та вказано, в яких місцях вони зустрічаються. Повнотекстовий запит повертає всі документи, які містять як мінімум один збіг (відоме також як потрапляння).

Пошук по метаданим - це пошук за деякими атрибутам документа, підтримуваним системою: стандартними - такими як назва документа, дата створення, розмір, автор, або ж атрибутами що визначає безпосередньо користувач - наприклад, категорія документу, номер поїздки (зимівки), відповідальна особа і т.д. [4]

Пошук по зображеннях - пошук по змісту зображення. Пошукова система розпізнає вміст фотографії (завантажена користувачем або додана URL-адреса зображення). [5]

Так як пошук необхідно здійснити по Національному Антарктичному Центрі Даних, який в свою чергу побудований на основі платформи Microsoft SharePoint 2016, розглянемо метод пошуку який належить до SharePoint. Пошук в SharePoint можна віднести до інформаційного пошуку, що виконує повнотекстовий пошук, включаючи пошук по метаданим та по різнотипій інформації. Даний метод пошуку використовує індексування елементів (використання пошукового індексу файлів) для підвищення ефективності пошуку. Пошук в SharePoint реорганізовано в єдину корпоративну пошукову платформу. Архітектура пошуку включає наступні області: обхід та обробка контенту; індексування елементів; обробка запитів пошуку; адміністрування пошуку; аналітика пошукових запитів. При початку роботи пошукового алгоритму виконується обхід контенту, компонент обходу збирає властивості для обходу та метадані з обхідних елементів і передає їх у компоненти обробки контенту. База даних обходу містить інформацію про оброблені елементи, наприклад, останній час обходу контенту, ідентифікатор останнього обходу і тип поновлення під час останнього обходу. Компонент обробки контенту обходить джерела контенту, щоб зібрати властивості і метадані з обійдених компонентів, та відправляє отриману інформацію в компонент індексування. Компонент індексування отримує від кодека контенту оброблені елементи і записує їх в індекс пошуку. Крім того, цей компонент обробляє вхідні запити, отримує інформацію від пошукових індексів і відправляє набір результатів назад компоненту обробки контенту. Компонент обробки запитів аналізує і обробляє пошукові запити і результати. Після чого оброблений запит відправляється в компонент індексування, який повертає набір результатів пошуку для даного запиту [6]. Детальніше алгоритм роботи даного методу пошуку зображений на рисунку 1.

Веб-частина пошуку контенту це веб-частина, що відображає динамічний контент, який раніше був обійдений і доданий в індекс пошуку. Кожен екземпляр веб-частини пов'язаний з індексом пошуку і відображає результати для даного конкретного запиту. Коли користувачі переглядають сторінку, яка містить веб-частину пошуку контенту, автоматично видається запит, і від індексу пошуку повертаються результати пошуку.

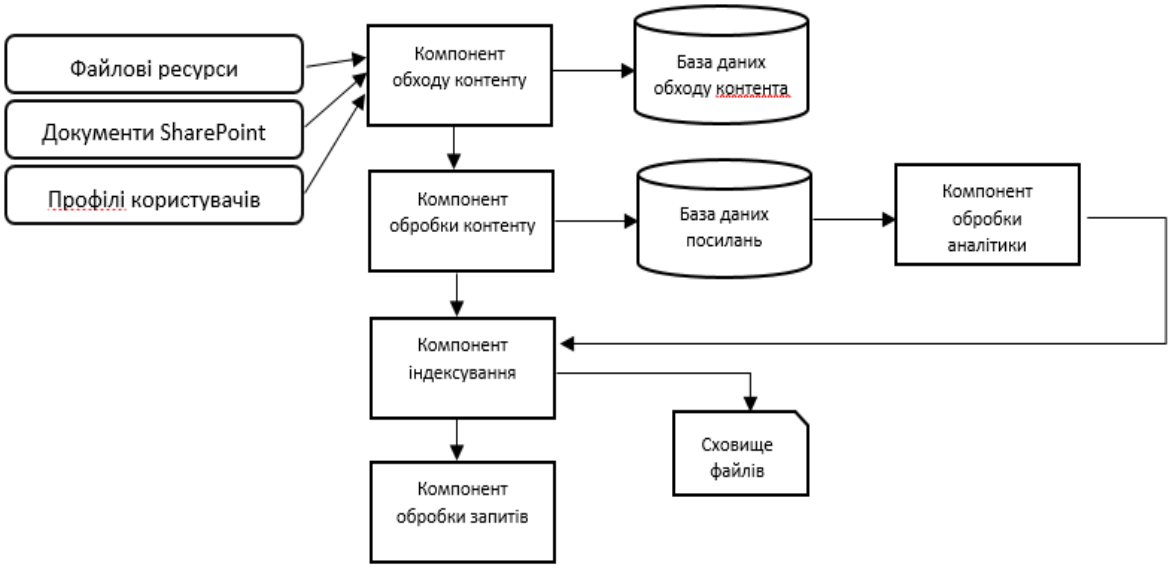


Рис. 1. Алгоритм пошуку в SharePoint.

Таким чином, проаналізувавши даний алгоритм пошуку можна зробити висновки, що він є найоптимальнішим для реалізації на порталі Національного Антарктичного Центру Даних. Адже за допомогою нього можна реалізувати ефективний пошук не лише по всьому вмісту всіх стандартних типів файлів, а й виконати пошук по всім стандартним та користувацьким метаданим. Заданий алгоритм пошуку забезпечує швидке оброблення великої кількості інформації за рахунок застосування індексування, та забезпечує подальшу аналітику пошукових запитів за рахунок наявності компонента обробки запитів. Даний алгоритм вже присутній на платформі SharePoint 2016, що спрощує задачу його застосування для Національного Антарктичного Центру Даних.

Література

1. Глоба Л.С., Мороз І. В., Новогрудская Р.Л., Мочалкина К.С., Кузін І.О.Создание единого информационного пространства данных антарктических исследований, Український Антарктичний Журнал, №10-11, 2011, с. 343-351.
2. Ланде Д. В., Снарский А. А., Безсуднов И. В. Интернетика: Навигация в сложных сетях: модели и алгоритмы. — М.: Либроком (Editorial URSS), 2009. — 264 с.
3. Manning C., Raghavan P., Schütze H. Introduction to Information Retrieval. — Cambridge University Press, 2007.
4. [Електронний ресурс] Інформаційний пошук даних на веб ресурсах та електронних каталогах http://www.viaduk.net/viaduk/notes_client.nsf/f4b82fbb75e942a6852566ac0037f284/25fa84a86061aaafc32570c800598252?OpenDocument Дата доступу: 19.02.18.
5. Shapiro Linda. Computer Vision. — Upper Saddle River, NJ: Prentice Hall, 2001.
6. [Електронний ресурс] Пошук в SharePoint https://docs.microsoft.com/uk-ua/sharepoint/dev/general-development/search-in-sharepoint#bk_crawl, Дата доступу 20.03.18.

UDC 621.391+004.7

MODEL FOR ALLOCATION OF NETWORK SLICES IN HETEROGENEOUS ENVIRONMENT

Sulima S.V.
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: lilthirteen@gmail.com

МОДЕЛЬ РОЗМІЩЕННЯ МЕРЕЖЕВИХ СЛАЙСІВ У ГЕТЕРОГЕННОМУ СЕРЕДОВИЩІ

У статті наводиться опис моделі розміщення мережевих функцій мережевих слайсів у гетерогенному середовищі, в якому наявні виділені апаратні блоки з фіксованим ресурсом обслуговування та віртуалізовані блоки, ресурси яких налаштовуються.

The article describes the network functions allocation model of network slices in the heterogeneous environment, where there are dedicated hardware blocks with fixed service resource and virtualized blocks with configurable resources.

Global mobile data usage is growing exponentially. Recent innovations in the mobile communication technologies and mobile terminals drive the proliferation of different services with a wide range of demands in terms of latency, mobility and reliability among others [1]. Network slicing has the capability of enabling (through the network architecture) future 5G networks that encompasses the required scalability and flexibility characteristics, thus supporting diverse service scenarios and services. A network slice can be broadly defined as an end-to-end logically isolated network that includes 5G devices as well as access, transport, and core network functions [2].

The network slicing concept is enabled by the Network Functions Virtualization (NFV) technology and closely related to a Virtual Network Embedding (VNE) problem that is presented in the current paper. The problem is aimed at determining the placement and amount of resources dedicated to each network function in each function chain, i.e. network slice. The general embedding approach is extended by defining network functions placement model, incorporating the notion of heterogeneous networks containing both physical devices offering services and virtualized services as well as binding network function productivity with the amount of allocated resource is proposed similar to the approach [3]. Also the differentiation of slicing objectives and its peculiarities are added to the model. The proposed enhanced optimization model incorporates the parameters and variables shown in Table I.

Table 1. Model parameters

Physical model	
G	the graph $G=(N,E)$ represents substrate network
N	$n \in N$ set of nodes include compute nodes N^c and physical network functions N^p
E	$e=(n_1,n_2) \in E$ is the set of edges within the network
Γ	$\gamma \in \Gamma$ types of resources
C^{γ}_n	γ resource capacity of node n
$CE_{n1,n2}$	bandwidth capacity of physical link $(n_1,n_2) \in E$
$L_{n1,n2}$	transmission delay of physical link $(n_1,n_2) \in E$
NF model	
τ_n^r	processing delay of a physical NF r on node n
NS model	
SFC	$ch \in SFC$ set of all service chains that must be allocated
R_{ch}	$r_c \in R_{ch}$ is set of logical node of function chain ch
L_{ch}^{max}	tolerance delay of fuction chain ch
Variables	
$x^{r,ch}_n$	value is 1 when function chain ch node r is allocated on physical node n
$F_{ch,e,\, r1,\, r2}$	value is 1 when request of function chain ch link (r_1,r_2) is mapping to physical link $e=(n_1,n_2)$
$D^{r,ch}_{\gamma}$	integer specifies the amount of type γ resource used by function chain ch node r
$DE_{ch,r1,\, r2}$	integer specifies the amount of bandwidth used by function chain ch link (r_1,r_2)

The optimization problem is formulated as follows:

Objectives:

$$\min_{x_n^{r,ch},F_{ch,e,r_1,r_2},D_\gamma^{r,ch},DE_{ch,r_1,r_2}} (a \cdot \sum_{n\in N} x_n \cdot NC_n + b \cdot \sum_{n\in N}\sum_{\gamma\in\Gamma}\sum_{ch\in SFC}\sum_{r\in R_{ch}} (virt_n \cdot x_n^{r,ch} \cdot D_\gamma^{r,ch} + phys_n{}^r \cdot x_n^{r,ch}) \cdot NC_n^\gamma + c \cdot \sum_{(n_1,n_2)\in E} NC^{band}_{(n_1,n_2)} \cdot \sum_{ch\in SFC}\sum_{(r_1,r_2)\in R_{ch}{}^2} F_{ch,(n_1,n_2),r_1,r_2} \cdot DE_{ch,r_1,r_2} + d \sum_{ch\in SFC} FC_{ch} \cdot (1 - \Phi^{ch})) \tag{1}$$

$$\max_{F_{(n_1,n_2),r_1,r_2},DE_{ch,r_1,r_2}} \sum_{(n_1,n_2)\in E} (CE_{n_1,n_2} - \sum_{ch\in SFC}\sum_{(r_1,r_2)\in R_{ch}{}^2} F_{ch,(n_1,n_2),r_1,r_2} \cdot DE_{ch,r_1,r_2}) \tag{2}$$

Subject to:

$$\forall n \in N: \forall \gamma \in \Gamma: \sum_{ch\in SFC}\sum_{r\in R_{ch}} (virt_n \cdot x_n^{r,ch} \cdot D_\gamma^{r,ch} + phys_n{}^r \cdot x_n^{r,ch}) \le C_n^\gamma \tag{3}$$

$$\forall ch \in SFC: \forall r \in R_{ch}: \sum_{n\in N} x_n^{r,ch} = 1 \tag{4}$$

$$\forall n \in N: \forall ch \in SFC: \forall r \in R_{ch}: x_n^{r,ch} \le suit_n^{r,ch} \tag{5}$$

$$\forall ch \in SFC: \forall (r_1,r_2) \in R_{ch}{}^2: \forall n \in \mathrm{N}: x_n^{r_2,ch} + \sum_{e\in E_n^{out}} F_{ch,e,r_1,r_2} = x_n^{r_1,ch} + \sum_{e\in E_n^{in}} F_{ch,e,r_1,r_2} \tag{6}$$

$$\forall ch \in SFC: \forall (r_1, r_2) \in {R_{ch}}^2: \forall n \in \mathrm{N}: x_n^{r_2,ch} + \sum_{e \in E_n^{out}} F_{ch,e,r_1,r_2} \leq 1 \quad (7)$$

$$\forall ch \in SFC: \forall (r_1, r_2) \in {R_{ch}}^2: \forall n \in \mathrm{N}: x_n^{r_1,ch} + \sum_{e \in E_n^{in}} F_{ch,e,r_1,r_2} \leq 1 \quad (8)$$

$$\forall (n_1, n_2) \in \mathrm{E}: \sum_{ch \in SFC} \sum_{(r_1,r_2) \in {R_{ch}}^2} F_{ch,(n_1,n_2),r_1,r_2} \cdot DE_{ch,r_1,r_2} \leq CE_{n_1,n_2} \quad (9)$$

$$\forall ch \in SFC: \quad (10)$$

$$\sum_{r \in R_{ch}} \sum_{n \in N} x_n^{r,ch} \cdot \left(virt_n \cdot \sum_{\gamma \in \Gamma} \frac{s_\gamma^r}{D_\gamma^{r,ch}} + {phys_n}^r \cdot {\tau_n}^r \right) + \sum_{(r_1,r_2) \in {R_{ch}}^2} \sum_{(n_1,n_2) \in E} F_{ch,(n_1,n_2),r_1,r_2} \cdot L_{n_1,n_2} \leq {L_{ch}}^{max}$$

where *a, b, c, d* – weight coefficients;

NC_n, NC^{γ}_n, $NC^{band}_{(n1,n2)}$ – node, resource and bandwidth cost;

FC_{ch} – *ch* service allocation failure cost.

The objectives of the model are to minimize the total cost of the service function chains allocations (1) and leave more bandwidth on each physical link (2). The constraints are: (3) the available capacity constraint, (4) ensures that every network function shall be mapped only once, (5) ensures that network function can be mapped only on suitable nodes, (6) the flow conservation constraint, (7)-(8) to make sure there is no incoming flow in source nodes or outgoing flow in sink nodes, (9) the available bandwidth constraint, (10) the required latency constraint.

Conclusion. The paper considers the mobile network slicing. The model for resource allocation of the system of data centers for determining optimal amount of the resources allocated to network functions in the slice has been presented. The model can be used in the management of deployment of network functions in heterogeneous hardware environment in order to minimize the operator costs and improve quality of experience.

References

1. Sama M. R. Reshaping the mobile core network via function decomposition and network slicing for the 5G Era / M. R. Sama, X. An, Q. Wei, S. Beker. // 2016 IEEE Wireless Communications and Networking Conference. – Doha, Qatar, 2016. – P. 90-96.
2. Yousaf F. Z. Reshaping the mobile core network via function decomposition and network slicing for the 5G Era / F. Z. Yousaf, M. Gramaglia, V. Friderikos, B. Gajic, et al.// 2017 IEEE International Conference on Communications Workshops. – Paris, France, 2017. – P. 1195-1201.
3. Skulysh M. Model for Efficient Allocation of Network Functions in Hybrid Environment / M. Skulysh, L. Globa, S. Sulima // Information and Telecommunication Sciences. — 2016. — № 1. — P. 39–45.

УДК 621.391

ОГЛЯД ОСНОВНИХ ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА ЯКІСТЬ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ LTE

Грицко А.В., Гаттуров В.К.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: alla.hrytsko@gmail.com, gvk51@bigmir.net

Overview on the main factors, which have impact on data transfer quality in LTE networks

This article defines main reasons of data transfer quality loss in LTE mobile networks and ways to decrease this impact in order to have appropriate quality of service and quality of subscriber's experience.

LTE (Long Term Evolution - довгострокова еволюція) - багатообіцяюча технологія високошвидкісного мобільного доступу в Інтернет. Ряд ключових особливостей робить LTE привабливою технологією для операторів і користувачів - використання MIMO, OFDMA / SC-FDMA на радіоінтерфейсі значно підвищує спектральну ефективність, збільшує швидкість передачі даних; flat і all-IP-архітектура, оптимізована під передачу пакетних даних значно знижує час відгуку мережі (latency), що дозволяє говорити про розвиток click-bang- послуг, а також про динамічне управління якістю обслуговування (QoS). Нещодавно серед найбільших операторів мобільного зв'язку в Україні було проведено тендер на ліцензії на частоти в діапазонах 2600 МГц та 1800 МГц. Кожен оператор заявляє про свою готовність запустити 4G прямо зараз - як тільки будуть дотримані всі необхідні процедури і відбудеться обмін частотами. Перші кроки 4G можна буде побачити вже в кінці весни, але повноцінно, обіцяють, мережа запрацює в великих містах не раніше липня. Для абонента запуск мережі LTE в першу чергу означає можливість користуватися високошвидкісним мобільним зв'язком, що рази перевершує можливості мереж третього покоління. Відповідно до специфікації Міжнародного союзу електрозв'язку, мінімальна швидкість передачі даних в мережі LTE-A повинна становити 1 Гбіт / с для стаціонарних об'єктів і користувачів, які прямують з низькою швидкістю. Обсяг трафіку в мобільних мережах неухильно зростає. З'являються нові сфери застосування. Все більш високими стають вимоги до якості послуг, які надаються мобільними операторами.

Коли основним сервісом мобільних операторів був "голос", технологічна оцінка мережі базувалася на площі радіопокриття, якості мовлення (MOS) і відсотку успішних з'єднань.

З ростом споживання послуг передачі даних і стрімким розвитком онлайн-сервісів, оцінка мережі, з точки зору абонента, стала критично важливою для операторів. Змінилися показники якості, а сама оцінка набула

нового позначення - якість користувацького досвіду [2,3]. Очевидно, що із переходом на технології 4G наявні стандарти на показники роботи мережі та методики проведення вимірювань повинні бути замінені такими, що враховують специфіку мереж LTE та передачі даних (в тому числі пакетну передачу голосу) як основну послугу, на якій зосереджена увага користувача

Особливості радіоінтерфейсу LTE мереж. Говорячи про тих швидкостях, які може забезпечити технологія LTE та LTE-A в низхідному і висхідному каналах (від базової станції до мобільного пристрою і назад), важливо брати до уваги кілька важливих параметрів - метод дуплексування каналів, наявний діапазон частот, вид модуляції піднесуть, метод завадостійкого кодування даних , використання технологій MIMO, витрати ресурсів на управління, тривалість циклічних префіксів [2] та ін. Розглянемо окремо вплив цих параметрів на швидкості передачі даних в низхідному каналі LTE.

OFDMA і SC-FDMA. Принципово новим рішенням для радіоінтерфейсу LTE стало використання нових методів множинного доступу - OFDMA в низхідному каналі (Orthogonal Frequency Division Multiple Access) і SC- FDMA (Single Carrier Frequency Division Multiple Access) - у висхідному. Детальний опис цих технологій можна знайти в рекомендаціях 3GPP [2]. Важливо, що весь наявний спектр розбивається на ортогональні піднесучі по 15 кГц (в низхідному каналі), кожна з яких в свою чергу модулюється певним видом модуляції (від QPSK до QAM64). 12 піднесучих - мінімальна смуга, що виділяється для одного абонента. Очевидно, що використання багатопозиційних методів модуляції вимагає каналів з високим рівнем сигнал / шум, погіршення же радіоумов призведе до зниження порядку модуляції, а, відповідно, і швидкості передачі даних. Таким чином, при поганих радіоумовах максимальні швидкості передачі даних в низхідному каналі можна сміливо розділити на 3 (при QPSK одночасно передаються 2 біти інформації, при QAM64 - 6 біт) [4,5].

MIMO. Важливим фактором при оцінці можливостей LTE є застосування технології MIMO (Multiple Input Multiple Output). Існують кілька варіантів застосування MIMO - для збільшення абонентської ємності, при цьому з різних антен передається різна інформація, і для поліпшення покриття. В останньому випадку з декількох антен передається одна і та ж інформація, що дозволяє абонентським пристрою комбінувати сигнал з різних антен, покращуючи його якість. Як правило, для збільшення абонентської ємності, оператори використовують першу опцію MIMO. У цьому випадку використання MIMO 2x2 (NMIMO = 2 - порядок MIMO) призведе до збільшення швидкості передачі даних в низхідному каналі вдвічі. Однак реалізація такої схеми потребуватиме додаткових частотно-часових ресурсів для передачі опорних пілот-сигналів антен.

Канали управління. Інформація, передана на радіоінтерфейсу, ділиться на службову інформацію, яка транслюється по різних каналах управління, і на призначені для користувача дані каналу PDSCH (Physical

Downlink Shared Channel). Радіоінтерфейс LTE підтримує як частотне, так і тимчасове дуплексування висхідного і низхідного каналів (FDD і TDD), що дозволяє розгортати мережі навіть при відсутності спарених діапазонів[4]. Так як більшість операторів, які запустили LTE, мають спарені смуги частот, то в рамках даної статті розглянемо особливості саме FDD режиму, його структуру кадру і співвідношення між призначеними для користувача і службовими ресурсами.

Масштабованість. Найважливішою особливістю мереж LTE є масштабованість займаного ними частотного спектра від 1.4 до 20МГц (можливі смуги - 1.4, 3, 5, 10, 15 і 20 МГц), яка сприяє швидкому впровадженню технології в умовах обмеженості радіоресурсів. Очевидно, що, чим ширше смуга, тим більше будуть швидкості. Нижче в таблиці 1 наведені співвідношення між шириною смуги і кількістю піднесучих і ресурсних блоків (ресурсний блок - це 12 піднесучих в частотної області і один тайм-слот або 7 OFDM-символів в часовій області) [5].

Таблиця 1. Співвідношення між шириною смуги та кількістю піднесучих

Смуга, МГц	**1.4**	**3**	**5**	**10**	**15**	**20**
Число піднесучих	72	180	300	600	900	1200
Число ресурсних блоків	6	15	25	50	75	100

Висновок: проаналізовано основні чинники, які впливають на якість передачі даних в мережі LTE. Цей вплив необхідно враховувати вітчизняним операторам зв’язку під час розгортання мережі задля підвищення якості наданих послуг, боротьби з відтоком абонентів і відповідним економічним ефектом. Адже 4G - це не тільки більш висока швидкість підключення до інтернету. В першу чергу, ці мережі мають більш високою якістю голосових послуг - HD Voice, який реалізується на базі технології VoLTE (Voice over LTE). Також поява нового покоління створює простір для новаторських комплексних рішень - наприклад, розумних міст, транспорту, інновацій в агросекторі і т.д. Частково початок таким ініціативам може бути покладено і в 3G-мережах, як це можна спостерігати в Україні. Однак для повного розкриття потенціалу розумних рішень необхідні мережі наступного покоління.

Література

1. H. Holma, LTE for UMTS – OFDMA and SC–FDMA Based Radio Access, John Wiley & Sons, 2009 – 450 с.
2. А.Л. Гельгор Е.А. Попов - Технология Lte Мобильной Передачи Данных [Електронний ресурс] // Режим доступу до ресурсу: http://www.cee.spbstu.ru/Polozhintsev/popov3.pdf.
3. Александр Константинов - Методы тестирования радиооборудования сети LTE. Подробный анализ К.: Наук. думка, 2004. - 264 с.
4. Recommendation ITU-R BS.1387-1. Method for objective measurements of perceived audio quality.
5. Fermin Armenta-Cano, Andrei Tchernykh, Jorge M. Cortés-Mendoza, Ramin Yahyapour, Alexander Yu. Drozdov, Pascal Bouvry, Dzmitry Kliazovich, Arutyun Avetisyan “Min_c: Job Consolidation for Power Aware Scheduling with Quality of Service”, Russian Supercomputing Days, Moscow, 2015.

УДК 621.391

ОСОБЛИВОСТІ ПЕРЕДАЧІ МУЛЬТИСЕРВІСНИХ ПОТОКІВ В СТАНДАРТІ DVB-T2 ТА ВИКОРИСТАННЯ ЇХ У ДУПЛЕКСНІЙ ЛІНІЇ ЗВ'ЯЗКУ

Уривський Л.О., Шевченко М.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: leonid_uic@ukr.net, marshelka@meta.ua

The features of multiservices flows transfer in the DVB-T2 standard and the using their in duplex communication line

In this paper, the features of using the DVB-T2 television broadcasting standard are considered in terms of transferring its properties from a one-way transfer system to duplex multi-user systems. The types of multi services transmitted by this TV system in detail are considered.

У даній роботі розглядаються особливості використання стандарту телевізійного мовлення DVB-T2 з точки зору перенесення його властивостей з системи с односторонньої передачею в дуплексні багатокористувальницькі системи. Детально розглянуті види мультисервісів, що передаються даною телевізійною системою.

Стандарт DVB-T2 являється потужним інструментом мультисервісного мовлення, в який закладено величезні можливості по розширенню функціоналу.

Система DVB-T2 здатна передавати кілька незалежних мультимедійних потоків, кожен з яких має власну схему модуляції, швидкість кодування та часові інтервали. Канал PLP (Physical Layer Pipe) у стандарті DVB-T2 є логічним каналом, що несе одну або більше послуг зі своєю схемою модуляції та надійністю [1].

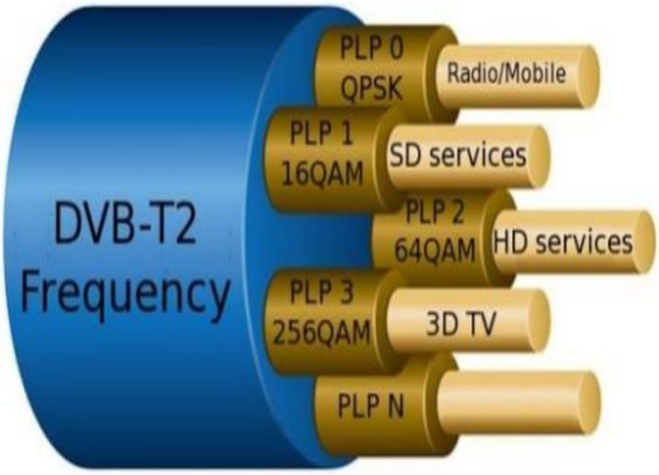


Рис. 1. Логічний канал PLP

Стандарт DVB-T2 передбачає надання різних цифрових сервісів та послуг на підставі мультисервісності потоків, серед них: багатоканальне мультиплексування, телебачення стандартної чіткості SDTV в форматах співвідношення сторін екрану 4:3 і 16:9, телебачення високої чіткості HDTV, телебачення надвисокої чіткості UHDTV, 3D-телебачення в стандарті DVB 3D-TV, інтерактивне гібридне телебачення в стандарті HbbTV, відео за запитом, телетекст, субтитри, стереозвук, цифрове радіо та інші.

Кілька PLP дозволяє операторам передавати послуги високої чіткості HD з низькою надійністю й одночасно послуги середньої чіткості SD, але з високою надійністю. Наприклад, в одному каналі одночасно можуть передаватися до 16 мобільних послуг, що вимагають швидкості передавання до 10 Мбіт/с, і 3-4 види HD послуг в одному каналі мовлення [2].

Для передавання сервісу більш високої якості необхідно використовувати більш високі види кратності модуляцій, але збільшення позиційності модуляції призводить як до збільшення продуктивності, так водночас до погіршення достовірності, адже застосування завадостійкого кодування дозволяє забезпечити необхідну достовірність. В стандарті DVB-T2 використовуються потужні LDPC коди та коди БЧХ з високою швидкістю виправлення помилок.

Достовірність інформації, що передається, являється однією з найважливіших характеристик, що визначає якість інформаційного обміну, та є одним з показників якості обслуговування.

Очевидно, що стандарт DVB-T2 має великий набір різних сервісів і послуг для передачі та при цьому повинен мати високу продуктивність. Всі ці особливості, з точки зору якості та продуктивності системи, передбачені в телевізійному стандарті, але такі ж характеристики і показники були б корисними і в інших телекомунікаційних системах.

Тому доцільно буде використати ці інструменти та особливості зі стандарту DVB-T2 у дуплексній системі зв'язку, яка буде реагувати на зміни на лінії, наприклад, у випадку термінового розгортування мережі у надзвичайних умовах, коли часу на точні розрахунки енергетики немає, а умови багатопроміневості змінюються. В цьому випадку умови передачі сигналу будуть відповідати конкретним умовам використання та пристосовуватися до змін умов завдяки відповідним адаптивним реагуванням системи.

Приклад дослідження відповідності енергетичних станів каналу зв’язку (через показник h^2) значенню показника інформаційної ефективності η [3] відображено на рис. 2, де ілюструється досягнення найбільшого значення показника η = 0,74 при модуляції QAM-16 і значенні швидкості кодування 4/5 при $h^2 = 20$.

В свою чергу, показник інформаційної ефективності η визначено як відношення реально досягнутою продуктивності каналу зв’язку R до його пропускної спроможності $C_н$:

$$\eta = \frac{R}{C_н}. \quad (1)$$

Показник енергетичного стану каналу зв'язку визначається через потужність сигналу P_S в точці прийому, швидкість передавання символів V_C та спектральну густину шуму N_0:

$$h^2 = \frac{E_S}{N_0} = \frac{P_S}{V_C \cdot N_0} \quad (2)$$

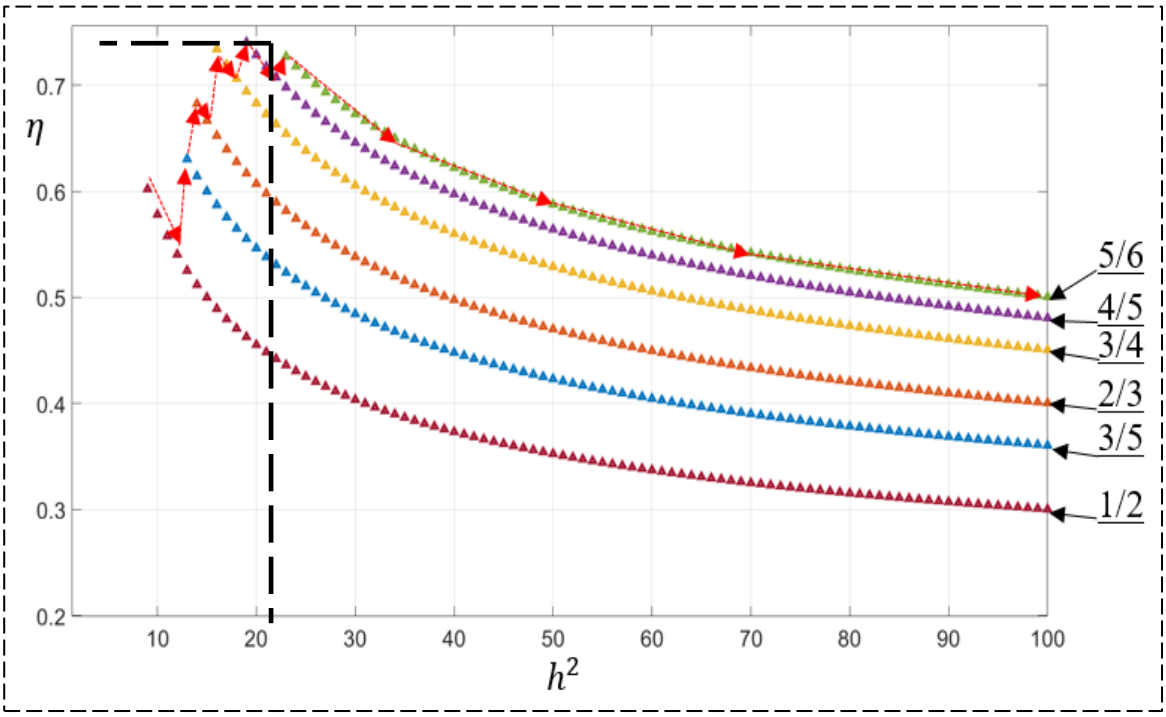


Рис. 2. Ефективність інформації η як функція SNR для модуляції QAM-16 та каскадного кодування (код LDPC та неперервний код)

Отже, стандарт DVB-T2 є прикладом реалізації сучасної мультисервісної системи з надійною передачею інформації для багатьох користувачів, але в режимі односпрямованого передавання. Перспективною слід вважати завдання реалізації сформульованих принципів при створенні новітніх мультисервісних систем двостороннього, в тому числі дуплексного, зв'язку.

Література

1. Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2). – Draft ETSI EN 302 755 V1.4.1, February 2015.
2. Баляр В. Б. Порівняльна характеристика систем цифрового наземного телевізійногомовлення у стандартах DVB-T/T2 / В. Б. Баляр, О. В. Гофайзен // Цифрові технології. - 2012. - Вип. 11. - С. 31-46.
3. Ilchenko M.Yu., Uryvsky L., Moshynska A., Osypchuk S.Empirical and analytical energy thresholds of Modulation-Coding Schemes research in IEEE 802.11n devices. – TCSET-2018 Lviv /14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering. – Lviv - Slavske, Ukraine.

УДК 004.052.42

ЕНЕРГЕТИЧНИЙ ПОТЕНЦІАЛ АТМОСФЕРНИХ ОПТИЧНИХ СИСТЕМ ПЕРЕДАЧІ

Яровий О.В., Пархомей І.Р.
Департамент навчальної роботи КПІ імені Ігоря Сікорського,
Факультет інформатики та обчислювальної техніки
КПІ ім. Ігоря Сікорського, Україна
E-mail: getem13@ukr.net

Energy potential of atmospheric optical transmission systems

An analysis of the parameters that determine the value of the potential energy potential of atmospheric optical transmission systems is carried out. The directions of increasing the reliability of atmospheric optical transmission systems due to the use of new optimization approaches are considered.

Проведено аналіз параметрів, які визначають значення можливого енергетичного потенціалу атмосферних оптичних систем передачі. Розглянуто напрямки підвищення надійності роботи атмосферних оптичних систем передачі за рахунок використання нових оптимізаційних підходів.

Атмосферні оптичні системи передачі (АОСП) забезпечують передачу даних модульованим випромінюванням в інфрачервоній частині спектра через атмосферу. На сьогодні, застосування зазначених систем отримує все більше поширення в сегменті високошвидкісного безпроводового транспортування даних. Перспективність їх використання ґрунтується на певних особливостях даної технології. Це насамперед використання випромінюючих засобів, що працюють на частотах значно більших від встановленої для радіочастотного діапазону межі (400 ГГц). Отже такі системи не використовують радіодіапазон і не створюють перешкод в радіочастотному спектрі. Крім того, АОСП потребує невеликого часу для розгортання та має мінімальне енергоспоживання (десятки Вт). В результаті вище зазначеного, застосування АОСП може забезпечувати реалізацію ряду технічних переваг, зокрема: відсутність чутливості до радіоперешкод, висока скритність та розвідзахищеність, висока швидкість передачі, прозорий механізм передачі (можливість транспортування потоків створених за різними протоколами *SDH, ATM, Ethernet*).

На якість зв’язку в АОСП впливає цілий ряд чинників, які при певних обставинах можуть суттєво знизити позитивний ефект від їх застосування. Найбільше це стосується особливих погодних умов, таких, як дощ, сніг, туман і т. д., що можуть значно погіршити видимість і, таким, чином понизити ефективність використання діапазону інфрачервоного зв’язку [1]. Крім того, в атмосфері спостерігаються турбулентні явища, які приводять до флуктуації показника заломлення середовища, коливанням світла і спотворенням сигналу, що приймається. Деякі з зазначених чинників можуть призводити до збільшення значення показника затухання на десятки дБ. Проте найбільше зростання втрат виникають в умовах щільного туману, коли вони можуть складати до 100 дБ/км і навіть більше. Це безумовно призводить до зменшення рівня сигналу на прийомі, і, як наслідок, до збільшення коефіцієнту помилки. Реальні зразки апаратури, які на сучасному етапі пропонуються для практичного використання, гарантують дальність зв’язку до 4 км (при швидкості передачі 100 Мбіт/с і надійності зв’язку 99,9 %) [2]. Це цілком конкурентоздатні показники, але все ж такі досить скромні, якщо порівнювати їх з сучасними радіорелейними інтервалами або системами безпроводового широкосмугового доступу WiMax.

Для збільшення енергетичного потенціалу АОСП і, відповідно, підвищення надійності їх роботи можливе використання наступних підходів:

– збільшення потужності оптичних випромінювачів (передавачів);

– збільшення чутливості оптичних детекторів (приймачів);

– звуження діаграми спрямованості передавальних антен;

– використання адаптації за довжиною хвилі;

– використання методів рознесеного прийому та інших.

В якості оптичних випромінювачів у АОСП використовують світловипромінюючі або напівпровідникові лазери.

Світловипромінюючий діод (СВД) є напівпровідниковим приладом з p-n переходом, протікання електричного струму через який викликає інтенсивне спонтанне випромінювання. Найбільше застосування отримали торцеві або суперлюмінесцентні СВД.

Лазер – прилад, що генерує оптичне когерентне випромінювання на основі ефекту вимушеного, стимульованого випромінювання. Принцип роботи лазера заснований на створенні активного середовища, в якому під впливом зовнішнього поля створюються електрони, що перебувають у збудженому стані. Так же саме, як і в СВД під впливом модулюючого струму, створюється спонтанне випромінюється. Електромагнітна хвиля, яка випромінюється лазером вважається когерентною, оскільки її амплітуда, частота, фаза, напрям поширення і поляризація постійні або змінюються впорядковано. Сучасні напівпровідникові лазери здатні забезпечити випромінювання з потужністю декілька сотень Вт, з кутом розходження порядку до 5˚ (у вертикальній площині) і до 15˚ (у горизонтальній) та шириною спектра випромінювання до 3 нм.

Очевидно, що з економічної точки зору доцільним є використання СВД. Однак для роботи на великі відстані, де важливо забезпечити високу потужність випромінювання та зменшити втрати пов’язані із великим кутом розходження, що призводить до невлучення частини випромінювання у приймальну антену, перевагу має застосування лазерів. Отже потенційно можливе використання, оптичного випромінювача (лазера) з потужністю до 100 Вт (зразки, що випускають серійно). Проте треба зазначити, що існують також обмеження щодо використання високопотужних оптичних джерел випромінювання, які пов’язані із встановленими вимогами до безпеки персоналу. Максимальне допустиме лазерне випромінювання залежить від типу використовуваного лазерного діода (довжини хвилі).

В якості приймачів АОСП використовують, як правило, фотодіоди *p-i-n* або лавинні фотодіоди (ЛФД). Фотодіоди *p-i-n* відрізняються простотою конструкції, високою надійністю, низкою вартістю.

Фотострум дрейфу, величина якого прямо пропорційна величині потужності прийнятого оптичного випромінювання, розраховується за формулою:

$$I_{\text{ф}} = \frac{P \cdot \lambda \cdot e}{h \cdot c} \eta , \qquad (1)$$

де P – потужність оптичного випромінювання, λ – довжина хвилі оптичного випромінювання,

e – заряд електрона, h – постійна Планка, c – швидкість світла та η – квантова ефективність фотодіода.

Чутливість фотодіода оцінюється відношенням утвореного фотоструму до потужності оптичного випромінювання, що його утворила:

$$S = \frac{I_{\text{ф}}}{P} = \frac{\lambda \cdot e}{h \cdot c} \eta . \qquad (2)$$

Реальні приймальні оптичні модулі обладнані p-i-n фотодіодами мають чутливість порядку –20 дБм [3] (для швидкості передачі сигналу 10 Гбіт/с).

У лавинному фотодіоді досягається підсилення первинного фотоструму за рахунок керованого лавинного множення числа носіїв заряду. Цьому сприяє конструкція ЛФД.

Процес збільшення числа носіїв зарядів розвивається лавиноподібно і характеризується відповідним коефіцієнтом, який залежить від матеріалу виготовлення і може складати від 2 (для германієвих ЛФД) до 100 (для кремнієвих ЛФД). Відповідно до (2) цей процес призводить до аналогічного збільшення чутливості. Таким чином практична чутливість ЛФД може складати до –40 дБм [3] (для швидкості передачі сигналу 10 Гбіт/с). Крім того, приймачі обладнані ЛФД мають значну швидкодію, що дозволяє їхнє використання на швидкостях передачі даних вище 10 Гбіт/с.

Можливий інший варіант збільшення енергетичного потенціалу АОСП – шляхом використання декількох передавачів і декількох приймачів. Таке рішення дозволяє реалізувати схему рознесеної передачі, що є фактично безальтернативним заходом для боротьби із впливом турбулентності атмосфери та іншими явищами, що носять випадковий характер впливу. Одночасно збільшується сумарна площина приймальної поверхні, без збільшення апертури приймача, що дозволяє компенсувати порушення юстировки і при цьому уникнути збільшення ймовірності потрапляння до приймальної лінзи стороннього випромінювання (наприклад, сонячного світла). При певній реалізації, заходів адаптації діаграми спрямованості та рознесеної передачі можливо повністю мінімізувати втрати за рахунок неузгодженості.

Таким чином, враховуючі все вище зазначене, можна порівняти характеристики типового існуючого обладнання АОСП та перспективного. Результати порівняння, які були зроблені для випадку найгірших умов передачі (щільний туман), коли втрати будуть складати порядку 100 дБ/км, наведені у таблиці 1.

Таблиця 1. Порівняльний аналіз енергетичного потенціалу АОСП

№ з/п	***Назва параметру***	***Значення параметру для***	
		існуючих АОСП	***перспективних АОСП***
1	Потужність випромінювання	50 мВт (17 дБм)	100 Вт (50 дБм)
2	Чутливість приймача	10 нВт (–50 дБ)	10 пВт (–80 дБ)
3	Втрати юстировки	3 дБ	0 дБ
4	Енергетичний потенціал	64 дБ	130 дБ
5	Дальність зв’язку в ясну погоду/в туман	21 км / 0,64 км	43 км /1,3 км

Література

1. Яременко Ю.И. Применение открытых оптических систем передачи в сетях связи [Текст] / Яременко Ю.И. – Радиоэлектроника и телекоммуникации № 1 (37), 2005. – С. 35 – 42.
2. Атмосферные оптические системы передачи [Електронний ресурс]. – Режим доступу: http://www.micromax.ru/catalog/comparePAV.shtml.
3. Корнійчук В.І. Аналіз чутливості приймальних пристроїв ВОСП-СРК [Текст] / Корнійчук В.І., Барба І.Б., Дойжа Г.І. – Збірник наукових праць ОНАЗ ім. О.С. Попова. – № 2 / 2010.

УДК 621.396.722

ОПТИМАЛЬНИЙ НЕКОГЕРЕНТНИЙ ДЕМОДУЛЯТОР ВФМ-2 СИГНАЛІВ ІЗ МАНЧЕСТЕРСЬКИМ КОДУВАННЯМ МОДУЛЮЮЧОГО СИГНАЛУ

Парфенюк В.Г., Сабадаш С.С.
Житомирський військовий інститут імені С.П. Корольова
E-mail: strob243@gmail.com

Optimal incoherent demodulator of DPSK signals with Manchester encoding of modulating signal

The proposed algorithm and scheme of the optimal incoherent demodulator of the DPSK signals with the Manchester encoding of the modulating signal, which provide a higher noise immunity to it when used in digital radio communication systems, and retains the advantages of Manchester encoding. The performed mathematical modeling confirmed the efficiency of the proposed technical solutions and its higher noise resistance.

Теорія оптимального когерентного та некогерентного приймання ФМ-2 та ВФМ-2 сигналів достатньо детально описана у багатьох публікаціях, зокрема в [1, 2, 3, 4]. В усіх відомих автору публікаціях алгоритми оптимального приймання розглядаються для біполярного представлення модулюючого двійкового сигналу $x(t)$ без повернення до нуля (*NRZ* представлення). Відомо також, що використання в цифрових радіосистемах передачі інформації манчестерського кодування огинаючої радіосигналу дає суттєві переваги при формуванні сигналів символьної синхронізації демодулятора.

Отримати алгоритми оптимального приймання, при яких використовується вся енергія бітової посилки при манчестерському кодуванні огинаючої можна, якщо реалізувати не посимвольне приймання, а приймання в цілому по відношенню до бітової посилки, що включає дві символьні посилки [2].

При ВФМ-2 кодування бітового потоку проводиться із використанням диференційного манчестерського коду. При цьому значення переданого інформаційного символу визначають не самі по собі два символи манчестер-коду на інтервалі часу (0, T), а послідовність чотирьох символів манчестер-коду на інтервалі (0, 2T).

Нехай символу 0 манчестер-коду тривалістю $T/2$ відповідає елементарний сигнал $-S_0\cos\omega_0 t$, а символу 1 – $+S_0\cos\omega_0 t$. Тоді значення переданого інформаційного символу буде визначати послідовність чотирьох елементарних сигналів на інтервалі (0, 2T) із врахуванням того, що символам 1 та 0 відповідають сигнали $s_1(t)$ та $s_0(t)$:

$$s_1(t)=\begin{cases}-S_0\cos(\omega_0 t+\varphi), & 0<t<T/2;\\ S_0\cos(\omega_0 t+\varphi), & T/2<t<3T/2;\\ -S_0\cos(\omega_0 t+\varphi), & T/2<t<3T/2;\end{cases}$$

$$s_0(t)=\begin{cases}S_0\cos(\omega_0 t+\varphi), & 0<t<T/2;\\ -S_0\cos(\omega_0 t+\varphi), & T/2<t<T;\\ S_0\cos(\omega_0 t+\varphi), & T<t<3T/2;\\ -S_0\cos(\omega_0 t+\varphi), & 3T/2<t<2T,\end{cases} \qquad (1)$$

де φ – випадкова початкова фаза із рівномірним законом розподілу.

При ВФМ-2 рішення щодо переданого інформаційного символу приймається відповідно до співвідношення фаз двох сусідніх бітових сигнальних посилок. Алгоритм оптимального некогерентного приймання ВФМ-2 сигналів передбачає обчислення квадрата модуля кореляційного інтеграла для кожного із сигналів та порівняння їх значень між собою [2]:

$$\begin{aligned} &Z_1^2 \geq Z_0^2, \quad \text{переданий сигнал } s_1(t); \\ &Z_1^2 < Z_0^2, \quad \text{переданий сигнал } s_0(t), \end{aligned} \tag{2}$$

де

$$\begin{aligned} Z_1^2 &= \left[\int_0^{T_c} y(t)s_1(t)dt\right]^2 + \left[\int_0^{T_c} y(t)s_1^*(t)dt\right]^2; \\ Z_0^2 &= \left[\int_0^{T_c} y(t)s_0(t)dt\right]^2 + \left[\int_0^{T_c} y(t)s_0^*(t)dt\right]^2, \end{aligned} \tag{3}$$

де $s_i^*(t)$, $i = 0, 1$ – сигнал ортогональний сигналу $s_i(t)$, T_c – тривалість сигналів $s_1(t)$, $s_0(t)$, Z_1^2, Z_0^2 – квадрати кореляційних інтегралів, відповідно до співвідношення значень яких приймається рішення щодо переданого біту двійкового коду u_k.

Із врахуванням (3) та (1) алгоритм оптимального некогерентного приймання ВФМ-2 сигналів із манчестерським кодування (2) матиме наступний вигляд:

$$\begin{aligned} &Z_1^2 = z_1(0,T/2)z_1(T,3T/2) - z_1(0,T/2)z_1(3T/2,2T) - \\ &-z_1(T/2,T)z_1(T,3T/2) + z_1(T/2,T)z_1(3T/2,2T) \geq Z_0^2 = \\ &= z_2(0,T/2)z_2(3T/2,2T) + z_2(T/2,T)z_2(T,3T/2) - \\ &-z_2(T/2,T)z_2(3T/2,2T) - z_2(0,T/2)z_2(T,3T/2), \quad \text{переданий сигнал } s_1(t); \\ &Z_1^2 = z_1(0,T/2)z_1(T,3T/2) - z_1(0,T/2)z_1(3T/2,2T) - \\ &-z_1(T/2,T)z_1(T,3T/2) + z_1(T/2,T)z_1(3T/2,2T) < Z_0^2 = \\ &= z_2(0,T/2)z_2(3T/2,2T) + z_2(T/2,T)z_2(T,3T/2) - \\ &-z_2(T/2,T)z_2(3T/2,2T) - z_2(0,T/2)z_2(T,3T/2), \quad \text{переданий сигнал } s_0(t), \end{aligned} \tag{4}$$

де

$$\begin{aligned} &z_1(0,T/2) = \int_0^{T/2} y(t)\cos\omega_0 t dt; \qquad z_1(T/2,T) = \int_{T/2}^{T} y(t)\cos\omega_0 t dt; \\ &z_1(T,3T/2) = \int_T^{3T/2} y(t)\cos\omega_0 t dt; \quad z_1(T/2,2T) = \int_{T/2}^{2T} y(t)\cos\omega_0 t dt; \\ &z_2(0,T/2) = \int_0^{T/2} y(t)\sin\omega_0 t dt; \qquad z_2(T/2,T) = \int_{T/2}^{T} y(t)\sin\omega_0 t dt; \\ &z_2(T,3T/2) = \int_T^{3T/2} y(t)\sin\omega_0 t dt; \quad z_2(T/2,2T) = \int_{T/2}^{2T} y(t)\sin\omega_0 t dt. \end{aligned} \tag{5}$$

Структурна схема когерентного демодулятора, що реалізує алгоритм (4) представлена на рис. 1. Схема включає синфазний канал, який обчислює квадрат модуля кореляційного інтеграла Z_1^2 та квадратурний канал, який обчислює квадрат

модуля кореляційного інтеграла Z_0^2. Їх обчислення проводиться на інтервалі чотирьох елементарних символів манчестер-коду (0, 2T). Інтегратори каналів обчислюють значення складових Z_1^2 та Z_0^2 на інтервалі тривалості символу манчестер-коду $\tau = T/2$.

Крім помножувачів та інтеграторів (Інтегр), що обчислюють значення кореляційних інтегралів, схема містить пристрій відновлення носійної (ПВН), лінії затримки та пристрій прийняття рішення (ППР) щодо переданого інформаційного символу.

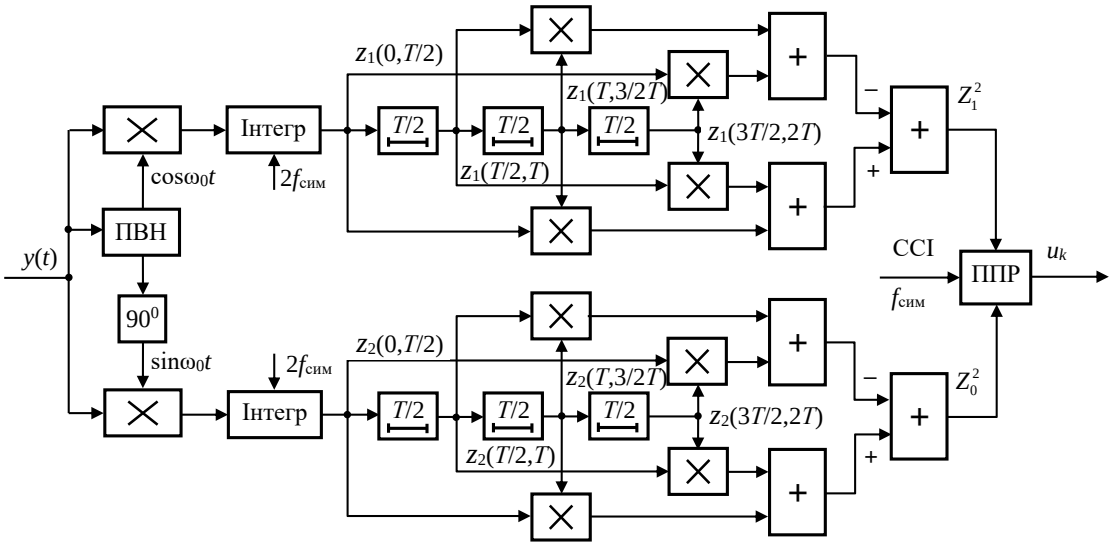


Рис. 1. Структурна схема оптимального некогерентного демодулятора ВФМ-2 сигналів із манчестерським кодуванням.

Пристрій символьної синхронізації (не показаний на схемі) формує символьні синхроімпульси (ССІ) із частотою $f_{сим} = 1/T$, які визначають моменти часу прийняття рішення пристроєм прийняття рішень та використовуються для скиду інтегратора (після подвоєння частоти).

Для оцінки потенційної завадостійкості некогерентного демодулятора ВФМ-2 сигналів можна використати загальну формулу для оптимального некогерентного приймання ВФМ-2 сигналів, зважаючи, що сигнали (1) ортогональні в посиленому розумінні [2]. Тоді, зважаючи на (4), (5) та враховуючи у якості відношення сигнал/шум q^2 відношення енергії сигналу на інтервалі тривалості інформаційної посилки T до спектральної щільності шуму N_0 потенційна завадостійкість некогерентного демодулятора сигналів ФМ-2 буде визначатись за формулою [2]:

$$P_{пом} = 0,5\exp\left(-q^2\right), \tag{6}$$

де $q^2 = E_b/N_0$, $E_b = 2E_s = P_c T$, – енергія сигналу, що приходиться на двійковий символ (біт), E_s – енергія символу манчестер коду, $P_c = 0,5S_0^2$ – потужність сигналу.

Для перевірки працездатності розробленої схеми демодулятора та експериментальної оцінки його потенційної завадостійкості було проведене математичне моделювання із використанням розроблених на ПЕОМ у середовищі графічного програмування LabVIEW віртуальних демодуляторів.

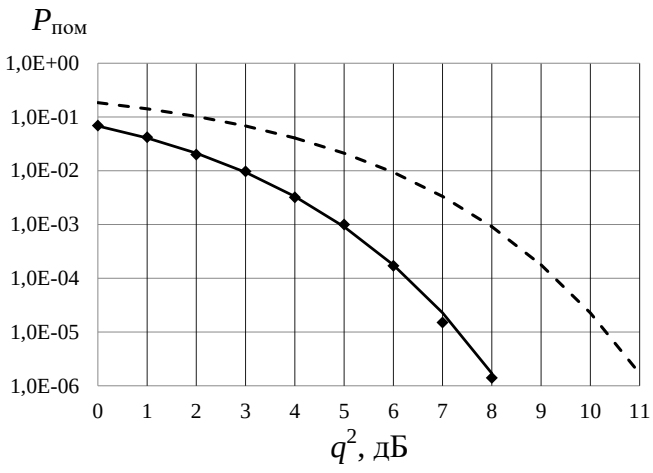


Рис. 2. Криві потенційної завадостійкості некогерентного приймання ВФМ-2 сигналів із манчестерським кодуванням

Проведене математичне моделювання підтвердило працездатність запропонованої схеми демодулятора сигналів із манчестерським кодуванням та можливість використання для оцінки його потенційної завадостійкості формули (6). Результати розрахунків та експериментальні дані для некогерентного демодулятора ВФМ-2 наведені на рис. 2.

Показані на рис. 2 штрихові лінії відповідають оптимальному посимвольному прийманню сигнальних посилок манчестер-коду, суцільні лінії – розрахункам по формулі (6), а маркери – результатам моделювання.

Із аналізу отриманих графіків слідує, що результати моделювання підтверджують очікуваний потенційний енергетичний виграш у 3 дБ для запропонованої схеми демодулятора.

Отримані результати дозволяють стверджувати, що запропонована схема демодулятора може бути використана у складі приймальних пристроїв цифрових систем передавання інформації, зокрема, для підвищення завадостійкості комплексу приймання та обробки інформації дистанційного зондування Землі інституту у форматі High Resolution Picture Transmission (HRPT), який на сьогоднішній день використовується в радіолінії середнього розрізнення в діапазоні 1,7 ГГц.

Література

1. Тихонов В. И. Оптимальный прием сигналов. – М.: Радио и связь, 1983. – 320 с.

2. Финк Л. М. Теория передачи дискретных сообщений / Л. М. Финк. – М. : Сов. радио, 1970. – 728 с.

3. Прокис Дж. Цифровая связь / Дж. Прокис; под ред. Д. Д. Кловского; пер. с англ. – М.: Радио и связь, 2000. – 520 с.

4. Окунев Ю. Б. Цифровая передача информации фазомодулированными сигналами / Ю. Б. Окунев. – М.: Радио и связь, 1991. – 296 с.

УДК 621.382

ПОКРАЩЕННЯ ТЕХНОЛОГІЇ ЛОКАЛІЗАЦІЇ ПРОТОКОЛУ OLSR

Максимов В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: maksimov46@ukr.net

Improving OLSR protocol localization technology

In the paper, with the same reach of nodes for the same choice, MPRs are proposed to calculate the cross-sectional area of nodes coverage with the coverage area of an already selected MNR.

В оригінальному протоколі OLSR [1] розглядається набір вузлів *N*, що знаходяться в радіусі дії центрального вузла A, а також набір *N*2 – двоскачкові сусіди вузла A, зв'язок з якими може бути встановлено через один проміжний вузол-ретранслятор, за виключенням: вузлів, що доступні тільки через вузли з набору N з готовністю WILL_NEVER; вузлів, що здійснюють обчислення; всі симетричні сусіди: вузли, для яких існує симетричний лінк до вузла на деякому інтерфейсі. Також вводиться поняття D(y) – кількість сусідів вузла y (де y є членом набору *N*), за виключенням всіх вузлів з набору *N* і вузлів, що виконують обчислення.

Згідно з оригінальним евристичним алгоритмом для визначення MPR вузлів потрібно зробити наступні кроки: включити до набору N всі вузли з готовністю WILL_ALWAYS; розрахувати D(y), де y є членом набору N, для всіх вузлів з набору N; додати в набір MPR ті вузли, що входять до набору N і є єдиними вузлами, що забезпечують доступність до вузлів з набору N2; якщо ще існують вузли з N2, які залишились непокритими хоча б одним вузлом з набору MPR, то для кожного вузла з набору N порахувати досяжність – кількість вузлів з набору N2, які ще залишились непокритими хоча б одним вузлом з набору MPR, і які досяжні через односкачкового сусіда; вибрати як MPR вузол з найбільшою готовністю серед вузлів з набору N з не нульовою досяжністю. У випадку, коли існує декілька таких вузлів, то вибрати вузол як MPR, що покриває максимальну кількість вузлів N2. У випадку, якщо існує декілька таких вузлів, то вибрати вузол як MPR, що має найбільше значення D(y).

Завдяки використанню даного алгоритму було досягнуто зменшення кількості службового трафіку в мережі для оригінального протоколу OLSR. Але даний алгоритм має недолік, що і був використаний для розробки технології локалізації, а саме: відсутній механізм, що вирішує конфлікт для однакових значень *D(y)* при виборі MPR вузлів на останньому етапі. Цей недолік вносить певну «сліпоту» в оригінальний алгоритм, адже при рівних значеннях *D(y)* вибір здійснюється випадково. В свою чергу це може привести до меншого покриття MPR вузлами зони, де знаходяться вузли з набору N2.

Для того, щоб кожен вузол в мережі знав координати своїх односкачкових та двоскачкових сусідів достатньо передавати в повідомленні HELLO їх координати *x, y, z*. В той же час немає необхідності передавати ці дані в повідомленнях TC. На основі даних про місце розташування вузлів було внесено зміни в роботу оригінального алгоритму вибору MPR і розроблена так звана «технологія

локалізації» [2].

Згідно даної технології локалізації новий алгоритм вибору MPR вузлів працюватиме наступним чином: 1. Побудувати набори *N* та *N*2. Включити до набору *N* всі вузли з готовністю *WILL_ALWAYS*. 2. Встановити для вузла *S* набір MPR такий, що MPR(S)=∅; 3. Розрахувати *D(y),* де *y* є членом набору *N*, для всіх вузлів з набору *N*. 4. Додати в набір MPR(S) ті вузли, що входять до набору *N* і є єдиними вузлами, що забезпечують доступність до вузлів з набору *N2*. Наприклад, якщо вузол *b* з набору *N2* може бути доступний тільки через симетричний лінк до вузла *a* з набору *N*, тоді додати вузол *a* до набору MPR(S). Видалити вузли з набору *N2*, які вже покриті вузлами з набору MPR(S). 5. Вибрати базовий вузол, що має найбільше значення *D(y).* У випадку, якщо таких вузлів декілька, то вибрати будь-який один з них. Перевірити чи базовий вузол був доданий до набору MPR(S), якщо ж ні, то додати його. Видалити з набору *N*2 вузли, що покриті базовим вузлом. 6. Якщо ще існують вузли з *N2*, які залишились непокритими хоча б одним вузлом з набору MPR, то:

- для кожного вузла з набору N порахувати досяжність – кількість вузлів з набору N2, які ще залишились непокритими хоча б одним вузлом з набору MPR, і які досяжні через односкачкового сусіда;
- вибрати як MPR вузол з найбільшою готовністю серед вузлів з набору N з ненульовою досяжністю. У випадку, коли існує декілька таких вузлів, то вибрати вузол як MPR, що покриває максимальну кількість вузлів N2. У випадку, якщо існує декілька таких вузлів, то вибрати вузол як MPR, що найбільш віддалений від усіх вузлів з набору N. Для цього порівняти площі трикутників, що формують ці вузли з вузлом S, з них вибрати найбільшу. У цьому трикутнику є два сусідні вузли, вибрати найбільш віддалений з них від вузлів з набору N. Додати його до набору MPR(S). Видалити з набору N2 вже покриті вузли.
- якщо ще існують непокриті вузли в наборі N2, то повторити пункт 6 ще раз.

На рис.1 наведено тестову мережу з 19 вузлів, на рис. 2 наведено результат розрахунку MPR згідно оригінального протоколу OLSR (вузли 2, 3, 4), на рис. 3 наведено результат розрахунку MPR згідно технології локалізації (вузли 2, 3, 6). Видно, що дана технологія дозволяє збільшити площу покриття двоскачкових MPR вузлів, за рахунок вибору в якості MPR вузла 6 замість вузла 4. Важливим критерієм для перерахунку MPR вузла було обрання базового вузла 4 з досяжністю 5 (вузли 14, 15, 16, 17, 18), в той час як вузли 5, 6 мають досяжність 4 (вузли 15, 16, 17, 18). Вибір вузла 6 в якості MPR в свою чергу призводить до зменшення кількості службової інформації при появі нових вузлів в наборі *N*2 (вузол 19).

Але якщо видалити з тестової мережі зв'язок вузла 4 з вузлом 14, тоді досяжність вузла 4 буде така ж сама як у вузлів 5, 6 і вибір базового вузла серед вузлів 4, 5 і 6 теж стане випадковим.

Для вирішення цієї проблеми пропонується розраховувати площу перетину зон покриття найближчих вузлів MPR з зонами покриття проблемних вузлів. Для даного випадку це площі перетину зони покриття MPR вузла 3 з зонами покриття вузлів 4, 5 і 6. З рисунків 2 і 3 видно, що площа перетину зони покриття вузла 3 з зоною покриття вузла 6 є найменшою. Тобто вузол 6 покриває більшу площу, ніж вузли 4, 5 і може бути вибраний в якості MPR.

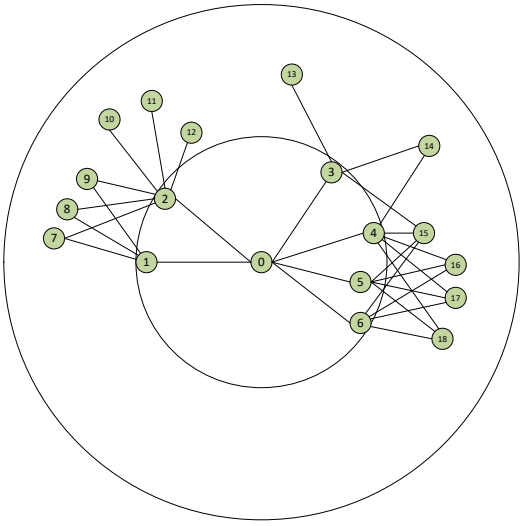


Рис. 1. Тестова мережа

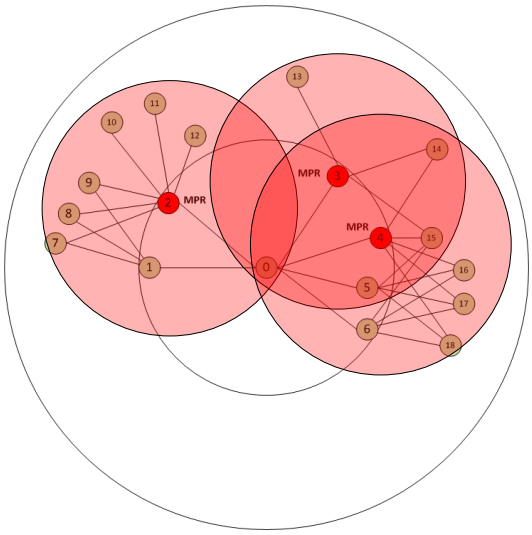


Рис.2. Розраховані MPR згідно оригінального протоколу OLSR

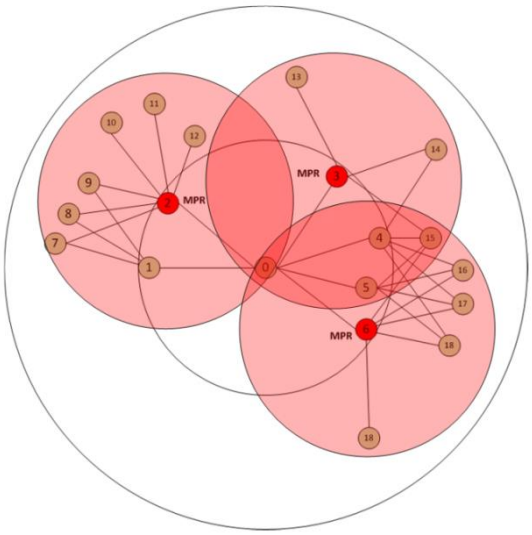


Рис. 3. Розраховані MPR згідно технології локалізації

Враховуючі, що радіус дії вузлів R однаковий, площу перетину i-го вузла знайдемо як:

$$S_i = R^2(F - \sin(F)),$$

де $F = 2\mathrm{acos}(D/2R)$, D – відстань між центрами окружностей.

Висновки. В роботі показано, що алгоритм вибору MPR вузлів, який базується на технології локалізації, іноді може бути випадковим. Для вирішення цієї проблеми запропоновано вимірювати не найбільшу площу трикутників, а найменшу площу перетину зон досяжності вузлів-кандидатів в MPR з зоною найближчого обраного вузла MPR.

Література

1. T. Clausen, and P. Jacquet. Optimized Link State Routing Protocol”, RFC 3626, October 2003. – Електронний ресурс: https://tools.ietf.org/html/rfc3626.
2. Wang Anbao, Zhu Bin. Improving MPR Selection Algorithm in OLSR Protocol Based on Node Localization Technology // Journal of Networks, vol. 9, № 7, July 2014 – Електронний ресурс: https://pdfs.semanticscholar.org/b290/453b8d62e5978a1091933729ca8dd15d4b29.pdf.

УДК 621.391

ПЕРЕВАГИ ВИКОРИСТАННЯ ТА МЕТОДИ ПІДВИЩЕННЯ ЕКОНОМІЧНИХ ПОКАЗНИКІВ СИСТЕМИ МОНІТОРИНГУ NAGIOS ДЛЯ ОПЕРАТОРУ ЗВ'ЯЗКУ

Воронюк М.М., Гаттуров В.К.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: mariyka.voronyuk.18@gmail.com

Advantages of using and methods of increasing the economic indicators of the monitoring system of Nagios for the telecom operator

In this paper, we consider several methods to help revolutionize the work of monitoring systems for data centers. Disclosed brief concept of these methods and the benefits they provide.

Система моніторингу є основним інструментом, що використовується для діагностики, запобігання та вирішення мережевих проблем. Зростання високої пропускної спроможності та надзвичайно важливої міграції за допомогою локальної мережі (LAN) у мережі WAN вимагає більш ефективних інструментів моніторингу. Без належних інструментів, які дозволяють аналізувати та відображати мережевий трафік та будь-яку пов'язану з ними проблему, мережевий адміністратор обмежується методом спроб і помилок, що триває багато часу, щоб спробувати визначити проблему.

Пропонується сучасний і популярний інструмент для моніторингу комп'ютерних систем і мереж Nagios. Це безкоштовний веб-монітор мережі з відкритим кодом, розроблений Ethan Galstad та призначений для роботи як на Linux, так і на інших операційних системах. Nagios відслідковує стан хост-систем та мережевих служб і повідомляє користувача про проблеми. Необхідно зазначити, що Nagios здійснює моніторинг таких сервісів, як SMTP, POP3, HTTP, PING та такі ресурси, як використання диска та пам'яті, файли журналів, завантаження процесорів, що інтегрується з сенсором IT Temperature Monitor, що дозволяє контролювати і прогнозувати температуру серверної кімнати та пристрою за певними параметрами[1].

Nagios дозволяє прогнозувати та контролювати виникнення мережевого збою та недоступність хостів, надавати службові сповіщення. Nagios - це мережевий інструмент реального часу, що використовується для аналізу, інтерпретації та відображення мережевого трафіку. Робоча станція та клієнт можуть відслідковувати певний потік трафіку в мережі, не порушуючи роботу мережі одночасно. Програма також надає інструменти для технічного контролю та ефективності роботи системи. Nagios демонструє використання пропускної здатності мережі, а також повідомляє адміністратора мережі по відповідно налаштованому ресурсу, якщо в мережі виникають певні

проблеми з доступом або пропускна здатність потрапляє на певний поріг. Інтегрований MRTG (Multi Router Traffic Grapher) також дає змогу адміністратору мережі переглядати завантаженість пропускної здатності під час пікових годин. Аналіз мережі в режимі реального часу допомагає швидко виявляти мережеві помилки та швидкодію, запобігаючи падінню мережі.

Переваги використання системи моніторингу Nagios.

Основним завданням Nagios є контроль стану мережевих пристроїв і їх служб, а також повідомлення системних адміністраторів про проблеми в мережі. Ядром Nagios є демон планувальника, який регулярно перевіряє зазначену мережу пристроїв та послуги, що вони надають. Коли виникають проблеми Nagios попереджає мережевих адміністраторів через канали повідомлень, таких як служба електронної пошти і миттєвих повідомлень. В свою чергу, мережевий адміністратор може відкрити веб-інтерфейс для перегляду статусу інформації, журналів подій і звітів з будь-якого місця через доступ до інтернет мережі.

Плагін Nagios - автономний виконуваний файл, певний набір аргументів для виконання деяких дій і моніторингу. Існує два типи модулів, тобто контрольний плагін і плагін повідомлень. Nagios використовує результати перевірки плагінів для визначення поточного стану хостів і їх служб, в той час як модуль повідомлень використовується для відправки попереджень, при зміні статусу хоста. На додаток до регулярних мережевих служби, такі як HTTP, FTP, SMTP, Nagios також можуть контролювати локальні ресурси, такі як завантаження і пам'ять центрального процесору використані через NRPE (Nagios Remote Plug-in Executor) розширення. Однією з найбільш гнучких особливостей Nagios є те, що вона дозволяє користувачам розробляти власні плагіни[2].

Підвищення економічних показників використання системи моніторингу Nagios для оператору зв’язку. Одноплатний комп'ютер (Single-board computer) - самодостатній комп'ютер, зібраний на одній друкованій платі, на якій встановлені мікропроцесор, оперативна пам'ять, системи введення-виведення і інші модулі, необхідні для функціонування комп'ютера. Одноплатні комп'ютери виготовляються в якості демонстраційних систем, систем для розробників або освіти, або для використання в ролі промислових або вбудованих комп'ютерів.

Кількість завдань, з якими впорається такий комп'ютер, досить велике. Список починається домашнім комп'ютером і закінчується роутерами і модемами. Наприклад, на такий пристрій можна без проблем встановити майже повний Linux, перетворивши його в достатню потужну систему для роботи з документами, веб-серфінгу, прослуховування музики та інших нескладних завдань. Деякі моделі здатні перетравити навіть програвання відеороликів аж до HD[3].

В роботі пропонується одноплатний комп'ютер Raspberry Pi, як центральний вузол, на якому встановлюється і розгортається система моніторингу Nagios.

Перевагою використання Raspberry Pi є його не висока вартість на рівні близько 25$ (на відмінну, від серверів, що використовуються зараз, ціна яких складає від 300$). У сукупності з низькими вимогами відкритого програмного забезпечення (OpenSource) до апаратної частини і спеціально зібраним ядром операційної системи, оптимізованим під дане залізо, це дозволяє встановити на нього операційну систему Linux (або RiscOS), а також набір супутнього програмного забезпечення. Наприклад як варант, можна встановити операційну систему Debian Linux, під назвою Raspbian, браузер Midori, офісний пакет Koffice (аналог Word / Excel під Windows) і мову програмування Python. Все це програмне забезпечення безкоштовне, має низькі вимоги до ресурсів.

Також зі звичним графічним інтерфейсом Raspberry Pi заснований на процесорі з архітектурою ARM 11, частотою в 700 МГц (в останніх версіях прошивки офіційно дозволили розганяти процесор до 1000 МГц), це дозволяє досягти прийнятної продуктивності при низькому енергоспоживанні. Однією з важливих переваг цієї платформи, є споживана потужність Paspberry Pi - всього 1 Вт, в той час, як у традиційного системного блоку - мінімум 250 Вт. За допомогою даної платформи можливо зробити ребаланс доступної пам'яті[4].

Висновки. Nagios – дуже важливий інструмент в роботі будь-якого оператору зв'язку, система моніторингу дозволяє вчасно виявити проблеми та аварійні ситуації на мережі, для їх запобігання або починки. Nagios – приваблива для операторів система моніторингу в силу її безкоштовності і відкритих плагінів з можливістю їх редагування і створювання власних. При реалізації системи моніторингу на Raspberry Pi оператор мінімізує свої витрати на реалізацію Nagios в свою мережу, що не погіршує і не обмежує показники та можливості системи.

Література

1. Alpha boards in manufacture Raspberry Pi Foundation [Електронний ресурс] – Режим доступу до ресурсу: https://www.raspberrypi.org/blog/the-alpha-boards-are-here/
2. Nagios. (n.d.). [Електронний ресурс] – Режим доступу до ресурсу: http://nagios.org.
3. Sophon Mongkolluksamee, Panita Pongpaibool, Chavee Issariyapat, “Strengths and Limitations of Nagios as a Network Monitoring Solution” Proceedings of the 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010) Vol. 1, pp. 96-101, Bangkok, Thailand, May 2010
4. D. Doug, B. James R., M. High, “Best of open source networking software,”infoworld.com, Aug 31, 2009.

УДК 621.39

ДОСЛІДЖЕННЯ МЕТОДІВ ОБРОБКИ РИЗИКІВ В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Мокій А.В., Горицький В.М.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: andreymokiy@gmail.com

RESEARCH OF RISK MANAGEMENT METHODS IN THE INFORMATION SECURITY MANAGEMENT SYSTEM

The basic concept for ISMS on the basis of ISO 27001: 2013 is the risk of information security, and the toolkit is the risk management of the IB. The article deals with the methods of risk management IB based on the normative legal acts of the National Bank of Ukraine and international standards of the ISO 27K series.

Однією з важливих складових сучасних систем інформаційної безпеки (ІБ) є системи управління інформаційною безпекою (СУІБ). В концентрованому вигляді основні положення та вимоги щодо побудови СУІБ, які в подальшому можуть бути оцінені акредитованими органами з оцінки відповідності, викладені в серії міжнародних стандартів ISO 27K. Стандарт ISO 27001:2013 безпосередньо встановлює вимоги до СУІБ. Базовим поняттям для СУІБ на основі ISO 27001:2013 є ризик інформаційної безпеки, а інструментарієм – обробка ризиків ІБ. В статті розглядаються методи обробки ризиків ІБ на основі нормативно-правових актів Національного банку України та міжнародних стандартів серії ISO 27K.

Методологія оцінки ризиків може бути кількісною або якісною, або їх комбінацією.

На практиці якісна оцінка часто використовується спочатку для визначення загального рівня ризику і визначення основних ризиків. Далі може виникнути необхідність виконання більш специфічного або кількісного аналізу стосовно основних ризиків.

Кількісна оцінка ризиків є більш складною та потребує більше часу та ресурсів. Однак така оцінка буде дуже корисною у випадках, коли рішення щодо оброблення ризиків буде залежати від вартості заходів безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної

безпеки. Якісна методика оцінки ризиків використовує шкалу атрибутів для опису величини потенціальних наслідків реалізації загроз і вірогідність того, що такі наслідки виникнуть. Перевагою якісної методики є її простота розуміння всім персоналом. Недоліком такої методики є залежність від суб'єктивного вибору шкали атрибутів.

Для отримання якісної оцінки ризиків необхідно розглянути оцінки наслідків реалізації загроз разом із вразливостями, з виникненням яких ці загрози можуть реалізуватися, та оцінки ймовірності їх реалізації для кожного бізнес-процесу/банківського продукту, мережі, обладнання, програмного забезпечення, які забезпечують функціонування цього бізнес-процесу/банківського продукту, мережі банку в цілому,

Можливими варіантами оброблення ризиків можуть бути:

- зниження ризиків шляхом застосування належних заходів безпеки;

- свідоме та об'єктивне прийняття ризиків за умови, що вони чітко задовольняють політику організації та критерії прийняття ризиків;

- уникнення ризиків;

- перенесення відповідних бізнес-ризиків на інші сторони, наприклад, страхувальників, постачальників.

Для прийняття рішення щодо оброблення конкретних ризиків рекомендується визначити критерії стосовно кожного окремого ризику (низький ризик, середній ризик, високий ризик).

Застосування належних заходів безпеки дозволить зменшити ризики. Під час вибору цих додаткових заходів безпеки повинні бути враховані всі вимоги законодавства України, нормативно-правових актів Національного банку України, внутрішніх документів, політики та стратегії банку.

Крім того, цей вибір також повинен враховувати вартість додаткових заходів безпеки, час їх впровадження, вплив на технологію операційної роботи, інтерфейс користувача тощо.

З урахуванням цих факторів складається план оброблення ризиків. У разі необхідності тривалої підготовки до впровадження додаткових заходів безпеки деякі ризики можуть бути тимчасово прийняти як залишкові з включенням до наступного плану оброблення ризиків після перегляду оцінки

ризиків. Прийняття всіх залишкових ризиків повинно бути задокументовано і затверджено керівництвом банку. Це стосується середніх та високих ризиків і повинно бути ретельно розглянуто. У документах стосовно прийняття залишкових ризиків має бути надана причина прийняття ризику та, за необхідністю, строки впровадження додаткових заходів безпеки для зниження ризику. Наприклад, якщо банком використовується програмно-технічний комплекс із застарілими технологіями, який має великий ризик реалізації однієї або декількох загроз і який планується замінити на новий більш сучасний комплекс протягом 2 років, то ці ризики можуть бути прийняти як тимчасове рішення до заміни цього програмно-технічного комплексу з наданням терміну впровадження нового.

Деякі ризики є властивістю існуючого бізнес-процесу/банківського продукту/програмно-технічного комплексу. Особливу увагу слід звернути на вразливості саме програмно-технічних комплексів, які використовують застарілі або новітні незахищені технології. В деяких випадках слід розглянути питання щодо уникнення ризиків за рахунок зміни операційного середовища, баз даних, програмно-технічного комплексу, технології оброблення та зберігання інформації, оскільки це буде вимагати менших витрат, ніж впровадження додаткових заходів безпеки.

Сучасні системи вразливі до ряду мережевих загроз, які можуть бути результатом реалізації несанкціонованого доступу, а також розкриття, викривлення або модифікації інформації. Щоб захистити сучасні інформаційні ресурси та послуги від загроз, необхідно застосовувати відповідні заходи управління безпекою та обробкою ризиків з послідуючою сертифікацією СУІБ в акредитованому органі з оцінки відповідності.

Література

1. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України від 01.03.2011.
2. ГАЛУЗЕВИЙ СТАНДАРТ УКРАЇНИ. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010.

УДК 004.056

ОСНОВИ ПРОВЕДЕННЯ АУДИТУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Павленко В.В., Горицький В.М.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: pavlenkov1996@gmail.com

Basic concepts of conducting audit of information security management system

Considered the main stages of conducting audit of information security management system such as analysis for compliance documentation management system implementation, planning, preparation and improvement.

Проблема створення ефективних систем управління інформаційної безпеки (СУІБ) з метою забезпечення стабільного розвитку сучасної організації та успішної протидії загрозам в умовах жорсткої конкуренції добре відома. Дану систему необхідно піддавати повноцінному аудиту на відповідність вимогам інформаційної безпеки, наприклад стандартам серії ISO 27k [1,2]. Тому важливість проведення якісної перевірки СУІБ важко переоцінити.

Під інформаційною безпекою зазвичай розуміється захищеність інформації та підтримуючої її інформаційної системи від випадкових і навмисних впливів природного або штучного характеру, що завдають шкоди власникам або користувачам цієї інформації і самій підтримуючій її інформаційній системі [1].

Аудит СУІБ дозволяє визначити найбільш вразливі місця в захисті компанії, допомагає оцінити ефективність діючих організаційно-технічних заходів щодо захисту інформаційної системи організації [3]. Рівень забезпечення інформаційної безпеки різниться в залежності від конкретної компанії, але повинен відповідати деякому мінімальному набору вимог безпеки. Сьогодні існує ряд стандартів в області інформаційної безпеки, найбільш відомий - міжнародний стандарт ISO/IEC 27001: 2013, що містить вимоги щодо створення СУІБ компанії [2].

Основним завданням аудиту є підтвердження конфіденційності, цілісності і доступності інформації, що обробляється в корпоративній системі підприємства.

Аудит на відповідність вимогам інформаційної безпеки - це комплексний, циклічний процес, який складається з наступних етапів:

- планування аудиту;
- планування заходів по аудиту (розробка, узгодження і затвердження планів заходів);
- перевірка на відповідність групі вимог (наприклад, на відповідність стандарту ISO/IEC 27001: 2013);
- систематизація результатів обстеження і формування звітності.

Ці чотири етапи складають життєвий цикл аудиту [4].

Найбільш складним етапом, звичайно, є практичне проведення аудиту. Безпосередньо перед проведенням аудиту аудиторська група повинна мати чітко сформульовані завдання аудиту і його область, критерії аудиту, документи різних рівнів (політики, процедури, інструкції, стандарти організації та ін.), перелік процесів і активів компанії, що підлягають перевірці, узгоджену
програму аудиту від об'єктів аудиту, підтвердження проведення аудиту.

Аудит починається зі вступної наради з представниками організації, на якому обговорюється порядок денний, програма аудиту. Після цього аудитори починають перевіряти організацію. Спочатку перевіряються документи верхнього рівня: політика інформаційної безпеки або концепція інформаційної безпеки, приватні політики, стандарти організації. Перераховані документи повинні відображати не тільки ідеологію організації в цілому в області інформаційної безпеки, але і відображати розподіл відповідальності між співробітниками і керівництвом організації. Обов'язково необхідно перевіряти обізнаність про зміст цих документів у співробітників організації і розуміння цілей, принципів і зобов'язання щодо захисту активів компанії.

Аудитор повинен по черзі пройти кожний заявлений в програмі підрозділ і перевірити виконання необхідних вимог. В ході перевірки може бути використано інтерв'ювання, часткова перевірка процесу, перевірка з допомогою вибірки (перевірка виконання в певні проміжки часу), або повна перевірка всіх складових процесу. При цьому логічним буде виглядати аналіз та перевірка:

- вразливості політики безпеки;
- вразливості організаційних заходів;
- вразливості класифікації і контролю ресурсів;
- вразливості процедур, пов'язаних з персоналом;
- вразливості фізичної безпеки;
- вразливості експлуатації систем;
- вразливості контролю доступу;
- вразливості обслуговування і розробки систем;
- уразливості інцидентів інформаційної безпеки [4].

В процесі аудиту важливим фактором є збір фактів і свідчень для подальшого аналізу і звіту. Дані завжди повинні бути об'єктивними, аудитор не повинен використовувати власну фантазію для отримання картини, що відбувається. Відомості можуть бути отримані за допомогою спостереження, вимірювання, випробування або будь-яким іншим розумним способом. Хорошою практикою вважається відкритість аудитора і вміння ставити правильні питання, які мотивують розповісти про процес або пояснити необхідні деталі.

Відомості аудиту використовуються для опису невідповідностей, формування висновків і рекомендацій. Так як при перевірці часто аналізуються результати попередніх аудитів, то зібрані свідчення про невідповідності повинні бути простежені і легко відновлюваними для

аудиторів в одній області.

Після перевірки всіх необхідних процесів, заявлених у програмі аудиту, представляється звіт за виявленими невідповідностями. У ньому відбиваються всі відмінності, будь-яка двозначність неприпустима. Він деталізований: всі зібрані факти по кожному процесу або пункту стандарту повністю відображені.

Звіт про невідповідності повинен бути ретельно перевірений на наявність помилок і неточностей, і, по можливості, не мати великих обсягів.

Далі складається комплексний звіт по проведеному аудиту. Він може вміщувати рекомендації щодо усунення невідповідностей і календарний план робіт щодо поліпшення СУІБ.

Завершити аудит рекомендується заключною нарадою, на якій підводяться підсумки аудиту, обговорюються спірні питання, що виникли в ході проведення перевірки, узгоджуються терміни усунення зауважень. Важливо отримати підтвердження розуміння необхідності поліпшення СУІБ і узгодити терміни початку і завершення робіт щодо усунення недоліків [5].

Аудит інформаційної безпеки в сучасних умовах є одним з найбільш ефективних інструментів отримання незалежної і об'єктивної оцінки поточного рівня захищеності будь-якого економічного суб'єкта як від існуючих, так і потенціальних загроз. Результати аудиту інформаційної безпеки дозволяють сформувати стратегічні установки розвитку, що відповідають сучасним викликам системи забезпечення інформаційної безпеки для вказаного суб'єкта. Однак слід розуміти, що застосування на практиці аудиту інформаційної безпеки має бути не епізодичним, а регулярним, що дозволяє не тільки виявити вже доконаний факт, а й передбачити потенційні загрози [6].

Література

1. ISO/IEC 27007:2011 «Information technology-Security techniques-Guidelines for information security management systems auditing».
2. Цвілій О.О. «Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою» - Науковий журнал «Телекомунікаційні та інформаційні технології», - 2014. – № 2. – с. 73-79.
3. Цвілій О.О. Системи управління інформаційною безпекою: гармонізація з міжнародними стандартами, правилами та процедурами. - Перша всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації». 2015. Збірник тез, с. 107-11.
4. Агафонова М.Е., Шахалов И.Ю. К вопросу о проведении внутреннего аудита системы менеджмента информационной безопасности //Вопросы кибербезопасности №3 – 2013. – 6 с.
5. Ситнов А. А., Уринцов А. И. Аудит информационных систем: монография для магистров. М.:Юнити-Дана – 2014. 239 с.
6. Ситнов А. А. Организация аудита информационной безопасности. – 2016. – 9 с.

УДК 004.056

ОЦІНОЧНІ СТАНДАРТИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Цвілій О.О., Некраш І.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: o.tsviliy@ukr.net

APPRECIATE STANDARDS IN SCOPE OF INFORMATION SECURITY

The comparison of the results of independent security assessments in accordance with the appreciate standards in the scope of information security is considered. The application of criteria for assessing the safety of IT products in Ukraine is explored.

Розглядається забезпечення зіставлення результатів незалежних оцінок безпеки у відповідності до оціночних стандартів у сфері інформаційної безпеки. Досліджується застосування критеріїв оцінки безпеки продуктів ІТ в Україні.

Зіставлення результатів незалежних оцінок безпеки досягається наданням єдиного набору вимог до функціональних можливостей безпеки продуктів ІТ і до заходів довіри, що застосовуються до цих продуктів ІТ при оцінці безпеки. Дані продукти ІТ можуть бути реалізовані у вигляді апаратного, програмно-апаратного або програмного забезпечення.

В процесі оцінки досягається певний рівень впевненості у тому, що функціональні можливості безпеки таких продуктів ІТ, а також заходи довіри, вжиті по відношенню до таких продуктів ІТ, відповідають вимогам, що пред'являються. Результати оцінки можуть допомогти споживачам вирішити, чи відповідають продукти ІТ їхнім потребам в безпеці.

На сьогоднішні день у приватному та банківському секторах використовується міжнародний стандарт ISO/IEC 15408 в трьох його частинах, нова редакція яких знаходиться в стадії розробки [1].

Цей міжнародний стандарт розробляє Об'єднаний технічний комітет ISO/IEC JTC 1, підкомітет SC 27 «IT Security techniques».

Стандарт ISO/IEC 15408-1:2009 «Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model» встановлює загальні концепції та принципи оцінки безпеки інформаційних технологій та визначає загальну модель їх оцінки безпеки, надану різними частинами стандарту ISO/IEC 15408 [2].

Він надає огляд усіх частин стандарту ISO/IEC 15408, визначає терміни й скорочення, встановлює основну концепцію цільової оцінки та контекст оцінки, а також і описує аудиторію, до якої відносяться ці критерії оцінки. Дається вступ до основних концепцій безпеки, необхідних для оцінки ІТ-продуктів.

Інформація, що міститься в системах або продуктах ІТ, є критичним ресурсом, що дозволяє організаціям успішно вирішувати свої завдання. Крім того, приватні особи вправі очікувати, що їх персональна інформація, розташована в продуктах або системах ІТ, залишається приватною, доступною їм за мірою необхідності і не буде піддаватися несанкціонованій модифікації.

При виконанні продуктами або системами ІТ своїх функцій слід здійснювати належне управління інформацією для забезпечення її захисту від небезпек небажаного або необґрунтованого розповсюдження, зміни або втрати. Термін «безпека ІТ» використовується для того, щоб розглянути запобігання та зменшення цих та подібних небезпек.

Багато споживачів ІТ з-за недоліку знань, компетентності чи ресурсів, не впевнені в безпеці застосовуваних продуктів та систем ІТ, можливо, не захочуть покладатися виключно на запевнення розробників. Щоб підвищити свою впевненість у заходах безпеки продуктів або систем ІТ, користувачі можуть замовити аналіз безпеки цього продукту або системи (тобто оцінку безпеки).

У стандарті ISO/IEC 15408-1 представлені очікувані результати оцінки профілів захисту (ПЗ) та оцінки об'єктів (ОО). Оцінки ПЗ або ОО дозволяють створювати каталоги ПЗ або ОО, що пройшли оцінку. Оцінка завдань по безпеці (ЗБ) дає проміжні результати, які потім використовуються при оцінці ОО.

Необхідно, щоб оцінка ПЗ та ОО приводила до об'єктивних і повторюваних результатів, на які можна потім посилатися як на свідчення навіть при відсутності об'єктивної шкали для представлення результатів оцінки безпеки ІТ. Наявність сукупності критеріїв оцінки є необхідною попередньою умовою для того, щоб оцінка призводила до значного результату, надаючи технічну базу для взаємного визнання результатів оцінки різними органами з оцінки відповідності.

Наразі, може стати питання щодо створення таких органів з оцінки відповідності, акредитованих у Національному агентстві з акредитації України.

Практичне застосування критеріїв включає в себе як об'єктивні, так і суб'єктивні елементи оцінки, тому отримання абсолютно точних та універсальних рейтингів безпеки ІТ не представляється можливим.

Рейтинг, отриманий згідно ISO/IEC 15408, представляє підсумкові дані специфічного типу дослідження характеристик безпеки ОО. Такий рейтинг не гарантує придатності до використання у будь-якому конкретному середовищі застосування. Рішення про прийом ОО до використання у конкретному середовищі застосування базується на обліку багатьох аспектів безпеки, включаючи також висновки оцінки.

Зміст та подання функціональних компонентів безпеки в комп'ютерній системі, які повинні бути оцінені визначає стандарт ISO/IEC 15408-2:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components» [2]. Він містить повний каталог заздалегідь визначених функціональних компонентів безпеки, які організовані за допомогою ієрархічної структури класів, сімей та компонентів.

Стандарт ISO/IEC 15408-2 також дає вказівки щодо специфікації індивідуальних вимог безпеки, якщо немає відповідних заздалегідь визначених функціональних компонентів безпеки.

Вимоги до забезпечення критеріїв довіри до безпеки в комп'ютерній системі визначає ISO/IEC 15408-3:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components» [2], який визначає зміст та подання вимог довіри до безпеки у формі класів, сімей та компонентів, які представлені в ієрархічному порядку в

сімействах, а також містить рекомендації щодо організації нових вимог щодо довіри.

Загальна інформація про методологію оцінки та схема оцінки представлена в стандарті ISO/IEC 18045:2008 «Information technology - Security techniques - Methodology for IT security evaluation», нова редакція якого також знаходиться в стадії розробки [2].

На відміну від ISO/IEC 15408, де кожен елемент у всіх компонентах одного сімейства довіри має один і той же номер, вказаний останньою цифрою його умовного позначення, стандарт ISO/IEC 18045 може вводити нові кроки оцінювання при зміні елемента дій оцінювача з ISO/IEC 15408 в залежності від підвиду діяльності; в результаті остання цифра умовного позначення наступних кроків оцінювання зміниться, хоча крок оцінювання залишиться тим же самим.

Крім того, стандарт ISO/IEC 18045:

а) описує загальні завдання оцінки без визначення вердиктів, пов'язаних з ними, оскільки ці завдання не відображаються на елементи дій оцінювача з ISO/IEC 15408;

б) описує роботи, необхідні для отримання результату оцінки профілю захисту;

в) визначає дії по оцінці, згруповані за класами довіри, та охоплює базові методи оцінки, які використовуються для надання технічних свідоцтв результатів оцінки;

г) наводить пояснення критеріїв оцінки вразливостей і приклади їх застосування.

Варто зазначити, що розширення сфери застосування ISO/IEC 15408 з урахуванням ряду критичних аспектів операційних систем, які не розглядаються в оцінці ISO/IEC 15408, передбачено в стандарті ISO/IEC TR 19791:2010 «Information technology - Security techniques - Security assessment of operational systems», який містить керівництво та критерії оцінки безпеки операційних систем [2]. Основні розширення, що вимагають адресної оцінки операційного середовища, пов’язані з цілями оцінки та декомпозиції складних операційних систем у сфері безпеки, які можуть бути окремо оцінені.

Стандарт ISO/IEC TR 19791 передбачає:

а) визначення та модель для операційних систем;

б) опис розширень до концепцій оцінки ISO/IEC 15408, необхідних для оцінки таких операційних систем;

в) методологію та процес здійснення оцінки безпеки операційних систем;

г) додаткові критерії оцінки безпеки для вирішення тих аспектів операційних систем, які не охоплені критеріями оцінки ISO/IEC 15408.

Цей стандарт дозволяє включити продукти безпеки, що оцінюються відповідно до ISO/IEC 15408, до операційних систем, які оцінюються в цілому за допомогою ISO/IEC TR 19791.

ISO/IEC TR 19791 обмежується оцінкою безпеки операційних систем та не враховує інші форми оцінки системи, а також не визначає методи ідентифікації, оцінки та прийняття операційного ризику.

Методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів

в Україні визначає НД ТЗІ 1.1-002-99.

Спільним наказом Мінюсту та Адміністрації Держспецзв'язку було затверджено Перелік стандартів у сфері електронного цифрового підпису, перспективних для перегляду та гармонізації з європейськими та міжнародними стандартами відповідно до встановлених законодавством процедур, а також, затверджено Перелік національних стандартів у сфері електронного цифрового підпису, що підлягають перегляду. А 25.12.2014 до цього наказу були внесені зміни (№ 2170/5/703) та актуалізовано як Перелік міжнародних та європейських стандартів, інших актів технічного регулювання для гармонізації з метою реформування, розвитку та забезпечення інтероперабельності системи електронного цифрового підпису, де розділ XI «Методи та механізми захисту від несанкціонованого доступу» передбачає в т.ч. стандарти ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 [1].

У 2015 році наказом від 18.12.2015 № 193 було затверджено та прийнято ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (ISO/IEC 18045:2008, IDT).

Вперше в Україні наказом від 04.08.2017 № 207 [3] було затверджено та прийнято ДСТУ ISO/IEC 15408-1:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT)», ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT), ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT), що є дуже важливим кроком для фахівців в області інформаційної безпеки, які сьогодні не можуть обійтися без знань відповідних стандартів.

Література

1. Цвілій О.О., Майстренко А.В. Застосування в Україні критеріїв оцінки безпеки в комп'ютерній системі. - Матеріали 7-ї Міжнародної науково-практичної конференції "ІНФОКОМУНІКАЦІЇ - СУЧАСНІСТЬ ТА МАЙБУТНЄ". 2017. Збірник тез. ст. 131-133.
2. International Organization for Standardization [Електронний ресурс]// – Режим доступу: http://www.iso.org/iso/home.html.
3. Наказ ДП "УкрНДНЦ" від 04 серпня 2017 № 207 «Про прийняття національних нормативних документів, гармонізованих з європейськими нормативними документами, поправки до національного нормативного документа, скасування національних нормативних документів»

УДК 621.391.63/621.316.5

НАРОЩУВАННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ ТРАНСПОРТНИХ СИСТЕМ

Романишин В.С., Бердников О.М.
Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського, Україна
E-mail: romanyshynvasyl@ukr.net

Requirements to increase the capacity of information transmission systems

One of the most effective methods for solving this problem is the WDM (Wavelength Division Multiplexing) optical waveguide compaction method. The use of this method has allowed to increase the throughput of fiber-optic systems to a value greater than 10 Tbit / s, which will ensure that the needs of today and the next 3-5 years will be exceeded.

Для реалізації методу мультиплексування оптичних трактів (ОТр) по довжинах хвиль оптичного випромінювання (або хвильове мультиплексування – ХМ) були розроблені такі оптичні елементи: оптичні мультиплексори (ОМХ) і демультиплексори (ODMX), оптичні фільтри, напівпровідникові лазери з малою напівшириною лінії на фіксованій (заданій) довжині хвилі випромінювання, методи і засоби, які забезпечують необхідну стабільність оптичної частоти, оптичні підсилювачі з широкою полосою пропускання і інші активні та пасивні елементи. Для підвищення економічної ефективності регіональних і міських оптичних мереж доступу, в тому числі абонентських ліній в мережах загального користування, активно запроваджується технологія пасивної оптичної мережі ПОС (PON). Такі мережі включають тільки пасивні елементи, такі як оптичний кабель разом із з’єднувальними муфтами відгалужувачів, розгалужувачі, ОМХ і ODMX, оптичні фільтри, оптичні ізолятори і інші елементи [1, 2, 3].

Враховуючи еволюцію традиційних мереж у напрямку повністю оптичних мереж (AON – All Optical Network), вже зараз, особливо на етапі проектування телекомунікаційних транспортних систем ХМ (ТТС ХМ), необхідний підхід до вибору оптичних волокон. Відповідно до міжнародної системи класифікації, оптичні волокна (ОВ) розподіляються на два основних класи: А-багатомодові (MMF – Multi-ModeFiber) та В – одномодові (SMF – Single-ModeFiber). При цьому, як пояснює таблиця 1, категорія MMF волокна визначається матеріалом осердя і оболонки та профілем показника заломлення (ППЗ), а категорія SMF волокна– центральною довжиною хвилі та довжиною хвилі нульової дисперсії [3, 4].

На транспортній телекомунікаційній мережі (ТТМ) зв’язку України при побудові високошвидкісних ТТС ХМ переважно використовуються одномодові волокна, які в свою чергу поділяються на:

– стандартні волокна з незміщеною нульовою дисперсією (SF – Standard

Fiber);

– волокна зі зміщеною нульовою дисперсією (DSF – Dispersion Shifted Single-Modefiber);

– волокна з ненульовою зміщеною дисперсією (NZDSF – Non ZeroDispersion Shifted Single Modefiber).

Таблиця 1. Категорії оптичних волокон згідно Рекомендації ITU-T

Клас ОВ	Категорія ОВ	Матеріал	Тип волокна	Номінальна довжина хвилі нульової дисперсії, нм	Номінальна довжина хвилі, нм
Багатомодові	A1	Скляна серцевина, скляна оболонка	З градієнтним ППЗ	-	-
	A2.1		З квазісхідчастим ППЗ	-	-
	A2.2		З східчастим ППЗ	-	-
	A3		З східчастим ППЗ	-	-
	A4	Полімерне волокно	С	-	-
Одномодові	B1.1	Скляна серцевина, скляна оболонка	-	1300	1310
	B1.2		-	1300	1550
	B2		-	1550	1550
	B3		-	1300 та 1550	1310 та 1550

Для використання у ТТС ХМ оптичне волокно повинне задовольняти такі вимоги [5, 6]:

– низька дисперсія сигналу (для отримання високої швидкості передавання сигналів у ОТр), яка забезпечується компенсацією нахилу хроматичної дисперсії та зниженням поляризаційної модової дисперсії;

– низька нелінійність осередку волокна, що забезпечує передачу оптичних сигналів на великі відстані;

– однорідність оптичних характеристик, ТТС щільного ХМ;

– низька вартість та велика пропускна здатність.

Всі три типи ООВ близькі по значенню коефіцієнту затухання у вікнах прозорості одномодової передачі 1310 нм (1270…1350 нм) та 1550 нм (1470…1580 нм), але відрізняються своїми дисперсійними характеристиками. Хроматична дисперсія є досить важливим фактором, вплив якого посилюється зі збільшенням відстані та швидкості передавання оптичних сигналів, а також зростанням щільності розносу між центральними довжинами хвиль оптичних трактів.

Зважаючи на поширеність ТТС ХМ , найбільший інтерес викликають дисперсійні характеристики ООВ у вікні прозорості 1550 нм (1470…1580 нм), яке використовується оптичними мультиплексорами. Стандартні ООВ мають в робочому діапазоні довжин хвиль ТТС ХМ занадто велике значення хроматичної дисперсії, що обмежує швидкість передавання сигналів по оптичним трактам. За умови забезпечення ненульового (але близького до нуля та такого, що не перевищує визначену, достатньо малу

величину) значення хроматичної дисперсії та низької крутизни (нахилу) дисперсійної характеристики, найбільш придатними до використання у ТТС ХМ є волокна DSF та NZDSF, що пояснює рисунок 1.

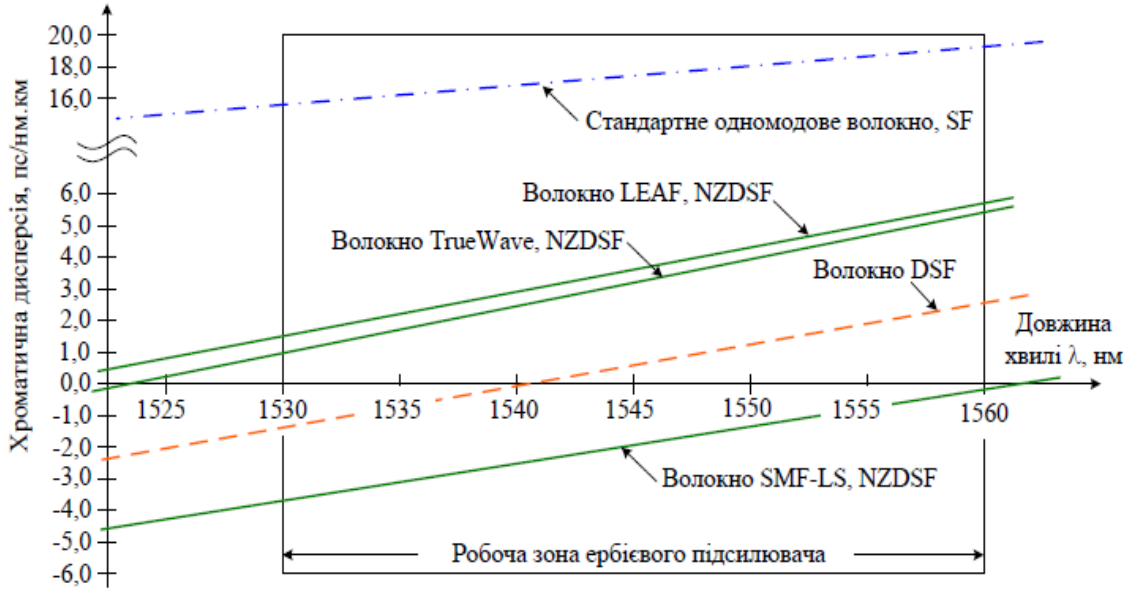


Рис. 1. Хроматична дисперсія ООВ у вікні прозорості 1550 нм, в межах області ербієвого волоконно-оптичного підсилювача підсилення (EDFA) 1530…1560 нм

Іншим важливим фактором, який обумовлює придатність оптичного волокна до використання у ТТС ХМ, є нелінійні властивості його осередку. Так, при розміщенні довжини хвилі нульової дисперсії в діапазоні довжин хвиль групового мультиплексного сигналу починають проявлятись небажані нелінійні ефекти (зокрема, чотирьох хвильове змішування), що призводять до викривлення оптичного сигналу. Тому, з точки зору мінімізації нелінійних ефектів, використовувати волокно DSF у ТТС ХМ не бажано.

Отже, найбільш прийнятним до використання є ООВ типу NZDSF (Non Zerodispersion Shifted Single Modefiber), відоме також як волокно з ненульовою зміщеною позитивною або негативною дисперсією, в якому вплив нелінійних ефектів зменшений, завдяки винесенню довжини хвилі нульової дисперсії за межі смуги пропускання EDFA.

На сьогодні виробництво таких волокон, наприклад, типу AllWave, LEAF, TrueWave, MetroCor, SMF-LS тощо здійснюється фірмами Lucent Technologies, Corning та Fujikura.

Література

1. Фриман Р. Волоконно-оптические системы связи. – М.: Техносфера, 2003. – 440 с.
2. Бейли Д. Волоконная оптика, теория и практика. – М.: Кудиц-обрез, 2006. – 326 с.
3. Слепов Н.Н. Современные технологии цифрових оптоволоконних сетей связи. – М.: Радио и связь, 2003. – 468 с.
4. Каток В.Б., Руденко І.Е., Ранський Є.Г., Однорог П.М. Волоконно – оптичний зв'язок. – К., Логос, 2015. – 380 с.
5. Хмелев К.Ф. Основы фотонного транспорта. – Киев: Техніка. 2008. – 680 с.
6. Бердников О.М., Хмельов К.П. Застосування технології *WDM* на телекомунікаційних мережах / Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2003. – № 3. – с. 5…11.

УДК 621.391.63/621.316.5

ПОРІВНЯННЯ ШЛЯХІВ ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ ЛІНІЙНИХ ТРАКТІВ ТЕЛЕКОМУНІКАЦІЙНИХ ТРАНСПОРТНИХ СИСТЕМ

Щирий А.В., Бердников О.М.
Інститут спеціального зв'язку та захисту інформації
КПІ ім. Ігоря Сікорського, Україна
E-mail: shchiriy21@gmail.com

Comparison of ways to increase the throughput of optical linear paths

With the development of information technology, there is a need to increase the bandwidth of optical linear pathways. There are several ways to solve this problem. The paper considers the comparison of technologies that can be applied to existing fiber-optic transmission systems.

Метою порівняння є дослідження доцільності застосування методів хвильового (ХМ) Wavelength Division Multiplexing (WDM) і часового мультиплексування Time Division Multiplexing (TDM) для збільшення пропускної здатності волоконно-оптичних систем передачі (ВОСП), що застосовують для формування лінійних трактів одномодові оптичні волокна (ООВ).

Порівнювати такі методи, як метод частотного мультиплексування Frequency-Division Multiplexing (FDM) і мультиплексування по поляризації Polarization-Division Multiplexing (PDM), немає необхідності в зв'язку з тим що вони не знайшли застосування для телекомунікаційних транспортних систем (ТТС) [2].

Технології ХМ і TDM передбачають об'єднання декількох вхідних “низькошвидкісних” трактів в один високошвидкісний тракт, але в ВОСП TDM – технології застосовується одна довжина хвилі (λ), а в ВОСП технології ХМ – декілька центральних довжин хвиль ($\lambda_1, \lambda_2, \ldots, \lambda_N$) [1, 2].

У зв'язку з цією обставиною, для нарощування кількості трактів в 4 рази за технологією TDM ієрархії PDH перехід на наступний щабель ієрархії ВОСП здійснюється за принципом 30 × 4 × 4 × 4 × 4, що дозволяє збільшити пропускну здатність ТТС з кожною сходинкою в 4 рази, а за технологією ХМ – шляхом додавання нових оптичних несучих $\lambda_{N+1}, \lambda_{N+2}, \ldots, \lambda_{N+i}$ або шляхом зменшення розносу між центральними довжинами хвиль.

Для нарощування кількості трактів за технологією TDM ієрархії SDH необхідно збільшувати швидкість передачі STM-1 за принципом 4 × 4 × 4 × 4 тобто в STM-256, що дозволяє отримати тракт зі швидкістю передачі 40 Гбіт/с, або STM-N в STM-1 × N, а за технологією ХМ – шляхом додавання нових оптичних несучих $\lambda_{N+1}, \lambda_{N+2}, \ldots, \lambda_{N+i}$ або шляхом зменшення розносу між центральними довжинами хвиль.

При високій швидкості передачі ТТС значний вплив на якість передачі мають такі характеристики ООВ, як поляризаційна модова дисперсія і хроматична дисперсія. При цьому в більшої мірі зростає складність кінцевого та проміжного обладнання ТТС та в цілому значно підвищується загальна вартість проекту.

Для нарощування кількості трактів за технологією ХМ можливо

використання k потоків технології TDM, що модулюються окремо в оптичні сигнали на різних довжинах хвиль оптичних трактів (ОТр). Потім ОТр об'єднаються в оптичному мультиплексорі в єдиний груповий мультиплексний сигнал виду $\lambda_{1+2+3\ldots N}$, який передається по лінійному тракту ТТС. В результаті пропускна здатність ВОСП збільшується в k раз [3].

Варто відзначити суттєвий позитивний момент – зменшення тих обмежень по дисперсії і іншими показниками, які були притаманні при використанні технології TDM. При цьому відзначається, що технологія ХМ може використовуватися паралельно з технологією TDM для підвищення її ефективності, залишаючи практично без змін більшу частину наявного обладнання.

Порівняльні характеристики двох методів мультиплексування наведені в таблицях 1 і 2, які пояснюють, що технологія ХМ є найбільш економічно вигідна в порівнянні з часовим методом мультиплексування.

Таблиця 1. Технічні характеристики

Параметри	TDM – часове мультиплексування	Хвильове мультиплексування
Надійність	Висока	Висока
Пропускна спроможність	Висока	Дуже висока
Комутаційні пристрої	Складна	Складна
Завантаженість ОВ	Середня	Висока
Об'єм апаратури	Великий	Середня

Таблиця 2 – Економічні характеристики

Параметри	TDM – часове мультиплексування	Хвильове мультиплексування
Вартість кінцевих пунктів	Практично однакові	
Вартість лінійного тракту	Середня	Середня
Вартість тракту	Низька	Низька
Вартість передачі інформації	Низька	Низька

З точки зору вартості обладнання системи ТТС порівняно з вартістю апаратурної частини за технологією TDM в побудові розгалуженої мережі, більш ефективно використовувати побудову обладнання ТТС за технологію ХМ (ТТС ХМ). Наприклад, виділення та ввід складних цифрових потоків в проміжних пунктах при часовому мультиплексуванні ієрархії PDH вимагає наявності великого обсягу обладнання, тоді як при технології ХМ для виділенні трактів для простої мережі досить декількох пасивних елементів (мультиплексорів і демультіплексорів).

Обидві технології ХМ та TDM застосовуються для збільшення інформаційної пропускної здатності ВОСП. Хоча вони не виключають, а скоріше доповнюють одна одну, тому можна порівняти такі їх характеристики, як гнучкість структури ліній зв'язку та швидкість передачі на телекомунікаційних транспортних мережах (ТТМ).

З точки зору гнучкості структури ліній передачі, що створюють мережу зв'язку, технологія TDM дає можливість передачі по лінії зв'язку трактів

різнорідних за типом та швидкістю передачі. Системи ТТС за технологією TDM також дозволяють створювати по оптичному кабелю (ОК) тракти і канали, по яких з різними швидкостями передаються різні типи трафику, шляхом застосування різних способів розподілу тайм-слотів, наприклад, IP-технології, Gigabit Ethernet, Fiber Channe, Coupling Links тощо. Вони можуть бути постійно закріплені за певними програмами або виділятися на вимогу за правилами DAMA (Demand Assignment Multiple Access). Можна змінювати тривалість тайм-слотів або повністю їх виключити. В останньому випадку трафик передається у вигляді окремих пакетів, кожен з яких включає адресу джерела і відправника (статистичне мультиплексування). Незважаючи на всі ці можливості, технологія TDM працює найкраще, коли за всіма логічних трактах передається один тип трафику, а всі тайм-слоти мають однакову тривалість і постійно закріплені за окремими трактами. Цей варіант технології TDM досить простий в реалізації і управлінні, і його експлуатаційні витрати також менше.

В технології ХМ тракти повністю незалежні, трафик передається по ОТр, що створюються за принципом з кінця в кінець, тобто формується комбінована технологія, наприклад, IP over ХМ. На практиці на ТТМ України застосовуються відомі типи IP over ХМ – IP over DWDM та IP over HDWDM (щільне та високо щільне ХМ відповідно). Отже технології ХМ дає більшу гнучкість для структур ліній і мереж зв’язку, ніж технологія TDM [1, 3].

З точки зору швидкості передачі, в технології TDM пропускна здатність збільшується за рахунок збільшення швидкості передачі в лінійному тракті системи передачі. Тому швидкість передачі сигналів обмежується можливостями перетворення в використовуваних електронних компонентах. Отримання цифрових потоків, зберігання, передача тощо – все це вимагає застосування цифрових інтегральних схем. Вони повинні працювати зі швидкістю майже на сумарній швидкості передачі лінії зв'язку. Для кожної лінії передачі має бути встановлено обладнання, що підтримує повну пропускну здатність лінії зв'язку.

Обладнання за технологією ХМ може підтримувати тільки швидкість передачі по окремому ОТр, а не повну швидкість складеного сигналу. Таким чином, повна пропускна здатність лінії зв'язку на ОК не обмежена швидкістю роботи використовуваних електронних пристроїв. Найшвидшу лінію зв'язку TDM, яку тільки можна створити з використанням найсучаснішої техніки, в ТТС ХМ на ОК можна передавати як один з багатьох трактів. Наведене порівняння надає, що технологія ХМ має незаперечну перевагу перед іншими технологіями за якими будуються телекомунікаційні транспортні системи.

Література

1. Хмелев К.Ф. Основы фотонного транспорта. – Киев: Техніка. 2008. – 680 с.
2. Каток В.Б., Руденко І.Е., Ранський Є.Г., Однорог П.М. Волоконно-оптичний зв'язок / Під ред. Катка В.Б. – К.: Логос, 2015 – 383 с.
3. Бердников О.М., Хмельов К.П. Застосування технології WDM на телекомунікаційних мережах. / Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2003. – № 3. – с. 5…11.

УДК 621.36

ДОСЛІДЖЕННЯ ВПЛИВУ ПАРАМЕТРІВ КАБЕЛЬНОГО СЕРЕДОВИЩА НА РОБОТУ ЦИФРОВИХ СИСТЕМ ПЕРЕДАЧІ ЗА XDSL ТЕХНОЛОГІЄЮ

Носков В.І., Большаков Ю.Є.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nvi2010@ukr.net, ybolshakov96@gmail.com

Investigation of the influence of cable environment parameters on the operation of digital transmission systems using xDSL technology

The main factors which essentially impact on digital transmission systems are investigated for M-pairs cable. The main factors are: losses of signal and cross-talking interference. Bandwidth calculation is done for prevalent xDSL technologies such as 16TC-PAM SHDSL, 32TC-PAM SHDSL, 128TC-PAM SHDSL, ADSL2+. Calculations are done with and without transitional obstacles.

Актуальність теми пов’язана з поширеністю технології xDSL у мережах доступу. Системи xDSL працюють переважно по існуючій кабельній мережі на основі кабелю типу ТПП, яка знаходиться під впливом різних завад, насамперед це перехідні завади між декількома системами передачі, що працюють в одному кабелі. Тому актуальним є дослідження перепускної спроможності систем xDSL в таких умовах.

Найбільш поширеними на теперішній час є наступні різновиди xDSL:

- 16TC-PAM SHDSL;
- 32TC-PAM SHDSL;
- 128TC-PAM SHDSL;
- ADSL2+.

Основні фактори, що впливають на передачу цифрових сигналів по мідним кабелям:

- Згасання рівня сигналу в наслідок впливу активних та реактивних складових опору сигналу;
- Перехідні завади між парами кабелю;

- Відлуння сигналів на неоднорідностях;
- Міжсимвольна інтерференція;
- Зовнішні завади.

Найбільший вплив здійснюють перші два фактори. Тому дослідження проводилось беручи до уваги саме ці фактори.

Розрахунки виконувались для міського кабелю ТПП 50 х 2 х 0,5 на основі рекомендацій по нормуванню параметрів впливу за допомогою програми xDSLcalc.

Результати представлені у вигляді графіків:

1) Без перехідних завад для 16TC-PAM SHDSL, 32TC-PAM SHDSL, 128TC-PAM SHDSL, ADSL2+;

2) З перехідними завадами для кількості одночасно працюючих ліній в кабелі: 10.

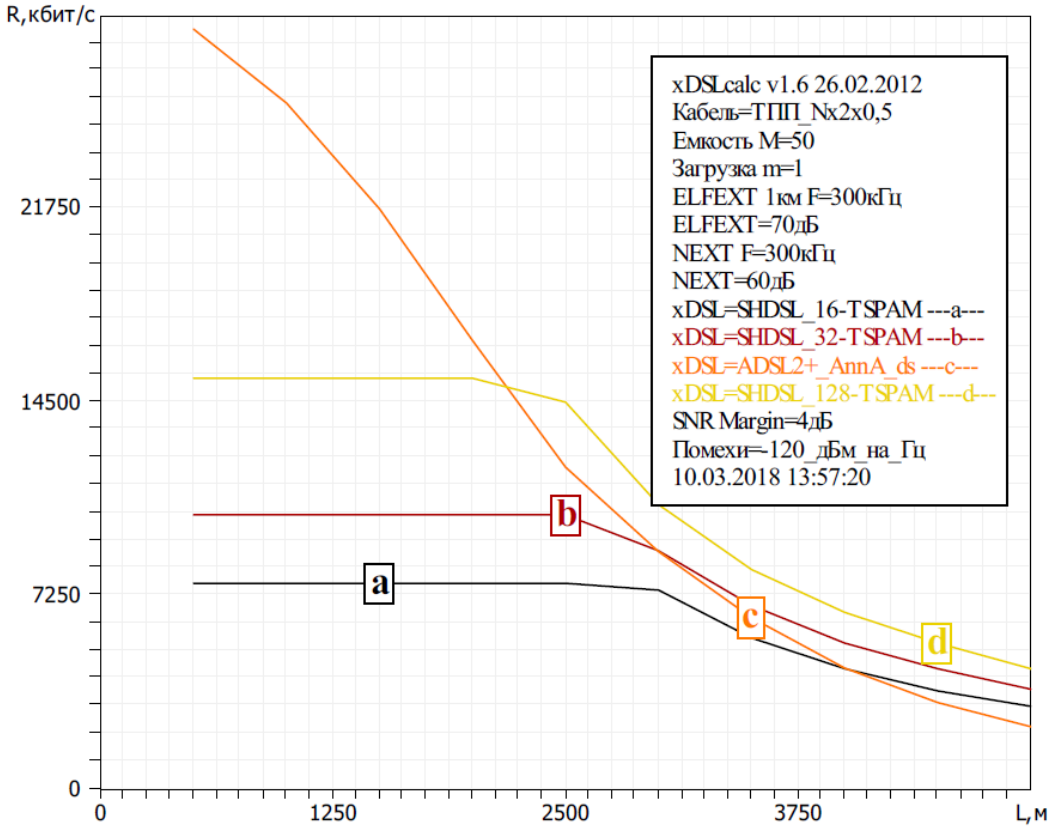


Рис. 1. Перепускна спроможність xDSL ліній під впливом тільки теплових шумів

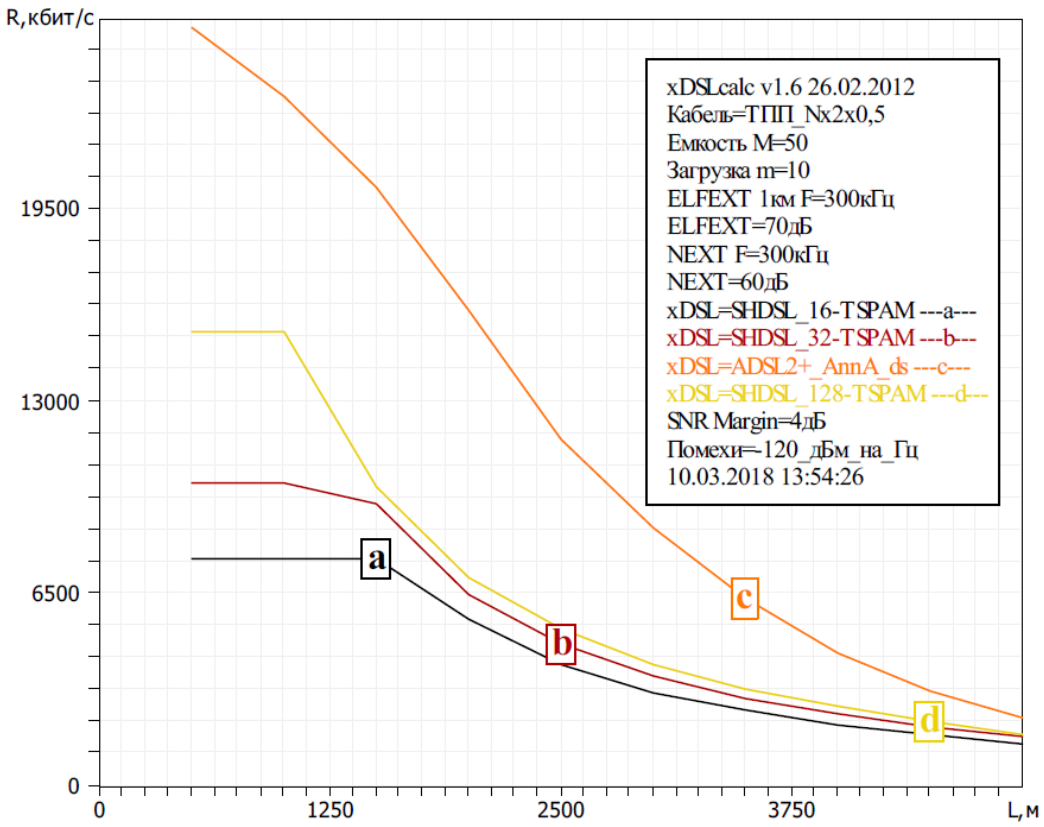


Рис. 2. Перепускна спроможність xDSL ліній під впливом перехідних завад

Наведені приклади перепускних спроможностей під впливом перехідних завад та без перехідних завад за допомогою програми xDSLcalc таких типів лінії xDSl як: 16TC-PAM SHDSL, 32TC-PAM SHDSL, 128TC-PAM SHDSL і ADSL2+. На рисунках показано, що швидкість передачі даних без завад і з завадами для ADSL2+ на малій відстані набагато більша ніж в інших типах лінії xDSl. Чим більша відстань тим швидкість передачі усіх типів ліній зменшується.

Література

1. В.А. Балашов, А.Г. Лашко, Л.М. Ляховецкий. Технологии широкополосного доступа xDSL. Инженерно-технический справочник / Под общей редакцией В.А. Балашова. М.: Эко Трендз, 2009. 256 с.: ил.
2. И.Г. Бакланов. Технологии ADSL/ADSL2+. Теория и практика применения. М: Метротек, 2007 – 394 с.: ил.
3. В.М. Горохов, В.А. Скаковский. Взаимное влияние линий ADSL и цифрового уплотнения. Подготовка и контроль линии. Методическое пособие. Тверь, 2009.
4. Г.Г. Бортник, В.М. Кичак, О.В. Стальченко. Системи доступу: підручник. Вінниця: ВНТУ, 2010. – 308с.
4. 5. Кочеров А.В. Расчет и контроль кабелей для цифровых линий SHDSL. М.: Вестник связи №4, 2012.

УДК 621.39

ПЕРЕВАГИ ВИКОРИСТАННЯ ПАСИВНИХ ОПТИЧНИХ МЕРЕЖ

Григоренко О.Г., Савченко П.П.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net

ADVANTAGES OF PASSIVE OPTICAL NETWORKS

The advantages and disadvantages of building broadband access networks based on the technology of passive optical networks (PON) are presented. The network architecture is well scalable, as well as promising in terms of continuous growth in bandwidth requirements.

Наведені переваги та недоліки побудови мереж широкосмугового доступу на основі технології пасивних оптичних мереж (PON). Архітектура мережі є добре масштабованою, а також перспективною з точки зору постійного зростання вимог до пропускної здатності.

Особливе місце серед сучасних технологій широкосмугового доступу займають технології пасивних оптичних мереж (PON – Passive Optical Network).

Мережа доступу на основі PON має деревовидну оптоволоконно-кабельну архітектуру з пасивними оптичними розгалужувачами на вузлах і здатна забезпечити широкосмугову передачу різноманітних додатків. При цьому архітектура PON (рис.1) володіє необхідною ефективністю нарощування як вузлів мережі, так і пропускної здатності, в залежності від теперішніх та майбутніх потреб абонентів.

Основні принципи побудови PON архітектури зводяться до наступного [1,2]:

- в мережі є два типи пристроїв: оптичний лінійний термінал (OLT – Optical Line Terminal), що розташовується на центральному вузлі телекомунікаційного оператора і абонентські термінали (ONT – Optical Network Terminal);
- в OLT використовується один передавач і один приймач для організації сегмента PON мережі;
- оптична розподільча мережа (ODN – Optical Distribution Network) побудована на основі одного оптичного волокна (пасивний шинний моноканал) і використовує пасивні розгалужувачі (спліттери).

Кількість абонентських вузлів ONT, підключених до одного приймально-передавального модуля OLT, може бути настільки великою, наскільки дозволяє бюджет потужності й максимальна швидкість приймально-передавальної апаратури. Для передачі низхідного потоку інформації, тобто від OLT до ONT, як правило, використовується довжина хвилі 1490 нм. Низхідий потік на рівні оптичних сигналів є мультиадресним. Кожний абонетський пристрій ONT читає адресні поля і виділяє із загального потоку інформацію, що призначена даному ONT (рис.1).

Потоки даних від різних абонентських вузлів ONT передаються на одній довжині хвилі 1310 нм і утворюють висхідний потік до OLT. При цьому використовується множинний доступ з часовим розподілом TDMA. Для кожного ONT встановлюється свій індивідуальний часовий інтервал для передачі даних із урахуванням корекції на затримку, зумовлену просторовим віддаленням даного ONT від центрального вузла OLT. В OLT і ONT вбудовані мультиплексори WDM, що розділяють вихідні та вхідні потоки.

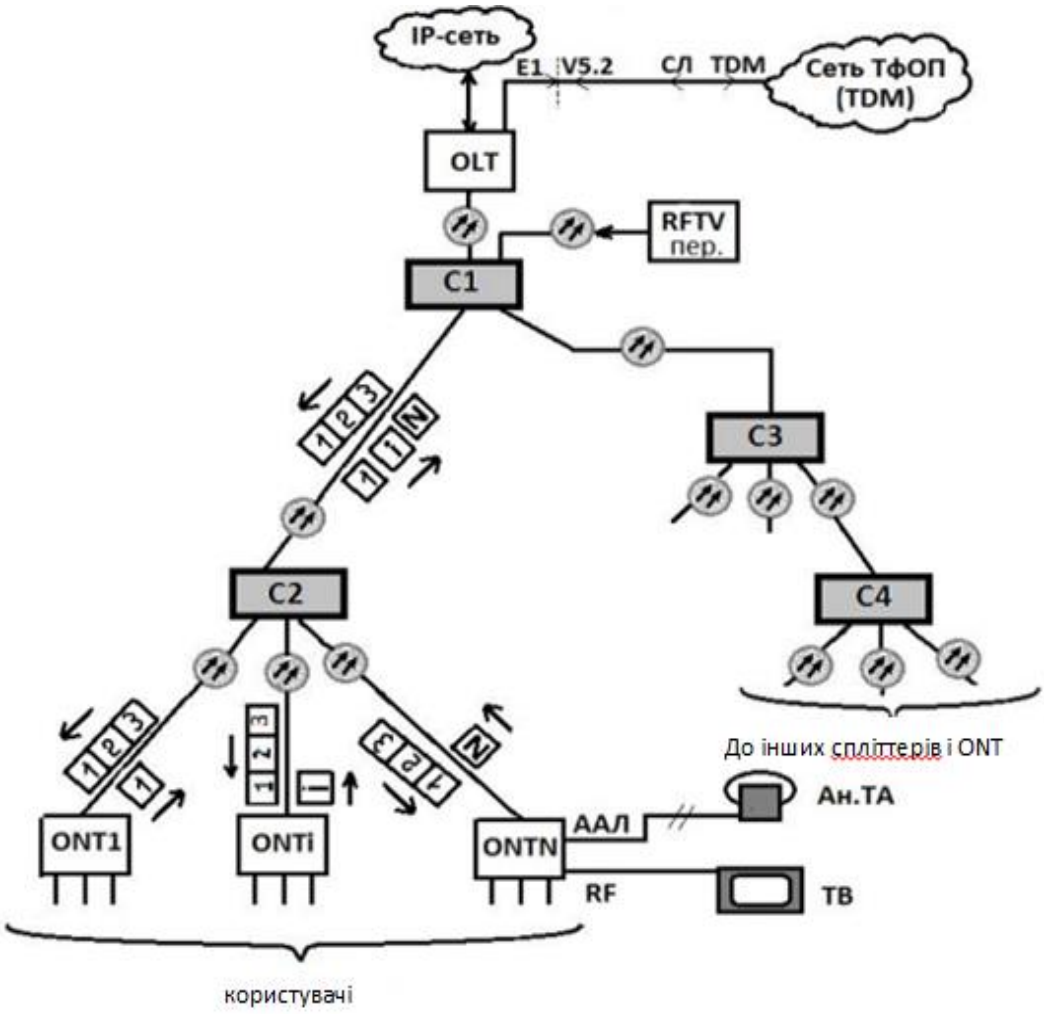


Рис. 1. Узагальнена структура мережі PON

Застосування технології PON в мережах доступу має чимало переваг:

- економія волокон в абонентських оптичних кабелях;
- значна економія оптичних випромінювачів на центральній станції;
- можливість надання трьох видів інформації (згідно концепції Triple Play): голосу, відео і даних;
- відсутня необхідність електроживлення елементів (крім кінцевих);
- невеликі витрати на обслуговування;
- легкість підключення нових абонентів без перерви зв'язку і зручність обслуговування (підключення, відключення або вихід з ладу одного або декількох абонентських вузлів ніяк не впливає на роботу інших);
- деревоподібна топологія P2MP (point to multipoint) дозволяє оптимізувати розміщення оптичних розгалужувачів, виходячи з реального

розташування абонентів, витрат на прокладку оптичного кабелю і експлуатацію кабельної мережі;

- можливість динамічного розширення смуги, тобто збільшення швидкості передачі працюючих абонентів за рахунок непрацюючих в даний момент;

- подальше збільшення швидкості передачі (до 10 Гбіт/с) і вище без заміни обладнання лінійного тракту (оптичні кабелі, розгалужувачі, з'єднувачі);

- мережі доступу на основі PON працюють на відстанях до 20 км, що також є перевагою у порівнянні з іншими технологіями доступу;

- подальша можливість значного збільшення швидкості передачі для кожного користувача за рахунок застосування технології оптичного мультиплексування (CWDM або DWDM).

Недоліки архітектури PON:

- необхідність шифрування потоку PON, так як PON – технологія, що використовує загальне середовище передачі даних, тому окремі потоки інформації доводиться шифрувати. Це може знижувати корисну швидкість передачі, а також не захищає інформацію від злому на фізичному рівні.

- складність системи. Це пояснюється тим, що в системі важко виявити неполадки на ділянці між спліттерами і кінцевою точкою - ONT. Тому для мінімізації проблем з мережею потрібно обирати професійного інсталлятора, який зможе якісно встановити, відстежувати стан і забезпечувати повноцінний сервіс.

Технології PON наступних поколінь мають два варіанти [3]. Перший, під назвою NG-PON1 передбачає співіснування «одногігабітного» PON (1G-PON) та NG-PON (10 Гбіт/с) на одній розподільної мережі (ODN). При цьому, навіть якщо оператор з часом повністю перейде на технологію нового покоління, він повинен підтримувати або емулювати 1G-PON для тих абонентів, яких задовольняє попереднє покоління.

Другий, NG-PON2 передбачає повне заміщення всієї інфраструктури разом з ODN і розрахований на операторів, що будують мережі доступу «з нуля», хоча може використовуватися на другому етапі міграції тими компаніями, які розвивають PON зараз, оскільки другий сценарій передбачає ще більш високі швидкості (10Гбіт/с, а в майбутньому можливо і більше).

Література

1. Мясин Н.И. Анализ возможности применения PON в интересах органов внутренних дел / Н.И. Мясин [Електронний ресурс] – Режим доступу: https://mvd.informost.ru/2015/pdf/1-26.pdf
2. Макаренко С.И. Системы многоканальной связи. Вторичные сети и сети абонентского доступа: учебное пособие /, В.Е. Федосеев. – СПб.: ВКА имени А.Ф. Можайского, 2014. – 179 с. [Електронний ресурс] – Режим доступу: http://sccs.intelgr.com/editors/Makarenko/Makarenko-mkss-sad.pdf
3. Ткаченко В. Новый PON не за горами / В. Ткаченко//Сети & Бизнес. — 2011. — №4 (59). — С. 72 – 86.

УДК 004.89

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ІНФОРМАЦІЇ В LTE

Варваринець С.В., Правило В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: sofiya.ponzel@gmail.com, valeriy_pravilo@ukr.net

Providing of safety of information transfer in LTE

In this article we will consider the concept of safety of information, procedure of its providing transfer (procedure of mutual authentication and agreement about the keys, encipherings and providing of integrity of information). Also will consider the basic requirements to safety of information transfer in the networks of LTE.

Останнім часом абревіатура LTE (Long Term Evolution – довготривала еволюція) на слуху. У всьому світі оператори мобільного зв’язку тестують, вивчають і впроваджують новий стандарт, який обіцяє стати дійсно чимось глобальним [1].

Безпека мережі – перш за все захист мережі і всіх підключених до неї ресурсів від різних загроз. Безпека включає в себе як фізичні, так і програмні міри протидії, які необхідні для захисту інфраструктури мережі від несанкціонованого доступу, некоректної роботи, неправомірного доступу, модифікації та руйнування [4].

Тому під безпекою будемо розуміти захист від несанкціонованого доступу до мережі і забезпечення конфіденційності при передачі як інформації користувача, так і інформації управління.

Захист від несанкціонованого доступу реалізується за допомогою процедури аутентифікації, яка ініціюється MME (Mobility Management Entity, блок управління мобільністю) при надходженні запитів на реалізацію певних процедур, а саме: підключення (Attach), оновлення даних місцезнаходження (Location updating), реалізації послуги (Service), відновлення з’єднання (Connection Reestablishment). А конфіденційність в свою чергу забезпечується за рахунок закриття (шифрації) переданої інформації.

В основі реалізації безпеки лежить використання часових ідентифікаторів та різних ключів.

Перша процедура забезпечення безпеки мережі LTE – взаємна аутентифікація і угода про ключі (AKA – Authentication and Key Agreement).

Вихідні дані для реалізації процедури AKA:

- IMSI – Міжнародний ідентифікатор UE (SIM карти);
- K – Абонентський ключ; SNID (Serving Network Identity) – ідентифікатор обслуговуваної мережі, рівний PLMN ID даної мережі;
- Network Type – тип мережі 0: GSM/UMTS, 1 – LTE;
- IMSI і K зберігаються як в HSS, так і на SIM карті UE.

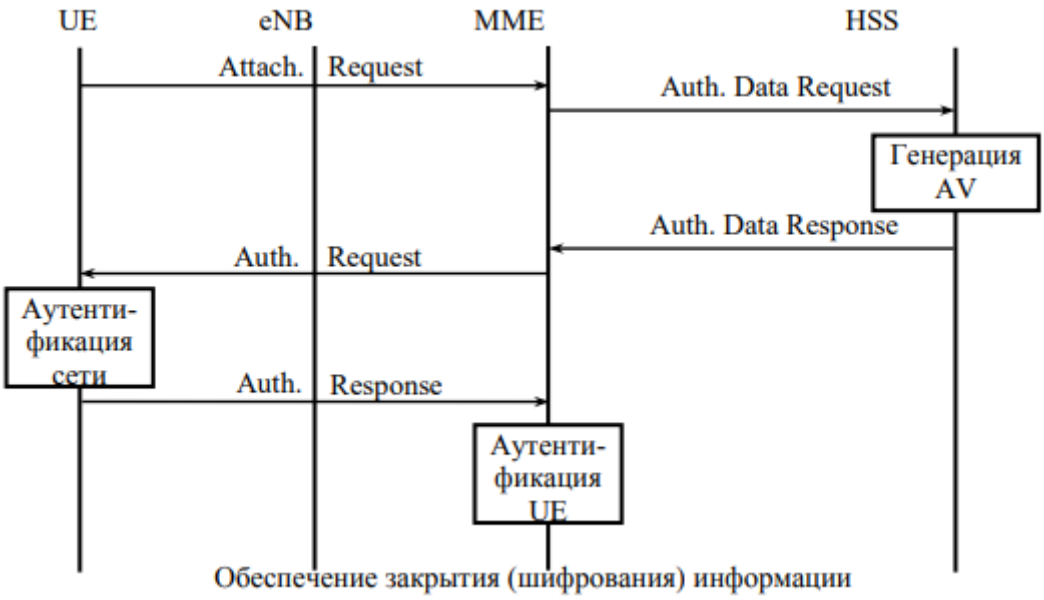


Рис. 1. Процес реалізації процедури АКА

Друга процедура забезпечення безпеки мереж LTE – це закриття (шифрування) і забезпечення цілісності інформації.

Шифрування та забезпечення цілісності інформації реалізується як і в площині управління, так і в площині користувача.

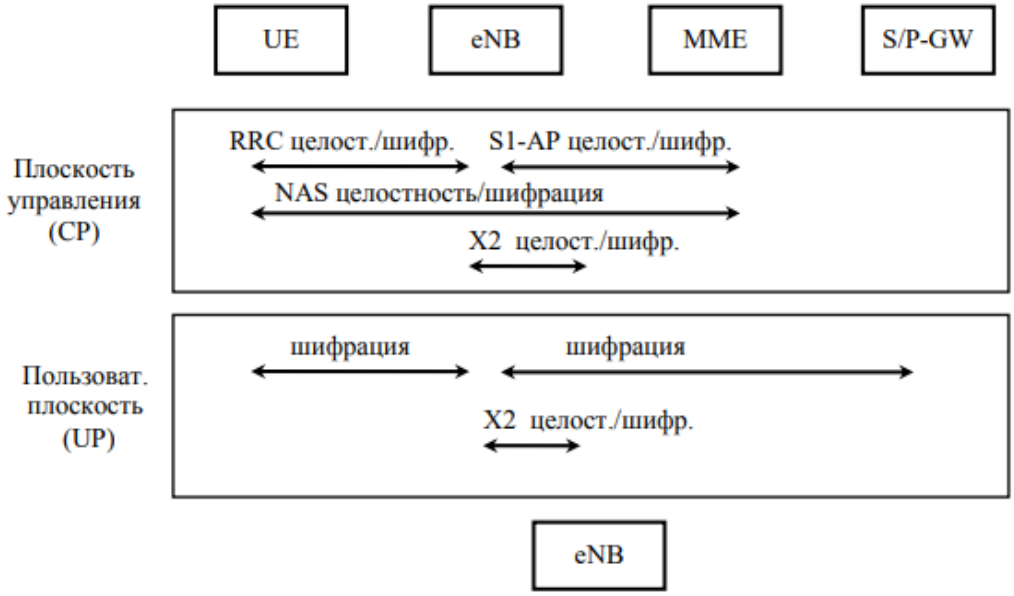


Рис. 2. Реалізація безпеки в площинах управління та користувача

А вже після успішного завершення процедури АКА MME, eNB і UE приступають до генерації ключів, які необхідні для шифрування і перевірки цілісності інформації [2].

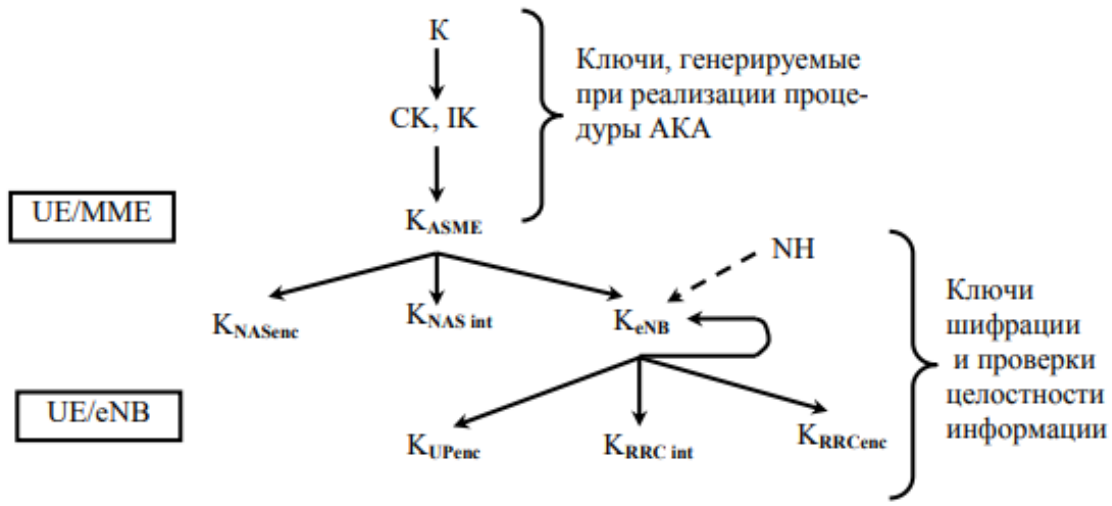


Рис. 3. Ієрархія ключів

Архітектура мереж LTE (Long Term Evolution) досить сильно відрізняється від схеми, яка використовується у вже існуючих мережах FOMA (3G). І саме ця відмінність породжує необхідність адаптувати та покращувати механізми забезпечення безпеки. Залишається найбільш важливою вимогою до механізмів безпеки гарантія хоча б того ж рівня безпеки, який на даний момент існує в мережах стандарту 3G. Наразі існує чотири основні вимоги до механізмів безпеки мережі LTE:

- Забезпечити (як мінімум) такий же рівень безпеки, як і в мережах стандарту 3G, не приносячи незручностей користувачам
- Забезпечити захист від Інтернет-атак
- Механізми безпеки для мереж LTE не повинні створювати завад для переходу зі стандарту 3G на стандарт LTE
- Забезпечити можливість подальшого використання програмно-апаратного мудулю USIM (Universal Subscriber Identity Module, універсальна сім-карта) [3].

Література

1. LTE: без пяти минут 4G [Електронний ресурс] - Режим доступу: https://itc.ua/articles/standart_lte_56151/
2. В. И. Данилов. Сети и стандарты мобильной связи
3. Защита данных в сетях LTE [Електронний ресурс] - Режим доступу: https://amonitoring.ru/article/lte_security/
4. Что такое безопасность сети [Електронний ресурс] - Режим доступу: https://www.hpe.com/ru/ru/what-is/network-security.html

УДК 621.391.3

ТЕНЗОРНА МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ СПРИЙМАННЯ КОРИСТУВАЧАМИ МУЛЬТИМЕДІЙНОГО ПОТОКУ

Лемешко О.В., Євдокименко М.О.
Харківський національний університет радіоелектроніки
E-mail: oleksandr.lemeshko.ua@ieee.org, marina.ievdokymenko@nure.ua

Tensor model of quality of experience routing

Tensor model for multipath routing with guaranteed the quality of Experience (QoE) is proposed. The novelty of the model consists in the updated version of flow conservation law, which is taking into account the possible packet loss caused by buffer overflow at the network routers. The accounting such losses is related to revise conditions associated with the quality of service. By using tensor approach analytical boundary conditions were obtained. The conditions allow ensuring different parameters of the quality of service (rate, average delay and packet loss probability) at the same time.

Однією з основних вимог, що висувається до інфокомунікаційних мереж, є надання послуг гарантованої якості обслуговування незалежно від типу інформації, що передається. З цією метою необхідно узгодити оцінки користувача про якість отриманих послуг та якість роботи мережі, що становить основу системного підходу до якості обслуговування [1-3]. Тому, виникає актуальна задача щодо формулювання в аналітичному вигляді умов по забезпеченню якості наданої послуги кінцевим користувачам в умовах реалізації багатошляхової стратегії маршрутизації та їх впровадження в існуючу математичну модель.

В рамках запропонованої моделі маршрутизації для обліку можливих втрат пакетів на вузлах мережі умова збереження потоку має вигляд [4]:

$$\begin{cases} \sum\limits_{j:(i,j)\in V} x^k_{(i,j)} = 1 \text{ при } k \in K,\ i = s_k; \\ \sum\limits_{j:(i,j)\in V} x^k_{(i,j)} - \sum\limits_{j:(j,i)\in V} x^k_{(j,i)}(1 - p^k_{(j,i)}) = 0 \text{ при } k \in \mathrm{K},\ i \neq s_k, d_k; \\ \sum\limits_{j:(j,i)\in V} x^k_{(j,i)}(1 - p^k_{(i,j)}) = \varepsilon^k \text{ при } k \in K,\ i = d_k, \end{cases} \quad (1)$$

де K – множина потоків в мережі; s_k – вузол-відправник; d_k – вузол-одержувач для пакетів k-го потоку; ε^k – частка k-го потоку, що обслуговується мережею, тобто пакети, які успішно доставлені до вузла-одержувача.

З урахуванням можливих втрат пакетів інтенсивність потоку в каналі в рамках введених вище позначень розраховується як

$$\lambda_{(i,j)} = \sum_{k \in K} \lambda_k^{\langle вим \rangle} x_{(i,j)}^k (1 - p_{(i,j)}^k), \tag{2}$$

де $\lambda_k^{\langle вим \rangle}$ – середня інтенсивність k-го потоку, що надходить в мережу на обслуговування, яка задає QoS-вимоги по швидкості передачі пакетів.

Для реалізації багатошляхової стратегії маршрутизації з балансуванням навантаження на керуючі змінні накладаються обмеження виду

$$0 \le x_{(i,j)}^k \le 1. \tag{3}$$

Для забезпечення керованості процесом боротьби з перевантаженням каналів і черг в структуру моделі вводяться наступні обмеження:

$$\sum_{k \in K} \lambda_k^{\langle вим \rangle} x_{(i,j)}^k (1 - p_{(i,j)}^k) < \varphi_{(i,j)} \ , \ \ (i, j) \in E, \tag{4}$$

де $\varphi_{(i,j)}$ – пропускна здатність j-го інтерфейсу i-го вузла.

Для оцінки та перевірки виконання вимог щодо наданої якості отриманих послуг кінцевими користувачами, згідно рекомендацій G.109 та Y.1540 [2, 3] використовується наступне обмеження на рівні QoE:

$$R \ge R_{вим}, \tag{5}$$

де R – рейтинг якості (Quality Rating).

Наприклад, в результаті вимоги користувача до наскрізної якості наданої послуги передачі мови при заданому типі термінального обладнання і використовуваному кодеку в загальному вигляді можуть бути записані наступним чином [2]:

$$R_0 - I_{dd}(T_a) - I_{e-eff}(P_{pl}) \ge R_{вим}, \tag{6}$$

де $I_{dd}(T_a)$ – коефіцієнт зниження якості, обумовлений тривалою затримкою в мережі, а $I_{e-eff}(P_{pl})$ – вплив втрати пакетів на якість передачі мови, які, в свою чергу, розраховуються за формулами:

$$I_{dd}(T_a) = \begin{cases} 0, \ T_a \le 100 \text{ мс}; \\ 25\left[\left(1+X^6\right)^{\frac{1}{6}} - 3\left(1+\left[\frac{X}{3}\right]^{\frac{1}{6}}\right)+2\right], \text{ при } T_a > 100 \ мс; \end{cases} \text{ та } I_{e-eff} = I_e + (95 - I_e)\frac{P_{pl}}{\frac{P_{pl}}{BurstR} + B_{pl}}.$$

В рамках тензорного опису інфокомунікаційної мережі в умовах реалізації багатошляхової стратегії маршрутизації [5-6], ймовірність доставки пакетів P_{pl} та середня затримка Ta із кінця в кінець може бути розрахована, як:

$$P_{pl} = \frac{\sum_{j=2}^{\phi} \lambda_{\eta}^{j}}{\lambda^{\langle вим \rangle}}, \qquad \text{та} \qquad T_a = \frac{\lambda^{вим} \varepsilon - G_{\pi\eta}^{\langle 4,2 \rangle} \left[G_{\pi\eta}^{\langle 4,4 \rangle} \right]^{-1} \Lambda_{\eta-1}}{\left(G_{\pi\eta}^{\langle 4,1 \rangle} - G_{\pi\eta}^{\langle 4,2 \rangle} \left[G_{\pi\eta}^{\langle 4,4 \rangle} \right]^{-1} G_{\pi\eta}^{\langle 4,3 \rangle} \right)} \tag{7}$$

де $\Lambda_{\eta-1}$ – вектор інтенсивностей втрачених пакетів на інтерфейсах маршрутизаторів з координатами λ_{η}^{j}; $G_{\pi\eta}^{\langle 4,1 \rangle}$, $G_{\pi\eta}^{\langle 4,2 \rangle}$, $G_{\pi\eta}^{\langle 4,3 \rangle}, G_{\pi\eta}^{\langle 4,4 \rangle}$ – проекція тензора G в системі координат контурів і вузлових пар для заданої інфокомунікаційної мережі.

В ході розв’язання задачі маршрутизації в якості критерію оптимальності одержуваних рішень обрано умову, пов’язану з максимізацією загальної продуктивності інфокомунікаційної мережі:

$$\max_{x,\varepsilon} \left[\sum_{k \in K} \lambda_{k}^{\langle вим \rangle} \varepsilon^{k} \right]. \tag{8}$$

Висновки. Таким чином, запропонована математична модель (1)-(8) багатошляхової маршрутизації з забезпеченнями QoE. Завдяки тензорній формалізації моделі вдалося отримати в аналітичному вигляді умови забезпечення якості обслуговування на рівні користувача (6)-(7). Крім того, в рамках запропонованого рішення забезпечується однакова мінімальна затримка пакетів для всіх розрахованих шляхів. Результати розрахунку підтвердили ефективність моделі з точки зору реалізації багатошляхової маршрутизації з підтримкою функцій QoE.

References

1. ITU-T G.109. Amendment 1 New Appendix I – The E-model-based quality loops for predicting speech transmission quality and user satisfaction from time-varying transmission impairments, 2007.
2. ITU-T Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters, 2016.
3. ITU-T Y.1541. Network performance objectives for IP-based services, 2011.
4. A.V. Lemeshko, O.Yu. Evseeva, and S.V. Garkusha, “Research on Tensor Model of Multipath Routing in Telecommunication Network with Support of Service Quality by Greate Number of Indices,” 2014 Telecommunications and RadioEngineering (BegellHouse), Vol.73, No 15, pp. 1339-1360.
5. O.V. Lemeshko, and O.S. Yeremenko, “Dynamics Analysis of Multipath QoS-Routing Tensor Model with Support of Different Flows Classes,” 2016 International Conference on Smart Systems and Technologies (SST), 12-14 Oct. 2016, Josip Juraj Strossmayer University of Osijek, Croatia, pp. 225-230.
6. O. Lemeshko, O. Yevsieieva, M. Yevdokymenko. Tensor Flow-Based Model of Quality of Experience Routing // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2018. – pp.1-4.

УДК 621.391

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ VLC ДЛЯ ПОБУДОВИ МЕРЕЖ LI-FI ТА ПРИНЦИП ЇЇ ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ

Романов А.І., Федюшина Д.М., Донг Т.Т.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net

The using of the VLC as a basic technology for building Li-Fi systems

Further development of wireless systems requires the solution for many issues related to energy efficiency or limited frequency resources. One possible way to overcome such issues is using the Li-Fi technology. This work describes the basic architecture of the Li-Fi system based on VLC technology.

У зв'язку зі збільшенням кількості технологічних розробок телекомунікаційних пристроїв, зростання різноманітності числа додатків, їх номенклатури і якості послуг, що надаються користувачам, значно зросли вимоги до швидкості передачі даних. Тому, мережі передачі даних в переважній більшості будуються за допомогою оптоволоконних ліній, що дозволяють досягти швидкості передачі даних порядку Тб/с. Проте, не завжди корисно і можливо розгортати кабельну інфраструктуру між кінцевими користувачами. Таким чином, важливість бездротового зв'язку збільшується із кожним днем. У наш час він широко використовується на останній милі, вдома, в офісних приміщеннях, тощо. У даній роботі розглянуто спосіб побудови мережі Li - Fi на базі технології VLC (visible light communication) для забезпечення користувачів бездротовим зв’язком в таких середовищах, як літаки, лікарні, тощо, де незручно та небезпечно використовувати радіочастотні хвилі [1]. Дана технологія використовує сигнали в інтервалі 380-780 нм. Таким чином можна домогтися одночасно і освітлення, і передачі даних за допомогою світлодіодних ламп [2].

На рис. 1 приведена структурно–функціональна схема системи зв'язку на базі технології VLC. Основними елементами системи VLC є передавач (набір світлодіодів), приймач (фотодетектор), блоки модуляції та демодуляції, тощо [3].

Розглянемо призначення і функції елементів системи бездротового доступу. Система складається з двох частин - тракту передачі і тракту прийому.

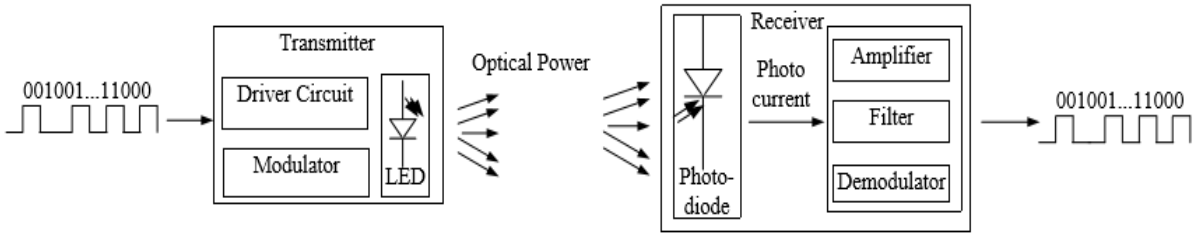


Рис. 1. Схематична архітектура мережі Li Fi на базі VLC

Тракт передачі:

Існують різні джерела світла, які зручно використовувати для освітлення. Однак, найбільш популярними вважаються лазерні діоди (LD) та світлодіоди (LED). Основна відмінність між LD і LED є те, що лазерні діоди є когерентним джерелом світла, а світлодіоди - некогерентним. Оскільки в даній роботі підтримується концепція одночасного освітлення і передачі даних, обговорення LDs виходить за рамки даної роботи. Отже, проаналізувавши рис. 1., маємо: при передачі інформації від першого користувача до другого, сигнал буде проходити через спеціальну схему керування джерелом світла, вираженого у вигляді набору LED ламп. Згадана схема керування (Driver circuit) використовується для живлення світлодіодних ламп. Вона повинна забезпечити достатній струм, щоб надати світлодіоду необхідну яскравість, при цьому не пошкодивши сам світлодіод.

Блок модуляції відповідає за вкладення інформаційної складової у сигнал. На сьогодні вибір способу модуляції доволі широкий: амплітудна маніпуляція, широтно-імпульсна, модуляція кольором, тощо. На сьогодні, найлегший спосіб – це On-Off модуляція, що має два інформаційних значення потужності, відповідних включеному і виключеному стану передавача. Дані модуляції закладаються у світло, при цьому, під час передачі та її відсутності, сигнали матимуть різну скважність, тому спостерігатиметься невелика зміна яскравості сигналу. Щоб уникнути неприємних для людського ока відчуттів, використовують компенсуючі паузи: при відсутності передачі, зверху вводяться паузи щоб зберегти яскравість освітлення на відносно сталому рівні.

Тракт прийому:

Фотодетектор поглинає фотони, що падають на його поверхню в зовнішньому інтерфейсі та генерує електричний сигнал. Перетворення фотонної енергії в електричну може бути досягнуто і альтернативним способом. Існує багато типів фотоприймачів, наприклад фоторезистори чи фототранзистори, що володіють специфічними якостями. Проте, фотодіоди вважаються найбільш поширеними у ролі фотоприймача через їх малий розмір, високу чутливість та швидку реакцію. P-I-N (PIN) і лавинний фотодіод (APD) є типовими прикладами використання фотодіодів як фотоприймачів. Існує кілька важливих вимог, яким має відповідати фотоприймач:

- чутливість, пов’язана з інтервалом довжин хвиль;
- тривалий термін експлуатації, надійність;
- мінімальний вплив температурних коливань;
- мати невеликі розміри;
- уміння подавляти шум (навколишнього середовища, затемнення і т.д.), тощо.

Після прийняття оптичного сигналу та його перетворення у електричний за допомогою фотодетектора, цей сигнал далі відфільтровується від завад та підсилюється за допомогою відповідних пристроїв.

У даному випадку було описано структуру передачі та прийому односпрямованої мережі на базі VLC. Можлива також двобічна передача в системі Li-Fi, для цього вводять у мережу додатковий пристрій: розгалужувач (duplexer). Duplexer використовується для підтримки двобічного зв'язку шляхом поділу переданого і прийнятого сигналу. Можливий варіант загальної структурної схеми такої мережі приведена на рис. 2.

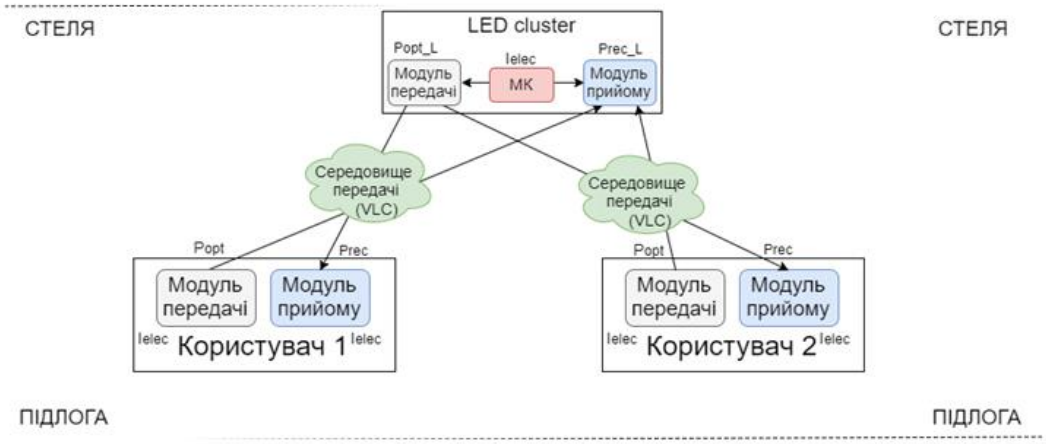


Рис. 2. Загальна структура мережі Li Fi

Найбільш важливими елементами такої системи є модуль прийому та модуль передачі, на рис.3 приведена їх деталізація: показаний приблизний перелік елементів та їх функціональне призначення.

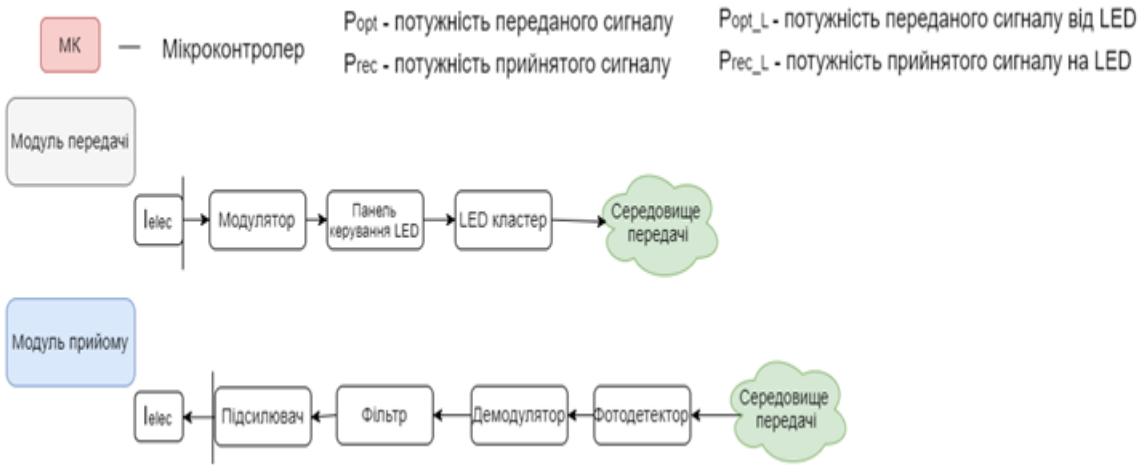


Рис. 3. Структурна схема модулів передачі і прийому мережі Li Fi

Таким чином, використання технології Li Fi дозволяє значно підвищити пропускну спроможність і якість бездротових телекомунікаційних мереж. Практична реалізація таких мереж та їх фізичного рівня не дуже складна, однак вимагає значних організаційних зусиль і зміни підходів до їх організації.

Література

1. Taner Cevik and Serdar Yilmaz “An overview of visible light communication system” International Journal of Computer Networks & Communications (IJCNC) Vol.7, No.6, November 2015.
2. Farooq Aftab, Muhammad Nafees Ulfat khan,Shahzad Ali «Light fidelity (Li-Fi) based indoor communication system» International Journal of Computer Networks & Communications (IJCNC) Vol.8, No.3, May 2016.
3. Романов А.И., Федюшина Д.М, Донг Т.Т. Использование VLC в качестве базовой технологии при построении беспроводных Li-Fi сетей. Материалы XXII МНТК «Современные средства связи», Минск, Респ. Беларусь ; 2017, С17-19.

УДК 621.382

ВЗАЄМОДІЯ РІЗНИХ ВИДІВ ТЕЛЕФОННИХ МЕРЕЖ ІЗ СУЧАСНИМИ МЕРЕЖАМИ ПЕРЕДАЧІ ДАНИХ НА БАЗІ ПЛАТФОРМИ IMS

Нестеренко М.М., Верес Л.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nesterenko_nik@ukr.net, veresleonid@gmail.com

Interaction of different telephone networks with modern data transmission networks on the IMS platform base

In today's telecommunications world, convergence of different types of telephone networks with modern data networks is required. IMS can solve this problem. The main task of this issue is to ensure compatibility of systems of different technologies at the level of management, signaling and traffic flows.

В сучасному світі телекомунікацій відбувається конвергенція різного виду телефонних мереж із сучасними мережами передачі даних. Однією із інтеграційних платформ виступає система *IMS*. Головним завданням даної системи є забезпечення сумісності систем різних технологій на рівні управління, сигналізації і транспортних потоків.

Архітектура *IMS* стала проривом технологій *NGN* [1]. Оскільки дана архітектура впритул наблизилась до концепції інтернетизації суспільства. За допомогою технології *IMS* можна забезпечити своїх клієнтів певним власним набором ресурсів із будь-якого доступного засобу комунікацій (який підтримує технологію *IMS)*, із будь-якої мережі (будь то мобільні, стаціонарні або бездротові), що і є основною задачею викладеною в концепції інтернетизації суспільства (доступ до інформації в будь-який час, в будь-якому місці із будь-якого засобу зв’язку).

IMS являє собою стандартизовану архітектуру управління мережею, яка використовує *SIP* протокол для управління послугами. Початково, представлена архітектура, розроблялася для бездротових мереж стандарту 3*GPP* для розвитку, вдосконалення та розширенні інформаційних послуг мобільних мереж *GSM*.

Концепція *IMS* визначає засновану на загальнопоширених протоколах сімейства *TCP/IP* архітектуру надання сервісів (послуг), яка забезпечує управління сеансами зв’язку і доставку в рамках цих сеансів основних типів інформації: - мови, даних, відео, мультимедіа.

Для з’ясування особливостей взаємодії різних типів телефонних мереж із сучасними *IP*-мережами, розглянемо основні сценарії встановлення з’єднання при використанні сегментів мереж із різними технологіями, які інтегруються в *IMS*-домені. Для спрощення сприйняття матеріалу розглянемо сценарії встановлення з’єднання, коли користувачі знаходяться в одному *IMS*-домені.

На рис. 1. представлено основні фази обміну сигнальними повідомленнями між клієнтами мобільного зв’язку [1, 2], при використанні ядра *IMS*.

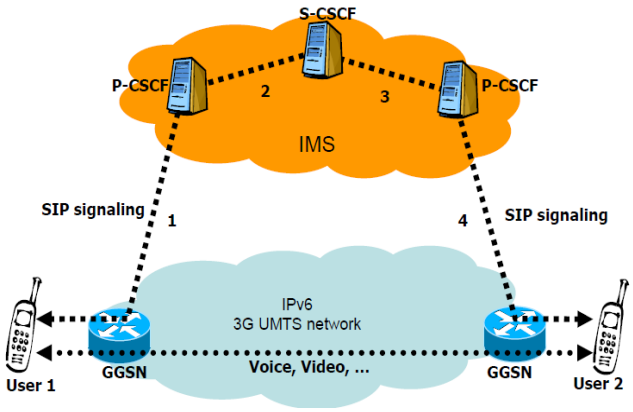
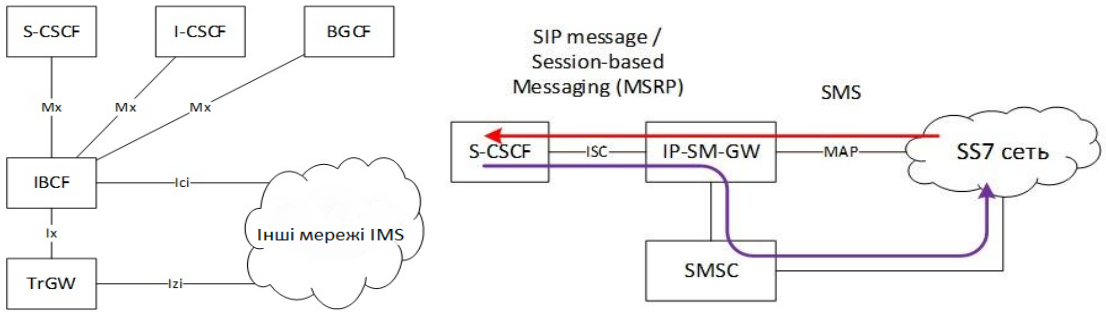


Рис. 1. Основний шлях *SIP*-сигналізації для безроумінгових клієнтів в одному домені *IMS*

Отже, при встановленні з'єднання між абонентами використовується протокол сигналізації *SIP*. Контактними точками *IMS* для агентів *SIP*-користувачів (*SIP-UA*) є *Proxies-CSCF* (*P-CSCF*), а *Serving-CSCF* (*S-CSCF*) є *SIP*-сервером, який встановляє та контролює сеанси зв'язку. Необхідно відмітити, що у випадку, якщо абоненти належать до інших доменів *IMS* (або існує декілька *Serving-CSCF* в одному домені) для знаходження необхідного *Serving-CSCF* використовується ще один *SIP*-сервер для опитування *Interrogating CSCF* (*I-CSCF*). Для передачі голосових та відео- потоків в *IP*-мережах використовують протокол передачі трафіку реального часу (*RTP*) і протокол управління та контролю передачею трафіку реальному часу (*RTCP*).

В свою чергу *GGSN* (*GPRS Gateway Service Node*) є шлюз (маршрутизатор) між мережею (її частиною) для передачі даних *GPRS* і зовнішніми інформаційними магістралями пакетної передачі даних *Packet Data Networks* (*PDNs*): *Internet*, корпоративними мережами *Intranet*, іншими *GPRS*-системами. Отже основна задача *GGSN* – це маршрутизація даних між *GPRS Core network* і зовнішніми *IP*-мережами.

На рис. 2. представлено взаємодію між *IMS* та різними мережами операторів зв'язку та порядок відправлення повідомлення *SMS* від мережі *SS7* до системи IMS [3, 4].



а) б)

Рис. 2. а) Схема взаємодії між *IMS* та різними мережами операторів зв'язку; б) Схема взаємодії *IMS* та *SS7* при передачі *SMS*-повідомлень

Функція взаємодії між *IMS* мережами різних операторів зв'язку (рис. 2. а) реалізуються за допомогою функціонального модуля управління прикордонним шлюзом (*Interconnection Border Control Function – IBCF*) і транзитного шлюзу (*Transition Gateway – TrGW*). При цьому вирішуються наступні завдання: трансляція між різними версіями протоколу *IP* (*IPv4, IPv6*), які використовуються на мережах операторів (*IBCF* модифікує *SIP* і *SDP* дані, дозволяючи користувачам, які використовують різні версії *IP*, взаємодіяти один з одним); приховування мережевої топології (*IBCF* виконує шифрування / дешифрування всіх заголовків повідомлень, які містять інформацію про топології мережі); фільтрація інформації в *SIP*-повідомленнях (*IBCF* видаляє або модифікує деякі *SIP* заголовки перед маршрутизацією повідомлень в напрямку сторонніх мереж).

IP short message gateway (*IP-SM-GW*) з'єднує найбільш поширену технологію мобільного зв'язку щодо обміну повідомленнями *SMS* із *IMS* (рис. 2. б). Коли *SMS* надсилається до *IMS* користувача – *SMS* маршрутизується по мережі сигналізації *SS*7 до *IP-SM-GW*, який потім вставляє отриману *SMS* в якості контенту спеціального типу в *SIP MESSAGE* і направляє його в *S-CSCF* для подальшої маршрутизації. Це дозволяє доставляти *SMS*-повідомлення користувачам, які зареєстровані не в 3*GPP* мобільних, а в *IP*-мережах (*Wi-Fi, WiMAX*), а також може розглядатися як альтернатива традиційним методам доставки *SMS* повідомлень (*CS, GPRS*). *IP-SM-GW* також дозволяє доставляти *SMS* в зворотному напрямку (від абонентів *IMS* мереж користувачам *CS* 2G/3G мереж). Коли *IMS* абонент відправляє
SIP-повідомлення, що містить *SMS* як спеціальний тип контенту (*special content type*), *IP-SM-GW* витягує його і направляє в *SMS*-центр (SMSC) для подальшої доставки по мережах *SS*7. Даний тип взаємодії дозволяє надавати всі існуючі *SMS* послуги абонентам, зареєстрованим в *IMS* мережах. Ця функціональність називається *SMS over IP* (3GPP TS 23.204).

Відповідно до сучасних технологій *IP*-телефонії та концепції побудови системи управління *IMS* сигнальний трафік та медіа-потоки відокремлені між собою. Тобто медіа потоки циркулюють на рівні транспортної мережі. А обробка сигналізації та управління винесені на вищі рівні, при чому функціональні блоки управління можуть бути територіально рознесені та адаптовані для надання всього спектру сучасних інформаційних послуг.

Література

1. Романов О.І., Нестеренко М.М., Верес Л.А., Гордашник Є.С. Модель розрахунку пропускної спроможності *IP*-мультимедійної підсистеми (IMS) // Збірник наукових праць ВІТІ. – Київ, 2017. – Вип. №2– С. 92 – 100.
2. Investigation IMS architecture According to Security and QoS context © AJMAL MUHAMMAD, March 2014. © RAJA MUHAMMAD SHAMAYEL ULLAH, March 2014.
3. ADeart V.Y. Multiservice network. 2011. (Softswitch / IMS). Moscow: Briz-M, 2011. - 198 p.
4. https://itechinfo.ru/content/%D0%BA%D1%80%D0%B0%D1%82%D0%BA%D0%BE-%D0%BE%D0%B1-ims

УДК 621.39

ПРИНЦИП ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ ОПТИЧНОГО ПІДСИЛЮВАЧА (EDFA) НА БАЗІ ТЕХНОЛОГІЇ LI-FI

Світанько Н.В., Веревкін Л.Л., Хрипко С.Л.
Запорізька державна інженерна академія, Україна
E-mail: svitnik_1973@ukr.net

The principles of telecommunication systems with EDFA development based on Li-Fi technology

The principles of telecommunication systems development based on Li-Fi technology, meeting the requirements of the standard IEEE 802.15.7 are considered. The possible directions of practical realization of EDFA systems are analyzed. The project implemented in intelligens optical systems are presented.

Безпроводові комунікаційні технології стали невід'ємною частиною повсякденного життя і продовжують інтегруватись в усі сфери людської діяльності, що зумовлено споживчим попитом користувачів та постійним розвитком телекомунікаційних технологій.

Світ інтернету речей нестримно зростає: по прогнозах консалтингової компанії Gartner, кількість підключених до мережі фізичних об'єктів склала в 2017 році 8 млрд., що на 30% більше, ніж в 2016. До 2020 року в інтернет речей буде об'єднано близько 20,8 млрд пристроїв, по оцінках ABI Research – більше 40 млрд. Значна частина цих пристроїв – «розумні» світлодіодні світильники.

Одним з можливих напрямків вирішення цих проблем є застосування Li-Fi технології. Li-Fi бездротова система зв'язку, в якій замість звичних радіочастот для передачі даних використовується світло. Здатність світлодіодів бути одночасно джерелом освітлення і каналом передачі інформації дозволила створити інтелектуальні інтегровані системи освітлення.[1] У них кожен світильник стає міні-комп'ютером, оснащується датчиками (руху, освітленості, вологості і іншими), поєднується з іншими інформаційними системами (переносними пристроями і домашніми міні комп’ютерами, системами управління будівлею (BMS), системами навігації і іншими).

Сьогодні вважається більш перспективним побудова телекомунікаційних систем з використанням спектра частот видимого світла (VLC).

Традиційна система передачі інформації із використанням елементів Li-Fi технології виглядає наступним чином:

Потужний світлодіод, який є джерелом передачі інформації.

Фотодетектор.

Система підсилення сигналу реєстрації.

Система обробки інформації.

Основним недоліком системи передачі інформації за технологією Li-Fi, є обмеженість у просторі та можливість зовнішнього доступу до безпеки системи при передачі інформації за межі приміщення, де розміщено світлодіоди. Для вирішення проблеми передачі інформації за межі приміщення, де розташована система, нами пропонується структура світлодіодної системи передачі інформації де окремі точки прийому з’єднуються із головним приміщенням за допомогою оптоволоконних ліній.

Основною характеристикою оптичного приймального пристрою (ОПрП) є чутливість – мінімальна потужність оптичного сигналу на вході фотодетектора, що

забезпечує необхідну якість прийому, яка оцінюється відношенням сигналу до шуму в аналогових системах та ймовірністю помилки у цифрових системах. Аналогічно передавальним оптичним модулям (ПрОМ) приймальні пристрої для розроблюваної волоконно-оптичної системи передачі реалізовано у вигляді функційно завершеного виробу оптоелектроніки – приймального оптичного модуля. Типовий ПрОМ вміщує: оптичний з'єднувач або армований відрізок оптичного кабелю для підключення до волоконно-оптичного кабелю, приймач випромінювання (фотодіод або лавинний фотодіод), електронні схеми підсилення та обробки електричного сигналу, а також пристрої для стабілізації режимів роботи.

На рис. 1 наведена структурна схема типового ПрОМ [2].

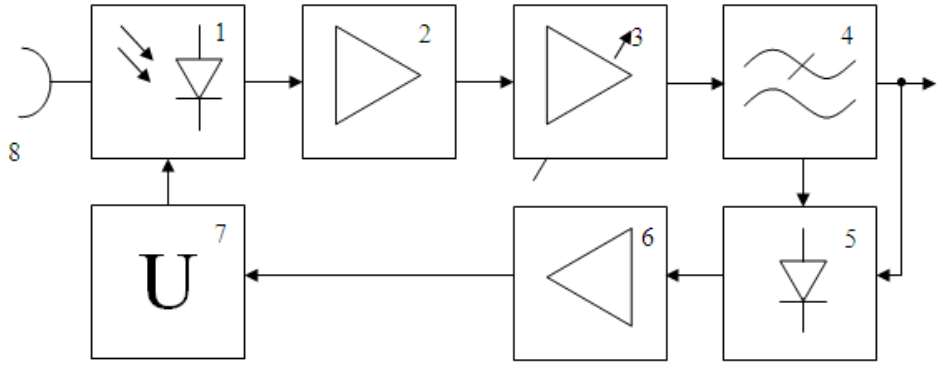


Рис. 1. Структурна схема ПрОМ: 1 - фотодіод, 2 - попередній підсилювач, 3 - основний підсилювач з автоматичним регулюванням підсилення (АРП), 4 - фільтр нижніх частот, 5 - піковий детектор, 6 – підсилювач АРП, 7 - джерело оберненого зміщення фотодіода, 8 – оптоволоконний канал з’єднання

У якості каналу з’єднання використовується звичайне оптичне волокно і з’єднувальними елементами інтегральної оптики [3].

Для ПрОМ нормуються такі параметри та характеристики:

Чутливість – мінімальна середня потужність на виході фотодетектора, що забезпечує необхідне відношення сигнал/шум або необхідний коефіцієнт помилок.

Рівень власних шумів – середньоквадратичне значення флуктуацій вихідної напруги ПрОМ в заданій смузі частот у відсутності вхідного оптичного сигналу.

Спектральна характеристика – залежність вольтової чутливості ПрОМ S_u(В/Вт) від довжини хвилі оптичного випромінювання, що приймається.

Робоча довжина хвилі – довжина хвилі оптичного випромінювання, що приймається, для якої нормуються параметри ПрОМ.

Смуга пропускання – інтервал частот, в якому значення амплітудно-частотної характеристики ПрОМ не менше половини її максимального значення.

Швидкість передачі – швидкість передачі символів цифрового сигналу на оптичному виході ПрОМ, при котрій його параметри зберігають задані значення.

Відношення сигналу до шуму – відношення амплітуди змінної складової вихідної напруги ПрОМ для заданих характеристик оптичного сигналу, що приймається, до середньоквадратичного значення флуктуацій вихідної напруги, коли приймається немодульване оптичне випромінювання тієї ж потужності.

Коефіцієнт помилок – відношення кількості помилок в цифровому сигналі на виході цифрового ПрОМ в заданому інтервалі часу до кількості символів на цьому інтервалі часу.

У якості попереднього підсилювача 2 (див. рис. 1) у роботі пропонується використати принцип спектрального ущільнення оптичного сигналу за рахунок використання оптичних волокон.

В основу роботи оптичного підсилювача покладений принцип стимульованого (примусового) випромінювання, аналогічний лазерному. Активним середовищем підсилювача є відрізок оптичного волокна (ОВ) короткої довжини (декілька десятків метрів).

Одним із шляхів підсилення оптичних сигналів в фотонних мережах передачі інформації є використання оптичних волокон, легованих ербієм. Оптичні підсилювачі на основі легованих ербієм оптичних волокон (ОПЕОВ), [англомовно – *Erbium Dopel Fiber Amplifiers (EDFA)*] вносять значні зміни в технологію оптичного зв'язку, знижуючи загальну вартість систем передачі SDH і одночасно підвищувати надійність та якісні показники роботи систем [4].

Принцип роботи EDFA засновано на тому, що випромінювання накачки проходить ербієвим волокном з довжиною хвилі 0,98 або 1,48 мкм. Іони ербію збуджуються і переходять від стаціонарного енергетичного рівня А до більш високих рівнів Б і В, тобто іони ербію поглинають світлову енергію джерела накачки, відбувається накачка іонів ербію і вони переходять на більш високий енергетичний рівень. Їх подальший перехід на низький енергетичний рівень супроводжується одночасним випромінюванням фотону з довжиною хвилі в інтервалі 1,53-1,56 мкм. Це може носити спонтанний характер (природний розлад збуджений іонів при відсутності будь-якого зовнішнього впливу) або стимульований характер (в присутності іонів, що здійснюють процес передачі енергії). Стимульована емісія виробляє додаткові фотони із швидкістю, пропорційною інтенсивності їх надходження.

Оптичний і інформаційний сигнал походить цим волокном, стимулює емісію світла і збуджених іонів, що в свою чергу, підсилює цей сигнал.

У зв'язку із тим, що на даний час відсутні вітчизняні системи ОПЕОВ, в представленій роботі було запропоновано використати нелінійно-оптичний матеріал $Sr_4B_{14}O_{25}:Pr^{3+}$ (SBBO). Кристал SBBO вперше було отримано у ЗДІА в лабораторії нелінійно-оптичних перетворювачів частоти (НОПЧ) [5]. Празеодимові структури мають найбільшу кількість каналів генерації в порівнянні з іншими матеріалами. Вони дозволяють отримати генерацію у видимому, ближньому та середньому ІЧ – діапазонах при кімнатних температурах, що дає можливість отримання на їх основі низькопорогового лазерного випромінювання з діодною накачкою.

Область застосування EDFA можна розділити на два основних направлення:

1. EDFA виконують роль підсилювачів оптичних передавачів, проміжних лінійних підсилювачів та передпідсилювачів. В цьому випадку основна мета використання EDFA – збільшити довжину регенераційної ділянки.

2. Абонентські лінії (лінії абонентського доступу). EDFA тут використовується як підсилювач потужності після передавачів з метою компенсації втрат, обумовлених наявністю таких елементів, як фідери, а також з метою підвищення рівня потужності сигналу в світловоді.

Таким чином, Li-Fi системи на EDFA можуть найближчим часом замінити систему Wi-Fi, підвищивши при цьому показники пропускної здатності, якості обслуговування та безпеки.

Література

1. Pankaj R. Patil. Introduction to li-fi (light fidelity) technology. IJTRE. 3(4), 600-603. (2015).
2. Стеклов В.К. Нові інформаційні технології: Транспортні мережі телекомунікацій. Київ: «Техніка» .- 2004. 488с.
3. Бондаренко В.Г. Современные технологии транспортных сетей связи. – К.,: Радоіаматор.-2006.-№12.-С.50-52.
4. Becker P., Olsson F., Simpson J. Erbium-Doped Fiber Amplifiers. Academic Press. (1999). 460pp.
5. Svitanko N.V. et al. The luminescence of the Praseodymium-doped Strontium borate $Sr_4B_{14}O_{25}:Pr^{3+}$. Ukr.J.Phys.Opt. 3(2). 155-160. (2002).

УДК 621.391:006

СИНХРОНИЗАЦИЯ В ТЕЛЕКОММУНИКАЦИЯХ НОВОГО ПОКОЛЕНИЯ: ОБЗОР ТЕХНОЛОГИЙ И СТАНДАРТОВ

Триска Н.Р.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: ntriska@ukr.net

Synchronization in new generation telecommunications: summary of technologies and standards

The recent ITU-T activities in the field of the modern packet networks synchronization are summarized. The need of adaptation of the existing technical specification to support the requirements of IMT-2020/5G is emphasized.

Высокие требования к техническим характеристикам и инфраструктуре сети, предъявляемые современными телекоммуникационными стандартами, ставят перед разработчиками новых технологий целый ряд задач, для решения которых традиционные методы и модели необходимо адаптировать к особенностям работы сетей следующего поколения. Так, при внедрении концепции развития телекоммуникаций 5-го поколения (5G) одним из критически важных показателей становится величина задержки пакетной передачи, которая напрямую зависит от параметров синхронизации по тактовой частоте и времени [1, 2]. Технические требования к системам 5G (в частности, стандарт IMT-2020) предполагают минимизацию дисперсии задержки пакетов до величин менее 1 мкс вплоть до десятков нс. Поэтому особую актуальность приобрели задачи разработки, апробации и стандартизации технических решений, позволяющих реализовать данные требования. Примером такой работы может служить принятый в феврале 2018 г. Технический отчет Исследовательской Комиссии 15 Международного Союза Электросвязи (ITU-T SG-15) GSTR-TN5G [3], определяющий направления стандартизации транспортных сетей для поддержки технологии 5G, в том числе в части синхронизации. Ниже представлен краткий анализ основных подходов ITU-T к синхронизации современных сетей в контексте поддержки 5G.

В рамках исследовательского вопроса Q13/15 (ITU-T SG-15) ведется активная работа по стандартизации технических решений в части синхронизации пакетных сетей [4, 5]. Действующие в настоящее время Рекомендации представлены в табл. 1. Сейчас акцент делается на доработку и совершенствование существующих технических решений на базе технологии синхронного Ethernet (SyncE) и протокола точного времени PTP (IEEE 1588) для поддержки требований 5G. При этом разграничивают требования для различных фрагментов сети 5G с учетом их технологических особенностей.

Таблица 1. Обзор стандартов ITU-T по синхронизации пакетных сетей

Направление стандартизации	**Частотная синхронизация – *серия G.826x***		**Фазовая (временная) синхронизация – *серия G.827x***
	syncE	**PTP**	**PTP**
Термины и определения, метрики	G.8260		
Общие принципы (базовая, рамочная рекомендация	G.8261		G.8271
Сетевые нормы	G.8261	G.8261.1	G.8271.1, G.8271.2
Генераторное оборудование	G.8262	G.8263, G.8266	G.8272, G.8272.1, G.8273, G.8273.2, G.8273.3
Архитектура сети синхронизации	G.8264	G.8265	G.8275
Профили протокола PTP	–	G.8265.1	G.8275.1, G.8275.2

В существующих сетях мобильной связи (2,3, 4G) выделяют транспортную, базовую сеть (Core Network), сеть радиодоступа (RAN) и промежуточную, “перевалочную” сеть (Backhaul Network) между контроллером базовых станций (BSC, RNC, BBU) и базовой станцией (BS, Node B, eNB). Концепция 5G в целом сохраняет эту структуру, но предполагает разделение функций контроллера базовых станций на две группы, соответствующие двум логическим элементам – “центральному” CU (Central Unit) и “распределенному” DU (Distribution Unit). В связи с этим стандарт IMT-2020 в общем случае выделяет три фрагмента на участке между контроллером 5G (CU + DU) и базовой станцией (в терминологии 5G обозначаемой как RRU – Remote Radio Unit):

- *Backhaul* (“ближний” фрагмент) – участки сети между блоками CU, а также участки между CU и базовой сетью (в терминологии 5G базовую сеть обозначают как NGC – Next Generation Core);
- *Midhaul* (“средний” фрагмент) – участки сети между блоками CU и DU;
- *Fronthaul* (“дальний” фрагмент) – участки сети между DU и RRU.

Технические требования ко многим параметрам (в частности, к задержке передачи) нормируются отдельно для каждого из указанных фрагментов сети. В то же время стоит отметить, что данная концепция пока находится в стадии разработки, и конкретные сценарии ее реализации подлежат уточнению и апробации. Так, возможны различные варианты физической реализации блоков CU, DU и RRU (например, объединение на одной площадке блоков CU и DU или DU и RRU) [3].

В части требований к синхронизации пакетных сетей с учетом перспективы 5G хотелось бы отметить следующее.

1. Многолетняя активная работа МСЭ-Т по стандартизации технических решений для синхронизации пакетных сетей (с участием ведущих производителей элементной базы и оборудования синхронизации, а также крупных телекоммуникационных операторов) подготовила достаточную базу для дальнейшей работы в направлении адаптации к стандартам IMT-2020/5G.

2. Существующие технические решения по синхронизации в пределах базовой транспортной сети, а также на фрагменте *Backhaul* (между базовой сетью и элементами уровня CU) при условии повышения ряда параметров генераторного оборудования в принципе позволяют обеспечить уровень, требуемый для поддержки 5G. При этом наилучший результат дает реализация “классической” концепции тактовой сетевой синхронизации на физическом уровне с применением технологии SyncE, которая создает основу для обеспечения более точной фазовой/временной синхронизации на базе протокола PTP с учетом возрастающих требований к параметрам задержки. В настоящее время ведется работа по пересмотру параметров генераторного оборудования SyncE (готовится проект новой Рекомендации G.8262.1), что позволит повысить точность синхронизации базовой сети как по частоте, так и по времени. Параллельно продолжается работа по стандартизации параметров генераторного оборудования, ориентированного на работу по протоколу PTP (проект новой Рекомендации G.8273.4).

3. Требования к точности синхронизации в сети радиодоступа, а также на промежуточных фрагментах (*Midhaul* и *Fronthaul*) еще находятся в стадии разработки. На данный момент эксперты ориентируются на существующие требования сетей 4G (LTE) с отклонением фазы порядка 1,5 мкс. Они будут корректироваться в соответствии с разрабатываемыми спецификациями стандарта IMT-2020/5G с учетом того, какие технологии и услуги на уровне RAN будут реализовываться в первую очередь. При этом предполагается, что повышенные требования к точности/стабильности на участке радиодоступа будут иметь локальный характер, т.е. подстройка фазы будет необходима для взаимодействия оборудования в пределах одной площадки без необходимости передачи опорных сигналов синхронизации от базовой сети.

4. Помимо разработки технических требований и стандартизации оборудования, существует целый ряд сопутствующих задач, важных для обеспечения синхронизации существующих и перспективных сетей. Это, в первую очередь, задачи планирования и эксплуатации сетей синхронизации с учетом смены технологий и инфраструктуры базовой сети, а также вопросы выбора оптимальных метрик и отработки методик измерений параметров синхронизации по тактовой частоте, фазе и времени.

Литература

1. S. Ruffini et al. A novel SDN-based architecture to provide synchronization as a service in 5G scenarios. – IEEE Communications Magazine, March 2017. – pp. 210-215.
2. Триска Н.Р. Актуальные задачи синхронизации на этапе развертывания сетей 5G. – Одинадцята Міжнародна науково-технічна конференція “Проблеми телекомунікацій” (ПТ-2017), 18-21 квітня 2017 р. Матеріали конференції. – ІТС НТУУ “КПІ”. – С. 102-104.
3. ITU-T Technical Report GSTR-TN5G: Transport network support of IMT-2020/5G. – ITU-T SG-15, February 2018.
4. Бирюков Н.Л., Триска Н.Р. Синхронный Ethernet как основа частотно-временного обеспечения современных и будущих сетей связи. – Электросвязь, 2013, № 2. – С. 8-12.
5. Бирюков Н.Л., Триска Н.Р., Худынцев Н.Н. Обзор направлений исследований МСЭ в области частотно-временного обеспечения современных сетей связи. – T-Comm, № 2-2014. – с.12-17.

УДК 621.396.43

ВИКОРИСТАННЯ LI-FI ДЛЯ ПЕРЕДАЧІ ДАНИХ ЗА ДОПОМОГОЮ ВИДИМОГО СВІТЛА

Наритник Т.М., Єрмаков А.В., Постернак Б.С., Клин І.М., Сарапулов С.В.
Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: yermak_antonio@ukr.net

Using Li-Fi to transmit data with visible light

Li-Fi wireless optical network technology is used to transmit data via LEDs. The technology relates to the class of communications in the visible light spectrum (VLC) and uses the transmission medium in many respects similar to Wi-Fi. Compared to the latter, it has better bandwidth, efficiency, availability and security.

Li-Fi передача двійкових даних за **допомогою видимого світла** (засновником і автором терміну вважається професор Харальд Хаас (Harald Haas)) може бути здійснена шляхом включення і виключення світлодіода. Оскільки зміна станів може відбуватися менш ніж за 1 мкс, то для людського ока світлодіод буде здаватися постійно включеним. Дані можуть кодуватися за допомогою різної швидкості спалахів світлодіода, що дозволяє отримувати різні рядки 1 і 0. Чутливий фотодіод отримує сигнал і перетворює його в двійкові дані. Цей метод використання швидких імпульсів світла для безпроводової передачі даних технічно відноситься до зв'язку за допомогою видимого світла (VLC). Термін Li-Fi це технологія, яка потенційно може конкурувати з Wi-Fi. VLC використовує видиме світло в діапазоні 400 ТГц (780 нм) - 800 ТГц (375 нм) в якості оптичного носія для передачі даних і освітлення. При використанні високошвидкісних світлодіодів з відповідною схемою модуляції можуть бути досягнуті швидкості передачі вище 3 Гб/с від одного джерела. Паралельна передача даних за допомогою масивів світлодіодів, кожен з яких передає окремий потік, може збільшити швидкість передачі. Розглянемо, чим Li-Fi відрізняється від VLC. VLC використовує світлодіоди для передачі двійкових даних за допомогою зміни інтенсивності випромінювання (Intensity Modulation, IM). На приймачі сигнал визначається фотодиодом з використанням принципу прямого детектування (Direct Detection, DD). VLC техніка зв'язку «точка-точка», по суті, як заміна кабеля, що призвело до ранньої стандартизації VLC IEEE 802.15.7. Тепер цей стандарт переглянутий, і він включає Li-Fi. На відміну від VLC стандарт Li-Fi описує двосторонній багато користувальний зв'язок, іншими словами, зв'язок «точка-багатоточка» і «багатоточка-точка». Li-Fi забезпечує повну мобільність користувача і тому утворює новий напрямок серед існуючих

гетерогених безпроводових мереж. Той факт, що світлодіод є природним формувачем променя, дозволяє локально обмежити сигнал Li-Fi і блокувати його непрозорими стінками.

Поскільки Li-Fi використовує електромагнітне випромінювання для передачі даних, то тут можуть бути використані для зв'язку методи з необхідною модифікацією. Більш того, завдяки використанню для безпроводового зв'язку видимого світла в Li-Fi можуть бути реалізовані унікальні і специфічні формати модуляції.

При модуляції однієї несучої (Single-Carrier Modulation, SCM) широко використовуються схеми, які включають амплитудну маніпуляцію (On-Off Keying, OOK), фазово-імпульсну модуляцію (Pulse Position Modulation, PPM) і амплітудно-імпульсну модуляцію (Pulse-Amplitude Modulation, PAM). OOK є однією з простих схем модуляції, і забезпечує гарний компроміс між продуктивністю системи і складністю реалізації. OOK передає дані послідовно включаючи і вимикаючи світлодіод, схема може за своєю суттю забезпечувати підтримку зменшення сили світла (діммінг). Як зазначено в стандарті IEEE 802.15.7, діммінг може бути досягнутий за рахунок налаштування рівнів вкл/викл або застосування компенсації символу. Діммінг за рахунок налаштування рівнів вкл/викл світлодіода може зберігати той же темп передачі даних, однак дальність надійність зв'язку буде зменшуватися при низьких рівнях зменшення сили світла. З іншого боку, діммінг за допомогою компенсації символу може бути досягнутий вставкою додаткових імпульсів вкл/викл, тривалість визначається бажаним рівнем зниження інтенсивності світла. Оскільки максимальна швидкість передачі даних досягається при рівні зменшення сили світла на 50%, який передбачає рівну кількість 1 і 0 в середньому, збільшення або зменшення яскравості світлодіодів буде викликати зниження швидкості передачі.

Для забезпечення високошвидкісного оптичного безпроводового зв'язку почали застосовувати модуляцію декількох несучих (MCM). У порівнянні з SCM, MCM є більш широкосмуговим, але менш енергоефективним. Однією і, мабуть, найбільш використовуваною реалізацією MCM в мережах Li-Fi є OFDM - мультиплексування з поділом сигналів по ортогональних частотах, при якому паралельні потоки даних передаються одночасно за допомогою набору ортогональних піднесучих, де складне формування амплітудно-частотних характеристик може бути опущено. Якщо кількість ортогональних піднесучих вибирається так, що ширина смуги модульованого сигналу менше, ніж ширина смуги когерентності оптичного каналу, то кожен підканал може розглядатися як плоский канал з завмиранням (сенс ширини смуги когерентності полягає в тому, що в діапазоні частот, який значно менше, ніж ширина смуги когерентності, частотна характеристика каналу може вважатися плоскою, тобто вона не сильно змінюється).

В Li-Fi використовуються також і специфічні схеми модуляції. Оскільки трансмітери Li-Fi розробляються, не тільки для безпроводового зв'язку, а й для освітлення, яке може бути реалізовано або з використанням

синіх світлодіодів з жовтим фосфорним покриттям, або за допомогою суміші кольорів від різнокольорових світлодіодів. Лампи, обладнані кольоровими світлодіодами, можуть надати додаткові можливості для модуляції і визначення сигналу в системі Li-Fi.

Будучи широкосмуговою безпроводовою технологією, Li-Fi може забезпечити одночасний доступ до мережі безлічі користувачів. При використанні передавачів з кутовим рознесенням може бути реалізована схема оптичного множинного доступу з просторовим розділенням (Space Division Multiple Access, SDMA). У порівнянні з оптичним множинним доступом з розділенням за часом (TDMA), SDMA може досягти десятикратного збільшення пропускної здатності в мережі Li-Fi. OFDM забезпечує більш простий метод множинного доступу, а саме, множинний доступ з поділом по ортогональних частотах (OFDMA), де користувачі обслуговуються і розділяються безліччю ортогональних піднесучих.

З метою підвищення пропускної спроможності для користувачів периферійних сот безпроводових систем зв'язку був запропонований неортогональної множинний доступ (NOMA). Використовуючи трансляційну природу світлодіодів, було показано, що продуктивність мережі Li-Fi може бути поліпшена, якщо використовувати NOMA. Відмінна від загальноприйнятих технологій OFDMA, NOMA може обслуговувати збільшену кількість користувачів за допомогою розподілу неортогональних частотних ресурсів, і вона розглядається як перспективна технологія для безпроводового зв'язку 5G. Поряд з перевагами Li-Fi, як і багатьом іншим технологіям, притаманні і ряд специфічних особливостей . Основна з них та, що світ не може проходити через перешкоди. Проблемами також є надійність і покриття мережі. Її роботу можуть ускладнювати зовнішні джерела світла, такі як сонце, звичайне електричне освітлення, непрозорі предмети на шляху поширення сигналу. Таким чином, Li-Fi технологія навряд чи замінить Wi-Fi технологію - вона може зайняти достойну нішу в широкосмугових безпроводових телекомунікаціях.

Література

1. http://laser-portal.ru/content_1193.
2. http://www.bbc.com/russian/science/2013/10/131029_li_fi_technology.
3. http://1234g.ru/novosti/li-fi.
4. http://li-fi.com.ua/li-fi/
5. https://www.ted.com/talks/harald_haas_wireless_data_from_every_light_bulb?language=ru.
6. https://www.ted.com/talks/harald_haas_a_breakthrough_new_kind_of_wireless_internet?language=ru.
7. https://www.eng.ed.ac.uk/about/people/prof-harald-haas.
8. https://www.lifi.eng.ed.ac.uk/

УДК 621.37

ХАРАКТЕРИСТИКА СИСТЕМИ ТАКТОВОЇ МЕРЕЖЕВОЇ СИНХРОНІЗАЦІЇ ДЛЯ ОЦІНКИ ЧАСУ ЗАТРИМКИ МЕРЕЖІ

Якимчук Н.М. *асистент кафедри ЕТ*
Луцький національний технічний університет, Україна
Олянський В.В. *головний енергетик ПРАТ «Едельвіка», Україна*
E-mail: n.yakymchuk@lntu.edu.ua

The description of time network synchronization system for estimation of time delay

The basic component delays of time in digital TCNS and reason of their origin are considered. The parameters of the systems of synchronization, which influence on the sizes of delays in networks and efficiency of the in-use system of synchronization, are selected.

При вирішенні завдань контролю і управління елементами телекомунікаційної мережі, конфігураціями, продуктивністю і безпекою необхідно отримувати статистику про стан різних режимів мережевих елементів. Ключовим елементом для оцінки продуктивності мережі, поряд з пропускною спроможністю, є затримка, оскільки затримка є визначальним фактором при проведенні віддаленого моніторингу, управлінні пріоритетами та маршрутами потоків даних.

Затримки при взаємодії (обмін інформацією, управління, моніторинг) обумовлені:

- затримкою при передачі від одного елемента до іншого (за рахунок обмеженої швидкості поширення сигналів в лініях зв'язку);
- затримкою в чергах буферних пристроях (Queue delay);
- затримкою при обробці і перетворенні сигналів(кодуванні, декодуванні, оцінюванні та ін.);
- затримкою (запізненням) на час отримання дозволу на передачу (latency).

При оцінці параметрів якості функціонування мультисервісних мереж (QoS — Quality of Service) опорною точкою є оптимальне задоволення потреб користувачів. З точки зору користувача очевидним є негативний вплив затримки на якість передачі аудіо і відео інформації, причому мережеві затримки визначені стандартами ITU і повинні вкладатися в певні межі: діапазон 0-150 мс є прийнятним для більшості користувацьких додатків, 150-400 – затрудняє спілкування в реальному часі, затримки більше 400мс неприйнятні для більшості додатків.

Затримки при передачі пакетів інформації по каналу зв’язку від одного користувача до іншого можна розділити на два типи:

- Затримки, що вносяться мережею, в основному мають змінний характер і включають затримки в чергах на кожному з вузлів зв’язку мережі: маршрутизатор, мережевий адаптер, комутатор. Зменшуються шляхом

покращення мережевої інфраструктури, використанням високошвидкісних каналів, стиснення даних, кешування, оптимізацією трафіку.

- Затримки при обробці і пересиланні інформації, відносяться до постійних, пов’язані з швидкістю проходження сигналу по лінії зв’язку на конкретну відстань, алгоритмом перетворення інформації – кодування, пакетування, тощо. Зменшується шляхом покращення алгоритмів обробки і перетворення інформації.

$$T(n) = \sum_{k=2}^{n} T_{пер}(k-1,k) + \sum_{k=2}^{n} T_{обр}(k)\ ,$$

$T_{обр}(k)$ - час обробки пакета у вузлі, $T_{пер}(k-1,k)$ - час пересилання пакета між вузлами.

Одним зі способів встановлення цих значень є порівняння часових міток, що відповідають двом сусіднім IP-адресам в досліджуваному сегменті. Для цього використовують властивості протоколу передачі шкали часу – PTP (Precision Time Protocol). Цей протокол призначений для синхронізації шкали часу віддалених пристроїв - клієнтів (Slave) зі шкалою опорного джерела (Crandmaster), при цьому здійснюється передача даних про поточне значення шкали часу джерела, згідно яких здійснюється налаштування шкали часу клієнта, події і часові мітки на всіх пристроях при цьому використовують одну і ту ж часову базу. Дані включають початкову фазу відліку чергового секундного інтервалу і номер цього інтервалу (Код Часу).

Елементи системи синхронізації розосереджені по мережі зв'язку і утворюють свою мережу тактової мережевої синхронізації, яка накладена на мережу зв'язку і визначається її структурою. В процесі експлуатації системи ТМС необхідно здійснювати вимірювання основних параметрів синхросигналів в контрольних точках мережі з метою визначення їх відповідності необхідним нормам.

Для систем PTP виділяють три основні контрольовані характеристики:

- точність синхронізації даних про поточне значення номера секундного відліку;
- точність відновлення інтервалу 1 Гц і еталонної частоти;
- точність синхронізації початкової фази секундних відліків.

Для перевірки значень коду часу застосовуються спеціалізовані прилади – аналізатори протоколу PTP, в яких реалізовані функції порівняння КЧ клієнта з КЧ від вбудованого приймача (GPS).

Для контролю початкової фази і тривалості інтервалу сигналу 1 Гц можуть використовуватися стандартні електронно-рахункові частотоміри, які отримують опорні сигнали 1Гц (1 імпульс в секунду – 1 PPS, 1 Pulse Per Second) від повіреного джерела.

При передачі по мережі синхросигнал піддається фазовим спотворенням, які прийнято розділяти на два види: швидка зміна фази з частотою 10 Гц і більше – тремтіння фази (джитер); повільна зміна фази з частотою нижче 10 Гц – дрейф фази (вандер). Враховуючи, що параметри фази і частоти пов’язані інтегральним співвідношенням, часто розглядають

джитер як варіацію частоти сигналу.

Тремтіння фази вимірюється в долях тактового інтервалу (одиничного інтервалу – UI), що дозволяє порівнювати параметр для каналів різних рівнів ієрархії, а дрейф фази визначаються помилкою часового інтервалу (ПЧІ), нс.

При передачі даних в цифровій формі порушення в синхронізації цифрового потоку, приводить до двох ефектів:

1) в процесі регенерації, порушення в синхронізації приводять до флуктуацій моментів часу прочитування дискрет відносно моментів часу, що відповідають максимальному рівню сигналів на виході демодулятора. В результаті, знижується пороговий рівень роботи по шумах, що приводить до появи бітових помилок. Такий вплив більшою мірою пов'язаний з джитером.

2) на виході асинхронних мультиплексорів (тобто на вході в комутаційну станцію) відхилення можуть привести до переповнювань еластичних буферів і прослизань з втратами циклової синхронізації, що приводить до значної деградації якості зв'язку, що зазвичай викликається вандером.

Єдиним способом досягнення точності при вимірюваннях джитера є надзвичайно висока якість аналізатора, з мінімальним значенням впливу власного джитера приладу, що тягне за собою значне збільшення вартості приладів. Крім того, оскільки, тремтіння фази гаситься за допомогою генераторів мережевих елементів цифрової мережі і, отже, не накопичується при розподілі по мережі ТМС, то основними параметрами, що визначають спотворення синхросигналу, є параметри дрейфу фази.

При виборі методики вимірювання параметрів синхросигналів додатково слід врахувати, що наслідки впливу вандера можна компенсувати, на відміну від наслідків джитера, зокрема шляхом розширення розміру еластичного буфера пам’яті. Оскільки період зміни частоти досліджуваного сигналу чималий, то рівень вандера можна фіксуватися при вимірюванням частоти цифрової передачі.

Висновки. Використання виділених систем тактової синхронізації дозволяє оцінити і зменшити величини затримок часу в цифрових телекомунікаційних мережах, проте породжує нові задачі оцінки якості функціонування систем синхронізації. Поряд з прямими методами визначення характеристик синхросигналів за допомогою промислових аналізаторів протоколів, доцільно використовувати непрямі оцінки засновані на аналізі показників бітових помилок BER, як для визначення параметрів джитера сигналу.

Література

1. Колинько Т. / Измерения в цифровых системах связи. // Киев: Век+, НТИ, 2002, 320 с.
2. Колтунов М.Н. / Организация измерений при эксплуатации системы тактовой сетевой синхронизации // Электросвязь. 2010. №12.
3. Колтунов М.Н., Леготин Н.Н., Шварц М.Л. / Сетевая синхронизация в системах связи. //М.: изд. SYRUS SYSTEMS. 2007. 240 с.
4. Marais A. /«IEEE 1588-2008 perspectives and opportunities»//EDN, October, 2010.

УДК 621.391

ТЕНЗОРНА МОДЕЛЬ ВІДМОВОСТІЙКОЇ QOS МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ

Лемешко О.В., Єременко О.С.
Харківський національний університет радіоелектроніки, Україна
E-mail: oleksandr.lemeshko.ua@ieee.org, oleksandra.yeremenko.ua@ieee.org

Tensor model of fault-tolerant QoS routing in the infocommunication network

The tensor model of fault-tolerant QoS routing has been proposed, the novelty of which is providing the required values of the average packet rate and average packet delay in the case when the multipath delay for the primary path should be no greater than the corresponding delay for the backup path. The fault-tolerant QoS routing problem has been reduced to the solution of the corresponding optimization problem of nonlinear programming.

На сьогоднішній день надзвичайно актуальною є задача, пов'язана з побудовою т.зв. відмовостійких інфокомунікаційних мереж (ІКМ), здатних забезпечити високий рівень і якості обслуговування (Quality of Service, QoS), і відмовостійкості [1, 2]. В роботі пропонується модель відмовостійкої QoS маршрутизації, в рамках якої структура мережі описується одновимірною мережею $S=(U,V)$, де $U=\{u_r, r=\overline{1,m}\}$ – множина вузлів мережі (маршрутизаторів), а $V=\{v_z=(i,j); z=\overline{1,n}; i,j=\overline{1,m}; i\neq j\}$ – множина дуг (каналів зв'язку). При цьому z-й канал моделюється дугою $v_z=(i,j)\in V$. Пропускна здатність $\varphi_{i,j}$ відома для кожного каналу (i,j) і вимірюється в пакетах за секунду (1/с).

Результатом розв'язання задачі відмовостійкої QoS маршрутизації є розрахунок двох типів маршрутних змінних – $x_{i,j}^k$ та $\bar{x}_{i,j}^k$, кожна з яких характеризує частку інтенсивності k-го потоку в каналі зв'язку (i,j), що входить до основного або резервного шляху відповідно; K – множина потоків в ІКМ. Стратегія багатошляхової маршрутизації в моделі реалізується на основі обмежень $0\le x_{i,j}^k\le 1$ та $0\le \bar{x}_{i,j}^k\le 1$, які накладаються на керуючі змінні.

Крім того, мають бути виконані умови збереження потоку на вузлах мережі, які накладаються на маршрутні змінні основного шляху [2]:

$$\begin{cases} \sum\limits_{j:(i,j)\in V} x_{i,j}^k - \sum\limits_{j:(j,i)\in V} x_{j,i}^k = 1,\ k\in K,\ i=s_k; \\ \sum\limits_{j:(i,j)\in V} x_{i,j}^k - \sum\limits_{j:(j,i)\in V} x_{j,i}^k = 0,\ k\in K,\ i\neq s_k, d_k; \\ \sum\limits_{j:(i,j)\in V} x_{i,j}^k - \sum\limits_{j:(j,i)\in V} x_{j,i}^k = -1,\ k\in K,\ i=d_k, \end{cases} \tag{1}$$

де s_k – вузол відправник, а d_k – вузол одержувач для k-го потоку. Аналогічні

умови (2) накладаються на маршрутні змінні резервного шляху.

В роботі [2] пропонується ряд умов, що відповідають за реалізацію схем захисту елементів мережі при відмовостійкій багатошляховій маршрутизації. При цьому захист каналу зв'язку ІКМ $v_z = (i, j) \in V$ реалізується таким чином:

$$0 \le \bar{x}_{i,j}^k \le \delta_{i,j}^k, \text{ де } \delta_{i,j}^k = \begin{cases} 0, \text{ при захисті каналу зв'язку } (i, j) \in V; \\ 1, \text{ в іншому випадку.} \end{cases} \quad (2)$$

Також мають місце обмеження щодо запобігання перевантаження пропускної здатності каналів зв'язку (умови захисту пропускної здатності):

$$\sum_{k \in K} \lambda_{req}^k \cdot \max[x_{i,j}^k, \bar{x}_{i,j}^k] \le \varphi_{i,j}, \ (i, j) \in V, \quad (3)$$

де λ_{req}^k – середня інтенсивність k-го потоку (1/с), що надходить до мережі.

З метою забезпечення міжкінцевої QoS перейдемо до тензорної моделі ІКМ [1], в якій структура мережі визначає дискретний n-вимірний простір, де n – число каналів зв'язку в мережі. ІКМ розглядається в двох ортогональних системах координат (СК): гілок мережі $\{v_k, k = \overline{1,n}\}$, а також лінійно незалежних контурів $\{\pi_i, i = \overline{1,\mu}\}$ і вузлових пар $\{\eta_j, j = \overline{1,\phi}\}$, $\mu(S) = n - m + 1$ – цикломатичне число, а $\phi(S) = m - 1$ – ранг мережі, які визначають відповідно кількість базисних контурів і вузлових пар в мережі S. Тоді, наприклад, в разі моделювання функціонування інтерфейсу маршрутизаторів мережі СМО M/M/1 метрика простору буде представлена тензором G, координати проекції якого в СК гілок, представлені діагональними елементами матриці G_v розміру $n \times n$ і віднесені до кожного потоку в мережі, будуть розраховуватися так [1]:

$$g_v^{zz} = \lambda_v^z (\varphi_z - \Lambda_v^z), \quad (4)$$

де λ_v^z – інтенсивність аналізованого потоку в z-му каналі зв'язку при використанні наскрізної нумерації каналів; Λ_v^z – інтенсивність агрегованого потоку в каналі $v_z = (i, j) \in V$, яка згідно з виразом в лівій частині нерівності (3). Проекції тензора G при зміні СК його розгляду перетворюються як [1]:

$$G_{\pi\eta} = A^t G_v A, \quad (5)$$

де $G_{\pi\eta}$ – проекція тензора G в СК контурів і вузлових пар, A – $n \times n$ матриця коваріантного координатного перетворення [1], $[\cdot]^t$ – оператор транспонування, $[\cdot]^{-1}$ – оператор обернення матриці.

Як показано в [1], матрицю $G_{\pi\eta}$ можна представити таким чином:

$$G_{\pi\eta} = \left\| \begin{matrix} G_{\pi\eta}^{\langle 1 \rangle} & | & G_{\pi\eta}^{\langle 2 \rangle} \\ --- & + & --- \\ G_{\pi\eta}^{\langle 3 \rangle} & | & G_{\pi\eta}^{\langle 4 \rangle} \end{matrix} \right\|, \ G_{\pi\eta}^{\langle 4 \rangle} = \left\| \begin{matrix} G_{\pi\eta}^{\langle 4,1 \rangle} & | & G_{\pi\eta}^{\langle 4,2 \rangle} \\ --- & + & --- \\ G_{\pi\eta}^{\langle 4,3 \rangle} & | & G_{\pi\eta}^{\langle 4,4 \rangle} \end{matrix} \right\|,$$

де $G_{\pi\eta}^{\langle 1\rangle}$ и $G_{\pi\eta}^{\langle 4\rangle}$ – квадратні підматриці розміру $\mu\times\mu$ і $\phi\times\phi$ відповідно, $G_{\pi\eta}^{\langle 2\rangle}$ – підматриця розміру $\mu\times\phi$, $G_{\pi\eta}^{\langle 3\rangle}$ – підматриця розміру $\phi\times\mu$; $G_{\pi\eta}^{\langle 4,1\rangle}$ – перший елемент матриці $G_{\pi\eta}^{\langle 4\rangle}$.

Тоді умови забезпечення якості обслуговування для кожного k-го потоку за вимогами щодо параметрів середньої затримки τ_{req}^{k} і швидкості передачі пакетів λ_{req}^{k} приймають вид [1]:

$$\lambda_{req}^{k}\left(G_{\pi\eta}^{\langle 4,1\rangle}-G_{\pi\eta}^{\langle 4,2\rangle}\left[G_{\pi\eta}^{\langle 4,4\rangle}\right]^{-1}G_{\pi\eta}^{\langle 4,3\rangle}\right)^{-1}\le\tau_{req}^{k}. \qquad (6)$$

В лівій частині нерівності (5) записано вираз для розрахунку міжкінцевої затримки пакетів (τ_{MP}^{k}), які передаються основним шляхом (мультишляхом). При використанні резервного шляху вираз (6) для розрахунку середньої затримки $\bar{\tau}_{MP}^{k}$ за формою залишиться незмінним, проте в ньому будуть присутні компоненти матриці $\overline{G}_{\pi\eta}$, яка будується згідно з виразами (4) та (5) для геометричного простору, який не містить елементу (вузла, каналу) мережі, який захищається. Тоді в модель вводиться наступна умова-нерівність:

$$\tau_{MP}^{k}\le\bar{\tau}_{MP}^{k}\le\tau_{req}^{k}, \qquad (7)$$

за якої середня міжкінцева багатошляхова затримка для основного шляху τ_{MP}^{k} має бути не більшою за відповідну затримку для резервного шляху $\bar{\tau}_{MP}^{k}$.

В ході розв’язання задачі відмовостійкої QoS маршрутизації в ІКМ пропонується використовувати критерій оптимальності, пов’язаний з мінімізацією наступної цільової функції:

$$F=\sum_{k\in K}\sum_{E_{i,j}\in E}c_{i,j}^{k}x_{i,j}^{k}+\sum_{k\in K}\sum_{E_{i,j}\in E}\bar{c}_{i,j}^{k}\bar{x}_{i,j}^{k}, \qquad (8)$$

де $c_{i,j}^{k}$ і $\bar{c}_{i,j}^{k}$ – маршрутні метрики каналів зв’язку, які використовуються при обчисленні основного та резервного шляхів відповідно. Таким чином, вдалося звести задачу відмовостійкої QoS маршрутизації до розв’язання оптимізаційної задачі нелінійного програмування.

Література

1. Yeremenko, O.S. Method of Hierarchical QoS Routing Based on the Network Resource Reservation [Text] / O.S. Yeremenko, O.V. Lemeshko, O.S. Nevzorova, A.M. Hailan // 2017 IEEE First Ukraine Conference on ELECTRICAL AND COMPUTER ENGINEERING (UKRCON), 2017. – P. 971–976.
2. Лемешко, О.В. Розробка та дослідження лінійної оптимізаційної моделі швидкої перемаршрутизації з балансуванням навантаження в телекомунікаційних мережах [Текст] / О.В. Лемешко, О.С. Єременко // Радиоэлектроника и информатика. – 2017. – № 4 (79). – С. 18–25.

УДК 621.39

АСИМПТОТИЧНИЙ АНАЛІЗ ПРОТОКОЛУ ВИПАДКОВОГО МНОЖИННОГО ДОСТУПУ «НЕНАПОЛЕГЛИВИЙ МДКН-ВК» ПРИ РОЗВ'ЯЗАННІ ПАРНИХ КОНФЛІКТІВ НА ФІЗИЧНОМУ РІВНІ

Полякова А.С., Сбоєв Р.Ю., Єрохін В.Ф.
Інститут спеціального зв'язку та захисту інформації
КПІ ім. Ігоря Сікорського, Україна
E-mails: polnastasya@gmail.com, roman.sboyev@gmail.com, stddssss@gmail.com

Asymptotic analysis of the random multiple access protocol "Nonpersistent CSMA-CD" with pairwise conflicts resolving at the physical layer

There is described analysis of random multiple access protocol with carrier sense and collision detection (CSMA-CD) with pairwise conflicts resolving at the physical layer.

Наводиться аналіз протоколу випадкового множинного доступу з контролем несівної та виявленням конфліктів (МДКН-ВК) при розв'язанні парних конфліктів на фізичному рівні.

У сучасному суспільстві поширене застосування знайшли телекомунікаційні мережі з можливістю використання спільного каналу (каналів) зв'язку деякою множиною абонентів. При цьому вважається, що абоненти займають канальний ресурс епізодично, випадковим чином і взаємно незалежні, або ж ця залежність ґрунтується на спостереженні за станом каналу і є недетермінованою.

Зрозуміло, що якщо будь-яка система дозволяє використовувати спільні обмежені ресурси децентралізовано, то в ній неминуче виникають зіткнення і повторні передачі. В теорії обробки сигналів на теперішній час створена теорія багатокористувацького детектування [1]. В цій теорії стверджується, що за деяких додаткових умов можна успішно демодулювати

корисний цифровий сигнал в умовах адитивного впливу подібних йому завад. Тобто, існує можливість реалізації процедур успішного розв'язання конфліктів безпосередньо в демодуляторах приймальних пристроїв (згідно термінології семирівневої моделі взаємодії відкритих систем – на фізичному рівні).

В даній роботі пропонуються результати аналізу пропускної спроможності протоколу випадкового множинного доступу (ВМД) МДКН-ВК за додаткових умов - можливості розв'язання парних конфліктів на фізичному рівні та забороні обслуговування поодиноких заявок.

При цьому був застосований асимптотичний підхід у теорії масового обслуговування [2], який відіграє важливу роль при дослідженні різних математичних моделей, в тому числі таких, якими описується функціонування різних типів систем зв'язку з ВМД. Тут слід розуміти, що точні формули для рішень вдається отримати, як правило, лише у виняткових ситуаціях, що характеризуються накладенням обмежень на статистичну природу досліджуваних процесів. Однак часто, застосовуючи асимптотичні методи, можна отримати наближене рішення задачі при досить широких припущеннях щодо статистики потоку на вході та обслуговування навіть за відсутності «зручного» виду відповідних розподілів [2].

Було побудовано математичну модель відповідної системи масового обслуговування, у якій вимоги найпростішого потоку з параметром λ надходять в систему обслуговування з трьома обслуговуючими приладами на першому етапі з інтенсивностями μ_1 і трьома – на другому етапі з інтенсивностями μ_2.

Одержана відповідна система різницевих рівнянь досліджуваного процесу. Тут i - кількість заявок в джерелі повторних викликів (ДПВ), ν - стан процесу.

Позначаючи $P_\nu(i) \underline{\Delta} P(t,i,\nu) \underline{\Delta} P(i(t)=i,\ \nu(t)=\nu)$, маємо:

$$\begin{cases} P(t+\Delta t,i,0)=\left[1-(\lambda+i\sigma)\Delta t\right]P(t,i,0)+\mu_2\Delta t P(t,i,4)+3\mu_1\Delta t P(t,\ i-3,\ 3); \\ P(t+\Delta t,i,1)=\left[1-(\lambda+i\sigma)\Delta t\right]P(t,i,1)+\lambda\Delta t P(t,i,0)+(i+1)\sigma\Delta t P(t,\ i+1,\ 0); \\ P(t+\Delta t,i,2)=\left[1-(\lambda+2\mu_1+i\sigma)\Delta t\right]P(t,i,2)+\lambda\Delta t P(t,i,1)+(i+1)\sigma\Delta t P(t,\ i+1,\ 1); \\ P(t+\Delta t,i,3)=\left[1-(\lambda+3\mu_1)\Delta t\right]P(t,i,3)+\lambda\Delta t P(t,i,2)+(i+1)\sigma\Delta t P(t,\ i+1,\ 2)+ \\ +\lambda\Delta t P(t,\ i-1,\ 3); \\ P(t+\Delta t,i,4)=\left[1-(\lambda+\mu_2)\Delta t\right]P(t,i,4)+2\mu_2\Delta t P(t,i,5)+\lambda\Delta t P(t,\ i-1,\ 4); \\ P(t+\Delta t,i,5)=\left[1-(\lambda+2\mu_2)\Delta t\right]P(t,i,5)+2\mu_1\Delta t P(t,i,2)+\lambda\Delta t P(t,\ i-1,\ 5). \end{cases}$$

Якщо на першому етапі надходить більше двох заявок, то наступні спрямовуються безпосередньо в ДПВ, де можуть зберігатися необмежений час, породжуючи потік повторних викликів з інтенсивністю $i\sigma = x$.

На основі даної моделі отримано співвідношення для обслуженого навантаження та пропускної спроможності протоколу МДКН-ВК при розв'язанні парних конфліктів та забороні обробки поодиноких заявок. В результаті аналізу одержано рівняння стаціонарності у вигляді:

$$z^2\xi - z(9k\xi - 12k^2 + 9k^2\xi + 2\xi^2) + \xi^3 + 9k\xi^2 + 9k^2\xi^2 = 0.$$

Тут використано позначення: $\xi \underline{\Delta} \frac{\lambda}{\mu_2}$, $z \underline{\Delta} \frac{x}{\mu_2}$, $k \underline{\Delta} \frac{\mu_1}{\mu_2}$.

В доповіді наводиться графік залежності обслуженого навантаження як функції відношення *k* інтенсивностей обслуговування на першому та другому етапах. Зокрема, виявлено, що пропускна спроможність даного протоколу підвищується не менш ніж в 1,25 рази в порівнянні з протоколом МДКН-ВК, що не нехтує обробкою поодиноких заявок на другому етапі.

Література

1. Verdu S. Multiuser Detection. Cambridge: Cambridge University Press, 1998, 474p.
2. Назаров А. А. Асимптотический анализ марковизируемых систем. Томск: Издательство Томского университета, 1991.

УДК 621.39

АНАЛІЗ АРХІТЕКТУРНИХ ОСОБЛИВОСТЕЙ ВІРТУАЛІЗАЦІЇ ТА ПЕРЕВАГИ ВІРТУАЛЬНИХ КОНТЕЙНЕРІВ

Верес Л.А., Омельченко Р.Ю.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: aned@i.ua, enternadore@ukr.net

Analysis of architectural features of virtual containers and benefits of container virtualization

In this work the author has described container virtualization technology, also it shows the differences between server virtualization and OS-level virtualization and was given the advantages and disadvantages of using virtual containers.

Технологія віртуалізації наразі широко інтегрувалася в сферу інформаційних технологій. Віртуалізація дозволяє скоротити кількість фізичних серверів: замість декількох старих можна встановити один більш потужний і запустити потрібне число гостьових ОС у віртуальному середовищі, де вони будуть логічна ізольовані один від одного. До того ж таке середовище забезпечує гнучке адміністрування інфраструктури і підвищену відмовостійкість: в разі відмови одного з серверів кластера віртуальні машини автоматично «переїжджають» на інший сервер. Наявні технології дозволяють зробити це без зупинки сервісу, тобто непомітно для користувачів.

У серверній віртуалізації обчислень можна виділити два класи: гіпервізори з повноцінними віртуальними машинами і контейнери. Гіпервізори - це віртуалізація на рівні обладнання. Між хостовою і гостьовими системами є прошарок, що емулює апаратне забезпечення. Кожне гостьове середовище має власне ядро і заздалегідь визначений набір ресурсів.

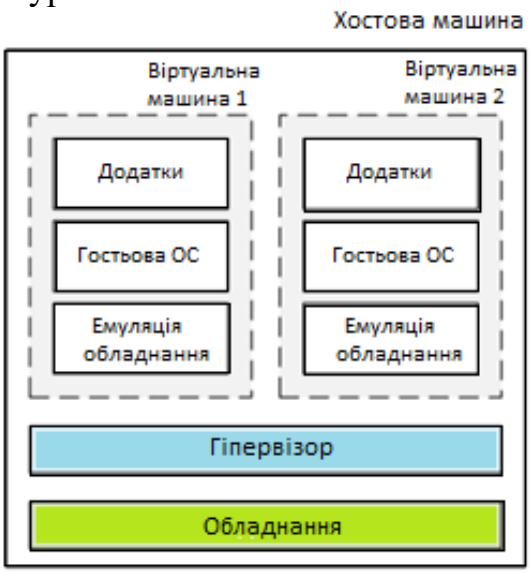


Рис. 1. Схема архітектури гіпервізора 1 типу

Завантаження численних копій ядра знижує щільність розміщення віртуальних машин на сервері. Час завантаження віртуальної машини становить кілька десятків секунд, що ускладнює оперативне виконання клієнтських запитів, коли потрібно швидко виділити додаткові ресурси [1].

Існує два основних типи гіпервізорів. Перший тип не вимагає наявності хостової ОС, містить в собі вбудовані драйвери пристроїв і планувальник. Архітектура системи, що використовує такий гіпервізор, зображена на рис. 1.

Другий же тип працює поверх хостової ОС і використовує її функціонал для таких операцій як управління пам'яттю, підтримка пристроїв вводу/виводу та інших. Архітектура системи, що використовує такий гіпервізор зображена на рис. 2.

Технологія контейнерної віртуалізації є так званою технологією «віртуалізації рівня операційної системи». Вона не використовує гіпервізор, але тим не менш надає можливість одночасного запуску декількох екземплярів ОС на одному обладнанні. Ці ОС використовують ядро хостової ОС, а їх одночасна робота забезпечується різними механізмами ізоляції і поділу ресурсів, за які відповідає ядро хостової системи і так званий віртуалізаційних прошарок (container engine). Архітектура системи, що використовує контейнерну віртуалізацію, представлена на рис. 3. [2]

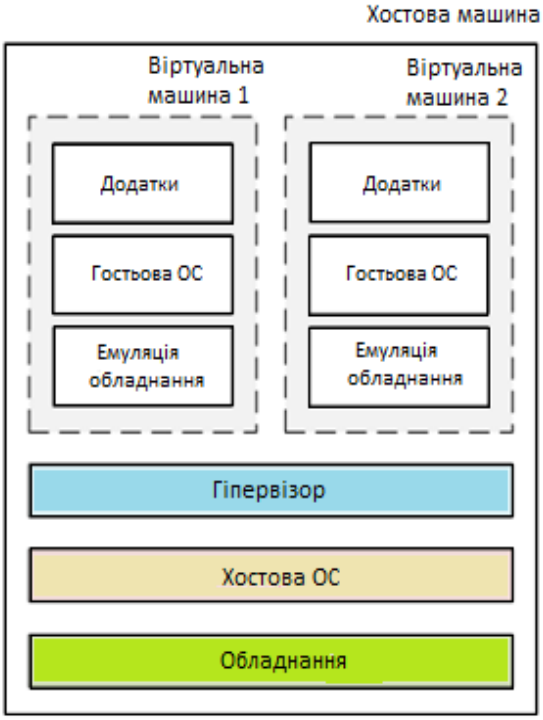


Рис. 2. Схема архітектури гіпервізора 2 типу

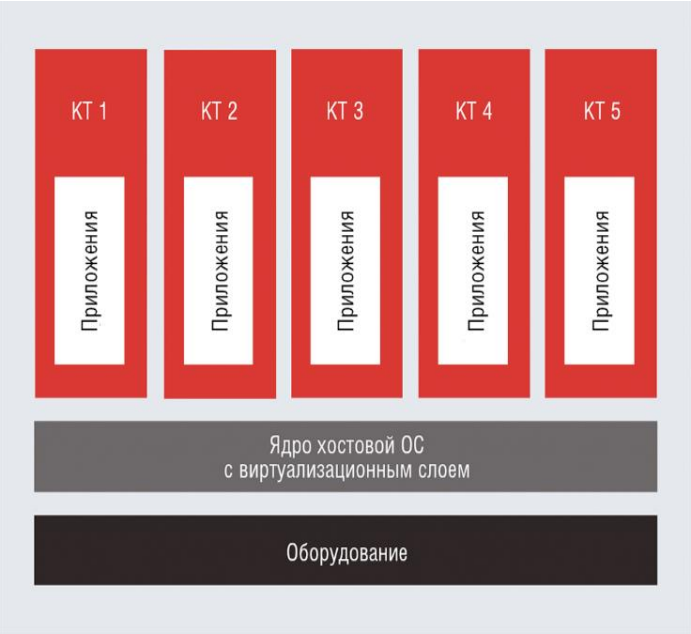


Рис. 3. Архітектура віртуального контейнера

В результаті Web-сервіси, упаковані в контейнери, можуть обслужити в кілька разів більше клієнтських запитів без необхідності підключати додаткове обладнання. Ці сервіси відмінно справляються з динамічним внесенням поправок в конфігурацію системи, забезпечуючи відповідність мінливої навантаженні при масовому наданні Web-послуг. Побудовані на основі контейнерної віртуалізації, вони демонструють вищу (до 50%) продуктивність, а це значить, що на одному і тому ж «залізі» можна реалізувати значно більше послуг.

На перший погляд віртуалізація і контейнеризація мають однакові характеристики. Однак, контейнери та віртуальні машини - це не одне і теж. Таким чином твердження, що віртуальні машини і контейнери працюють однаково, некоректно. Віртуальні машини і контейнери абсолютно різні за своєю природою технології, також вони вирішують різні проблеми віртуалізації. Ці відмінності видно на рис. 4.

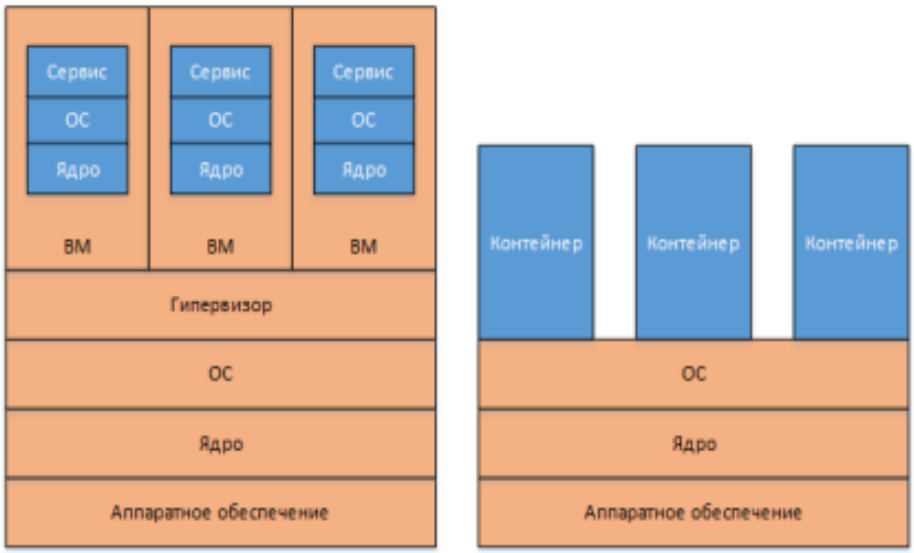


Рис. 4. Відмінності між апаратною віртуалізацією і віртуалізацією ОС

Таким чином, використання контейнерів має низку переваг. Оскільки контейнери використовують єдине ядро, це призводить, зокрема, до підвищення щільності їх розміщення, яка і без цього механізму спочатку вища, ніж у віртуальних машин, оскільки відсутні чисельні копії ядра. В результаті, у контейнерів щільність віртуальних середовищ, які можна запустити на сервері може бути до трьох разів вище, ніж у віртуальних машин, а на одному сервері цілком може розміщуватися кілька сотень контейнерів. Настільки висока щільність - одна з головних причин популярності контейнерів на ринку хостингу віртуальних виділених серверів.

Література

1. Рубанов В. Журнал сетевых решений/LAN 2017 № 01-02 Серверная виртуализация: гипервизоры против контейнеров / Владимир Рубанов. // «Журнал сетевых решений/LAN». – 2017.
2. Боттомли Д. Ажиотаж вокруг контейнеров / Джеймс Боттомли. // Журнал сетевых решений/LAN. – 2014. – №10.
3. Нанян С.М. Виртуальные контейнеры Docker: назначение и особенности применения / Нанян С.М., Ничушкина Т.М. // Инженерный вестник. – 2015. – №2.

УДК 261.396

МЕРЕЖА ПІДПРИЄМСТВА З ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ ASTERISK PBX НА ОСНОВІ ТЕХНОЛОГІЇ PLC

Письменний І.С., Романов А.О.
Факультет телекомунікацій та захисту інформації НАУ, Україна
Інститут спеціального зв'язку та захисту інформації
КПІ ім. Ігоря Сікорського, Україна
E-mail: pysmenniy95@gmail.com, anton3329@gmail.com

Enterprise network with software Asterisk PBX based on the PLC technology

Presents the software Asterisk PBX solution design in enterprise PLC network (Power Line Communication). The subject of the article is cross/connection of exchanges Asterisk PBX and hardware PBX.

Технологія VoIP (Voice over IP) має ряд переваг, на відміну від телекомунікаційної мережі загального користування PSTN (Public Switched Telecommunication Network). Найбільшою перевагою є економія витрат. Замість того, щоб оплачувати телефонні лінії і схеми, клієнти платять тільки за з'єднання даних. Крім того, IP-пакети можуть бути перенаправлені в будь-яке місце з підключенням до Інтернету. В рамках економії коштів співробітники можуть безкоштовно телефонувати в корпоративну мережу. Іншою перевагою є використання наявної мережевої інфраструктури, тому більше не потрібно використовувати традиційні телефонні кабелі для мережевого з'єднання УАТС. Також можлива конфігурація УАТС з будь-якого місця через CLI командного рядка або веб-інтерфейс [1,2]. Технологія VoIP характеризується сумісністю зі телефонною мережею загального користування PSTN. Крім того, голос в технології VoIP не вимагає високої пропускної здатності (декілька кбіт/с) і, отже, перебуває у фактичних викликах в корпоративній мережі, побудованої на основі технології PLC (Power Line Communication). Тому технологія PLC з недорогим програмним забезпеченням PBX Asterisk підходить для створення телекомунікаційної платформи для мереж малого і середнього бізнесу [3].

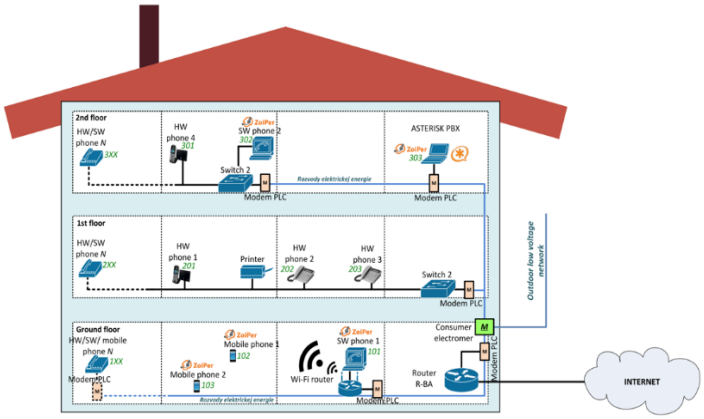


Рис. 1. PLC мережа підприємства

PBX Asterisk - вільно доступне програмне забезпечення на базі Linux. В доповнення, ця АТС дозволяє використовувати цифрову ISDN (Integrated Services Digital Network) і аналогові телефони, які все ще використовуються в багатьох компаніях. Asterisk також підтримує підключення до PSTN і інших мереж VoIP.

Приклад реалізації корпоративної мережі на базі програмного забезпечення PBX Asterisk і технології PLC представлено на рис.1.

Мережа PLC підприємства розташована на трьох поверхах. Поверхи з'єднані один з одним технологією PLC по лінії електропередачі в будівлі. До складу мережі входять програмні і апаратні IP-телефони, два комутатора, персональні комп'ютери, маршрутизатор R-BA, принтер і маршрутизатор Wi-Fi, який забезпечує підключення мобільних телефонів з додатком Zoiper. Router
R-BA використовується для підключення мережі PLC підприємства до зовнішніх мереж або Інтернету. Утиліта Asterisk працює на персональному комп’ютері. Нумерація і план IP-адресації забезпечують підключення до 100 IP-телефонів на кожному поверсі.

Однак, підприємствам потрібно не тільки швидке, але і безпечне спілкування як всередині однієї будівлі, так і між віддаленими офісами, які часто розташовані за кордоном. Для забезпечення якості і безпеки послуг використовується тунелювання [4,5].

Загалом, існує кілька протоколів тунелювання, які відрізняються один від одного в реалізації, можливості використання та безпеки. Найбільш поширеними протоколами тунелювання є: GRE, IPsec, PPTP, L2TP, 6to4, SSH і т.д. Однак, для підвищення ефективності функціонування мережі доцільно використовувати комбінацію протоколів тунелювання, наприклад, пари GRE і IPsec або L2TP і IPsec.

GRE (інкапсуляція загальної маршрутизації) була розроблена Cisco і документально підтверджена в RFC 2784. GRE створює віртуальний зв'язок «точка-точка» між віддаленими точками маршрутизаторами Cisco через IP-мережу. Завдяки цим протоколом, які працюють на рівні 3 моделі RM OSI, є можливість інкапсулювати різні типи пакетів в IP-тунель. На рис.2 показана структура інкапсульованого пакета. Перевага GRE полягає в підтримці одноадресної, широкомовної і багатоадресної передачі між кількома сайтами. Також GRE дозволяє передавати статичні і динамічні протоколи маршрутизації, такі як RIP, OSPF і т.д. Інші протоколи тунелювання не можуть забезпечити таку функціональність.

Рис. 2. Структура інкапсульованого пакету

IPsec (Internet Protocol Security) - це стандарт IETF, який визначає безпечний доступ до віртуальних приватних мереж, а також забезпечує передачу захищених IP-пакетів. IPsec працює на рівні 3 моделі RM OSI в двох режимах: в транспортному і тунельному режимах. Він реалізується з протоколом IPv4 і IPv6. Однак IPsec не може інкапсулювати пакети і протоколи маршрутизації. З цієї причини функціональність протоколу GRE поєднується з безпекою протоколу IPsec. Універсальний тунель GRE розміщений всередині безпечного тунелю IPsec, представлений на рис.3.

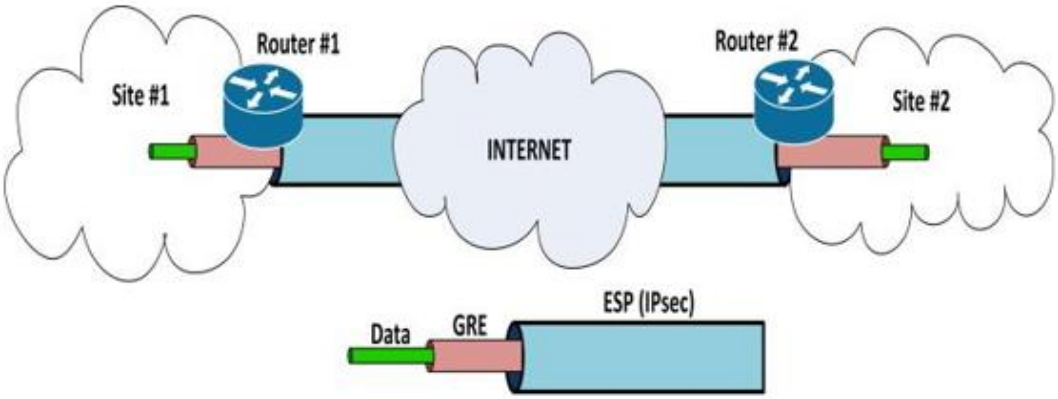


Рис. 3. GRE через IPsec

Таким чином, використання програмного забезпечення Asterisk PBX сумісно з PLC-мережею підприємства, дає можливість розгорнути повноцінну систему телекомунікацій з мінімальними витратами. Крім того, комплексне використання протоколів тунелювання, наприклад пари GRE і IPsec або L2TP і IPsec, через їх різну функціональність дозволяють збільшити ефективність мережі і забезпечити високий рівень безпеки інформації, яка циркулює за межами підприємства

Література

1. B. Hartpence, Packet Guide to Voice over IP, O'Reilly Media Inc., www.it-ebooks.info, Twitter: 2oreillymedia facebook.com/oreilly, Published by O´Reilly, Media, Inc. 1005 Gravenstein High North, Sebastopol, CA 95472, 2013, ISBN 978-1-449-33967-8.
2. M. Orgon, R. Roka, and J. Misurec,: Smart Grid and Power Line Communication, Publishing STU Bratislava, 396 pages, 2015, ISBN 978-80-227-4356-3.
3. J. Misurec and M. Orgon, Modeling of Power Line Transfer of Data for Computer Simulation, Int. J. Communication Networks and Information Security (IJCNIS) Vol. 3, No. 2, 2011, pp. 104-111, Pakistan, ISSN 2073-607X.
4. M. Orgon and I. Bestak, Performance Measurement of Encryption Algorithms used in PLC Devices, Int. J. of Research and Reviews in Computer Science. Vol. 2, No. 5, 2011, pp. 1218-1221, ISSN 2079-2557.
5. S. Klucik, J. Taraba, M. Orgon, and D. Adamko, The Use of PLC Technology in Broadband Services Offered to Households, Int. J. of Information and Computer Science (IJICTS), 2012, 4, pp. 1-8, ISSN: 2074-9007 (Print), ISSN: 2074-9015 (Online), MECS Publisher (http://www.mecs-press.org/), DOI 10.5815/ijicts.2012.04.01.

УДК 621.396.43

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В WI-FI МЕРЕЖІ СТАНДАРТУ 802.11

Єрмаков А.В., Постернак Б.С., Сарапулов С.В.
Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна
E-mail: yermak_antonio@ukr.net

Protecting personal data with 802.11 Wi-Fi network

Degree of protection off-wire networks. Methods of code mechanisms in the networks of Wi - Fi and code types.

Прилади стандарту 802.11 з'єднуються один з одним, використовуючи у якості переносника інформаційні сигнали, що передаються в спектрі радіочастот. Відомості переходять згідно радіомовлення відправником, який вважає, що радіоприймач крім того функціонує в обраному радіодіапазоні. Мінусом подібного пристосування вважається в цьому випадку, те, що будь-яка інша база, яка використовує даний спектр, також може здійснити ці відомості. У разі якщо не використовувати будь-який режим захисту, кожну базу вважаємо еталоною 802.11, яка взмозі обробити відомості, надіслані згідно з безпроводові місцеві мережі, в разі якщо тільки її радіоприймач функціонує в цьому ж радіодіапазоні. З метою надання хоча б одного мінімального ступеню захищеності потрібні наступні складові методи:

1. З метою прийняття постанови, що здатна застосовувати безпроводову LAN. Дана умова задовольняється за рахунок пристосування аутентифікації, яка забезпечує контролювання доступу до LAN.

2. Ресурси захисту даних, що подаються за допомогою безпроводової мережі. Дана умова задовольняється за рахунок використання алгоритмів кодування. У специфікації стандарту 802.11 регламентовано застосування механізму аутентифікації пристроїв з відкритим і до спільно використовуваним ключем та механізму WEP, що забезпечує захищеність даних.

Механізми кодування базуються в методах, які вважають за краще випадковим чином відомості. Застосовуються два типи шифрів: поточний та блочний шифри.

Шифри двох видів працюють, генеруючи першорядний потік (key stream). Ключовий потік змішується з відомостями, або не закритим словом, внаслідок чого ж утворюється кодований вихідний знак. Вище названі два типи шифрів розрізняються відповідно до розміру інформації, з якими вони можуть працювати в той же час.

Однопотоковий шифр виробляє безперервний проводовий потік, спираючись в значенні ключа. Наприклад, однопотоковий шифр здатний виробляти 15-розрядний ключовий потік з метою кодування однієї грані і 200-розрядним ключовим потоком з метою кодування другого. У рис. 1.1 проілюстрована діяльність поточного шифру. Більш популярним вважається однопотоковий шифр RC4, який і знаходиться в базі методу WEP. Блоковий шифр, навпаки, виробляє винятковий ключовий потік кодування зафіксованого обсягу. Розкритий документ ділиться в блоки чи будь-яке джерело, яке змішується з основним потоком незалежно. У разі якщо джерело прямого слова менш ніж джерело основного потоку, перший розширюється з вилученням блоку необхідного обсягу. У рис.1.2 проілюстрована діяльність блочного коду.

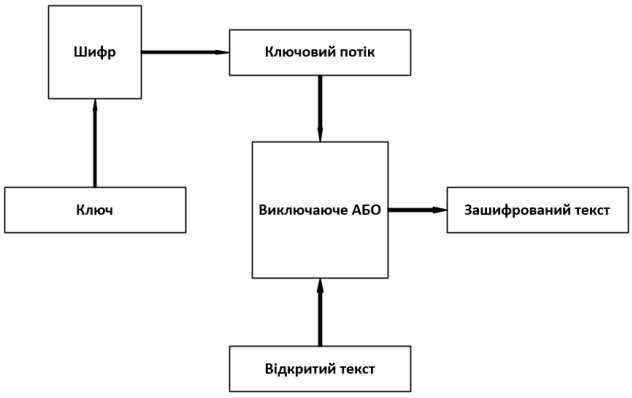


Рис. 1.1. Здійснюється потокове шифрування

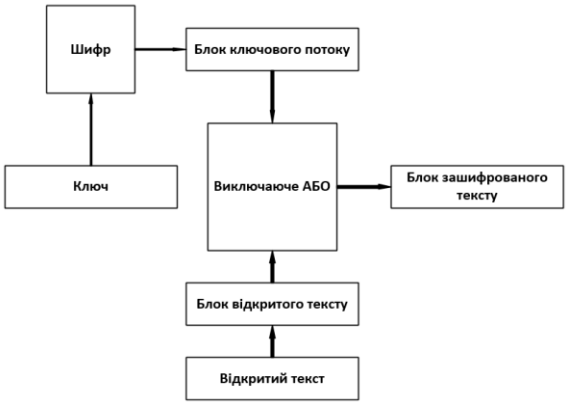


Рис. 1.2. Здійснюється блочне шифрування

Процедура кодування з механізмом поточних і блокових шифрів, називається порядком кодування с підтримкою бази електроних кодів (Electronic Code Book, ECB). Порядок шифрування ECB характеризується тим, що єдиний і цей же розкритий документ вже після кодування реорганізується в єдиний і цей же закодований документ.

Способи кодування дають можливість знайти рішення:

1. Вектори ініціалізації (initialization vectors, IV).

2. Режими зі зворотним зв'язком (feedback modes).

Вектор ініціалізації - це номер, що додається до ключа, кінцевим результатом цього вважається зміна даних основного потоку. Вектор ініціалізації весь час змінюється, в такому випадку те саме відбувається з основним потоком. У рис. 1.3 (а, б) представлені 2 сценарії. 1-ий належить до шифрування із застосуванням поточного коду в відсутності використання вектора ініціалізації. В даному випадку розкритий документ DATA вже після змішування з основним потоком 12345 постійно реорганізується в закодований документ AHGHE. Другий план демонструє, як той же

розкритий документ змішується з основним потоком, доповненим вектором ініціалізації з метою вилучення іншого зашифрованого тексту. Звернемо увагу на те, що закодований документ у другому випадку розрізняється в першому. Зразок 802.11 радить міняти вектор ініціалізації пофреймово (on a per-frame basis). Це означає, то що, якщо один і той же фрейм відданий двічі, досить високою виявиться можливість цього, то, що закодований документ стане різним.

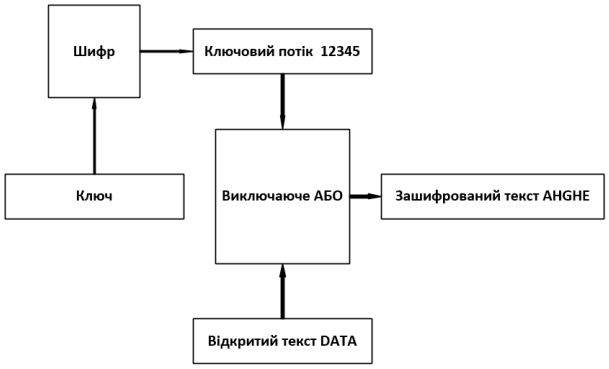


Рис. 1.3(а). Шифрування без вектора ініціалізації

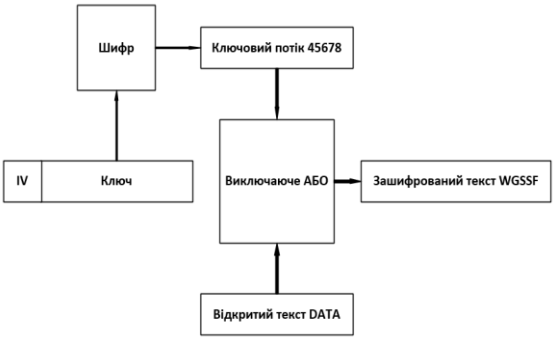


Рис. 1.3(б). Шифрування і вектори ініціалізації

Специфікація стандарту 802.11 передбачає гарантування захисту інформації з використанням методу WEP. Даний метод базується в застосуванні симетричного поточного коду RC4. Симетричність RC4 означає, те, що узгоджені WEP-шлюзи величиною 40 або 104 біт статично змінюються в клієнтських пристроях і в місцях доступу. Метод WEP був обраний ключовим способом внаслідок того, що він ніяк не вимагає занадто великих обчислень. Для того щоб виключити кодування в режимі ECB, WEP використовує 24-розрядний вектор ініціалізації, який додається до ключу перед виконанням оброблення згідно з методом RC4. Специфікація стандарту 802.11 вимагає, щоб схожі WEP-джерела були налаштовані як в клієнтах, таким чином і в пристроях інфраструктури мережі

Література

1. Свідоцтво про авторське право на твір №76226 від 24.01.2018 р. «Модель проектування бездротової мережі Wi-Fi на основі стандарту 802.11». Автори: Єрмаков А.В., Наритник Т.М., Авдєєнко Г.Л., Вальчук Д.С., Бондарчук С.О., Гошко А.П., Сердюк Д.О.
2. Свідоцтво про авторське право на твір №66937 від 29.07.2016 «Модель процесу управління захистом від перенавантажень мереж передачі даних». Автори: Романов А.І., Єрмаков А.В.

УДК 004.72

ПРОБЛЕМНА СИТУАЦІЯ РАДІОМОНІТОРИНГУ ТА НАПРЯМКИ ЇЇ ВИРІШЕННЯ

Макарова Д.О., Лопата Д.Г., Ільницький А.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: lodima17@gmail.com

PROBLEM OF RADIO MONITORING AND THE WAY TO SOLVE ITS

Considered the existing problems of radio monitoring in our time, in particular, problems with electromagnetic compatibility (EMC). The most widespread means and means of protection against electromagnetic disturbances are analyzed. An improved method for solving the problem is described.

В усі галузі економіки і різні сфери життя суспільства зростаючими темпами стали впроваджуватися мікроелектроніка, обладнання інформаційних технологій і засоби радіозв'язку, що володіють підвищеною чутливістю до електромагнітних завад.

Тому є необхідність посилити вимоги електромагнітної сумісності (ЕМС) і поширити регулювання в цій області на технічні засоби всіх видів і призначень, що піддаються впливу електромагнітних завад і є їх джерелами.

Забезпечення електромагнітної сумісності, тобто досягнення такого стану, коли електротехнічні, електронні і радіоелектронні апарати, системи і установки будуть придатні до виконання функцій з призначення при впливі перешкод, створюваних електротехнічними виробами і спричинені природними явищами, стало необхідною умовою науково-технічного прогресу, а отже, і стійкого розвитку економіки, суспільства і держави.

Будь-які електричні та електронні вироби, включаючи апарати, системи та стаціонарні і рухливі установки, здатні створювати електромагнітні завади і (або) чутливі до їх впливу, повинні бути виготовлені таким чином, щоб:
- створювані ними електромагнітні перешкоди не перевищували рівня, що забезпечує функціонування радіо- та телекомунікаційного обладнання та інших виробів відповідно до їх призначення;
- вироби мали достатній рівень власної стійкості до електромагнітних завад, що забезпечує їх функціонування відповідно до призначення.

Над проблемою ЕМС довгий час не замислювалися, поки не були зареєстровані збої в банківських системах при впливі перешкод. Сьогодні людина настільки залежить від використовуваної електро- та радіотехніки, що проблема забезпечення ЕМС стала для нього життєво важливою.

Практичне розв'язання проблем ЕМС спрощено зводиться до двох моментів: знання електромагнітної обстановки і завадостійкості обладнання, і в приведенні їх у відповідність один одному.

В даний час розширюється методична база, і створюються все більш досконалі засоби захисту від електромагнітних збурень.

Досвід експлуатації показує, що без застосування спеціальних захисних пристроїв (обмежувачів перенапруг) неможлива надійна експлуатація пристроїв електроживлення.

Забезпечення ЕМС радіоелектронних засобів (РЕЗ) представляє комплексну задачу, тому для її рішення не існує універсальних прийомів. В цілому це завдання можна ефективно вирішити лише за допомогою заходів різного характеру, що здійснюються на всіх етапах створення РЕЗ - від стадії проектування до експлуатації включно. Заходи, які використовуються для забезпечення ЕМС РЕЗ, діляться на дві групи - організаційні та технічні [3].

Технічні заходи являють сукупність системотехнічних, схемотехнічних, конструкторських і технологічних прийомів, спрямованих на вдосконалення характеристик радіоелектронних, електронних та технічних засобів. Застосування цих заходів має на меті зниження рівнів створюваних перешкод, збільшення їх ослаблення на шляху поширення, ослаблення сприйнятливості рецепторів до ненавмисних електромагнітних завад, ослаблення дії їх за рахунок вдосконалення способів передачі і обробки інформації.

Організаційні заходи полягають у поділі смуг частот між різними видами радіослужб, у виборі просторового розташування РЕЗ, обмеження потужностей передавачів і т.д. Вони включають також розробку і застосування деяких правил обмежувального характеру і ряд інших прийомів, спрямованих на впорядкування роботи різних РЕЗ з метою усунення ненавмисних електромагнітних завад. Організаційні заходи визначають напрямок розробки РЕЗ з урахуванням вимог ЕМС.

Граничний обсяг використовуваної частини радіочастотного ресурсу принципово обмежений: часом t функціонування РЕЗ, розташуванням в просторі V, смугою частот B, а також потужностями РЕЗ - джерел випромінювань і чутливістю рецепторів, які отримують сигнали.

Як зазначалося вище, розподіл, виділення і присвоєння частот є однією з організаційних заходів, що ефективно забезпечують ЕМС РЕЗ. При цьому, якщо розподіл і виділення ділянок спектру країнам, районам, службам і т. д. здійснюється на підставі вельми загальних міркувань, то присвоєння частот окремим РЕЗ проводиться з урахуванням технічних аспектів проблеми сумісності і вимагає відповідного обліку як місця розташування РЕЗ, так і його тимчасового режиму роботи.

Сутність вирішення проблеми ЕМС представляється у вигляді схеми, наведеної на рис. 1 [4].

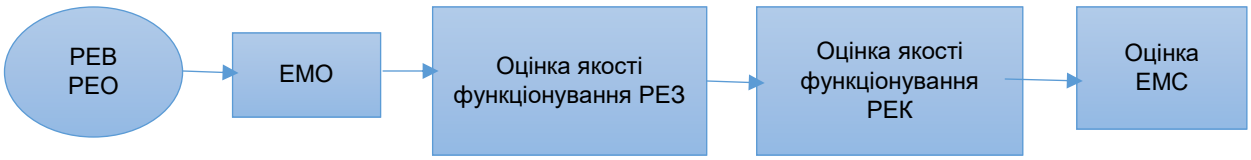


Рис. 1. Поетапна оцінка ЕМС

Спочатку з результатів електромагнітної взаємодії (ЕМВ) радіоелектронного обладнання (РЕО) проводитися оцінка електромагнітного обладнання (ЕМО), в результаті якої визначається детерміновані та імовірнісні характеристики корисних і заважаючих сигналів, які взаємодіють на приймально-аналізуючі тракти радіоелектронних систем. Причому ступінь взаємодії ненавмисних електромагнітних завад на якість функціонування РЕЗ, а через них на якість функціонування радіоелектронних комплексів (РЕК), розглядаються окремо. Після даних досліджень стає можливим проведення власне оцінки ЕМС.

Основним способом контролю та боротьби з РЕЗ є швидке отримання параметрів та визначання місця джерела завад [2].

Миттєва частота є однією з найважливіших характеристик сигналу у разі класифікації та розпізнаванні джерел радіовипромінювань. Більш того, у процесі визначення місцеположення джерел радіовипромінювань (моноімпульсного пеленгування) обов'язковою умовою є знання значення частоти сигналу, яке слід вимірювати з високою точністю і швидкодією [1]. Тому питання визначення миттєвого значення несучої частоти сигналів джерел радіовипромінювань в умовах високої апріорної невизначеності параметрів сигналів і обмеженого ресурсного потенціалу сил та засобів радіомоніторингу є актуальним науковим і практичним завданням.

На сьогодні завдання визначення несучої частоти сигналів джерел радіовипромінювань вирішується застосуванням відомих методів, які мають деякі переваги і суттєві недоліки [5].

Слід звернути увагу, що під час ведення радіомоніторингу отримуються не значення параметрів джерел радіовипромінювань, а їх оцінки, які повинні бути ефективними, незміщеними, оптимальними і однозначними.

Література

1. Уайт Д. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи: Пер. с англ. Вып. 1 / Под ред. А. И. Сапгира. - М.: Сов. радио, 1977. 348 с.
2. Теория и методы оценки электромагнитной совместимости радиоэлектронных средств / Под ред. Ю.А. Феоктистова. – М.: Радио и связь, 1988.5. Ильченко М.Е. Электродинамика диэлектрических резонаторов / М.Е. Ильченко, А.А. Трубин. - К.: Наук. думка, 2004. — 264 с.
3. Слободянюк П. В. Довідник з радіомоніторингу / П. В. Слободянюк, В. Г. Благодарний, В. С. Ступак; під. заг. ред П. В. Слободянюка. — Ніжин : ТОВ .Видавництво. Аспект-Поліграф., 2008. — 588 с.
4. Ільяшов О.А. Оцінка інформативності моніторингових ознак і сигнатур та міри їх невизначеності при розпізнаванні джерел та об'єктів моніторингу в інформаційному середовищі телекомунікаційних систем / О.А. Ільяшов // Вісник НТУУ .КПІ. Серія Радіотехніка. Радіоапаратобудування. — 2016. — № 67. — с. 77-83.
5. Радзиевский В.Г. Обработка сверхширокополосных сигналов и помех. / В.Г. Радзиевский, П.А.Трифонов. — М.: Радиотехника, 2009. — 288 с.

УДК 621.391:006

МОДЕЛЮВАННЯ ЗАТРИМОК ПАКЕТІВ ТОЧНОГО ЧАСУ

Бірюков М.Л., Тріска Н.Р.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nlbir2@ukr.net

The modeling of precise time packet delays

The precise time protocol (PTP) packet delays distribution depending on the conditions of data transmission in packet network has been analyzed. The statistical modeling of packet collisions between PTP and traffic packets for ITU-T defined traffic models was performed.

В сучасних телекомунікаційних мережах, що базуються на асинхронному, пакетному способі передавання, впроваджуються нові засоби забезпечення мережевої частотної та фазової/часової синхронізації. Це протокол обміну повідомленнями точного часу PTP (Precise Time Protocol – IEEE 1588 v.2) та його комбінація з технологією синхронного Ethernet (SyncE + PTP) [1, 2]. Алгоритм роботи буферної пам’яті елементів пакетної мережі (ЕМ) має суттєві відмінності від роботи проміжних пристроїв мережі з синхронним способом передавання в реальному часі. Тому практичний інтерес представляє оцінювання якості передавання пакетів з повідомленнями точного часу PTP (зокрема, величини затримки пакетів) в різних умовах роботи мережі.

Дослідження параметрів затримок пакетів провадилось експериментальними засобами [1, 2] та моделюванням. Вимірювання на мережах та в лабораторіях [3, 4] показали, що середня затримка та дисперсія пакетів зростає пропорційно навантаженню, наприклад, в мережі з 10 ЕМ затримка зростала майже в 4 рази від 180 до 650 мкс при збільшенні завантаження від 20 % до 80 %, відповідно. Середня затримка на ЕМ також зростає від 18 до 65 мкс. Точність передавання частоти пакетами PTP, оцінювана за максимальним відхилом часового інтервалу (МВЧІ), при зростанні навантаження в 1,9 рази може погіршуватись майже в 10 разів [4]. Взагалі при зростанні навантаження розподіл затримок може змінюватись досить довільно. Моделювання впливу трафіку виконувалось за наявності випадкової складової в часі обслуговування ЕМ пакетів PTP [5]. Зокрема, показано, що при випадковій складовій з експоненціально-розподіленим часом обслуговування, розподіл випадкової складової часу затримки двохстороннього обміну пакетами PTP відповідає розподілу Ерланга.

Рекомендації MCE-T G.8261 (08/13) та G.8261.1 (02/12) [6, 7] визначають декілька моделей завантаження, які мають забезпечити прийнятну якість частотної синхронізації пакетами PTP. З практичної точки зору, при проектуванні та оцінюванні відповідності пакетних мереж існує зацікавленість в можливості використати аналітичні співвідношення для оцінювання впливу рівня завантаження на якість передавання точної частоти

та часу. Для зменшення помилки частоти та часу необхідно, щоб пакети PTP мали точний період проходження тракту. З огляду на це, в даній роботі наведено результати статистичного моделювання з метою оцінювання ймовірності виникнення колізій, тобто таких ситуацій, коли мить зчитування пакету PTP припадає на той час, коли зчитування пакету загального трафіку ще не завершено, що призводить до вимушеного очікування.

При моделюванні розглядалась передача пакетів на інтервалі 1/16 секунди (62,5 мсек), що відповідає нижній швидкості обміну за протоколом PTP – 16 пакетів в секунду. Для обрахунків було обрано один варіант завантаження згідно Рекомендації MCE-T G.8261/Y.1361 (Додаток VI) [6] – Модель 1 (80 % трафіку становлять пакети по 64 байти, 5 % – пакети по 576 байт, 15 % – пакети довжиною 518 байт (див. табл. 1). Швидкість слідування пакетів становила 10^7 одиничних інтервалів в секунду. Модель буферної пам'яті елементу пакетної мережі (ЕМ) з трьома джерелами навантаження показана на рис. 1. На початковому етапі припускалася однорідна структура навантаження з довільним, випадковим вибором.

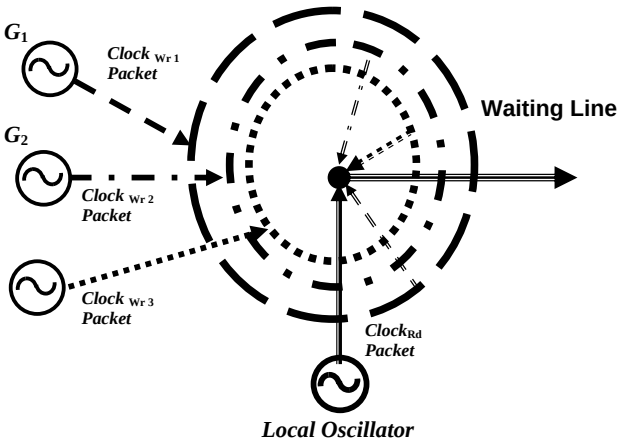


Рис. 1. Модель пам'яті елементу пакетної мережі

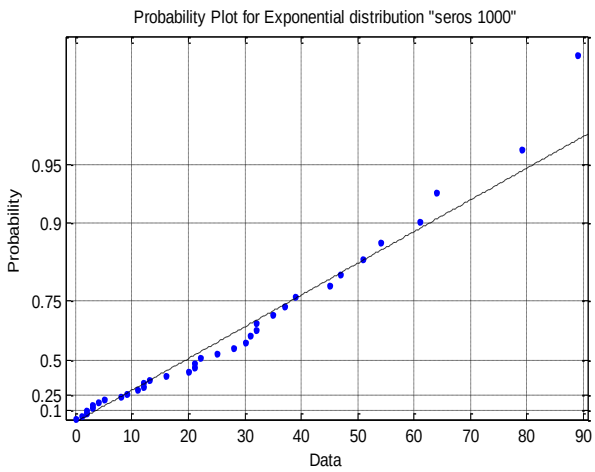


Рис. 2. Розподіл часових інтервалів між колізіями

З рис. 2 можна бачити, що часові інтервали між колізіями добре апроксимуються експоненціальним розподілом. Середньоквадратичний відхил експоненціального наближення до статистичних даних становить 0,93…0,95.

Розподіл кількості колізій пакетів PTP при 100-відсотковому завантаженні за результатами моделювання показано на рис. 3. Розподіл відповідає біноміальному розподілу та/або розподілу Пуассона та може бути обрахований пропорційно завантаженню відповідно до інтенсивності пакетів корисного трафіку. Інтенсивність колізій пакетів також можна апроксимувати розподілом Пуассона, як видно з рис. 4, де представлено розподіл часу між колізіями в одиничних інтервалах при 100-відсотковому завантаженні усіх бітів між пакетами PTP, які розділені 1/16 секундним інтервалом.

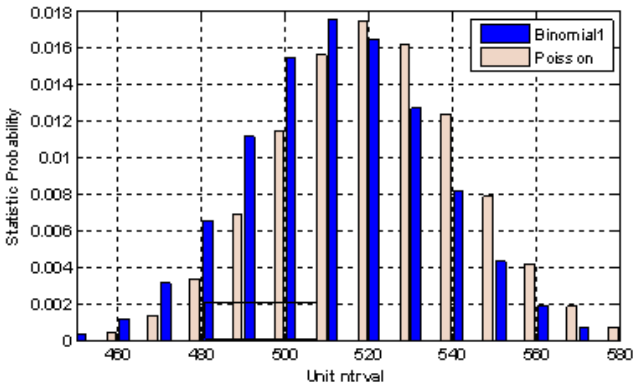


Рис. 3. Розподіл кількості колізій перекриття пакетів PTP при 100 % завантаженні 1/16 секундного інтервалу

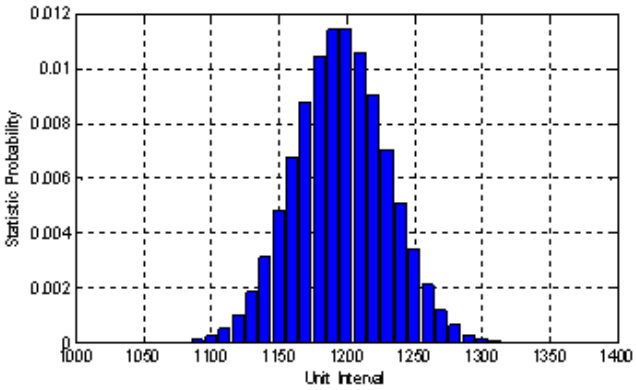


Рис. 4. Розподіл часу між колізіями пакетів PTP в одиничних інтервалах при 100% завантаженні 1/16 секундного інтервалу

При заданих припущеннях та вихідних даних, отримані результати мають свідомо завищені середні очікувані показники, але характер отриманих розподілів залишається незмінним зі зменшенням інтенсивності навантаження завдяки граничним властивостям розподілу Пуассона [8]. На наступному етапі планується дослідження тривалості очікування в залежності від розміру пакетів загального використання та їх впливу на фазові спотворення пакетів PTP. Для уточнення отриманих даних плануються натурні випробовування. Проведення досліджень в даному напрямку сприятиме пошуку оптимальних умов передавання сигналів точної частоти та часу в пакетних мережах.

Література

1. S. Ruffini et al. A novel SDN-based architecture to provide synchronization as a service in 5G scenarios. – IEEE Communications Magazine, March 2017. – pp. 210-215.
2. Бирюков Н.Л., Триска Н.Р. Синхронный Ethernet как основа частотно-временного обеспечения современных и будущих сетей связи. – Электросвязь, 2013, № 2. – С. 8-12.
3. www.symmetricom.com/products/ieee-1588-ptp-solutions.
4. Бирюков Н.Л., Макурин Н.А., Триска Н.Р Анализ использования двухстороннего протокола для подстройки сигналов тактовой синхронизации по сигналам времени. – “Наукові записки УНДІЗ”, № 4 (16), 2010. – С. 39-44.
5. N. Biriukov, N.Triska, M. Khudyntsev Evaluation of the two-way time stamps exchange in packet network. - 2017 4th International Scientific-Practical Conference “Problems of Infocommunications. Science and Technology (PIC S&T-2017), October 10-13, 2017 Kharkiv, Ukraine (IEEE Conference Record № 42018). Conference Proceedings. – Kharkiv, 2017. – p.342-345.
6. ITU-T Recommendation G.8261 (08/13) Timing and synchronization aspects in Packet Networks.
7. ITU-T Recommendation G.8261.1 (02/12) Packet delay variation network limits applicable to packet-based methods (Frequency synchronization)
8. Тихонов В.И. Статистическая радиотехника.–2-е изд., переработанное и доп. – М.: Радио и связь, 1982.–624 с.

УДК 621.391

АНАЛІЗ РІВНЯ БЕЗПЕКИ МЕРЕЖ СИГНАЛІЗАЦІЇ SS7

Романов О.І., Осокін М.Г.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, nikitos397@gmail.com

Security level analysis of SS7 signaling networks

The publication examines the risks associated with the vulnerability of the SS7 system, which leads to the leakage of information when using mobile and Internet services. An analysis of attacks and the effectiveness of using two-factor authorization for information security has been carried out.

Сьогодні більшість людей користуються мобільними та інтернет-послугами, зокрема соціальними мережами і поштовими скриньками. Для кожного важлива конфіденційність його листувань і інформації, в чому допомагає двофакторна авторизація [1].

Принцип отримання інформації зловмисником наступний. Необхідно знайти SS7-шлюз і підключитись до нього. Для цього існують багато способів потрапити в мережу через зламане операторське обладнання, GGSN або фемтостільники [2].

Далі, маючи доступ до SS7 і знаючи номер телефону жертви, можна підслухати розмову, визначити місце розташування людини, перехопити SMS для доступу до мобільного банку, відправити USSD-команду на платний номер і здійснити інші атаки.

Вразливості сигнальних мереж дозволяють здійснювати найрізноманітніші атаки. За допомогою команд SS7 MAP можна віддалено розблокувати стільникові телефони. Незахищеність SS7 загрожує не тільки користувачам мобільних телефонів, але і зростаючій екосистемі промислових і IoT-пристроїв, від банкоматів до GSM-систем контролю за роботою газових станцій. У подібних умовах забезпечення безпеки мереж SS7 - одна з першочергових задач при побудові комплексного захисту мобільного зв'язку.

Розглянемо дані, які зібрані спеціалістами Positive Technologies про безпеку мереж різних операторів станом на 2015 рік [3].

Загрози з боку потенційного порушника щодо мереж SS7 і абонентів мобільних операторів можна розділили на три класи:

- Шахрайство;
- Витік чутливої інформації;
- Збої в роботі.

Серед загроз інформаційної безпеки, що відносяться до класу витоку даних, можна виділити основні п’ять:

- Прослуховування дзвінків;
- Перехват SMS-повідомлень;
- Визначення місцезнаходження абонента в реальному часі;
- Крадіжка інформації про абонента.

У всіх мережах SS7, що увійшли до вибірки, були можливі: крадіжка інформації про абонента, перехоплення SMS, визначення місця розташування абонента.

Розглянемо основні і найефективніші методи атаки:

- Send Routing Info;
- Send Routing Info For SM;
- Send Routing Info For LCS;
- Send IMSI.

Відсоток успіху атак представлений на рис.1

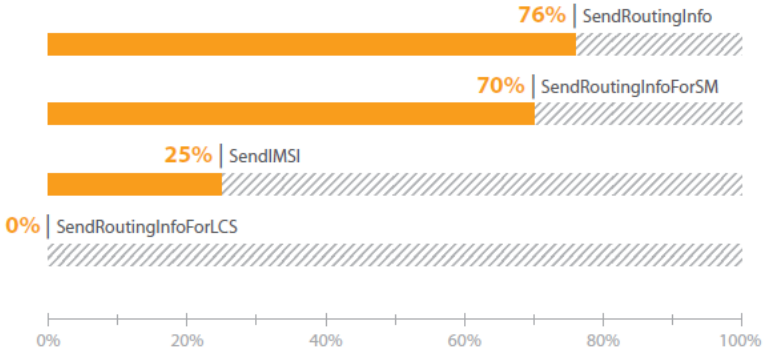


Рис. 1. Методи і доля успішних атак

Send RoutingInfo заснований на використанні вразливості, пов'язаної з відсутністю фільтрації невикористовуваних сигнальних повідомлень. Send Routing Info - повідомлення протоколу MAP, яке використовується про вхідний голосовий виклик і служить для запиту маршрутної інформації для локалізації абонента. Використовуючи даний метод, порушник може не тільки отримати інформацію про абонента, але і визначити його поточне місце розташування.

Send Routing Info For SM - повідомлення протоколу MAP, яке використовується при вхідному SMS-повідомленні і служить для запиту маршрутної інформації для локалізації абонента-отримувача. Це повідомлення повинно маршрутизироватися на обладнання SMS Home Routing, якщо воно встановлено в мережі оператора.

Send IMSI - повідомлення протоколу MAP, яке використовується для запиту ідентифікатора IMSI абонента за його телефонним номером. В даний час дане повідомлення практично не використовується операторами мобільного зв'язку, однак обладнання часто все ж обробляє його, відповідно до стандарту 3GPP.

Send Routung Info For LCS - повідомлення протоколу MAP, яке використовується в сервісах, що здійснюють розташування абонента, і служить для запиту маршрутної інформації. При нормальному режимі функціонування це повідомлення повинно передаватися тільки між елементами своєї мережі.

Розглянемо приклад атаки за допомогою Send Routing Info і фіктивного біллінгу. Атакуючий проникає в мережу сигналізації SS7, в каналах якої відправляє службове повідомлення Send Routing Info For SM (SRI4SM), вказуючи в якості параметра, телефонний номер абонента A, що атакується. У відповідь домашня мережа абонента A посилає атакуючому деяку технічну інформацію: IMSI (міжнародний ідентифікатор абонента) і адреса комутатора MSC, який зараз обслуговує абонента.

Далі атакуючий за допомогою повідомлення Insert Subscriber Data (ISD) впроваджує в базу даних VLR оновлений профіль абонента, змінюючи в ньому адресу білінгової системи на адресу своєї, псевдобіллінговой системи.

Потім, коли атакований абонент здійснює вихідний дзвінок, його комутатор звертається замість реальної білінгової системи до системи атакуючого, яка дає комутатору директиву перенаправити виклик на третю сторону, знову ж підконтрольну зловмисникові.

На цій третій стороні збирається конференц-виклик з трьох абонентів, два з яких є реальними (викликає А і викликається В), а третій впроваджений зловмисником несанкціоноване і має можливість слухати і записувати розмову.

Рекомендовані заходи для захисту:

- настройки конфігурації,
- впровадження додаткових засобів захисту,
- комбінацію цих двох методів.

Більшість недоліків, що дозволяють визначити місце розташування абонента, а також реалізувати крадіжку даних, можуть бути усунені в результаті зміни конфігурації мережевого обладнання [4]. Наприклад, якщо встановити заборону на обробку повідомлень Any Time Interrogation і Send IMSI на HLR.

Архітектурні проблеми протоколів і систем, що дозволяють здійснювати відмову в обслуговуванні, перехоплення SMS-повідомлень, перенаправлення викликів і прослуховування дзвінків, а також зміна профілю абонента, можуть бути вирішені шляхом фільтрації небажаних повідомлень (таких як Send IMSI, Send Routung Info For LCS, Send Routing Info). Необхідно реалізувати фільтрацію таким чином, щоб відсікалися тільки небажані повідомлення, які використовуються в рамках атак.

Таким чином, для забезпечення надійності систем SS7 необхідно використовувати двофакторну авторизацію в сукупності з сучасними методами захисту, уважно слідкувати за станом обладнання і його програмним забезпеченням.

Література

1. Signal System Number 7 (SS7) [Електронний ресурс] – Режим доступу: http://4g5gworld.com/wiki/signaling-system-number-7-ss7
2. Kim Zetter, The critical hole at the heart of our cell phone networks [Електронний ресурс] – Режим доступу: https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/
3. Positive Technologies, Эксперты Positive Technologies комментируют скандал со взломом украинских операторов связи [Електронний ресурс] – Режим доступу: https://www.securitylab.ru/news/454289.php
4. Романов О.І., Гордашник Є.С. Аналіз і класифікація атак в мережах IP-телефонії на базі SOFTSWITCH CLASS V. Матеріали десятої МНТК «Проблеми телекомунікацій», 2016 р. С 170-173.

УДК с

АНАЛІЗ СТРУКТУРИ СУБГАРМОНІЧНИХ ЗМІШУВАЧІВ ДЛЯ РАДІОЛІНІЙ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ

Наритник Т.М., Бондарчук С.О., Вальчук Д.С., Єрмаков А.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: bondserg8@ukr.net

Analytical review of subharmonic mixers for terahertz range radio links

The paper considers the main principles of subharmonic mixers design, shows their advantages. The mathematical model of subharmonic mixer is described. Conducted the work algorithm of frequency converter.

Пріоритетним напрямком розвитку телекомунікаційних систем є збільшення пропускної здатності. Цього можна досягти кількома шляхами, одним із яких є збільшення смуги частот, що використовується системою передачі інформації. Перехід у терагерцовий діапазон частот дозволить спростити процедуру виділення великих смуг частот, оскільки даний діапазон є практично не освоєним на даний час. Динамічний розвиток елементної бази радіоелектронних пристроїв надає можливість розробляти принципово нові пристрої та системи для роботи у даному діапазоні. Розробка радіотракту радіорелейної лінії терагерцового діапазону є актуальною задачею, оскільки така система буде мати суттєві переваги, такі як висока пропускна здатність, висока завадозахищеність і низьке споживання енергії [4].

Проте існує проблема із генерацією сигналів терагерцового діапазону, яка полягає у відсутності високостабільних опорних генераторів, що, в свою чергу, значно ускладнює процес реалізації приймально-передавального тракту. Одним із варіантів рішення даної проблеми є використання перетворювача частоти. Найбільшою його перевагою є простота реалізації, а такі проблеми як низька вихідна потужність таких перетворювачів можна вирішити використанням підсилювачів потужності, які на даний час активно розробляються, а на ринку уже існують робочі прототипи.

Перетворювач частот являє собою пристрій для переносу спектру сигналу в інший діапазон частот зі збереженням закону модуляції. Тому в перетворювачах використовується нелінійний елемент і гетеродин, що забезпечує режим роботи перетворюючого пристрою. В якості нелінійного елементу найчастіше використовується напівпровідниковий діод із бар'єром Шотткі. Іншим варіантом є використання резонансно-тунельного діода на основі двобар’єрної гетероструктури, що має антисиметричну вольтамперну

характеристику [1].

Розглянемо структурну схему субгармонічного змішувача (рис. 1). У ньому відбувається змішування сигналів радіочастоти (РЧ) або проміжної частоти (ПЧ) з другою гармонікою гетеродину. Таким чином, нелінійний пристрій (діод, металевий напівпровідниковий польовий транзистор та ін.) виконує як змішування, так і помноження частоти [2].

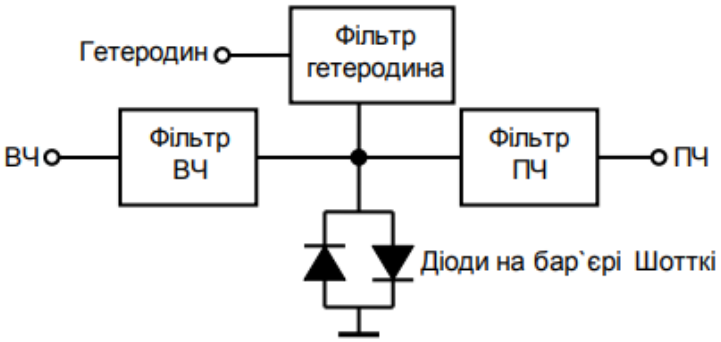


Рис. 1. Структурна схема субгармонійного змішувача

З метою реалізації субгармонійної схеми перетворювача з накачкою на половинній частоті в якості нелінійного елементу використані два діоди, що включені зустрічно-паралельно. Таке включення формує N-подібну результуючу вольт-амперну характеристику, симетричну відносно початку координат (рис. 2). Дана обставина зумовлює зміну параметрів нелінійного елементу з частотою вдвічі більшою ніж частота гетеродина [3].

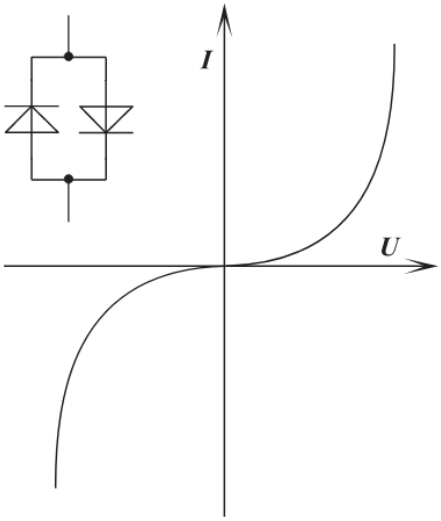


Рис. 2. Результуюча вольт-амперна характеристика двох зустрічно включених діодів Шотткі

Даний перетворювач може працювати як у режимі перетворення «вгору», так і у режимі перетворення «вниз», різниця полягає у тому, на які

входи будуть подаватися сигнали. Наприклад, для перетворення «вгору» корисний сигнал подається на вхід ПЧ, а вихідний високочастотний сигнал знімається на виході ВЧ. Розглянемо математичну модель такого змішувача при режимі перетворення «вгору» за умови, що результуючу ВАХ буде представлена у вигляді кубічної апроксимуючої функції.

Тоді $I_д = AU_д^3$, де $I_д$ - результуючий струм на виході діодного каскаду;
$U_д$ - результуюча напруга на виході діодного каскаду;
A - коефіцієнт пропорційності.

Напруга $U_д$ являє собою суму напруги сигналу гетеродину та напруги сигналу з входу ПЧ: $U_д = U_{пч\ макс} \cos(\omega_{пч}\ t + \varphi_{пч}) + U_{гет\ макс} \cos(\omega_{гет}\ t + \varphi_{гет})$. Після піднесення даної суми до кубу та виконання тригонометричних перетворень отримаємо одну із складових:
$0.75\ AU^2_{гет\ макс} U_{пч\ макс} \cos((2\omega_{гет} + \omega_{пч})t + \varphi_{гет} + \varphi_{пч})$.

Дана складова знаходиться на частоті, що є сумою 2 гармоніки гетеродину та частоти сигналу ПЧ. Звідси можна зробити висновок про один із основних недоліків даного методу – втрати потужності при перетворенні, оскільки з'являється коефіцієнт 0.75, а піднесення до квадрату завжди призводить до втрати потужності.

Отже, субгармонічний змішувач є хорошим варіантом вирішення проблеми перетворення частоти за умов відсутності високостабільного генератора. Переваги субгармонічного змішувача перекривають його недоліки, а збільшення елементної бази радіоелектронних пристроїв терагерцового діапазону дозволить ще більше спростити процес реалізації даного перетворювача.

Література

1. Madjar A. Novel General Approach for the Optimum Design of Microwave and Millimeter Wave Subharmonic Mixers // IEEE Transactions On Microwave Theory And Techniques – 1996. - VOL. 44, NO. 11. – P. 1997-2000.
2. Ильченко М.Е., Нарытник Т.Н., Радзиховский В.Н., Кузьмин С.Е., Лутчак А.В. Проектирование передающего и приемного радиотрактов радиорелейных систем терагерцового диапазона // Электросвязь. – 2016. – №2. – С. 42-49.
3. Авдєєнко Г.Л., Ільченко М.Ю., Наритник Т.М., Ємаков А.В., Лутчак О.В. Перетворювач частоти для прийомопередавача безпроводової телекомунікаційної системи фіксованого зв'язку терагерцового діапазону // Проблеми телекомунікацій. – 2017. - № 1(20). – С. 38-49.
4. Наритник Т.М. , Єрмаков А.В., Бондарчук С.О., Вальчук Д.С. Аналіз терагерцових технологій та їх застосування для створення інноваційних розробок // Проблеми телекомунікацій. – 2017. – № 1 (20). – С. 50 - 56.

УДК 391.39

ЗАБЕЗПЕЧЕННЯ QOS В TCP/IP МЕРЕЖАХ

Мєлєхова М.О., Носков В.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: maria.melekhova@gmail.com

Providing QoS in TCP / IP networks

Every moment traffic increases, so we need to implement stricter requirements for the quality of services. QoS can be organized using a wide range of instruments on different layers of the OSI model. Classification of the methods proposed in this paper will help for identifying of the methods that regulate the congestions more effectively.

Сучасні мережі висувають все більш жорсткі вимоги до якості обслуговування (QoS). Нові додатки для передачі відео і голосу в режимі реального часу пред'являють досить високі вимоги до якості послуг, що надаються. Затори виникають тоді, коли вимоги до смуги пропускання вище за можливості мережі. При передачі даних по мережі вимога до смуги пропускання мережі може перевищувати її можливості. Це призводить до затору в мережі.

Коли обсяг трафіку перевищує обсяг даних, який може передаватися по мережі, пристрої ставлять пакети в чергу або утримують їх в пам'яті до тих пір, поки ресурси не стануть доступні для передачі. Постановка пакетів в чергу призводить до затримки, оскільки нові пакети не можуть передаватися до тих пір, поки не будуть оброблені попередні. Якщо кількість пакетів, які повинні бути поставлені в чергу, продовжує збільшуватися, черги в пам'яті заповнюються і пакети відкидаються[1].

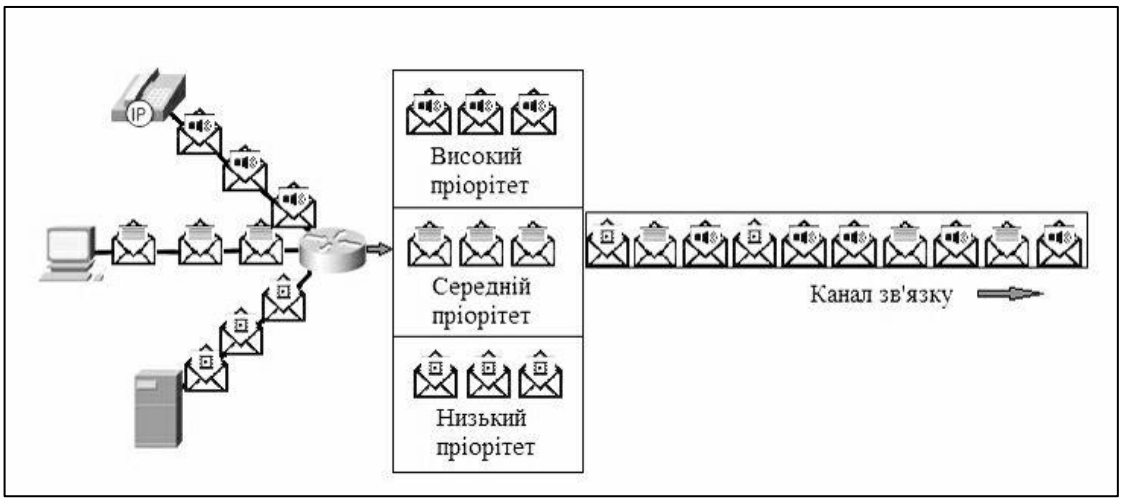


Рис. 1. Використання черг для пріоритизації з'єднань

Для забезпечення необхідної якості передачі трафіку використовують певні інструменти [2], наприклад:

1. *Класифікація і маркування.* Сеанси чи потоки аналізуються на належність певному класу трафіку. Після визначення класу пакети отримують відповідну мітку.

2. *Запобігання заторів.* Для класів трафіку виділяються фрагменти

мережевих ресурсів відповідно до політики якості обслуговування. Політика якості обслуговування також визначає порядок видалення, затримки чи перемаркування деякого трафіку для запобігання заторів. Основним інструментом запобігання перевантаження є Weighted Random Early Detection (WRED), він використовується для регулювання трафіку даних протоколу транспортного рівня Transmission Control Protocol (TCP) з метою оптимізації пропускної здатності і запобігання відкидання останнього елемента через переповнення черги.

3. *Управління заторами.* Коли обсяг трафіку перевищує доступні мережеві ресурси, трафік ставиться в чергу очікування доступних ресурсів (рис.1). Для управління заторами, наприклад на пристроях компанії Cisco, можна використовувати алгоритми Class-Based Weighted Fair Queuing (CBWFQ) і Low Latency Queuing (LLQ)[2].

Класифікація та маркування дозволяють ідентифікувати типи пакетів. Класифікація визначає клас трафіку, до якого належать кадри. Застосовувати політики можна тільки до ідентифікованого трафіку.

Класифікація пакета залежить від реалізації політики якості обслуговування. При класифікації потоків трафіку на рівні 2 і 3 використовуються інтерфейси, списки контролю доступу і карти класів. Трафік також можна класифікувати на рівнях з 4-го по 7-й за допомогою розпізнавання додатків за параметрами мережевого трафіку

Маркування означає додавання деякого значення у заголовок пакету. Пристрої, які приймають пакет, порівнюють значення цього поля зі значенням, визначеним політикою приоритезації. Маркування необхідно проводити максимально близько до вихідного пристрою. Вона встановлює межі довіри [3].

Рішення про маркування трафіку на рівні 2 і 3 має прийматися з урахуванням наступних факторів [2]:

- Маркування рівня 2 для кадрів можна виконувати для не тільки для IP-трафіку.
- Маркування рівня 2 для кадрів є єдиним можливим варіантом реалізації якості обслуговування для комутаторів 2го рівня.
- Маркування рівня 3 забезпечує наскрізну передачу даних про якість обслуговування.

Управління заторами передбачає планування і формування черг, які передбачають буферизацію зайвого трафіку або приміщення його в чергу на час очікування відправки такого трафіку на вихідному інтерфейсі або навіть його видалення. Засоби запобігання заторів легше реалізувати. Вони відстежують розподіл мережевого трафіку, намагаючись передбачити і запобігти затори в типових вузьких місцях у мережі і між мережами до того, як затор перетвориться в серйозну проблему. Вони пропонують пріоритетну обробку для високопріоритетного трафіку при виникненні затору, паралельно максимально збільшуючи використання пропускної здатності мережі і мережевих потужностей і зводячи до мінімуму втрату пакетів і затримки.

Шейпінг трафіку (рис. 2) зберігає зайві пакети в черзі, а потім планує подальшу передачу цих пакетів через певні проміжки часу. Результатом процесу шейпінгу трафіку є більш плавна інтенсивність відправки пакетів.

Для шейпінгу трафіку потрібна наявність черги і достатній обсяг пам'яті для буферизації затриманих пакетів, тоді як для полісінгу трафіку це не потрібно.

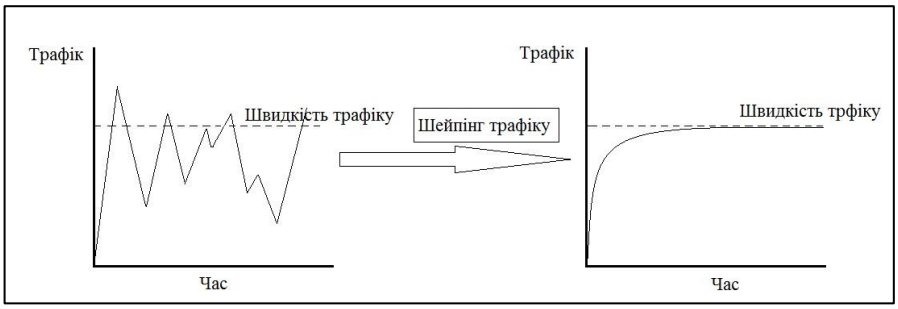


Рис. 2. Приклад шейпінгу трафіку

Полісінг, коли швидкість передачі трафіку досягає встановленого максимуму, зайвий трафік відкидається чи заново маркується. В результаті швидкість передачі має пилкоподібний графік з піками і падіннями (рис.3).

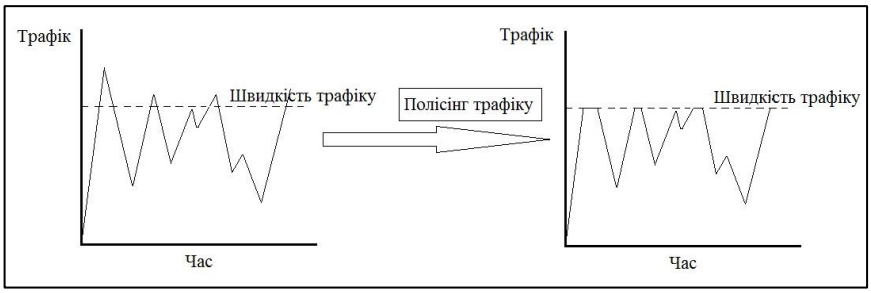


Рис. 3. Приклад полісінга трафіку

Організація черг пов'язана з управлінням вихідним трафіком. Пакети, які виходять через інтерфейс, поміщаються в чергу, і до них може застосовуватися шейпінг трафіку. До вихідного трафіку на інтерфейсі може застосовуватися тільки полісінг[4].

При включенні шейпінгу трафіку необхідно переконатися в наявності достатнього обсягу пам'яті. Крім того, для шейпінгу потрібно функція планування для подальшої передачі всіх відкладених пакетів. Ця функція планування дозволяє розбивати трафік в черзі на кілька черг. Функціями планування є, наприклад, CBWFQ і LLQ[2].

Таким чином, для забезпечення якості обслуговування в IP-мережах використовують наступні методи:

1. Класифікація та маркування, завдяки яким можна ідентифікувати типи пакетів.

2. Використання методів запобігання заторів визначає порядок видалення, затримки чи перемаркування деякого трафіку для запобігання заторів.

3. Управління заторами дозволяє мережі моніторити себе і підлаштовуватись під зміни в залежності від навантаження на мережу. Шейпінг дозволяє забезпечити "плавність" передачі даних, деякий час тримаючи пакети в буфері, що є перевагою особливо при передачі голосового трафіку. Полісінг же дозволяє відкидати пакети, аби при передачі не утворився затор. За допомогою цих механізмів використання мережевих ресурсів є більш ефективним, а можливість утворення заторів є меншою.

Література

1. Вегешна Ш. Качество обслуживания в сетях IP: Пер. с англ. – М.: Изд. дом Вильямс», 2003. – 368 с.
2. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCETN/CCNA ICND1 640-822 / Третье издание , 2013 - 720 с.
3. Олифер В., Олифер Н. Искусство оптимизации трафика / Журнал сетевых решений / LAN №12, 2001 - 38-47с.
4. Большаков С. Cisco QoS – классификация и маркировка / [Електронний ресурс] / http://twistedminds.ru/2013/02/cisco-qos-classifying-and-marking/, 2016.

УДК 621.391.63/621.316.5

АНАЛІЗ ВПЛИВУ ХРОМАТИЧНОЇ ДИСПЕРСІЇ В ОПТИЧНИХ ТРАКТАХ НА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Романишин В.С., Бердников О.М.
Інститут спеціального зв'язку та захисту інформації
КПІ ім. Ігоря Сікорського, Україна
E-mail: romanyshynvasyl@ukr.net

One of the most effective methods for solving this problem is the WDM (Wavelength Division Multiplexing) optical waveguide compaction method. The use of this method has allowed to increase the throughput of fiber-optic systems to a value greater than 10 Tbit / s, which will ensure that the needs of today and the next 3-5 years will be exceeded.

Для реалізації методу мультиплексування оптичних трактів (ОТр) по довжинах хвиль оптичного випромінювання (або хвильове мультиплексування – ХМ) були розроблені такі оптичні елементи: оптичні мультиплексори (ОМХ) і демультиплексори (ODMX), оптичні фільтри, напівпровідникові лазери з малою напівшириною лінії на фіксованій (заданій) довжині хвилі випромінювання, методи і засоби, які забезпечують необхідну стабільність оптичної частоти, оптичні підсилювачі з широкою полосою пропускання і інші активні та пасивні елементи. Для підвищення економічної ефективності регіональних і міських оптичних мереж доступу, в тому числі абонентських ліній в мережах загального користування, активно запроваджується технологія пасивної оптичної мережі ПОС (PON). Такі мережі включають тільки пасивні елементи, такі як оптичний кабель разом із з’єднувальними муфтами відгалужувачів, розгалужувачі, ОМХ і ODMX, оптичні фільтри, оптичні ізолятори і інші елементи [1, 2, 3].

Враховуючи еволюцію традиційних мереж у напрямку повністю оптичних мереж (AON – All Optical Network), вже зараз, особливо на етапі проектування телекомунікаційних транспортних систем ХМ (ТТС ХМ), необхідний підхід до вибору оптичних волокон. Відповідно до міжнародної системи класифікації, оптичні волокна (ОВ) розподіляються на два основних класи: А-багатомодові (MMF – Multi-ModeFiber) та В – одномодові (SMF – Single-ModeFiber). При цьому, як пояснює таблиця 1, категорія MMF волокна визначається матеріалом осердя і оболонки та профілем показника заломлення (ППЗ), а категорія SMF волокна– центральною довжиною хвилі та довжиною хвилі нульової дисперсії [3, 4].

На транспортній телекомунікаційній мережі (ТТМ) зв’язку України при побудові високошвидкісних ТТС ХМ переважно використовуються одномодові волокна, які в свою чергу поділяються на:

– стандартні волокна з незміщеною нульовою дисперсією (SF – Standard Fiber);

– волокна зі зміщеною нульовою дисперсією (DSF – Dispersion Shifted Single-Modefiber);

– волокна з ненульовою зміщеною дисперсією (NZDSF – Non ZeroDispersion Shifted Single Modefiber).

Таблиця 1. Категорії оптичних волокон згідно Рекомендації ITU-T

Клас ОВ	Кате-горія ОВ	Матеріал	Тип волокна	Номінальна довжина хвилі нульової дисперсії, нм	Номінальна довжина хвилі, нм
Багато-модові	A1	Скляна серцевина, скляна оболонка	З градієнтним ППЗ	-	-
	A2.1		З квазісхід-частим ППЗ	-	-
	A2.2		З східчастим ППЗ	-	-
	A3		З східчастим ППЗ	-	-
	A4	Полімерне волокно	С	-	-
Одно-модові	B1.1	Скляна серцевина, скляна оболонка	-	1300	1310
	B1.2		-	1300	1550
	B2		-	1550	1550
	B3		-	1300 та 1550	1310 та 1550

Для використання у ТТС ХМ оптичне волокно повинне задовольняти такі вимоги [5, 6]:

– низька дисперсія сигналу (для отримання високої швидкості передавання сигналів у ОТр), яка забезпечується компенсацією нахилу хроматичної дисперсії та зниженням поляризаційної модової дисперсії;

– низька нелінійність осередку волокна, що забезпечує передачу оптичних сигналів на великі відстані;

– однорідність оптичних характеристик, ТТС щільного ХМ;

– низька вартість та велика пропускна здатність.

Всі три типи ООВ близькі по значенню коефіцієнту затухання у вікнах прозорості одномодової передачі 1310 нм (1270…1350 нм) та 1550 нм (1470…1580 нм), але відрізняються своїми дисперсійними характеристиками. Хроматична дисперсія є досить важливим фактором, вплив якого посилюється зі збільшенням відстані та швидкості передавання оптичних сигналів, а також зростанням щільності розносу між центральними довжинами хвиль оптичних трактів.

Зважаючи на поширеність ТТС ХМ , найбільший інтерес викликають дисперсійні характеристики ООВ у вікні прозорості 1550 нм (1470…1580 нм), яке використовується оптичними мультиплексорами. Стандартні ООВ мають в робочому діапазоні довжин хвиль ТТС ХМ занадто велике значення хроматичної дисперсії, що обмежує швидкість передавання сигналів по оптичним трактам. За умови забезпечення ненульового (але близького до нуля та такого, що не перевищує визначену, достатньо малу

величину) значення хроматичної дисперсії та низької крутизни (нахилу) дисперсійної характеристики, найбільш придатними до використання у ТТС ХМ є волокна DSF та NZDSF, що пояснює рисунок 1.

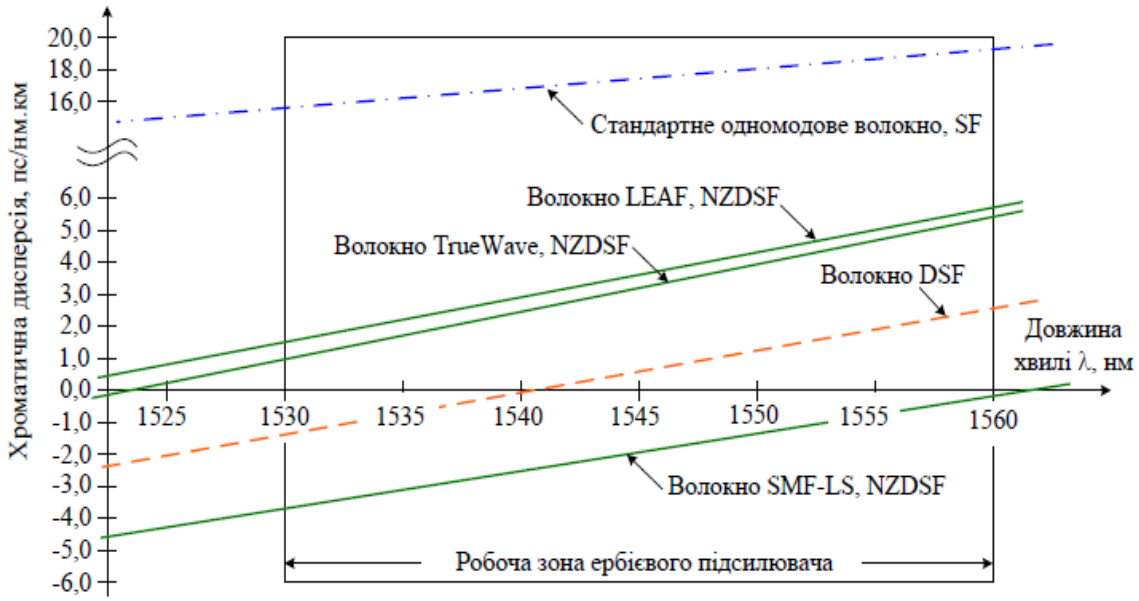


Рис. 1. Хроматична дисперсія ООВ у вікні прозорості 1550 нм, в межах області ербієвого волоконно-оптичного підсилювача підсилення (EDFA) 1530…1560 нм

Іншим важливим фактором, який обумовлює придатність оптичного волокна до використання у ТТС ХМ, є нелінійні властивості його осередку. Так, при розміщенні довжини хвилі нульової дисперсії в діапазоні довжин хвиль групового мультиплексного сигналу починають проявлятись небажані нелінійні ефекти (зокрема, чотирьох хвильове змішування), що призводять до викривлення оптичного сигналу. Тому, з точки зору мінімізації нелінійних ефектів, використовувати волокно DSF у ТТС ХМ не бажано.

Отже, найбільш прийнятним до використання є ООВ типу NZDSF (Non Zerodispersion Shifted Single Modefiber), відоме також як волокно з ненульовою зміщеною позитивною або негативною дисперсією, в якому вплив нелінійних ефектів зменшений, завдяки винесенню довжини хвилі нульової дисперсії за межі смуги пропускання EDFA.

На сьогодні виробництво таких волокон, наприклад, типу AllWave, LEAF, TrueWave, MetroCor, SMF-LS тощо здійснюється фірмами Lucent Technologies, Corning та Fujikura.

Література

1. Фриман Р. Волоконно-оптические системы связи. – М.: Техносфера, 2003. – 440 с.
2. Бейли Д. Волоконная оптика, теория и практика. – М.: Кудиц-обрез, 2006. – 326 с.
3. Слепов Н.Н. Современные технологии цифрових оптоволоконних сетей связи. – М.: Радио и связь, 2003. – 468 с.
4. Каток В.Б., Руденко І.Е., Ранський Є.Г., Однорог П.М. Волоконно – оптичний зв'язок. – К., Логос, 2015. – 380 с.
5. Хмелев К.Ф. Основы фотонного транспорта. – Киев: Техніка. 2008. – 680 с.
6. Бердников О.М., Хмельов К.П. Застосування технології *WDM* на телекомунікаційних мережах / Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2003. – № 3. – с. 5…11.

УДК 621.391

МОДЕЛЬ ОПТИМІЗАЦІЇ УПРАВЛІННЯ ТРАФІКОМ В МЕРЕЖАХ MPLS

Нестеренко М.М., Денисюк С.В.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: serhiy.denysiuk@gmail.com, nikolaiy.nesterenko@gmail.com

Optimization model for traffic management in MPLS networks

Traffic Engineering becomes a good decision for traffic optimization in modern MPLS networks and gives high parameters of quality of service QoS. One of the most effective approach is based on queuing balancing.

При оптимізації управління трафіком в мережах MPLS (Multi Protocol Label Switching), важливу роль відіграє технологія інжинірингу трафіку (Traffic Engineering, TE) для забезпечення параметрів якості обслуговування QoS. В свою чергу технологія MPLS для реалізації функції QoS використовує інтегровану службу забезпечення якості обслуговування Integrated Services (резервування смуги пропускання і ресурсів пристроїв для кожного з’єднання) і диференційовану службу Differentiated Services (на кожному мережевому вузлі задається правила обслуговування класів потоків даних з різними вимогами QoS) [1].

Одним з найбільш ефективних є підхід, заснований на балансуванні черг та принципах технології інжинірингу трафіку (Traffic Engineering Queues). А саме, використовуються механізми Differentiated Services. Основна ідея полягає в тому, що різні потоки класифікуються в інтегровані класи, потім маркуються. Далі, при пересиланні потокам забезпечують відповідну якість обслуговування для різного типу трафіку на кожному мережевому активному елементі в залежності від пріоритету на наявних ресурсів. Клас пакета (пріоритет) в заголовку IP-пакета відзначається за допомогою 6-бітової кодової комбінації (6-bit differentiated services code point - DSCP). [2].

LSR-пристрої мережі MPLS не аналізують зміст IP-заголовка і відповідно значення поля DSCP, як вимагає механізм DiffServ. Це означає, що відповідне значення PHB має бути отримано із значення мітки, проміжний заголовок MPLS має 3-бітове поле CoS.

Тобто поле (Class of Service – CoS) визначає пріоритет пакету. А саме перших 3 біта поля DSCP на кордоні MPLS мережі копіюються в поле Exp

заголовка MPLS, а кожний LSR-комутатор на маршруті LSP перетворює біти поля Exp в значення PHB.

Ця функція дозволяє встановлювати поле Exp MPLS замість того, щоб переписувати значення призначеного для користувача поля IP-пріоритету відкидання, що надає можливість зберегти IP-заголовок в початковому стані і використовувати його в подальшому. При передачі пакету по MPLS-магістралі клас CoS не змінюється.

Вважається, що число окремих трафіків M. Максимальне число черг на мережевому вузлу також фіксоване і дорівнює N [3].

Позначимо, a_i - інтенсивність трафіку i -го класу, що надходить на обслуговування мережевим вузлом; bj - частина пропускної здатності вихідного КС, яка виділена j -й черзі.

В ході управління чергами необхідно виконати умову відсутності перевантаження каналу зв'язку:

$$\sum_{j=1}^{N} b_j \le b, \tag{1}$$

де b - пропускна здатність вихідного КС.

Крім того, з метою запобігання перевантаження мережевого вузла необхідно забезпечити виконання наступного умови:

$$\sum_{i=1}^{M} a_i \le b. \tag{2}$$

Надати динамічний характер процесу обслуговування черг в рамках пропонованої моделі можна шляхом введення керуючої змінної xij, під якою малася на увазі частка i-го трафіку, що надходить для обслуговування в j-ю чергу. Згідно з фізичним змістом x_{ij} можуть маи місце такі умови:

$$x_{ij} \in \{0,1\} \quad (i = \overline{1,M},\ j = \overline{1,N}), \tag{3}$$

$$\sum_{j=1}^{N} x_{ij} = 1 \quad (i = \overline{1,M}), \tag{4}$$

$$\sum_{i=1}^{M} a_i x_{ij} \le b_j \quad (j = \overline{1,N}). \tag{5}$$

Виконання умови (4) гарантує відсутність втрат пакетів на даному мережевому вузлу.

Умова (5) вводиться для запобігання перевантаження пропускної здатності КС. В якості шуканого вектору виберемо вектор

$$\bar{x} = \begin{bmatrix} x_{ij} \\ -- \\ b_j \end{bmatrix} \quad (i = \overline{1,M}\,;\, j = \overline{1,N}\,), \tag{6}$$

в ході розрахунку якого вдається забезпечити узгодженість у вирішенні завдань обслуговування черг і динамічного розподілу пропускної здатності вихідного каналу зв'язку.

У загальному вигляді шукані умови матимуть вигляд:

$$\overline{n}_j \le n_j^{\max} \quad (j = \overline{1,N}\,), \tag{7}$$

і завдання тепер зводиться лише до вибору (обґрунтування) аналітичного виразу для розрахунку середньої довжини черги в процесі обслуговування.

Була запропонована модель балансування черг на вузлах MPLS-мережі. Новизна моделі полягає в тому, що вона на відміну від раніше відомих моделей враховує особливості технології Traffic Engineering Queues, націленої на забезпечення збалансованої завантаженості буферного ресурсу - черг мережевого вузла.

Література

1. Оліфер В. Г. Мистецтво оптимізації трафіку / В. Г. Оліфер, Н. А Оліфер // Журнал мережевих рішень LAN. - № 12.- 2001.
2. Зайченко Ю. П. Аналіз і оптимізація характеристик мереж MPLS за заданими показниками якості / Ю. П. Зайченко, Ахмед А. М. Шарадка // Вісник національного технічного університету України КПІ сер. Інформатика управління та обчислювальна техніка. Вип. 43, с. 113-123
3. Романов О.І., Пасько С.П. Оцінка часу затримки в мережах IP і MPLS при обслуговуванні повідомлень у складних багатотранзитних напрямках зв’язку. Наукові вісті Національного технічного університету …, 2011, № 5, С. 11-20.

УДК 621.391

ЗАГРОЗИ БЕЗПЕЦІ У SDN СЕРЕДОВИЩАХ

Роговий В.П.
Інститут телекомунікаційних систему КПІ ім. І. Сікорського, Україна
E-mail: vitalii.rohovyi@gmail.com

Security threats in SDN environments

Networks based on the Software-Defined Networking (SDN) technology has the same security problems as traditional analogues. The description of main network attacks typical to SDN networks is presented in this paper.

Мережі, що працюють на базі технології програмно-визначених мереж (SDN) все ще мають такі ж вимоги до безпеки, що й традиційні мережеві інфраструктури, так як вони переносять таку ж приватну та конфіденційну інформацію. SDN повністю змінює архітектуру та міжкомунікаційні особливості компонентів в мережі - з цього виникає зовсім новий «стартовий майданчик» для зловмисників, які бажають атакувати SDN-мережі. Це призводить до необхідності підтримання аналогічного рівня безпеки як при використанні традиційних мереж, але потрібно ще зважати на небезпеки програмної природи. Далі у статті будуть приведені деякі загрози, що становлять небезпеку й в SDN мережах.

A. DDoS / DoS атаки.

1) DDoS (Distributed Denial-of-Service): численні типи звичайних атак DDoS можуть виконуватися і в SDN середовищі, але це вже буде варіація атаки з використанням підроблених записів потоку, яка може бути націлена супротивником на контролер, а саме на компрометування його доступності. Флудінг контролеру запитами щодо рішення вибору потоку призводить до того, що обчислювальні ресурси контролеру можуть перевантажитись, і контролер не зможе відповідати на коректні запити. Якщо атакованою буде централізована точка керування мережею, а саме таким пристроєм є SDN-контролер, то частина мережі, що підпорядкована цьому контролеру буде доступною тільки деякий малий період часу, поки мережеві пристрої (МП) по тайм-ауту не опитають контролер щодо нових правил у мережі. Після того, як МП не отримали відповідь контролеру під атакою, вони чи обнуляють свої таблиці комутації/маршрутизації, чи використовують попередні версії цих таблиць. Це призводить до «падіння» мережі.

2) DoS (Denial-of-Service): на рівні площини даних інші МП можуть бути підвержені флудінгу помилково створеними записами потоків, котрі займають все вільне місце в таблиці потоків. Це призведе до того, що маршрутизуючі МП не зможуть додати будь-які коректні записи потоків в свої таблиці і частина мережі стане розрізненою. Одна з основних проблем з пристроями на рівні площини даних в мережах SDN полягає в неможливості комутаторів розрізняти коректні запити щодо потоків від скомпрометованих.

B. Викрадений / підроблений контролер. Контролер можна розглядати як централізований "мозок" мережі SDN. Він контролює всю мережу з однієї точки, що робить це найважливішою особливістю SDN архітектури. Зловмисник, якому вдається скомпрометувати контролер по суті контролює всю мережу. Можливість контролювати дії контролера дозволить зловмиснику маніпулювати даними потоків будь-яким способом, який він обере, наприклад, може припини передачу певних типів даних на деякі кінцеві вузли та перенаправити їх на «свої» пристрої. Таким чином захоплені мережеві пристрої починають працювати як вузли «man-in-the-middle» або «black hole / grey hole».

Це дозволяє злодію маніпулювати вмістом будь-якого пакету, що отримує скомпрометований пристрій. Також зловмисник може успішно зареєструвати "підроблений" контролер в площині управління мережі. За допомогою цього контролера зловмисник може мати можливість впливати на доступність інших контролерів в мережі, змінювати правила, встановлені в кеш-пам'яті та ефективно зупиняти / маніпулювати роботою додатків в площині додатків.

C. Шкідливі додатки. Враховуючи можливість фреймворку SDN інтеграції сторонніх програм, існує проблема встановлення зловмисних програм на контролер. Дії додатків, що показують шкідливу поведінку в межах SDN середовища, можуть мати катастрофічні наслідки.

Додатки, що займаються глибоким аналізом пакетів можуть стати потенційними носіями ризику для мережі - вони можуть бути в змозі опосередковано контролювати всю мережу через інформацію, яку зібрали під час аналізу пакетів.

Збільшений об'єм даних та спосіб, яким він централізовано локалізується є тим, що дає можливість шкідливим програмам загрожувати цілісності та конфіденційності інформації про користувача / мережу.

D. Атаки на площину управління-даних. Ще одне місце SDN, яке дає можливість здійснити атаку – це абстрактне місце між площинами управління та даних. Специфікація OpenFlow передбачає використання TLS (Transport Layer Security) опціонально, що робить цю площину уразливою до безлічі типів атак, таких як man-in-the-middle, black hole тощо.

1) Атака man-in-the-middle: атаки цього типа відбуваються коли скомпрометований мережевий пристрій встановлюється / стоїть між контролером та шляхами передачі даних на площині даних. Замість безпосереднього пересилання повідомлень до контролера (або навпаки), вузол "man-in-the-middle" може маніпулювати / перевіряти вміст пакетів [13].

2) Атака Black hole : атаки такого типу відбуваються, якщо скомпрометований мережевий пристрій встановлюється між пристроєм, на який спрямована атака, і контролером, і просто відклоняє будь-які отримані ним пакети, не пересилаючи їх до контролера. Це призводить до проблем у мережевих комунікаціях та наданні послуг, що становляться недоступними реальним користувачам.

E. Підслуховуючі атаки. Зловмисники, які намагаються отримати незаконний доступ до мереж SDN або зупинити доступність служб, можуть вдаватися до підслуховування трафіку (акт незаконного захоплення та перевірки пакетів, що передаються через мережу) на певних підключеннях в мережі. Це може дозволити їм зібрати суттєву інформацію, яка потім може бути використана для здійснення більш потужних атак. Атаки з підслуховуванням тривалий час проводилися в традиційних мережевих інфраструктурах - бездротові архітектури особливо вразливі через передачу даних по повітрю. Проте, в контексті SDN, підслуховування можна здійснювати з метою перевірки пакетів на площині управління-даних, а також виключно на площині даних. На площині даних режим "підслуховування", що інтегрований у комутатори OpenFlow, може бути використаний зловмисником, який міг скомпрометувати комутатор, щоб перевірити пакети, передані навколишніми комутаторами. У певному сенсі підслуховування, яке здійснюється на площинах даних та управління, є більш пасивною атакою і не впливає безпосередньо на доступність, конфіденційність чи цілісність даних. Однак, така атака дає змогу зловмисникам здійснювати додаткові атаки на базі зібраних даних.

F. Порівняння типів атак. Нижченаведена таблиця підсумовує наведені вище атаки і дозволяє побачити площини абстракції, які можуть знаходитися під впливом визначених типів атак в SDN-архітектурі, та конкретні аспекти безпеки, які вони потенційно можуть скомпрометувати.

Таблиця 1. Підсумок впливу атак на площини SDN

Тип атаки	**Уразлива площина SDN**	**Вражені аспекти безпеки**		
		Доступність	*Конфіденційність*	*Цілісність*
DDoS	Управління, даних	+		
DoS	Управління, даних	+		
Викрадений / підроблений контролер	Управління, даних, додатків	+	+	+
Шкідливі додатки	Управління, даних		+	+
Man-in-the-middle	Управління, даних, управління-даних		+	+
Black hole	Управління, даних управління-даних	+	+	
Підслуховування	Управління, даних, додатків		+	

Література

1. Jakob Spooner A Review of Solutions for SDN-Exclusive Security Issues // IJACSA // Jakob Spooner, Dr Shao Ying Zhu // Vol. 7, No. 8, 2016. – P. 113-122.
2. “OpenFlow Specification 1.5.1” - Open Networking Foundation, March 15, 2015.

УДК 621.39

АНАЛІЗ ІСНУЮЧИХ АЛГОРИТМІВ РОЗПОДІЛУ НАВАНТАЖЕННЯ НА МОБІЛЬНІ МЕРЕЖІ НА ОСНОВІ ХМАРНИХ ІНФРАСТРУКТУР

Полонський А.М., Міночкін Д.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: andriy.polonskiy@gmail.com

Analysis of existing algorithms of load-balancing in mobile network based on cloud infrastructure

Analyzed the main tendencies of cloud computing development in terms of mobile networks. Reviewed existing ways of load balancing in mobile networks based on modern infrastructures and technologies.

Хмарні обчислення як основа для побудови та використання перспективних мобільних мереж можуть суттєво вплинути на ситуацію в цій сфері. Враховуючи останні тенденції в швидкості розповсюдження мобільних пристроїв, таких як планшети та мобільні телефони, та розвиток мобільної інфраструктури користувачі все більше мають постійний доступ в інтернет.

Інтеграція хмарних обчислень в мобільне середовище породило новий термін «мобільні хмарні обчислення» MCC (mobile cloud computing), які вважають перспективним напрямком розвитку у мобільних обчисленнях та з великим потенціалом. MCC, використовуючи потужну обчислювальну платформу хмарних обчислень, дозволяє розвантажити обчислювальні потужності і вимоги до сховищ даних в мобільних пристроях, подолати розрив між збільшенням обчислювальних вимог і технологіями традиційних мобільних обчислень з обмеженими ресурсами мобільних пристроїв на проведення обчислень, зберігання даних та енергії [1].

З іншого боку, потужні технології хмарних обчислень можуть бути корисними для мереж радіодоступу RAN (radio access networks), що призвело до появи нової концепції хмарних мереж радіодоступу C-RAN (cloud radio access networks). На відміну від існуючих мереж стільникового зв'язку, де обчислювальні ресурси для обробки сигналів основної смуги частот розташовані в кожному стільнику, в C-RAN обчислювальні ресурси знаходяться в центрі безпроводової хмари-мережі з пулом, що має потужні ресурси обчислень [1].

В свою чергу виникає проблема розподілу навантаження на таку мережу. В даний момент цю проблему вирішують за допомогою декількох способів.

Навантаження комірки вимірюється з точки зору використання різних ресурсів у межах їх доступних лімітів [2].

Це загальна потужність передачі, загальна отримана потужність, втручання в комірку, пропускна здатність комірки у низхідній / висхідній лінії зв'язку, збільшення блокування, частота відмов у передачі.

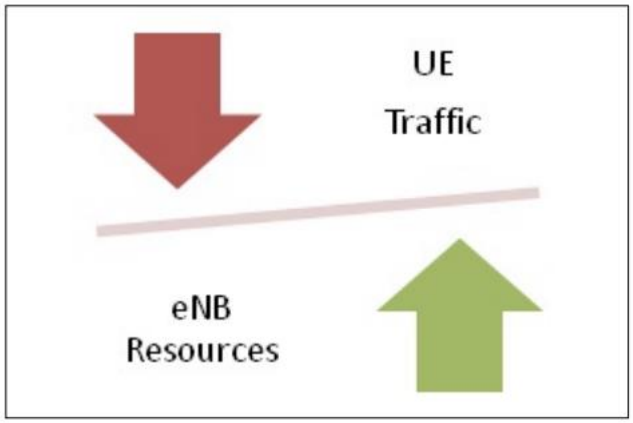


Рис. 1. Розподіл навантаження в стільникових мережах

Активне балансування навантаження дозволяє активним UE (User Equipment - обладнання користувача) бути збалансованим по всіх елементах, щоб знизити загальні затори в камерах. Перевага активного розподілу навантаження полягає в тому, що система має прямий механізм вимірювання та знання вимог до трафіку кожного користувача та стан радіостанцій, перед прийомом рішення про розподіл навантаження. Таким чином, за допомогою планувальника та інтерфейсів інших базових станцій (інтерфейс X2 для інтерфейсу LTE та / або S1 для inter-RAT), можна приймати точні рішення для завантаження на основі HO. Код причини на основі навантаження (HO) включається під час передачі повідомлень на передачу (HO), щоб дозволити цільовій комірки дізнатися усе для контролю надходження.

Автори Інь та Лін пропонують механізм балансування навантаження з багатьма шляхами, названий як MALB [3]. MALB ітеративно регулює трафік на кожному виявленому маршруті. Регулювання швидкості руху використовується для мінімізації середньої затримки від мережі до кінця [4]. Подібний механізм пропонується в [5] для протоколів багатоканальної маршрутизації джерел. У [6] Ву та Хармс описали зв'язок між двома вузлами непересічних шляхів як число зв'язків між вузлами на окремих шляхах. Результати, показані в [6], демонструють гіпотезу про те, що при збільшенні кореляції зростає затримка від кінця до кінця по обидва числа маршрутів. Для зменшення затримки від кінця до кінця пропонується протокол маршрутизації, який забезпечує балансування трафіку на найменш

корельованих шляхах [6].

Проте, в одношляхових підходах, між джерелом-цільовою парою вузлів встановлюється лише шлях. Було запропоновано декілька універсальних механізмів балансування навантаження, такі як різні метрики маршрутизації, як у [7], кешування пакетів, як у [8], спрямовані антени, як у [9] та ін. Автори Жу і Хассанін [10] представили новий протокол маршрутизації під назвою LBAR. LBAR містить метрику маршрутизації, яка враховує ступінь активності вузла, що є числом активних шляхів через вузол.

Література

1. Міночкін Д.А., Кравчук С.О. Застосування розподілених обчислень в телекомунікаційних системах // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2015. – № 50. – С. 41– 44
2. Sumita Mishra, Nidhi Mathur Load Balancing Optimization in LTE/LTE-A Cellular Networks: A Review [Електронний ресурс] // arxiv.org: портал електронних статей. URL: https://arxiv.org/pdf/1412.7273.pdf
3. D.Maheshwar, R. Nedunchezhian, Load Balancing in Mobile Ad Hoc Networks: A Survey [Електронний ресурс] // semanticscholar.org: портал електронних статей. URL: https://pdfs.semanticscholar.org/8c61/adf76723447f9573fbd50c221307025e65f8.pdf
4. S. Yin, X. Lin, MALB: MANET adaptive load balancing, in: IEEE Vehicular Technology Conference (VTC2004-Fall), vol. 4, September 2004, pp. 2843– 2847.
5. L. Zhang, Z. Zhao, Y. Shu, L. Wang, O.W., W. Yang, Load balancing of multipath source routing in ad hoc networks, in: Proceeding of the IEEE International Conference on Communications (ICC 2002), May 2002.
6. K. Wu, J. Harms, Performance study of a multipath routing method for wireless mobile ad hoc networks, in: Proceeding of the Ninth International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS'01), August 2001.
7. L. Wang, L.F. Zhang, Y.T. Shu, M. Dong, O.W.W. Yang, Multipath source routing in wireless ad hoc networks, in: Proceeding of IEEE CCECE, 2000, p. 479.
8. A. Valera, W. Seah, S.V. Rao, Cooperative packet caching and shortest multipath routing in mobile ad hoc networks, in: Proceeding of IEEE INFOCOM, 2003.
9. S. Roy, S. Bandyopadhyay, T. Ueda, K. Hasuike, Multipath routing in ad hoc wireless networks with omni directional and directional antenna: a comparative study, in: Proceeding of the Fourth International Workshop on Distributed Computing, Mobile and Wireless Computing (IWDC), 2002, pp. 184–191.
10. A. Zhou, H. Hassanein, Load-balanced wireless ad hoc routing, in: IEEE Canadian Conference on Electrical and Computer Engineering, vol. 2, 2001, pp. 1157–1161.

УДК 004.89

ЗАСТОСУВАННЯ LTE-R ТЕХНОЛОГІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ЗАЛІЗНИЦІ

Міночкін Д.А., Сушин І.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: rubin268@ukr.net

Application of LTE-R technology in telecommunication systems of railway

An approach is presented to the construction of modern telecommunication systems on the railway. The analysis of the use of the standard LTE-R for the development of future wireless telecommunication systems was conducted.

За останні кілька десятиліть мобільний зв'язок зазнав неймовірних змін та інновацій, головним чином завдяки значному збільшенню вимог до призначених для користувача даних. Одним з важливих етапів стало створення служб на основі IP-послуг. Революційна зміна була реалізована шляхом об’єднання мереж з комутацією каналів і з комутацією пакетів в мережі з комутацією пакетів. Іншими важливими віхами були впровадження ортогонального багаточастотного доступу з частотним поділом (OFDMA) і архітектури нової базової мережі, так званої Evolved Packet Core (EPC), які привели до стільникового зв'язку четвертого покоління (4G) [1]. В останні роки, крім стільникового зв'язку 4G, очікується неминуча поява ери зв'язку 5G. У 5G ми очікуємо, що максимальна швидкість передачі даних буде вимірюватися десятками гігабіт на секунду, надаючи кінцевим користувачам 1 Гбіт / с [2].

На відміну від швидких і новаторських змін в комерційних мобільних комунікаціях, розвиток залізничних сполучень було більш вимірюваних. В останні роки дослідження і розробки в системах залізничного зв'язку просуваються до бездротового зв'язку з комутацією пакетів [3-7]. Міжнародний союз залізниць (МСЗ) погодився з тим, що нинішній GSM-R не є достатнім для надання нових залізничних послуг, таких як відеоспостереження і моніторинг в режимі реального часу. Крім того, оператори комерційного мобільного зв'язку почали розгортати та використовувати Long Term Evolution (LTE), а попит на пристрої GSM знизився. Отже, придбання GSM-пристроїв стало складнішим, що викликало проблеми з точки зору обслуговування. Ці проблеми викликали різні альтернативи, в тому числі загальну послугу пакетного радіозв'язку (GPRS), з метою підвищення ефективності звичайних систем [3, 4], але в підсумку був зроблений висновок про те, що найбільш розумним підходом було прийняття нової системи. В даний час дослідницькі зусилля орієнтовані на LTE в якості технології наступного покоління [5-7]. Насамперед з точки зору майбутніх

експлуатаційних потреб в залізничному транспорті на даний час розглядається проект системи рухомого зв'язку залізниці майбутнього (СРЗЗМ - FRMCS), який був ініційований МСЗ у 2013 році. У цій ситуації розумно очікувати, що залізничні сполучення будуть йти в ногу з мобільним зв'язком. Було запропоновано LTE Railway (LTE-R) в якості інтегрованої системи бездротового залізничного зв'язку [7].

LTE-R складається з обладнання базової станції, основного обладнання і серверів обслуговування LTE-R. Базова станція складається з декількох радіопристроїв (РП) і цифрового блоку (ЦБ). РП призначені для передачі та прийому радіохвиль, а ЦБ відповідає за різні види обробки, включно з використанням радіо ресурсів для планування пакетів і ефективної обробки на фізичному рівні. Основне обладнання включає в себе обслуговуючий і пакетний шлюз, об'єкт управління мобільністю (ОУМ), домашній абонентський сервер (ДАС) і функцію правил політики та тарифікації (ФППТ). Ці об'єкти в основному призначені для ефективного управління носіями, управління мобільністю, включно з управлінням передачею обслуговування (handover), управління абонентами і якістю обслуговування, на основі пріоритету.

Сервера LTE-R складаються з сервера обробки викликів, Push-to-talk сервера (PTT), конференц-сервера, відеосервера, сервера управління і сервера перекодування. Ці сервера підтримують різні групові комунікації, включаючи екстрені виклики, приватні виклики та мультимедійне мовлення через протокол реального часу, управління групами, управління викликами, блокування за допомогою ФППТ і т.д.

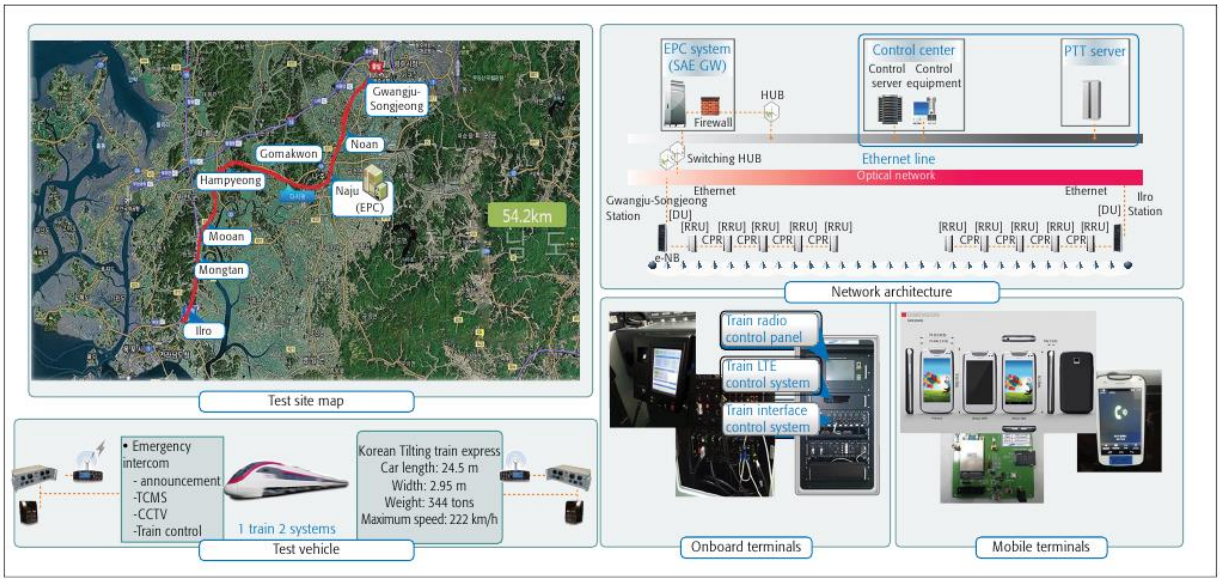


Рис. 1. Випробувальний стенд LTE-R

Що стосується терміналів, то існують два типи: бортовий термінал і мобільний термінал [6]. Бортовий термінал розташований в кабіні кожного машиніста і виконує передачу і прийом сигналу через антену на даху поїзда. Він взаємодіє бортовими пристроями, такими як система телебачення із замкнутим контуром (CCTV) через панель радіокерування поїзда (ПРКП) і інтерфейсом керування поїзда (ІКП), відповідно. Слід зазначити, що архітектура мобільного терміналу аналогічна архітектурі комерційного мобільного терміналу, за винятком того, що є фізична кнопка для управління телефоном для послуги PTT.

На рисунку 1 показаний огляд стенда LTE-R, побудованого на комерційній залізниці. Випробувальна ділянка проходила від станції Кванджу-Сонджонг до станції Ілро на лінії Хонам. На шляху довжиною 54,4 км розгорнуто Samsung Rel. 9 мережевих пристроїв LTE, які включали 51 РП, 7 ЦБ і 1 Evolved Packet Core (EPC). Кожний РП, що має спрямовані антени, розташовувався поряд з коліями, а ЦБ були розташовані для покриття РП. EPC був розташований на станції Naju і підключений до ЦБ по провідних лініях.

Таким чином, в перший етап проведеного дослідження показує можливість застосування технології LTE-R для побудови сучасних високопродуктивних, та високошвидкісних бездротових залізничних телекомунікаційних систем, що дозволить зменшити витрати на обслуговування та підтримку старих систем для операторів зв’язку. А також дасть можливість впровадити нові сервіси.

Література

1. E. Dahlman, S. Parkvall, and J. Skцld / 4G LTE, LTE-Advanced for Mobile Broadband // 2nd ed., Academic Press, 2014.
2. C.-X. Wang et al. / Cellular Architecture and Key Technologies for 5G Wireless Communication Networks // IEEE Commun. Mag., vol. 52, no. 2, Feb. 2014, pp. 186–95.
3. Banedanmark // Boundaries between ETCS and the GSM-R Network, 2008.
4. Banedanmark // Requirements on the GSM-R Network for ETCS support, 2009.
5. W. Luo, R. Zhang, and X. Fang, /A CoMP Soft Handover Scheme for LTE Systems in High Speed Railway // EURASIP J. Wireless Commun. and Net., vol. 2012, no. 1, June 2012, pp. 1–9.
6. A. Sniady and J. Soler / LTE for Railways: Impact on Performance of ETCS Railway Signaling // IEEE Vehic. Tech. Mag., vol. 9, no. 2, Apr. 2014, pp. 69–77.
7. A. Sniady et al. / LTE Micro-Cell Deployment for High-Density Railway Areas // Commun. Tech. Vehicles Proc., Springer, 2014, pp. 143–55.

УДК 621.396

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ OPEN VIRTUAL SWITCH В МЕРЕЖАХ SDN

Лящук А.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: aliashchuk@outlook.com

Researches of using Open vSwitch in SDN networks

The article describes the most important characteristics and design considerations preferences Open Virtual Switch (OVS).

Open vSwitch являє собою програмний комутатор, що працює як з фізичними інтерфейсами, так і з віртуальним інтерфейсами віртуальних машин. Це багаторівневий віртуальний комутатор з відкритим вихідним кодом, який поширюється під ліцензією Apache. Open vSwitch підтримує найбільш популярні Open-source гіпервізори, такі як VirtualBox, Xen, KVM і XenServer. Також Open vSwitch може використовуватися в якості заміни мостового модулю (bridge module), що використовується в Linux.

Гіпервізори потребують можливості переміщувати трафік між віртуальними машинами та зовнішнім світом. Для гіпервізорів на базі Linux, це зазвичай означає використання вбудованого комутатора L2 (the Linux bridge), що є швидким і надійним. Отже, виникає питання, для чого використовувати Open vSwitch?

Відповідь полягає в тому, що Open vSwitch призначений для розгортання багатосерверної віртуалізації. Ці середовища часто характеризуються високо динамічними кінцевими точками, підтримкою логічних абстракцій та (іноді) інтеграцією або розвантаженням на спеціальне комутуюче обладнання [1].

Наступні характеристики допомагають Open vSwitch впоратися з вищенаведеними вимогами.

Мобільність стану. Весь стан мережі, пов'язаний з мережевим об'єктом, повинен легко ідентифікуватися та мігрувати між різними хостами. Це може включати традиційний "м'який стан" (наприклад, запис у таблицю вивчення L2), стан переадресації L3, політику маршрутизації, список контролю доступу (ACL), політику QoS, конфігурацію моніторингу (наприклад, NetFlow, IPFIX, sFlow) тощо.

Open vSwitch підтримує конфігурування та міграцію як повільного так і швидкого стану мережі між екземплярами. Наприклад, якщо віртуальна машина мігрує між кінцевими хостами, можна не тільки перемістити пов'язану конфігурацію (правила SPAN, ACL, QoS), а й будь-який стан мережі (включаючи, наприклад, існуючий стан, який може бути складним

для реконструкції). Крім того, стан Open vSwitch набирається та підтримується реальною моделлю даних, що дозволяє розробляти структуровані системи автоматизації.

Реагування на динаміку мережі. Віртуальне середовище характеризується високими темпами змін(додавання та видалення віртуальних машин, їх переміщення та зміна в середовищі мережі).

Open vSwitch підтримує ряд функцій, які дозволяють мережевій системі реагувати та адаптуватися при будь-яких змінах середовища. Це включає в себе просту підтримку обліку та видимості(NetFlow, IPFIX та sFlow). Але більш корисним є те, що Open vSwitch підтримує базу даних про стан мережі (OVSDB), яка підтримує віддалені тригери. Тому, частина програмного забезпечення для оркестровки може "спостерігати" різні аспекти мережі та відповідати, коли вони змінюються. Сьогодні це використовується, наприклад, для реагування та відстеження міграцій віртуальних машин.

Open vSwitch також підтримує OpenFlow як метод експортування віддаленого доступу для керування трафіком. Для цього існує безліч застосувань, включаючи глобальне виявлення мережі через перевірку трафіку, відкриття або зв'язку (наприклад, LLDP, CDP, OSPF тощо).

Технічне обслуговування логічних тегів. Розподілені віртуальні комутатори (такі як VMware vDS та Cisco Nexus 1000V) часто підтримують логічний контекст у мережі за рахунок додавання або маніпулювання тегами в мережевих пакетах. Це може бути використано для унікальної ідентифікації віртуальної машини (у спосіб, стійкий до апаратних спотворень), або для зберігання іншого контексту, який є відповідним лише в логічному домені. Значна частина проблеми з побудовою розподіленого віртуального комутатора полягає в тому, щоб ефективно і правильно керувати цими тегами.

Open vSwitch включає в себе кілька методів для визначення та підтримки правил позначення, всі з яких доступні для віддаленого процесу для оркестровки. Крім того, у багатьох випадках ці правила додавання тегів зберігаються в оптимізованій формі, тому їх не потрібно поєднувати з важкими мережевими пристроями. Це дозволяє, наприклад, налаштовувати, змінювати та переносити тисячі правил для повторного розміщення тегів або адрес.

Аналогічно, Open vSwitch підтримує реалізацію GRE, яка може обробляти тисячі одночасних тунелів GRE і підтримує віддалену конфігурацію для створення, налаштування та розриву тунелів. Це, наприклад, може бути використане для підключення приватних віртуальних мереж до різних центрів обробки даних.

Апаратна інтеграція. Шлях пересилання в Open vSwitch (вбудований канал передачі даних в ядрі) призначений для «розвантаження» пакетної обробки на апаратні чіпсети, не зважаючи на те, чи розміщено це в класичному корпусі комутуючого обладнання або в мережевому адаптері кінцевого вузла. Це дозволяє шляху управління (control path) Open vSwitch

мати можливість контролювати як чисту реалізацію програмного забезпечення, так і апаратний комутатор.

Перевага апаратної інтеграції - це не тільки продуктивність в віртуалізованих середовищах. Якщо фізичні перемикачі також відображають абстракції управління Open vSwitch, тоді можна управляти як середовищем, так і віртуалізувати хостинг, використовуючи той же механізм автоматичного управління мережею.

Безпека. Open vSwitch надає найвищий рівень безпеки дозволяючи встановлювати політики для віртуальних інтерфейсів ВМ [2].

LACP і обізнаність про VLAN. Open vSwitch повністю підтримує агрегацію зв'язків LACP і позначку VLAN. Наявна можливість налаштовувати один окремий Open vSwitch з безліччю тегів VLAN, тим самим зменшуючи накладні витрати управління безліччю віртуальних мостів для тегів VLAN.

Quality of Service. Повна підтримка QoS або рівнів сервісів.

Моніторинг мережевої середовища. Присутня можливість отримати найвищий рівень управління проходженням пакетів через Open vSwitch шляхом реалізації потужного моніторингу з застосуванням Netflow і sFlow.

IPv6. Open vSwitch повністю підтримує IPv6.

Протокол тунелювання. Open vSwitch має повну підтримку безлічі протоколів тунелювання, наприклад, GRE, VXLAN, STT, IPsec і тому подібних.

Підтримка Proxmox. Open vSwitch повністю інтегрований і підтримується Proxmox, роблячи його життєздатним вибором для настройки віртуальної мережі.

Підсумовуючи вищенаведене бачимо, що багато в чому, Open vSwitch націлюється на іншу точку дизайнерського простору, ніж попередні версії гіпервізорів, зосереджуючи увагу на необхідності автоматичного та динамічного управління мережею у великих середовищах віртуалізації на базі Linux.

Отже метою Open vSwitch є забезпечення мінімального обсягу вбудованого коду (так як це необхідно для продуктивності) та повторне використання існуючих підсистем. Open vSwitch включено як частину ядра і є доступним в більшості популярних дистрибутивів.

Література

1. Open vSwitch Documentation. – 361 с. – (Release 2.9.90).
2. Wasim Ahmed. Mastering Proxmox / Wasim Ahmed. – Birmingham B3 2PB, UK: Packt Publishing Ltd.

УДК 621.391

ЯКІСТЬ ОБСЛУГОВУВАННЯ (QOS) В LTE

Харченко Т.П., Правило В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: harchenko0512@gmail.com, valeriy_pravilo@ukr.net

Quality of service (QoS) in LTE

In this article, we review concepts of QoS in LTE, QoS parameters, principles of work, types of EPS bearer.

Є абоненти преміум-класу, які завжди хочуть мати кращу якість користуючись пристроєм 4G LTE. Ці користувачі готові платити більше за високу пропускну здатність та кращий доступ до мережі на своїх пристроях. Не лише передплатники, але й деякі служби потребують кращого управління пріоритетом у мережі (наприклад, дзвінок через VoIP). QoS визначає пріоритети для певних клієнтів/послуг під час високої завантаженості мереж [3].

QoS (англ. Quality of service), у широкому значенні - якість послуг, які надає комунікаційна мережа. У вузькому технічному значенні в IT, цей термін означає - набір методів для управління ресурсами пакетних мереж [1].

Основні параметри QoS:

- Пропускна смуга (Bandwidth) - описує доступну пропускну здатність каналу зв’язку. Вимірюється у бітовій швидкості - bit/s (bps), kbit/s (kbps), Mbit /s (Mbps);
- Затримка при передачі пакета (Delay), вимірюється в мілісекундах;
- Джітер (Jitter) - нерівномірність затримок (Delay variation) при передачі пакетів;
- Втрата пакетів (Packet loss) - визначає кількість пакетів, загублених у мережі під час передачі.

Для простоти розуміння канал зв'язку можна представити у вигляді умовної труби, а пропускну здатність описати як функцію двох параметрів: ширини труби і її довжин.

Коли передача даних зіштовхується із проблемою «вузького місця» для прийому й відправлення пакетів на роутерах звичайно використається метод FIFO: перший прийшов - перший пішов (First In - First Out). При інтенсивному трафіку це створює затори, які вирішуються вкрай простим чином: всі пакети що не ввійшли до черги FIFO (на вхід або на вихід) ігноруються роутером, і відповідно губляться безповоротно. Розумніший метод - використати «розумну» чергу, у якій пріоритет у пакетів залежить від типу сервісу - ToS (Type of Service). Необхідна умова - пакети повинні вже нести мітку типу сервісу для створення «розумної» черги [1].

Для того, щоб забезпечити дотримання параметрів QoS для безлічі додатків, створюються різні EPS потоки. Всі можливі EPS потоки в залежності від типу ресурсу можна розбити на дві групи: потоки з гарантованою мінімальною швидкістю передавання (Minimum Guaranteed Bit Rate, GBR) і потоки без гарантій по швидкості передавання даних (Non-GBR):

- *GBR потоки*. Потоки цього типу мають задане значення мінімальної швидкості передавання, яке встановлюється під час процедур створення потоку або його зміни. При цьому, можлива передача даних з більшою швидкістю, ніж мінімально встановлена, якщо є вільні ресурси на радіо каналі. Також може бути встановлено обмеження на максимальну швидкість передавання даних (Maximum Bit Rate, MBR). Потоки такого типу використовуються, наприклад, при передавання VoIP (технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP) трафіку;

- *Non-GBR потоки*. Потоки даного типу не гарантують ніякої мінімальної швидкості передавання даних. Тому ці потоки використовуються для передавання трафіку при перегляді інтернет сторінок і при передавання файлів по FTP (англ. File Transfer Protocol).

На ділянці між eNodeB і UE забезпеченням параметрів QoS займається eNodeB (рис. 1).

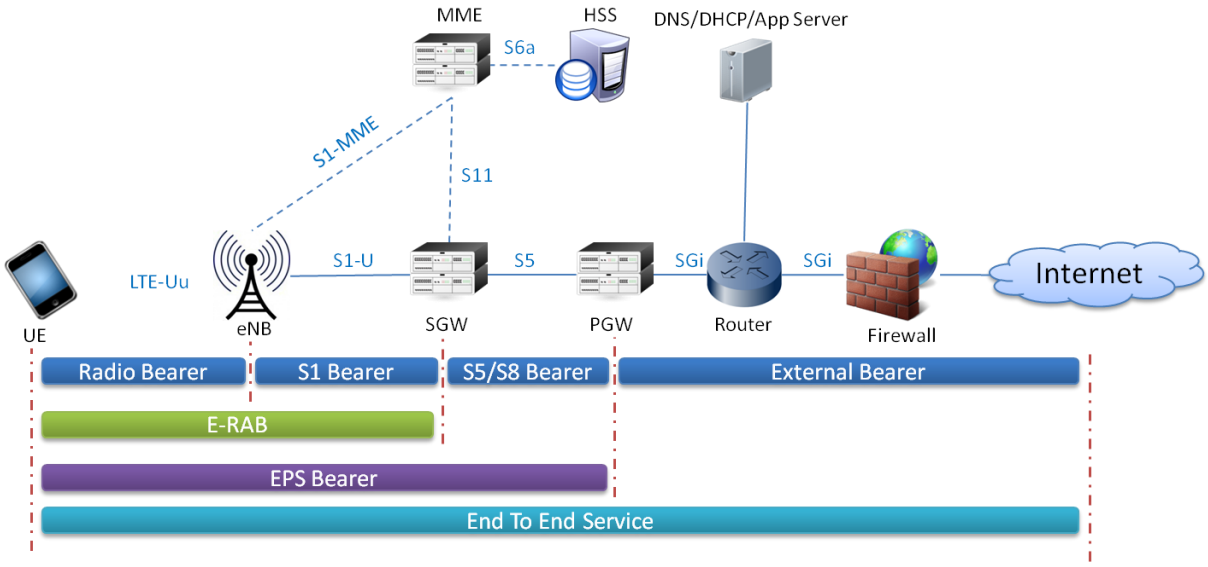


Рисунок 1.

Для цього кожному потоку приписаний ідентифікатор QoS класу (QoS Class Identifier, QCI). Кожен QCI визначає значення для наступних параметрів QoS: пріоритет, допустима затримка і допустима кількість втрачених пакетів. Всі можливі значення QCI, а також значення параметрів QoS, що відносяться до конкретного QCI, визначені в специфікації. У таблиці 1 наведена визначена множина QCI та їх характеристики. Відзначимо, що значення допустимої затримки визначається на ділянці між P-GW і UE.

Як правило, значення пріоритету і допустимої затримки визначають яким чином планувальник на eNodeB буде обробляти пакети даних. Якщо значення допустимих втрат рівне 10^{-6}, то буде використовуватися передача з підтвердженням.

Таблиця 1.

QCI	Тип	Пріоритет	Допустима затримка, мс	Допустимі втрати	Приклад
1	GBR	2	100	10^{-2}	VoIP виклик
2		4	150	10^{-3}	Відео виклик
3		5	300	10^{-6}	Онлайн ігри
4		3	50	10^{-3}	“Стрім” відео
5	Non-GBR	1	100	10^{-6}	IMS
6		7	100	10^{-3}	Електронна пошта, чат
7		6	300	10^{-6}	Голосові, відео, інтерактивні ігри
8		8	300	10^{-6}	Електронна пошта, чат
9		9	300	10^{-6}	

У разі передавання даних по мережі призначеній для користувача потоки повинні пройти кілька інтерфейсів (LTE-Uu, S1, S5/S8) перш ніж вони потраплять в зовнішню мережу або на UE. На кожному інтерфейсі EPS потоки відображаються на потоки більш низьких рівнів, які мають свої ідентифікатори. Кожен вузол забезпечує відповідність ідентифікаторів потоку на різних інтерфейсах (до яких цей вузол має відношення). Відзначимо, що на інтерфейсах S1 і S5/S8 потік визначається ідентифікатором GTP тунелю. Пакети, що відносяться до одного і того ж EPS потоку, завжди обробляються однаковим чином.

Класифікація вхідних пакетів для визначення до якого потоку вони відносяться здійснюється за допомогою TFT (Traffic Flow Template). Ці шаблони використовують таку інформацію з IP заголовка пакета, як IP адреси відправника і одержувача та номери TCP портів [2].

Література

1. QoS [Електронний ресурс] - Режим доступу: https://uk.wikipedia.org/wiki/QoS.
2. Качество обслуживания в LTE [Електронний ресурс] - Режим доступу: http://anisimoff.org/lte/qos.html.
3. Quality of servise(QoS) [Електронний ресурс] - Режим доступу: http://www.simpletechpost.com/2013/01/quality-of-service-qos-in-lte.html.
4. Рыжков А.Е. и др. «Стандарты и сети радиодоступа 4G»/ Уч. Санкт-Петербург: изд-во Линк , 2012, 226 с.

УДК 621.396.1

ЙМОВІРНІСТЬ ПЕРЕРИВАННЯ ЗВ'ЯЗКУ В КОГНІТИВНІЙ ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ НА БАЗІ АЕРОПЛАТФОРМИ

Кравчук С.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

Outage probability of communication in a cognitive radio system based on an aeroplatformy

The mathematical model of the multi-stage outage probability of communication is developed, on the basis of which one can estimate the influence of the new (recently) activated system on the existing active system by taking into account the thermal noise and interference occurring in radio channels in one band of shared frequencies.

Функціонування радіосистем в одному спільному спектрі є одним із рішень збільшення пропускної здатності сучасних радіосистем та способів тимчасового задіяння смуг спектру первинного оператора, що в даний момент часу не використовуються [1-3]. Особливо це актуально для системи широкосмугового радіодоступу (СШР), що має значну площу покриття де вона взаємодіє з іншими СШР. Для нашого випадку це телекомунікаційна система на основі висотної аероплатформи (ТСВА) і СШР наземного базування.

Розглянуто сценарій розгортання двох базових станцій, відповідно, на аероплатформі і наземній вежі. Остання формує стільник в межах зони покриття ТСВА і відстоїться від точки проекції висотної станції на поверхню Землі на відстань десятка км. Прийнята направлена антена для висотної станції, яка спрямована до центру зони покриття ТСВА. Усі користувачі випадково розподілені по фіксованим локаціям, а їх антени направлені на свої обслуговуючі базові станції.

Багатоступенева ймовірність відмови є визначальним параметром для оцінки характеристики радіосистеми. На її основі можна оцінити вплив нової (оновленої) активованої системи на існуючу активну систему шляхом врахування теплових шумів та завад, що викають в радіоканалах в одній смузі частот спільного користування. В залежності від активацій системи (визначені як ступені) ймовірність переривання зв'язку може приймати декілька видів. Щоб розрізняти останні в даному сценарії розглянемо ступені, де немає активованих систем як «0», а де одна система активована – як «1». Тоді ступінь «2» - коли буде активована нова система (рис. 1).

Приймемо P як ймовірність переривання зв'язку і X як позначення користувацьких видів. H і T позначають користувачів ТСВА і наземних систем, відповідно. HT позначає користувачів ТСВА в зоні наземної базової станції, а TH користувачів наземної базової станції в зоні покриття ТСВА.

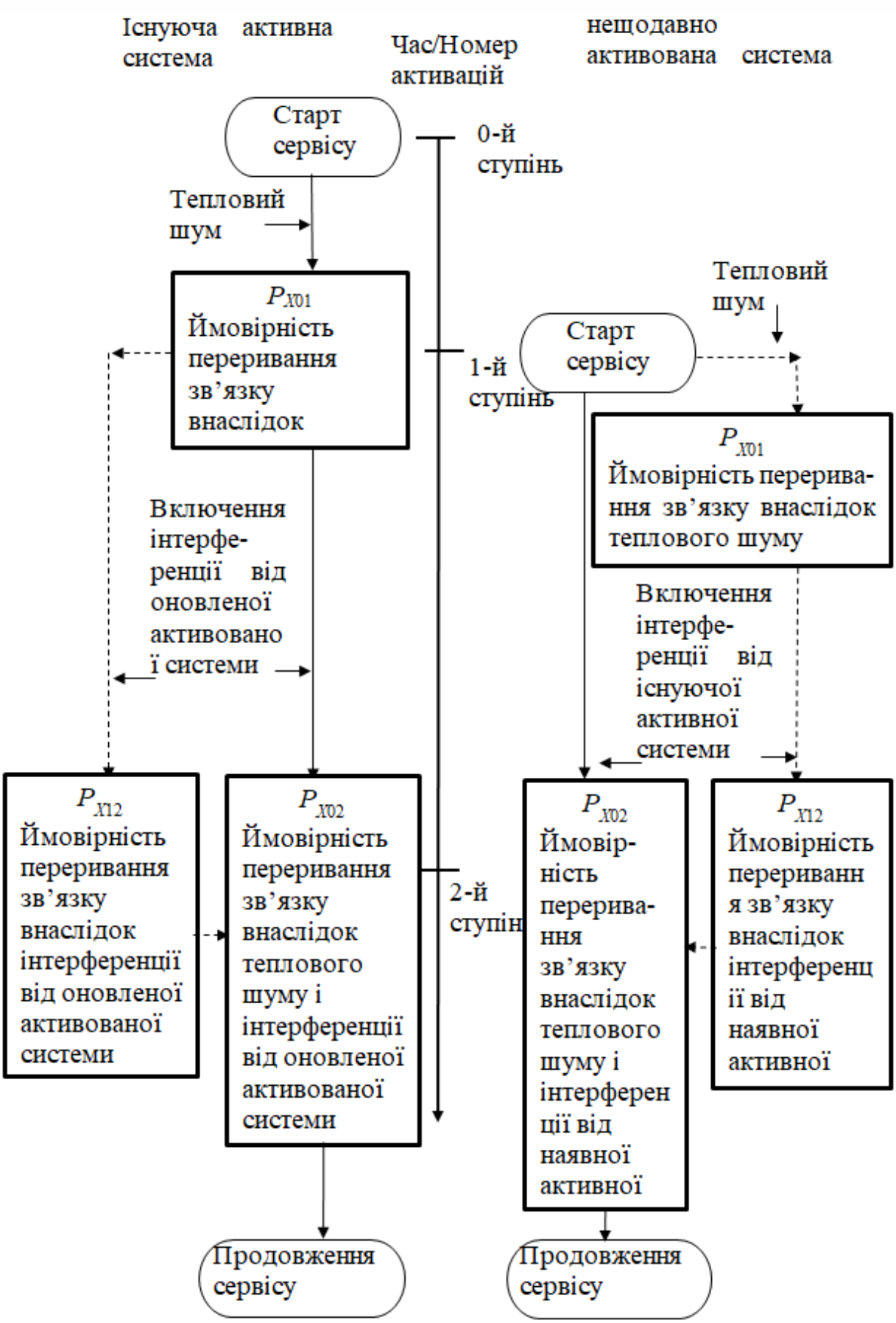


Рис. 1. Ймовірність переривання зв'язку на кожному ступені

Тоді запис P_{X01} позначає ймовірність переривання зв'язку, що обумовлена шумом, а P_{X12} – додаткову ймовірність переривання зв'язку, що обумовлена інтерференцією нової активованої системи; P_{X02} – загальна ймовірність переривання зв'язку. Індекс X відповідає типу користувача (H, T, HT або TH).

Приймемо множину U_X як множину усіх користувачів певного (X) типу. Множина користувачів в межах U_X, які поточно активні, може бути визначена як $A_{X0} = \{u \in \mathrm{U_X} : u -$ обслуговування на вимогу$\}$.

Для того, щоб визначити ймовірність переривання зв'язку, що обумовлено шумом (P_{X01}) в розглядаємому діапазоні частот, введемо множину користувачів в межах A_{X0}, для яких значення CNR більше чи рівне мінімальному порогу (T_{rM}) певної модуляційної схеми M.

Загальний вираз для ймовірності переривання зв'язку даного сценарію можна записати у вигляді

$$P_{Xij,\min M} = 1\text{-}|A_{Xj,\min M}|/|A_{Xi,\min M}|;\ A_{Xi,\min M} \neq \phi \qquad (1)$$

Індекси i і j відповідають ступеням ймовірності переривання зв'язку ($i < j$).

Для покращення електромагнітного оточення шляхом зменшення ймовірності переривання зв'язку, що зазнають користувачі, нами запропоновано два методи одночасного використання спектру засновані на відношеннях інтерференція/шум (ВІШ) чи несуча/(шум + інтерференція) (ВНІШ), відповідно.

Дані методи можуть змінювати потужність передавача базової станції нещодавно активованої системи при спілкуванні з конкретним користувачем. Метод на базі ВІШ використовує INR(interference to noise ratio)-рівень на вході приймача існуючого діючого користувача як референтний рівень, який задіється для контролю за потужністю передавача радіолінії вниз нещодавно активованої системи. Метод на базі ВНІШ використовує CINR(signal to interference ratio)-рівень на вході приймача діючого користувача в якості референтного рівня, який слугує для контролю потужністю передавача радіолінії вниз нещодавно активованої системи. В сценарії, що розглядається, приймемо, що в якості первинної системи слугує наземна система радіодоступу, а ТСВА – як вторинна система, що буде активована.

Для аналізу характеристик запропонованих методів було згенеровано множину випадковим чином розташованих користувачів (на фіксованих позиціях) для базових станцій наземної системи та ТСВА. Випадковим чином вибирається один користувач з кожної множини користувачів для формування тестової пари і оцінюємо продуктивність для цієї конкретної пари користувачів. Потім підраховується загальна статистика продуктивності, що базується на результатах, отриманих для всіх пар користувачів (вибірка становила 250 000), де кожна пара являє собою випадково вибрану пару користувачів із двох наборів (наземної системи і ТСВА). Таким чином, отримані результати відображають середню продуктивність по відношенню до відповідних областей покриття.

Розглядаються три різні способи оцінки ефективності схем. Перший направлений на оцінку загальної характеристики відключення (переривання зв'язку) кожної системи з урахуванням як теплового шуму, так і завад від сусідньої системи, що співіснує. Другий спосіб направлений на ту ж оцінку відключення (переривання зв'язку), але тепер в залежності від місця розташування користувача, і, нарешті, третій спосіб оцінює відключення, що викликані в діючій наземній системі, в результаті завад від співіснування з ТСВА. Спрямованість антени користувача значно знижує вплив завад від однієї системи до іншої, і, отже, підвищує продуктивність співіснування. Також для порівняння представлено результати ймовірності переривання зв'язку з різними ширинами променя антен користувачів.

Із результатів моделювання отримано наступне. Не застосовуючи будь-які методи одночасного використання спектру до ТСВА і дозволяючи передавати їй з максимальною потужністю, то ймовірність переривання зв'язку, викликана шумом та завадами від новоствореної системи (P_{02}) користувачів ТСВА, є найнижчою, і це буде найкраща продуктивність ТСВА, яка може бути досягнута.

Таким чином, розроблено два методи та відповідні алгоритми одночасного використання спектру в спадних радіолініях базових станцій висотної аероплатформи і наземних фіксованих широкосмугових систем, призначених для застосування з когнітивними користувацькими радіотерміналами із спрямованими антенами. Дані методи базуються на співвідношенні інтерференція/шум на приймачі користувача. Ширина діаграми спрямованості антени та рівні модуляційної схеми визначає параметри співіснування радіовузлів. Показано, що ефективність спільного існування може бути покращена шляхом задіяння надлишкової потужності передавача наземної системи, що дозволяє існуючій наземній системі знизити додаткові завади від активованої ТСВА.

Розроблено математичну модель багатоступеневої ймовірності переривання зв'язку, на основі якої можна оцінити вплив нової (нещодавно) активованої системи на існуючу активну систему шляхом врахування теплових шумів та завад, що виникають в радіоканалах в одній смузі частот спільного користування.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Діденко І.В., Кравчук С.О. Канальна оцінка та адаптивна модуляція в системах когнітивного радіо // Матер. 10-ї міжнар. наук.-техн. конф. "Проблеми телекомунікацій", 19–22 квітня, 2016 р. – К.: Хімджест, 2016. – С. 312–314.
3. Журавель А.С., Кравчук С.О. Безпроводові мережі доступу з динамічним вибором спектру // Матер. 11-ї міжнар. наук.-техн. конф. "Проблеми телекомунікацій", 18–21 квітня, 2017 р. – К.: Хімджест, 2017. – С. 172–174.

УДК 621.396

ПРОБЛЕМИ ВИКОРИСТАННЯ СЕРВІСУ LBAAS В OPENSTACK ДЛЯ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

Кибенко А.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: endryu-kibenko@outlook.com

The problems of using LBaaS service in OpenStack for load balancing

The advantages of using cloud technologies are considered. OpenStack software conceptual architecture is considered and essence of its main elements is revealed. The problems of using LBaaS (Load Balancing-as-a-Service) service are considered.

Cloud computing – «хмарні обчислення» – концепція «обчислювальної хмари», згідно з якою програми запускаються і видають результати роботи в вікно стандартного web-браузера на локальному ПК, при цьому всі додатки і їх дані, необхідні для роботи, знаходяться на віддаленому сервері в Інтернеті.

Термін «cloud computing» став широко вживатися в США з 2005 року після запуску компанією Amazon проекту Elastic Compute Cloud (Amazon EC2) і широко поширився в бізнесі, серед постачальників інформаційних технологій і в науково-дослідному середовищі.

До переваг хмарних обчислень можна віднести наступні: знижуються вимоги до обчислювальної потужності ПК, зростають відмовостійкість і безпека, багатократно збільшується швидкість обробки даних, знижуються витрати на апаратне і програмне забезпечення, на обслуговування, електроенергію, економиться дисковий простір [1].

Одним із інструментів для побудови хмари є комплекс вільного програмного забезпечення для створення обчислювальних сервісів та хмарних сховищ OpenStack, який складається з наступних компонентів:

- Horizon – надає web-портал самообслуговування для взаємодії з основними службами OpenStack;
- Nova – керує життєвим циклом обчислювальних екземплярів (планування та виведення з експлуатації віртуальних машин);
- Neutron – засіб управління мережевою інфраструктурою;
- Swift – засіб для зберігання довільних об’єктів даних за допомогою RESTful API;
- Cinder – сервіс для постійного зберігання блоків даних для запуску екземплярів;
- Keystone – надає службу автентифікації та авторизації для інших служб OpenStack;
- Glance – сховище образів віртуальних машин;
- Ceilometer – сервіс для моніторингу, масштабованості і білінгу хмари.
- Heat – сервіс для автоматизації хмарних додатків;.
- Trove – надає сервіс бази даних;

- Sahara – сервіс для масштабування кластерів Hadoop [2].

На рис. 1 зображена концептуальна архітектура OpenStack.

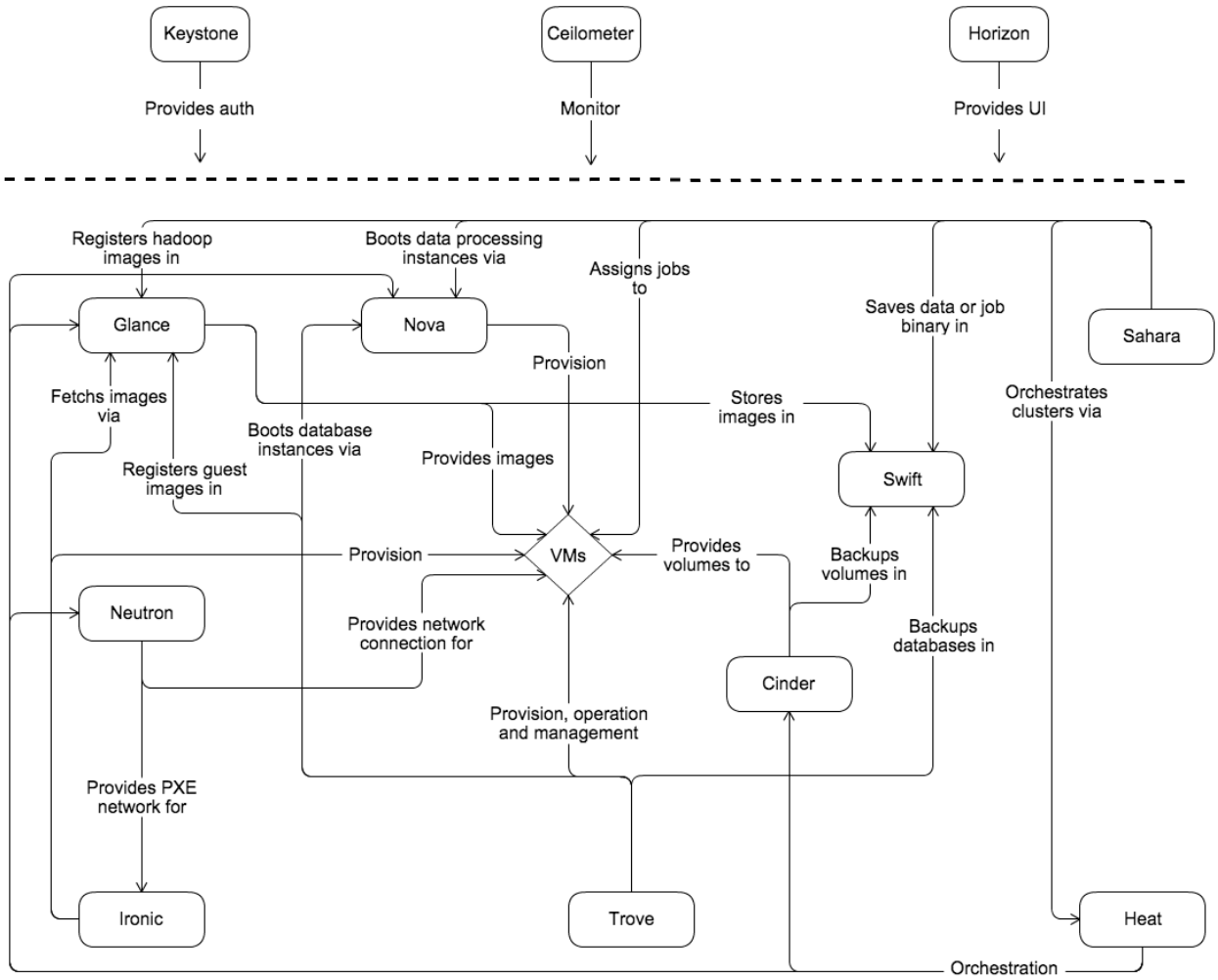


Рис. 1. Концептуальна архітектура ПЗ OpenStack

Одним з основних випадків використання будь-якої хмарної платформи є швидкий і простий спосіб масштабування додатків. Найпростішим способом досягнення цієї мети є розміщення балансувальника навантаження перед програмами і розділити навантаження.

На даний момент в OpenStack інтегрована служба балансування навантаження (LBaaS), яка вбудована в сервіс Neutron. Однак, існує багато моментів, в яких LBaaS не відповідає вимогам для масштабування додатків.

Neutron LBaaS традиційно використовує стандартний інструмент Linux, який має назву HAProxy, який є стандартом для балансування навантаження в Linux. Останній має ряд недоліків для використання в OpenStack.

Недоліки LBaaS:

Еластичність. Основна концепція розміщення «речей» в балансувальника навантаження має два пункти: по-перше, потрібно забезпечити можливість лінійного масштабування додатків, а по-друге,

потрібно забезпечити відмовостійкість і резервування для додатку. Даний спосіб, переміщує точку відмови додатку у сферу застосування, аж до моменту, коли саме балансування навантаження є точкою відмови.

Спочатку LBaaS був виконаний як процес на вузлах мережі як єдиний процес без надмірності. Не було жодного моніторингу процесу HAProxy і ніякого способу дізнатися, чи працює процес балансування коректно. Якщо мережевий вузол вийшов з ладу, весь трафік, який мав протікати через балансувальник, зупинився і реального способу відновлення потоку трафіку не було.

Дана проблема вирішувалась у версії LBaaS v2, де замість того, щоб мати єдиний процес, функція балансування навантаження тепер була виконана як окремий екземпляр. Але на сьогоднішній день даний підхід знову ж таки є єдиною точкою відмови.

Один порт. Багато людей зацікавлені в керуванні трафіком між їхніми екземплярами і тому важливо, щоб екземпляр обслуговував трафік лише на одному порті. Завдяки LBaaS, на сьогоднішній день, для кожного порту, потрібен власний балансувальник. Тому при великій кількості екземплярів стає очевидним, що кількість ресурсів, що використовуються для балансування навантаження, може бути значно більше, ніж ресурсів необхідних для надання послуг.

Гнучкість. Гнучкість, яка доступна сьогодні в LBaaS для керування трафіком у балансувальниках навантаження, є дуже обмеженою. Є багато варіантів, як наприклад, формування трафіку, розвантаження SSL та інші, які сьогодні можна використовувати в HAProxy, однак, вони неможливі при використанні LBaaS в OpenStack.

Логування. Одним з основних принципів управління є можливість відслідковувати трафік. Це зазвичай виконується за допомогою логування (ведення журналу). На даний час, ця функціональність недоступна в OpenStack.

Таким чином, рішення щодо балансування навантаження є важливою частиною хмарної інфраструктури. Дане рішення повинно бути інструментом, яким можна керувати багатьма способами, які повинні відповідати потребам, повинні забезпечувати максимальну гнучкість і еластичність [3].

Література

1. Балансировка нагрузки в облачных вычислениях / [Е. Н. Десятирикова, А. М. Хадж, А. Ходар та ін.]. // Научный журнал «Вестник» Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2017. – №3. – С. 103.
2. OpenStack Documentation [Електронний ресурс] // OpenStack Foundation. – 2018. – Режим доступу до ресурсу: https://docs.openstack.org/install-guide/get-started-with-openstack.html.
3. Ronen Kofman. Load Balancing in OpenStack without LBaaS [Електронний ресурс] / Ronen Kofman // Stratoscale. – 2016. – Режим доступу до ресурсу: https://www.stratoscale.com/blog/openstack/load-balancer-openstack-without-lbaas/.

УДК 621.373

СХЕМОТЕХНІЧНЕ МОДЕЛЮВАННЯ ГЕНЕРАТОРІВ UWB СИГНАЛІВ ДЛЯ БЕЗПРОВОДОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Авдєєнко Г. Л., Бунін С. Г., Наритник Т. М.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
E-mail: django2006@ukr.net

Modeling of UWB signal generators for wireless communication systems

Structural and electrical diagrams for UWB generator based on the step recovery diode (SRD) usage are presented. The simulation results of the SRD UWB generator indicate the possibility of receiving at its output an UWB signal with a duration less than 1 ns and an amplitude that does not exceed 0.3...0.45 V. This thesis may be useful for UWB wireless communication system developers.

На даний час на світовому ринку електронних компонентів доступні для продажу інтегральні мікросхеми трансиверів з використанням над широкосмугових (UWB) сигналів DW1000 фірми Decawave стандарту IEEE 802.15.4-2011, що призначені для застосування у пристроях визначення місцеположення та системах передачі інформації [1].

Зазвичай, генератор UWB сигналів є невід'ємною частиною будь-якого сучасного передавально-приймального пристрою безпроводової системи зв'язку, що використовує UWB сигнали. Аналіз літератури [2-12] по генераторам UWB сигналу показує, що його узагальнену структурну схему можна подати у вигляді, що відображений на рис. 1.

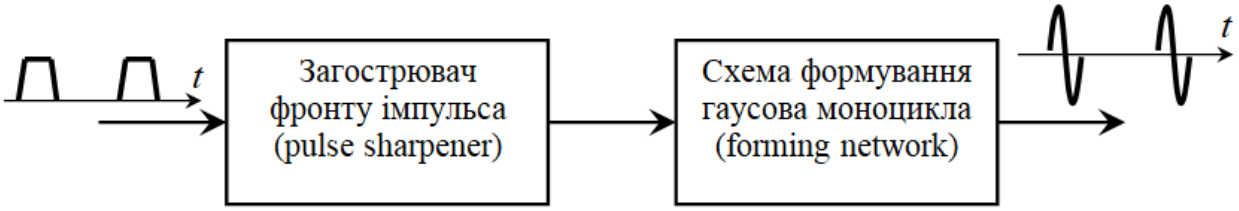


Рис.1. Структурна схема генератору UWB сигналів

В якості загострювача фронтів імпульсу вхідного сигналу генератора як правило використовуються спеціальні напівпровідникові пристрої: лавинний транзистор, біполярний діод, тунельний діод, імпульсний діод з накопиченням заряду (ДНЗ) та польовий транзистор. Лавинний транзистор має перевагу в тому, що дозволяє отримати загострення фронту для імпульсу значної потужності, але має недоліком обмежену частоту повторення імпульсу через значний рівень дисипативних втрат в транзисторі. Тунельні діоди мають найменший час перемикання – декілька пікосекунд, але при дуже малій потужності в декілька мВт. Діод з накопиченням заряду є компромісним варіантом, оскільки він має надмалий час перемикання близько 100 пс при середньому рівні потужності від сотень мВт до десятків Вт з високою частотою повторення імпульсів. Ці властивості роблять

актуальним саме їхнє використання в генераторах UWB сигналів.

ДНЗ працює як контрольований перемикач, який дуже швидко може змінювати свій опір з малого на великий. Ця властивість ДНЗ використовується для загострення тривалих фронтів вхідних інформаційних імпульсних сигналів.

Схема формування моноциклу представляє собою диференцюючий ланцюг, який як правило реалізується на базі використання зосереджених елементів (конденсаторів та резисторів) або короткозамкненого відрізку мікросмужкової лінії передачі.

При використанні короткозамкненої мікросмужкової лінії, електрична схема генератора UWB в САПР AWR Microwave Office матиме вигляд, показаний на рис. 2.

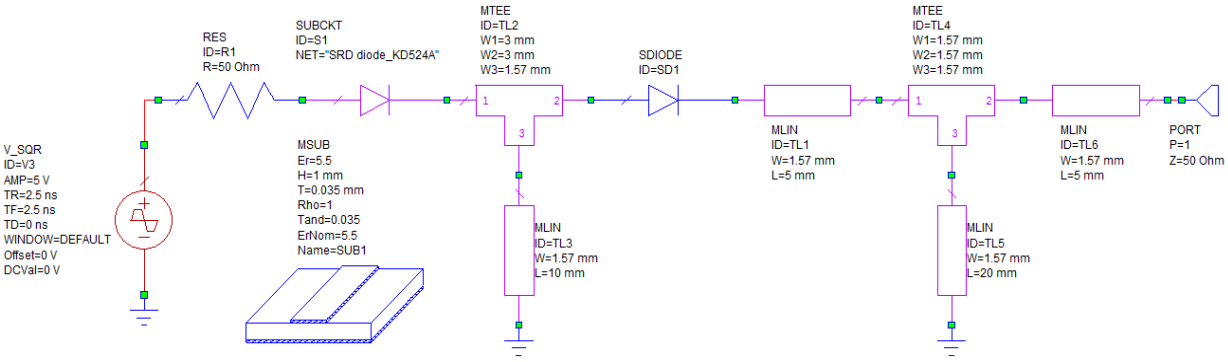


Рис. 2. Електрична схема генератору, що формує моноцикл за допомогою диференціюючого кола у вигляді короткозамкненої мікросмужкової лінії

Вхідним сигналом UWB генератора (рис.2) від джерела V_SQR є періодична послідовність двополярних імпульсів (меандр) з частотою слідування f = 10 МГц (періодом T = 100 нс), скважністю σ = 2, тривалістю імпульсу τ = 50 нс, часом нарощування переднього фронту t_R = 2,5 нс, часом спадання заднього фронту t_F = 2,5 нс, амплітудою U_m = 5 В.

На рис. 3 зображено часові форми моноциклу на виході UWB генератору при різних значеннях довжини другої короткозамкненої мікросмужкової лінії при його моделюванні за допомогою САПР AWR Microwave Office. З рис. 3 видно, що тривалість моноциклу не перевищує 1 нс, а амплітуда $U_m \approx 0{,}3..0{,}45$ В.

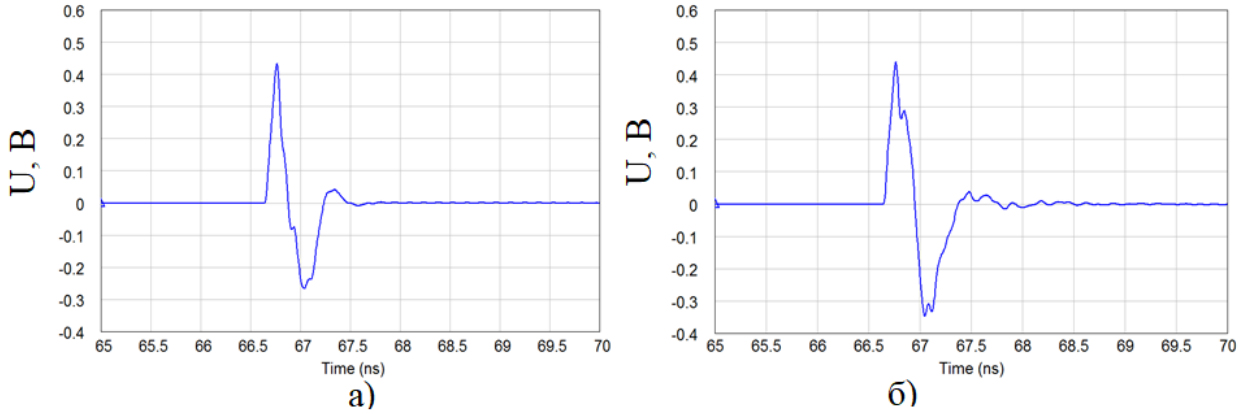


Рис.3. Часові форми моноциклу на виході UWB генератору для різних значень довжини другої короткозамкненої лінії: а) при L = 10 мм; б) при L = 20 мм.

Формування UWB сигналу у вигляді гаусівського моноциклу як правило обумовлено тим фактом, що спектр такого радіосигналу, що зображений на рис. 4 має малий рівень низькочастотних складових (вони майже відсутні), що в свою чергу дозволяє випромінювати та приймати такий сигнал малогабаритною широкосмуговою антеною, забезпечуючи малий рівень його спотворення в приймачі UWB сигналів.

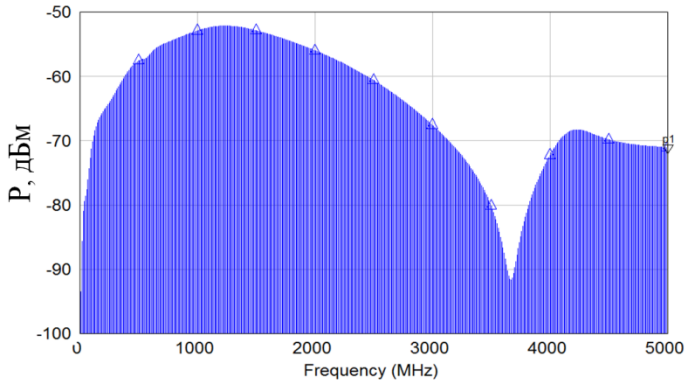


Рис. 4. Спектр моноциклу на виході генератору при довжині короткозамкненої лінії L = 20 мм

Література

1. ScenSor DW1000 Unrivalled Indoor Precision Location abd Communication for Numerous Markets [Електронний ресурс] – Режим доступу: https://www.decawave.com/products/dw1000 – Назва з екрана.
2. Pavel Protiva, Jan Mrkvica, Jan Macháč «Universal Generator of Ultra-Wideband Pulses», Radioengineering, Vol. 17, №.4, December 2008, p.74-78.
3. Sertac Yilmaz, Ibrahim Tekin “Ultra-Wideband N-bit Digitally Tunable Pulse Generator”, IEEE International Conference on Ultra-Wideband, 5-8 Sept, 2005. Zurich, Switzerland, p.438-442.
4. Bo Qin, Xin Wang, Haolu Xie, Lin Lin, He Tang, Albert Wang, Hongyi Chen, Bin Zhao, Liwu Yang, Yumei Zhou, "1.8 pJ/Pulse Programmable Gaussian Pulse Generator for Full-Band Noncarrier Impulse-UWB Transceivers in 90-nm CMOS", *Industrial Electronics IEEE Transactions on*, vol. 57, pp. 1555-1562, 2010, ISSN 0278-0046.
5. C. Zhang and A. E. Fathy, “Reconfigurable Pico-Pulse Generator for UWB Applications” in IEEE MTT-S Int. Microw. Symp. (IMS), San Francisco, CA, Jun. 2006, pp. 407 – 410.
6. Erika Pittella “UWB Radar System for Breath Activity Monitoring”, Dottorato di Ricerca in Ingegneria Elettronica XXIII Ciclo, Department of Information Engineering, Electronics and Telecommunications, SAPIENZA, University of Rome, December, 2010
7. Y.W. Yeap, “Ultra Wideband Signal Generation”, Microwave Journal, September 2006.
8. Дьяконов В. П. Сверхскоростная твердотельная электроника. Т. 1: Приборы общего назначения – М.: ДМК Пресс, 2013. – 600 с.
9. Гордеев Б.Н., Зивенко А.В., Наконечный А.Г. Формирование зондирующих импульсов для полиметрических измерительных систем // Автоматика. Автоматизація. Електротехнічні комплекси та системи, 2010, №1(25), стр. 69-72
10. Hewlett-Packard Application Note AN918: Pulse and Waveform Generation with Step Recovery Diodes. Hewlett-Packard, 1984.
11. Jianming Zhou, Qiuyuan Lu, Fan Liu, Yinqiao Li «A Novel Picosecond Pulse Generation Circuit Based on SRD and NLTL», PLOS ONE, February 2016, p.1-10.
12. Han, J., Nguyen, C. A new ultra-wideband, ultra-short monocycle pulse generator with reduced ringing. *IEEE Microwave and Wireless Components Letters*, 2002, vol. 12, no. 6, p. 206 - 208.

УДК 621.396.1

ДИНАМІЧНИЙ ДОСТУП ДО СПЕКТРУ В МЕРЕЖАХ КОГНІТИВНОГО РАДІО: ПІДХІД, ЩО ВИКОРИСТОВУЄ ТЕОРІЮ ІГОР

Журавель А.С., Кравчук С.О.
Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна
E-mail: anseezhur@gmail.com

Dynamic spectrum access in cognitive radio networks: the game theoretic approach

The spectrum access problem in cognitive radio networks from the game theoretic approach perspective was considered. The problem was represented as a non-cooperative spectrum access game.

Зважаючи на широке застосування безпроводових мереж доступу, як основного методу передачі даних між системами, не можливо не брати до уваги проблему обмеженості вільного радіочастотного спектру, що з кожним роком вимагає більш прогресивних та оптимальних рішень щодо його використання [1].

Технологія когнітивного радіо дозволяє телекомунікаційним мережам безпроводового доступу використовувати спектр динамічним чином.

Найбільш відомим застосуванням технології когнітивного радіо є техніка динамічного доступу до спектру DSA (Dynamic spectrum access). На даний час існує декілька моделей та методів даної технології, серед яких варто виділити метод, що використовує теорію ігор GTA (Game Theoretic Approach).

GTA може бути пояснений як математична структура, що включає в себе моделі та методи, які використовуються для аналізу поведінки рішень індивіда, з огляду на його інтерес до власної вигоди. В загальному ж, це математичний інструмент, що аналізує та планує взаємодію між декількома особами, що приймають рішення.

Основними компонентами GTA є: особи, що приймають рішення; простір дій; комплект утиліт (чи функцій виграшу) [2].

Даний підхід є найбільш перспективним та прийнятним методом для систем CR (Cognitive Radio), завдяки своїй головній властивості – рівновазі Неша - Nash Equilibrium (NE). В NE, вважається, що кожен гравець знає

рівноважні стратегії інших гравців, і ніхто не матиме зиску за рахунок зміни стратегії [3]. Кожен з раціональних користувачів мережі дбає лише про власну вигоду і вибирає оптимальну стратегію, яка може максимізувати його/її функцію виграшу і такий результат називають рівновагою Неша в грі некооперативного спільного використання спектра [4].

Запропонована модель гри розглядається з урахуванням як нееластичних, так і еластичних вимог до трафіку (для моделювання програм у режимі реального часу та передачі даних), які можуть бути відправлені по одному або декількох діапазонах спектру частот, що належать різним первинним операторам PO (Primary Operator).

Система мережі когнітивного радіо розглядається з урахування набору V = {1, ..., N} первинних операторів, кожен з яких працює на окремому частотному спектрі Fn і має власних первинних користувачів, а також набір U = {1 , ..., I} вторинних користувачів SU (Secondary User), які бажають розділяти частотні спектри { F1, ..., Fn } з основними користувачами [5].

Кожен SU може одночасно передавати по декількох смугах спектра, розподіляючи свій трафік на безліч доступних каналів, тим самим вибираючи, які первинні оператори будуть транспортувати свій трафік. В роботі розглядається два різних типи трафіку:

1. Нееластичний трафік: кожен SU має фіксовану кількість потоку для передачі, і має на меті мінімізувати його об'єктивну функцію, що являє собою загальну вартість заторів (затримок), виявлену на всіх використовуваних каналах.

2. Еластичний трафік: у цьому випадку вимоги користувачів залежать від витрат через перевантаження каналів, а також від корисності, що визначається при передачі трафіку через доступні канали.

Для розгляду вищеописаної системи мережі когнітивного радіо може бути використаний наступний сценарій (рис.1):

Рис.1 ілюструє приклад сценарію мережі когнітивного радіо з одним первинним оператором та трьома вторинними користувачами (SU_1, SU_2 and SU_3): SU_1 та SU_2 взаємодіють один з одним на каналі *n*, в той час як SU_3 не взаємодіє з жодним з них [6].

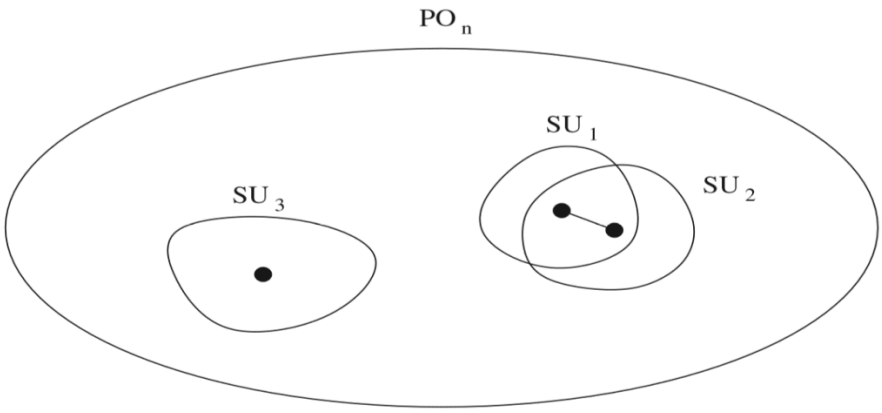


Рис. 1. Приклад сценарію мережі когнітивного радіо

В роботі було проведено розгляд проблеми доступу до спектру в мережах когнітивного радіо з теоретичної точки зору. Проблема була сформована як некооперативна гра, в якій вторинні користувачі отримують одночасно доступ до декількох діапазонів спектрів, залишених основними користувачами, оптимізуючи їх цільову функцію, яка враховує залежність від завищення функцій вартості. Було враховано як еластичні, так і нееластичні вимоги до трафіку, підтверджено та підкріплено розрахунками існування рівноваги Неша. Було також розглянуто декілька можливих мережевих сценаріїв, результати досліджень вказують на невелику різницю між рівновагою Неша та оптимальними рішеннями в усіх розглянутих сценаріях. Подальші дослідження з урахуванням отриманих результатів можуть бути спрямовані на розробку механізмів для створення соціально-оптимального використання мережі.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи широкосмугового радіодоступу. – К.: Наукова думка, 2009. – 312 с.
2. Журавель А.С., Кравчук С.О. Безпроводові мережі доступу з динамічним вибором спектру. – 2017.
3. Asma Amraoui, Badr Benmammar. Dynamic spectrum access techniques. LTT Laboratory, University of Tlemcen, ALGERIA.
4. Pinki Yadav, Subhajit Chatterjee, Partha Pratim Bhattacharya. A survey on dynamic spectrum access technique in cognitive radio. - International Journal of Next-Generation Networks, 2012.
5. Z. Ji, K. Liu. Dynamic spectrum sharing: a game theoretical overview. –IEEE Communications Magazine, 2007.
6. Jocelyne Elias, Fabio Martignon, Antonio Capone, Eitan Altman. Non-cooperative spectrum access in cognitive radio networks: A game theoretical model. – Computer networks, 2011.

УДК 62.799

СИСТЕМА ДЛЯ ВИЗНАЧЕННЯ КОНЦЕНТРАЦІЇ ДОМІШОК У ДИСПЕРСНОМУ СЕРЕДОВИЩІ

Адаменко І.О., Губар В.Г.
Факультет електроніки КПІ ім. Ігоря Сікорського, Україна
E-mail: ira_adamenko@ukr.net

System for determining the concentration of impurities in a dispersed environment

The project describes the way to create a new system for automatic control of the amount of impurities in a dispersed medium. The system consists of two units: a control unit and a measuring unit that are connected by wireless communication. The measurement unit is built on the basis of a nephelometric technique and modulation of the intensity of the light flux, it contains several optical channels, which increases the accuracy of the measurements. The measurement results are transmitted to the control unit and analyzed.

На сьогодні ситуація у світі з постачанням населенню якісної питної води не може вважатися задовільною. Критеріями якості питної води є її вплив на здоров'я людини при тривалому вживанні, відсутність шкідливих елементів, мікроорганізмів та бактерій. На жаль, більшість басейнів річок і водоймищ, із яких забезпечують потреби населення у воді, не можна вважати екологічно безпечними.

З розвитком і широким поширенням експрес-аналізу рідин, газів виникає потреба в простій, надійній та недорогій апаратурі, що дозволяє проводити аналіз дисперсних середовищ.

Метою даного проекту є розроблення автоматичної бездротової системи, яка дозволить проводити вимірювання концентрації дисперсних домішок у рідині, газах.

Для оптимального вирішення даного завдання було розглянуто існуючі базові методи, покладені в основу такої апаратури. Аналітична апаратура, існуюча у світовій практиці, відрізняється великою універсальністю й інформативністю. Однак, вартість подібних аналітичних комплексів - від сотень тисяч до мільйонів доларів. На цей час кількість простих, малогабаритних, автономних систем – невелика. В цілому це прилади кондуктометричного типу, аналітичні можливості яких не завжди можна вважати оптимальними.

Принцип контролю, який базується на релеєвському світлорозсіюванні, відомий дуже давно. Однак, існуючі на даний час прилади мають велику кількість вагомих недоліків, що заважає їх ширшому використанню.

Основні недоліки існуючих приладів:

- дуже чутливі до стороннього випадкового засвітлення;
- великі габарити;
- низька точність вимірювань;
- складність створення оптико-механічного перетворювача;

- складність організації подачі зразкової рідини;
- обмежені функціональні можливості.

Система складається з блока керування та блока вимірювання (передбачено розширення кількості блоків вимірювання). Кожний вимірювач використовує ефект Тіндаля та модуляцію інтенсивності світлового потоку, яка здійснюється електронним, а не механічним способом - це значно підвищує чуттєвість приладу. Для зменшення похибки вимірювання, використовують декілька окремих оптичних каналів. Точність вимірювання досягається цифровою обробкою даних, що забезпечується використанням мікроконтролеру. Це дозволяє також збільшити функціональні можливості та зменшити габарити вимірювальних блоків. Керування усіма вимірювальними блоками виконується головним блоком за допомогою бездротового зв'язку. Результати передаються на WEB-сторінку та РК-дисплей.

Система складається з двох умовних блоків: блока керування та N блоків вимірювання.

Блок керування складається з:
- блока Wi-Fi зв’язку,
- мікроконтролера,
- блока відображення,
- блока клавіатури,
- блока інтерфейсу керуючого пристрою.

Кожний блок вимірювання містить:
- блок інтерфейсу,
- мікроконтролер,
- декілька електронно-оптичних каналів.

На блок керування поступає сигнал початку роботи, режимів роботи (з блоку Wi-Fi зв’язку, або з блока клавіатури). Блок керування регулює запуск блоків вимірювання, приймає результати вимірювань з кожного блока вимірювань, аналізує отримані дані (у випадку відхилень від норми інформує користувача) та отримані результати вимірювань, у зручному для користувача форматі, передає на створену веб-сторінку та блок відображення.

Головним завданням блока керування є контроль роботи блоків вимірювання, аналіз, прийом та передача отриманих результатів. Для цього необхідно використовувати мікроконтролер, Wi-Fi модуль для передачі результатів вимірювань на веб-сторінку, блок інтерфейсу для зв’язку з блоками вимірювання, РК-дисплей для виводу результатів вимірювань та інформації по налаштуванню, кнопки для запуску системи. Параметри вимірювання задаються блоком керування через бездротовий зв’язок. Блок вимірювання містить монохроматичні освітлювачі (наприклад, світлодіодів), які працюють з різною довжиною хвилі. Світлові коливання з блоку монохроматичних освітлювачів йдуть на оптично-лінзову систему, яка формує для кожного каналу паралельний пучок світла, направлений на

бокову поверхню ємності з досліджуваним середовищем, яке містить домішки, концентрацію яких потрібно дослідити. У випадку, коли наявні домішки, то, згідно ефекту Тіндаля, світло розсіюється у всіх напрямках. Під прямим кутом до блоку монохроматичних освітлювачів розташовано оптично-лінзову систему, яка побудована на основі N короткофокусних лінз (для кожного каналу окрема), що концентрує потік розсіяного світла на поверхні окремого фотоперетворювача з блоку фотоперетворювачів. Сигнал з якого підсилюється своїм операційним підсилювачем та передається на смуговий фільтр, який виділяє частоту каналу. Таким чином, пристрій сприймає саме те світло, яке йде з освітлювача на визначеному каналі. Отриманий сигнал потрапляє на вхід аналого-цифрового перетворювача. Мікроконтролер виконує порівняння результату вимірювання з еталонним значенням (при абсолютно чистій вимірювальній рідині). Результати вимірювань поступають на двонаправлений вхід до блоку інтерфейсу для подальшої систематизації результатів вимірювань.

Приведено аналіз існуючих методів, технічних рішень, що дало змогу вибрати в якості базового методу для виконання вимірювання нефелометричний метод. Таке рішення дозволяє будувати прилади автоматичного, швидкого та точного вимірювання чистоти рідини. Наведено результати проведеного аналізу існуючих технічних рішень за даними літературних джерел та патентного пошуку. Це дозволило сформувати уявлення про конструктивні, структурні рішення, параметри, характеристики та розробити патентоспроможну структурну схему автономної фотометричної системи, яка відрізняється від існуючих розширеною кількістю оптичних каналів, збором та аналізом результатів у блоці керування, наявністю двонаправленого каналу обміну даних через блок інтерфейсу.

Література

1. Кульский А. Л. Автоматизация и регулирование электрохимических установок для обработки воды. Сб. «Интенсификация процессов обеззараживания воды». Киев, Наукова думка, 1978, с. 120
2. Аналитические приборы и приборы для научных исследований. М.: Информприбор, 1984 - Вып. 4. с. 327.
3. Карякин А.В., Грибовская И.Ф. Методы оптической спектроскопии и люминесценции в анализе природных и сточных вод. М.: Химия. 1987. 304с.
4. Рам А. Г. Рассеяние света малыми частицами. Оптика и спектроскопия. 1977 г.№3, с. 531
5. Пилипенко А. Т., Бабко А. К. Фотометрический аналіз. М., «Химия», 1974 г., 360 с.
6. КХХВ АН УССР. Кульский А. Л. «Исследование и разработка метода контроля и регулирования процессов электрохимической очистки воды». Диссертация на соискание ученой степени к.т.н. Киев -1981г.
7. Цифровые и аналоговые интегральные микросхемы: Справочник / С.В. Якубовский, Л.И. Ниссельсон, В.И. Кулишова и др.; Под ред. С.В. Якубовского. - М.: Радио и связь, 1990. - 496с.: ил
8. Савельев А.Я., Овчинников В.А. Конструирование ЭВМ и систем: Учебник для техн. вузов по спец. "Электрон. выч. маш." - М.: Высш. Шк., 1984. - 248с., ил.

УДК 621.396.1

РЕАЛІЗАЦІЯ MIMO-СИСТЕМИ ДЛЯ ТСВА ШЛЯХОМ ФОРМУВАННЯ ВІРТУАЛЬНОЇ АНТЕННОЇ РЕШІТКИ

Кравчук С.О., Кравчук І.М.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

Implementation of the MIMO-system for HAPS by forming a virtual antenna array

A mathematical model of the virtual antenna system MIMO was developed by combining a constellation of interconnected stations on the basis of a high-altitude aeroplatform lying in the field of view of the terrestrial terminal. In this case, in the case of shaded Raysov fading, a function of probability density (PDF), cumulative distribution function (CDF), probability of interruption of communication and ergodic bandwidth of the system for the signal / noise ratio on the receiver of the user terminal are developed.

Одним із шляхів створення нових систем широкосмугового радіодоступу 5G із значним зростанням пропускної здатності є застосування багатоантенної просторово-часової обробки MIMO. Однак впровадження такої технології вимагає значного ускладнення обладнання. Тому використовують спрощені системні підходи її реалізації, зокрема підхід віртуальної антенної решітки (ВАР) [1-4].

Модель нашого сценарію будується за припущенням, що кожна приймально-передавальна станція на висотній аероплатформі (СВА) має одну антену і спроможна встановлювати користувацький зв'язок із наземним терміналом. Також СВА підтримують міжплатформенні радіолінії одна з одною. Існують лінії зв'язку базової магістральної мережі від СВА до наземних станцій або супутникових систем. За допомогою синхронної обробки на наземній станції, кожна СВА може отримати необхідний вибір часу і синхронізацію несучої. Тому множина СВА може передавати сигнали на приймач на одній частоті і в одному часовому інтервалі. У результаті множина одноантенних СВА формують ВАР. Множина із $N_{\text{сва}}$ СВА є еквівалентом розподіленої антенної системи із $N_{\text{сва}}$ антен. В залежності від наявної кількості антенних елементів на наземній користувацькій станції можна формувати режим віртуального MISO (multiple-input single-output) при одинарній антені або MIMO – при багатоантенній системі.

Якщо наземний термінал може встановлювати зв'язки з кількома СВА, то його функціонування визначається з урахуванням кількості активних антенних елементів СВА. При цьому можна забезпечити цілий ряд додаткових переваг з точки зору користувачів: поліпшення швидкості

передачі даних та цілісності інфраструктури, гнучкість маршрутизації сигналів, кооперативна ретрансляція та подолання нестабільності аероплатформи, що погіршує продуктивність системи тощо.

В даному сценарії маємо виграш від рознесення, який пояснюється наявністю множини антен (антенних елементів), які використовують некорельовані сигнали в кожній приймальній антені, і дозволяють зменшити амплітуду завмирань шляхом об'єднання сигналів, а потім досягти виграшу в продуктивності. Принцип цього полягає в тому, що коли на кожен канал впливає незалежне завмирання, СВА передає ряд копій одного й того ж сигналу по різних каналах, що може одночасно значно зменшити ймовірність глибокого затухання у всіх копіях. Таким чином, завмирання радіоканалу може бути зменшено і продуктивність передачі також поліпшено. Крім того, різні шляхи некогерентних сигналів по-різному обробляються приймачем, що може значно зменшити частоту бітових помилок (BER) інформації та ефективно протистояти блокуванням перешкод.

Приймемо, що кількість СВА є Nсва = N_H, кількість приймальних антен на наземному терміналі - N_r, вектор передаваємого сигналу - $s(t) \in C^{N\text{сва x } 1}$, який має енергетичне очікування $M[|s(t)|^2] = 1$. Вектор формування променю в MIMO-передавача може бути записаний у вигляді $\mathbf{w}(N_{\text{сва}}\text{x}1)$. Сигнал передається через канал з матрицею комплексних коефіцієнтів передачі $\mathbf{H}(t) = [h_{ij}(t)]_{N\text{r}\text{x}N\text{сва}} \in C^{N\text{r}\text{x}N\text{сва}}$, і приймається з використанням вектору формування променю **v**.

Отримана ймовірність переривання зв’язку в радіоканалах сценарію, що розглядається, наступна:

$$P_{out} = P_r(SNR \leq SNR_{th}) = F_\gamma(SNR_{th}) = \frac{\exp(-\text{tr}(\lambda))|\Psi(\frac{\text{x}\sigma^2}{\delta^2 SNR_{th}})|}{|\mathbf{V}|\left(\Gamma(1+N_{Hr}-N_{rH})\right)^{N_{rH}}}, \qquad (1)$$

де N_{rH} = min $\{N_{\text{сва}}, N_r\}$; N_{Hr} = max $\{N_{\text{сва}}, Nr\}$; tr(…) - оператор трасування; $\mathbf{\Psi}$(x) – матрична функція розмірністю $N_{rH} \times N_{rH}$ з елементами $\{\Psi(x)\}_{i,j} = \int_0^\infty z^{t-i} exp(-z_0)_0F_1\left(1 + N_{Hr} - N_{rH};\ \lambda_j z\right)dz$; $i,j = 1, 2, \ldots, N_{rH}$; ${}_pF_q(.,.)$ - узагальнена гіпергеометрична функція з параметрами p і q; Γ(., .) - неповна гамма-функція; α^2 і $2\sigma^2$ - відповідно потужності компонент LOS і NLOS;

$\kappa = \alpha^2 / (2\sigma^2)$ – коефіцієнт Райсона; $\mathbf{H}_{LOS}(f)$ – канальна матриця затінених LOS-компонент; $\mathbf{H}_{NLOS}(f)$ – канальна матриця розсіяних та NLOS-компонент; $|V| = \prod_{i<j}^{NrH}(\lambda_i - \lambda_j)$. Розкладання по власних значеннях крос-кореляційної матриці слід, по-перше виконати рішення векторів формування діаграми

спрямованості **w** і **v**, щоб максимізувати SNR приймача. Його можна представити як

$$\mathbf{H}^H\mathbf{H} = [\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_{N_H}]\, diag\,(\lambda_1, \lambda_2, \cdots, \lambda_{N_H})\, [\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_{N_H}]^H, \quad (3)$$

де $\lambda_1 > \lambda_2 > \ldots$, $\lambda_N > 0$ - ненульові відмінні власні значення, а λ_1 і $\mathbf{u}_1$ - максимальне власне значення та відповідний вектор характеристики, відповідно. Оптимальний вектор формування променю може бути представлений: $\mathbf{w} = \mathbf{u}_1$ і $\mathbf{v} = \mathbf{H}\mathbf{u}_1 / \|\mathbf{H}\mathbf{u}_1\|_F$, де $\|\ldots\|_F$ - оператор норми Фробениуса. Тоді максимальне значення SNR приймача має вигляд $SNR = \lambda_1 SNR_s$.

Ергодична пропускна здатність системи за нашим сценарієм буде:

$$C_e = \mathrm{M}\left[\Delta f \sum_{i=1}^{r} \log_2\left(1 + \frac{P_i\lambda_i}{N_{\text{сва}}\sigma^2}\right)\right] = \\ = M\left[\Delta f \log_2 \prod_{i=1}^{r} (1 + P_i\lambda_i / N_{\text{сва}}\sigma^2)\right], \quad (2)$$

де Δf – ширина полоси частот підканалу.

Для моделювання запропонованого сценарію було застосовано середовище MATLAB R2014a. При цьому було прийнято: $N_{\text{сва}} = N_r = 1, 2, 4$; $SNR = SNR_{th} = 12$ дБ.

На рис. 1 наведено залежність ймовірності переривання зв'язку від середнього значення SNR при різній кількості СВА і антенних елементів наземного терміналу (пари цифр в скобках відповідають парі антен каналу MIMO).

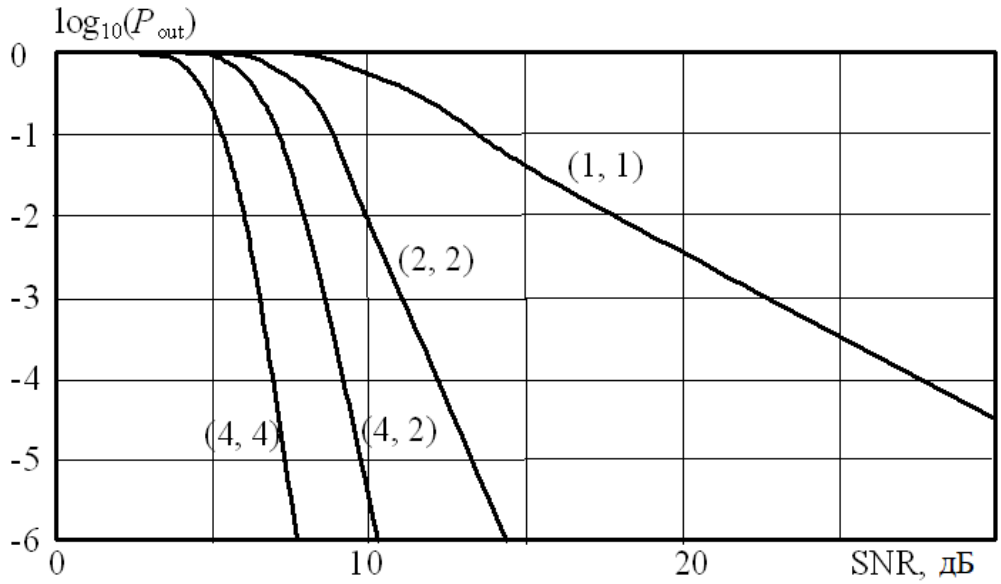


Рис. 1. Залежність ймовірності переривання зв'язку від середнього значення SNR при різній кількості СВА і антенних елементів наземного терміналу (пари цифр в скобках відповідають парі антен MIMO, $SNR_{th} = 12$ дБ)

Можна помітити, що продуктивність каналу MIMO (2, 4) краща, ніж (2, 2). Це відбувається тому, що хоча кількість СВА парна, кількість користувацьких антен збільшена, щоб забезпечити більше підканалів (або шляхів рознесення) зв'язків між передавачем та приймачем. Конфігурація (2, 2) має 4 підканалів, а (2, 4) має 8 підканалів. Таким чином, конфігурація (2, 4) може забезпечити більш високий коефіцієнт виграшу рознесеного прийому. Крім того, з рис. 1 можна спостерігати, що продуктивність (4, 4) краща, ніж у (4, 2), а продуктивність (4, 2) краща, ніж у (2, 2), а продуктивність (1, 1) - найгірша. Отже, це вказує, що в однакових умовах кілька СВА дійсно можуть забезпечити кращу продуктивність системи, ніж один СВА.

Таким чином, розроблено математичну модель віртуальної антенної системи MIMO шляхом об’єднання сузір'я взаємопов'язаних станцій на базі висотної аероплатформи, що лежать в полі зору наземного терміналу. При цьому за умов затінених райсовських завмирань розроблено функцію щільності ймовірностей, кумулятивну функцію розподілу, ймовірності переривання зв’язку та ергодичну пропускну здатність системи для відношення сигнал/шум на приймачі користувацького терміналу. Доведено можливість покращення відношення сигнал/шум на приймачі користувача шляхом збільшення кількості СВА в зоні видимості.

Результати проведеного моделювання підтвердили ефективність запропонованої конфігурації віртуальної антенної решітки для ТСВА та її високої ефективності. Доведено, що віртуальна антенна решітка на базі ряду СВА є перспективним рішенням для майбутніх високошвидкісних та частотно-ефективних інтелектуальних безпроводових мереж 5-го покоління.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Кравчук С.А. Преимущества беспроводной архитектуры распределенной антенной системы над традиционной сотовой структурой // Зб. тез 3-ї міжнародної наук.-техн. конф. "Проблеми телекомунікацій", 21–24 квітня 2009 р., м. Київ, Україна. – К.: НТУУ "КПІ", 2009. – С. 48.
3. Kravchuk S.O. The mathematical model of the outage probability in MIMO-system with Rician fading and limited signal-to-noise relation // Modern information technologies in the sphere of security and defence. – 2015. - Nr 1 (22). – P. 63-67.
4. Кравчук С.О., Міночкін Д.А. Застосування багатоантенної технології MIMO в системах мобільного зв’язку специфікацій Long Term Evolution // Зб. наук. праць ВІТІ НТУУ «КПІ». – 2011. – № 1. – С. 85-99.

УДК 621.396

РЕКОМЕНДАЦІЇ ДЛЯ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ХМАРНИХ СИСТЕМ НА ПРИКЛАДІ OPENSTACK

Кибенко А.В., Лящук А.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: endryu-kibenko@outlook.com, aliashchuk@outlook.com

Recommendations for improving the security of cloud systems by example of OpenStack

Different types of attacks on the elements of the cloud are considered. Solutions concerning the protection from cloud computing security threats are presented.

Не секрет, що хмарні технології, в даний час, перебувають на хвилі популярності: економічність, легкість розгортання, розрахована на багато користувачів архітектура – все це сприяє швидкому поширенню хмар і захоплення ними більшої частини ринку IT. Економічність хмар робить їх особливо популярними для зберігання інформації. Однак хмарна інфраструктура також представляє підвищені ризики і більш обмежену можливість контролю. В цьому і полягають головні проблеми хмарних обчислень – захист інформації та довіру користувачів по відношенню до хмарних провайдерів.

Ключовими елементами хмарної системи є гіпервізор, який керує віртуальним середовищем хмари, центр обробки даних, на якому міститься велика частина конфіденційної інформації, канал зв'язку між споживачем хмарного сервісу, а також ПЗ, встановлене на комп'ютері споживача (зокрема, інтернет-браузер) [1].

Як і будь-яка система, яка функціонує за допомогою Інтернету, хмарна система часто піддається атакам. Основними видами таких атак є: традиційні атаки на ПЗ, атаки на клієнта, мережеві атаки, атаки на сервери хмари і комплексні атаки.

Далі докладніше розглянемо рекомендації щодо підвищення рівня безпеки на серверах хмари, так як система OpenStack встановлюється безпосередньо на них. Для убезпечення даної системи, необхідно забезпечувати безпеку кожного компонента OpenStack, вибираючи для цього найбільш ефективні рішення відповідно до ролі кожного з компонентів і його важливістю в рамках комплексного середовища OpenStack.

Безпека OpenStack CLI. Використання інструментів OpenStack CLI вимагає застосування імені користувача та пароля. Рекомендовано використовувати змінні OS_USERNAME і OS_PASSWORD, встановлені у файлі OpenStack RC. Проте, зберігання в звичайному, незашифрованому файлі реквізитів для ідентифікації суперечить зарекомендованим практикам забезпечення безпеки.

Для додаткового забезпечення захисту, інструменти OpenStack CLI можуть запитувати ім’я користувача та пароль для кожного запиту, або ж

використовувати наданий токен ідентифікації. Також для цих цілей можуть бути використані вузол або віртуальна машина, розташовані в окремій внутрішній демілітаризованій зоні, або інструменти OpenStack CLI, розташовані в цьому додатковому вузлі виключно для подібних цілей. Таким чином важливо забезпечити три основні дії:

- впевнитись в тому, що всі непотрібні сервіси вимкнені;
- дозволити доступ тільки по SSH і через перевірену мережу;
- відключити bash history і зберігати всі логи в ізольованому, віддаленому, захищеному і високодоступному репозиторію зберігання.

Безпека Nova. Сервіс Nova є найскладнішим сервісом OpenStack, оскільки він пов'язаний майже зі всіма сервісами платформи і має велику кількість власних опцій конфігурації. Тому для даного сервісу потрібно приділити найбільшу увагу, пов’язану з посиленням заходів безпеки. Для досягнення найбільшої безпеки для сервісу Nova, потрібно зробити наступне:

- адміністратору системи, який займається конфігурацією файлів, потрібно надати права суперкористувача (root-права). Також потрібно дозволити читати та перезаписувати файли для власника та читати файли для групи;
- відключити PCI-транзитний шлюз на гіпервізорі для обмеження доступу з віртуальної машини до апаратної частини інфраструктури;
- для зниження рівня загроз на адресу тенантів, незалежних користувачів системи, потрібно відключити всі механізми оптимізації пам’яті гіпервізора;
- всі логи необхідно зберігати в захищеному і віддаленому сховищі;
- використовувати TLS для VNC-сесій;
- необхідно переконатись, що Nova безпечно з’єднується з іншими сервісами OpenStack, використовуючи TLS.

Безпека Glance. Даний сервіс дозволяє зберігати образи, які необхідні для запуску нових віртуальних машин. Тому для уникнення замахів на цілісність цих образів важливо підтримувати безпеку даного сервісу. Це забезпечується наступним шляхом:

- використання підписаних образів Glance;
- невикористання вбудованих образів чи контейнерів з неперевірених джерел, оскільки останні можуть містити вразливості або шкідливі програми.

Безпека Neutron. Сервіс Neutron необхідний для забезпечення зв’язаності мережі і IP-адрес для віртуальної машини в хмарі. Даний сервіс заснований на плагінах, тому важливо розуміти, які саме плагіни потрібні для виконання цих завдань, а які використовуються для сторонніх цілей. Тому потрібно забезпечити наступні умови:

- використовуйте лише ізольовану мережу управління для сервісів OpenStack;
- використовуйте ізоляцію L2 з сегментацією VLAN або GRE-тунелі;
- всі API-запити груп безпеки Nova повинні перенаправлятися в Neutron;
- використовуйте мережеві квоти для пом'якшення впливу DoS-атак.

Безпека черги повідомлень Message Queue (RabbitMQ). Черга повідомлень спрощує комунікації для сервісів OpenStack, а RabbitMQ є

найпопулярнішим рішенням в цьому класі для хмар на основі OpenStack. Платформа OpenStack не підтримує підписування повідомлень – таким чином, черга повідомлень повинна забезпечувати захищену передачу в рамках обміну між сервісами OpenStack. Забезпечте наступні умови:

- захистіть RabbitMQ API за допомогою TLS;
- зберігайте логи RabbitMQ в захищеному і віддаленому сховище;
- видаліть гостьового користувача RabbitMQ;
- використовуйте окремий віртуальний хост RabbitMQ для кожного OpenStack-сервісу;
- використовуйте унікальні ідентифікатори повноважень і відповідні права доступу для кожного віртуального хосту RabbitMQ.

Безпека Keystone. Даний сервіс ідентифікує всі сервіси OpenStack, тому повинен бути захищений від, так званого, спуфінгу та від інших атак. Сервіс не надає методів реалізації політики надійності паролів та невдалих спроб аутентифікації, проте він може використовувати зовнішню систему аутентифікації. Для досягнення найбільшої безпеки для сервісу Keystone, потрібно зробити наступне:

- мультифакторна аутентифікація повинна бути задіяна через систему зовнішньої аутентифікації, типу такої, яка присутня в Apache HTTP Server;
- використовуйте токени Fernet, які розроблені спеціально для REST API, так як вони є більш захищеними в порівнянні зі звичайними токенами, а також вимагають менше ресурсів;
- використовуйте домени Keystone для більш точного розмежування прав доступу для тенантів. Власник домену може створювати додаткових користувачів, групи, а також ролі всередині домену.

Безпека Cinder. Cinder забезпечує високий рівень API для управління блоковими пристроями зберігання даних і активно використовується сервісом Nova. Його слід захищати від DoS-атак, витоків інформації, несанкціонованого доступу та інших загроз. Для цого потрібно зробити наступне:

- встановіть розмір максимального запиту;
- для безпечного видалення томів Cinder використовуйте повну очистку томів.

Підсумовуючи можемо констатувати, що на додаток до згаданих вище рекомендацій, вкрай важливо постійно бути в курсі вразливостей OpenStack і прагнути підтримувати робоче середовище оновленим. Зміцнення безпеки середовища OpenStack має відбуватися на декількох рівнях, починаючи з фізичного і продовжуватись на рівні додатків і рівні організації процесів [2].

Література

1. ЕЗОПАСНОСТЬ ОБЛАКА В ДЕТАЛЯХ / П. В. Ивонин. // Безопасность информационных технологий. – 2013. – №2. – С. 37–40.
2. БЕЗОПАСНОСТЬ В OPENSTACK: ШАГ ЗА ШАГОМ [Електронний ресурс] // Сервионика. – 2016. – Режим доступу до ресурсу: http://servionica.ru/pressCenter/view/814/.

УДК 621.391

ДОСЛІДЖЕННЯ КОНВЕРГЕНЦІЇ МЕРЕЖ 2G ТА 3G НА БАЗІ ВУЗЛА IMS

Заболотна А.Ю., Гаттуров В.К.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: anechkazabolotnaya27@gmail.com

RESEARCH OF CONVERGENCE 2G AND 3G NETWORK ON IMS HUB BASE

This article shows the convergence of networks 2G and 3G on the basis of the node IMS and the solution to the task of creating a universal network infrastructure.

Конвергенція телекомунікаційних мереж - об'єднання декількох, які раніше були роздільними, послуг в рамках однієї послуги [1]. Конвергенція породжує нову парадигму, обумовлену можливістю доступу до інформації “у будь-який час, у будь-якому місці, з будь-якого пристрою” [2]. Рушійною силою конвергенції в інформаційно-телекомунікаційних системах є розвиток нових й удосконалення існуючих послуг. Конвергенція фіксованих і мобільних інформаційно-телекомунікаційних платформ і мереж слугує технологією спільного використання ресурсів мобільної та фіксованої мереж зв’язку для надання користувачу єдиного безперервного сервісу поза залежністю від його місця розташування, а також для організації єдиного обслуговування і єдиної тарифікації за послуги.

Протягом багатьох років стільниковий зв'язок розвивався для того, щоб забезпечити інфраструктуру яка буде передавати голос та дані в надійному середовищі обслуговування. На думку розробників, операторів та організацій стандартизації, вирішення задачі створення універсальної мережевої інфраструктури полягає у створенні концепції IMS – мультимедійної IP-орієнтованої підсистеми зв'язку.

Концепція IP Multimedia Subsystem (IMS) описує нову мережеву архітектуру, основним елементом якої є пакетна транспортна мережа, що підтримує всі технології доступу і забезпечує реалізацію великої кількості інфокомунікаційних послуг, які включають в себе голос, дані, відео, чат на

портативному пристрої. Завдяки своїй архітектурі, IMS має можливість надавати ці послуги, як для класичного сервісу так і для комбінованого режиму(пакетним режимом і комутацією каналів).

Так як IMS має незалежність мережевого доступу, це забезпечує конвергенцію з різними мережами які існують сьогодні.

Як відомо, в останні роки оператори стаціонарних мереж активно підтримують перехід від мереж з комутацією каналів до NGN(NEXT GENERATION NETWORK) з комутацією пакетів. Це пов'язано зі скороченням операційних витрат і капітальних вкладень, а також на розвиток нових послуг з метою істотного підвищення доходів.

З прийняттям архітектури Next Generation Networking в базовій мережі, все більше і більше привабливих послуг буде надаватися за допомого IMS. Незалежно від того, чи це послуги для мобільних, фіксованих або фіксованих мобільних конвергентних мереж, всі IP-мережі могли б виконувати перспективні послуги на базі багатих-IP з різноманітними терміналами. На рис.1 приведені складові елементи IMS та їх асоційовані площини, щоб належним чином контролювати активацію та доступ пристроїв або додатків. Будь-яке програмне забезпечення або програмне забезпечення пристрою завжди можуть бути в курсі останніх версій. Журнали кінцевих точок збираються автоматично для подальшого аналізу та діагностики.

В даній схемі варто відмітити елемент HSS. Home Subscriber Server (HSS)- сервер домашніх абонентів, є базою для користувача даних і забезпечує доступ до індивідуальних даних користувача, пов'язаними з послугами. У разі якщо в мережі IMS використовується кілька серверів HSS, необхідно додавання SLF (Subscriber Locator Function) який займається пошуком HSS з даними конкретного користувача. HSS поєднує HLR (база даних, яка містить інформацію про абонента мережі GSM-оператора) та UMS.

HSS забезпечує:

- Функції HLR / AuC для CS домену;

- Функції HLR / AuC для PS домену;

- Функції аутентифікації, авторизації, управління профілями послуг, локалізації для IMS (адреса S-CSCF).

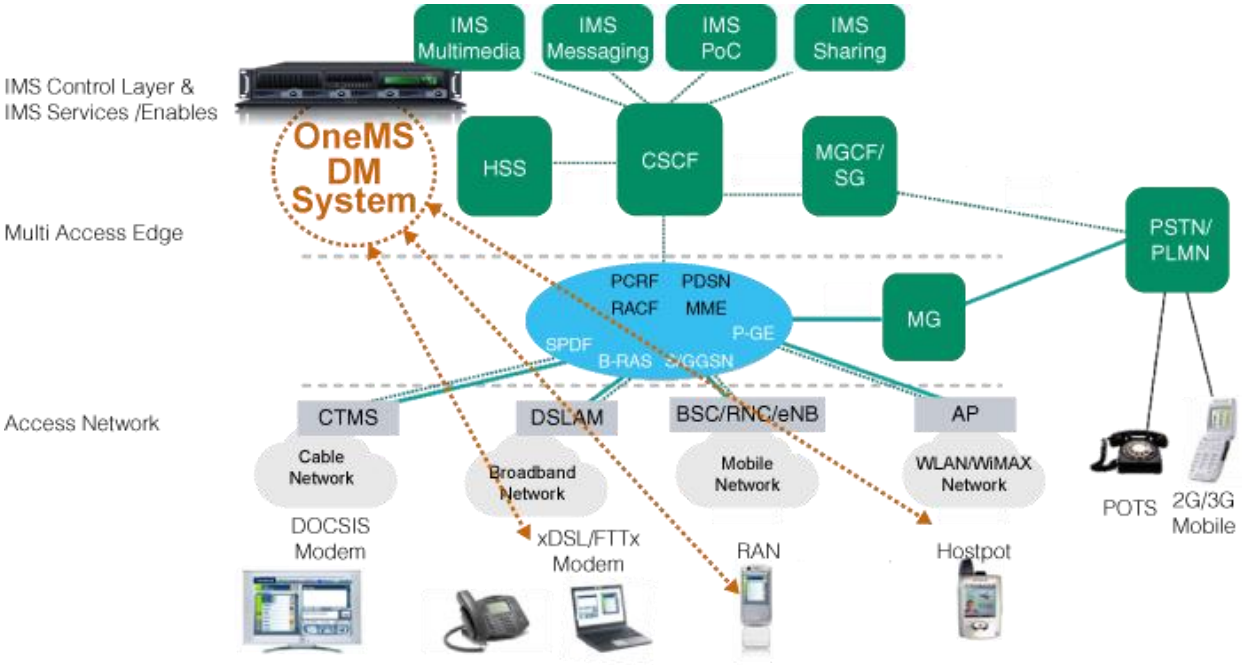


Рис. 1. Складові елементи IMS та їх асоційовані площини.

Висновки. Таким чином розробка та впровадження платформи IMS дозволяє реалізувати конвергенцію мереж на рівні доступу та забезпечити формування сервісів, що існують на пакетних мережах.

Література

1. Г.Г. Яновський – Конвергенція в інфокомунікаціях. [Електронний ресурс] // Режим доступу до ресурсу: http://www.seti.sut.ru/wp-content/uploads/2015/09/conv_info1.pdf.
2. Менаске Д., Алмейда В. Продуктивність WEB-служб.
3. Перспективи розвитку IP-телефонії: SIP та IMS. [Електронний ресурс] // Режим доступу до ресурсу: http://oldconf.neasmo.org.ua/node/860.

УДК 621.396.1

ІЄРАРХІЧНА СИСТЕМА УПРАВЛІННЯ І ТЕЛЕМЕТРІЇ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Кравчук С.О., Афанасьєва Л.О., Кравчук І.М.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

Hierarchical control system and telemetry for intelligent unmanned aerial vehicles

A hierarchical flight control system for intelligent UAVs is proposed that provides autonomy, allowing coordination between members of the swarm team. The UAV dynamics is identified by applying the parametric identification method to the collected flight data. A control method based on a multi-cyclic proportional-integral-differential controller and controller of a non-linear model of intelligent tracking is presented.

Запропоновано ієрархічну систему управління польотом для інтелектуальних БПЛА, що забезпечує автономію, дозволяючи координацію між членами команди рою. Динаміка БПЛА ідентифікується шляхом застосування методу параметричної ідентифікації до зібраних польотних даних. Представлено метод управління, що базується багатоцикловому пропорційно-інтегрально-диференціальному контролері і контролері нелінійної моделі інтелектуального відстеження [1-4].

Такий метод є відносно новим підходом, який дуже ефективний при адресній нелінійності, пов'язуванні, вхідному і насиченому стані.

Низький ступінь стабілізації аероплатформи підключається до планувальника стратегій вищого рівня за допомогою мови керування транспортним засобом VCL (vehicle control language), інтерфейсу мови сценарію для автономних агентів, а також операторів-людей, які керують приймаючою аероплатформою. Кожен автономний агент є частиною безпроводової мережі зв'язку, за допомогою якої складні завдання можуть виконуватися узгоджено.

В якості орієнтирних завдань розглядаються наступні сценарії: спосіб навігації по всьому шляху, ухилення від переслідування, відстеження наземних цільових місць та посадка. Ці сценарії є прикладом однієї або декількох функцій ієрархічної багатоагентної системи. Погоня-ухилення розглядається як імовірнісні міркування для планування стратегії, мультиагентної координації по безпроводовій мережі, динамічної роботи VCL, і бачення на основі зондування. Наземне цільове спостереження та зорієнтовані експерименти на посадку включають високошвидкісне управління відстеженням положень, технологію визначення та цільового призначення бортового модуля обробки зору (відео-інформації) як

планувальника стратегії.

«Інтелектуальний агент» безперервно (рис. 1. 1) сприймає умови в своєму середовищі, що динамічно змінюються, (рис. 1. 2) причини, щоб інтерпретувати сприйняту інформацію, для вирішення проблеми і визначення відповідні дії, і (рис. 1. 3) діє належним чином щоб вплинути на умови в його оточенні. На основі цих атрибутів описується кожен шар в ієрархічній системі управління польотом, представленої на (рис. 1. 7, 2).

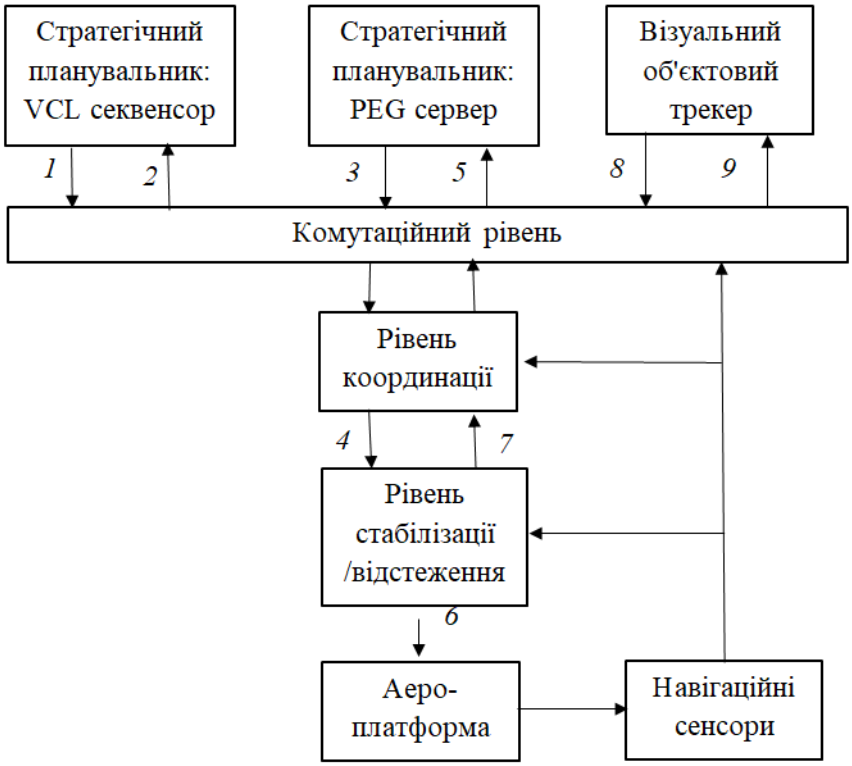


Рис. 1. Багатоциклічна ієрархічна система управління БПЛА:
1, 3, 8 - пункти призначення; *2, 5, 9* - повідомлення про конфлікт;
4 - довідкова траєкторія режиму польоту; *6* – контрольний вхід (ввід управління);
7 - помилка відстеження (VCL - vehicle control language, PEG - pursuit-evasion game)

Комп'ютер бортового польоту є центральним елементом управління, навігації та керування основним БПЛА. Він відповідає за керування аеропалатформи у режимі реального часу, інтеграцію з датчиками та зв'язок між агентами. Програмне забезпечення для управління польотом може бути реалізовано в операційній системі QNX в реальному часі. Вхід в систему керування сервоприводом обчислюється на частоті 50 Гц за допомогою алгоритмів керування польотом. QNX базується на ідеї роботи основної частини своїх компонентів (сервіси) поза ядром. Це відрізняє її від традиційних монолітних ядер, в яких ядро операційної системи — це одна велика програма, яка складається з багатьох «частин». Використання мікроядра в QNX дозволяє відключати будь-яку непотрібну в поточній

ситуації функціональність без зміни ядра.

QNX призначена для застосування в автоматизованих системах, що пред'являють до операційних систем підвищені вимоги з безпеки і захищеності: глибина контролю відсутності декларованих можливостей, наявність вбудованих механізмів захисту інформації від несанкціонованого доступу (НСД), можливість створення прикладних засобів захисту інформації від несанкціонованого доступу.

Система навігації побудована на основі INS (asinertial navigation system) і GPS (global positioning system). INS забезпечує розташування, швидкість, кути повороту та ставки за будь-якої високої швидкості. Недоліком INS є необмежена помилка, яка швидко зростає з часом. Це може бути ефективно виправлено датчиком зовнішньої позиції таким як GPS. Через природу додаткових INS і GPS, поєднання цих датчиків стала стандартною конфігурацією для безпілотних літальних апаратів. Для того, щоб отримати інформацію про навколишнє середовище, таку як відносна відстань від землі або до сусідніх об'єктів, мають місце лазерні далекоміри, ультразвукові датчики та датчики зору.

Запропонований контролер складається з трьох циклів: (рис. 1. 1) контролер внутрішніх відносин, (рис. 1. 2) регулятор швидкості лінійного середнього контуру, і (рис. 1. 3) регулятор положення зовнішнього контуру.

Функція багатоциклічного управління задається системою рівнянь

$$u_{a1s} = -K_\phi \phi - K_v v - K_y \; e_{yS} - K_{Iy} \int e_{yS} \, \mathrm{d}t,$$

$$u_{b1s} = -K_\theta \theta - K_u u - K_x \; e_{xS} - K_{Ix} \int e_{xS} \, \mathrm{d}t,$$

$$u_{\theta_M} = -K_w w - K_z \; e_{zS} - K_{Iz} \int e_{zS} \, \mathrm{d}t,$$

$$u_{r_{ref}} = -K_\psi \psi - K_{I\psi} \int e_\psi \, \mathrm{d}t,$$

де e_{xS}, e_{yS} і e_{zS} – помилки позиціювання по осям (x; y; z), відповідно; e_Ψ - помилка заголовку. Тут і далі: S і B - просторові координати і координати корпусу планера; x^B, y^B і z^B (u; v; і w відповідно, буде використовуватися для простоти запису) позначимо швидкість щодо координат рами кузова; θ, ϕ і ψ - крен, тангаж, нишпорення, а p, q і r – їх швидкості, відповідно; параметри a_{1s} і b_{1s} - поздовжні і бічні кути відбивання; u_{a1s} і u_{b1s} – сигнали управління бічного і поздовжнього циклічного кроку, відповідно.

Живучість каналу визначає спроможність зберігати працездатність в умовах ненавмисних і навмисних завад. Методи, що базуються на канальних параметрах, для покращення живучості були наведені раніше. В даному випадку досліджуються відхилення параметрів польотного управління як результат дії ненавмисних і навмисних завад на канал управління і телеметрії. Таким чином, аналіз живучості каналу управління і телеметрії

при використанні запропонованого багатоциклічного методу полягає в оцінці потенційних можливостей даного методу при внесенні збурень до параметрів курсу польоту утримувати останні в межах допусків з подальшим автоматизованим отриманням показників надійності для конкретного досліджуваного варіанту системи. Такий аналіз також дозволяє визначити рівні ризику експлуатації БПЛА.

При моделюванні системи для каналу телеметрії і управління випадковим чином (скважність 0,1 с) ставились навмисні завади плоского типу, що погіршували відношення сигнал/(шум+завада) на бортовому приймачі до порогового рівня декодування модуляції ФМ4. Це дозволяло моделювати підвищення коефіцієнту помилок каналу до рівня коли зв'язок присутній, але величина помилок (BER більше 10^{-2}) може викликати втрату інформації управління.

Для моделювання використано програмне середовище Matlab/Simulink, та його бібліотеку AeroSim Blockset. Необхідні параметри та моделі Simulink польоту та радіоканалу наведені в [5].

Результати моделювання продемонстрували високу стабільність по відношенню до референтних значень з точністю (±0,5; ±0,5; ±0,2 м; ±2,5 град) по осях (x; y; z; ψ). В цілому параметри крену, тангажу, нишпорення по всіх осях регулюються дуже точно як через канал телеметрії, так і через бортову інтелектуальну систему контролера управління. Наявність останньої зменшує вимоги на завадостійкість каналу телеметрії, виконуючи автономне корегування параметрів управління, що значно підвищує живучість системи управління.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Prospects of using of aerial stratospheric telecommunication systems / M. Zgurovsky, M. Ilchenko, S. Kravchuk, V. Kotovskyi, T. Narytnik, L. Cybulskyi // Proceedings of the 2016 IEEE International Scientific Conference "RadioElectronics & InfoCommunications" (UkrMiCo’2016), 11-16 September 2016, Kyiv, Ukraine. IEEE Conference Publications, 2016. – P. 20-23.
3. Kravchuk S., Kaidenko M. Features of creation of modem equipment for the new generation compact troposcatter stations // Proceedings of the International Scientific Conference "RadioElectronics & InfoCommunications" (UkrMiCo’2016), 11-16 September 2016, Kyiv, Ukraine. – IEEE Conference Publications (IEEE Xplore Digital Library, DOI: 10.1109/UkrMiCo.2016.7739634), 2016.– P. 365-368.
4. Kravchuk S.O., Kaidenko M.M. Modem equipment for the new generation compact troposcatter stations // Information and telecommunication sciences. – 2016. – Vol. 7. – Nu. 1. – P. 5–12.
5. Lindberg H. Modelling and Control of a Fixed-wing UAV for Landings on Mobile Landing Platforms: Master’s Thesis in Systems Engineering, Master Programme in Aerospace Engineering. - Royal Institute of Technology, Sweden. - Stockholm, 2015. – 82 p.

УДК 621.383, 621.396

ПІДХОДИ ДО ФІЗИЧНОГО МОДЕЛЮВАННЯ РАДІОКАНАЛІВ ЗВ'ЯЗКУ МІЛІМЕТРОВОГО ДІАПАЗОНУ ХВИЛЬ

Кременецька Я.А., Морозова С.В., Андреєва Н.О.
Державний університет телекомунікацій, Україна
E-mail: ya.cremen@ukr.net, svmorozova@ukr.net, nataliiandreeva55@gmail.com

Approaches to physical modeling of millimeter-wave communication channel

A quasi-optical multi-beam loss model is proposed that takes into account the divergence of millimeter-wave radiation at a constant aperture of the receiving antenna, channel loss (gain) associated with reflection, absorption, diffraction effects that are typical of the urban scenario. And it is also proposed to take into account in the radio channel models the noise associated with the millimeter-wave generation method.

Освоєння радіотехнологій міліметрового діапазону (ММД) хвиль є важливою ланкою в розвитку 5 G (і наступних поколінь), в мобільному стільниковому зв'язку, в «Інтернеті речей» , в системах зв'язку з використанням безпілотних літальних апаратів і т.д. Дослідження в області створення моделей енергетичного покриття і вибір методу модуляції сигналів ММД є основоположними для проектування таких систем. Розробка точних моделей поширення необхідна для довгострокового розвитку майбутніх бездротових систем ММД, особливо в мобільній індустрії. Наприклад, для реалізації мобільних систем ММД у міському сценарії найбільш перспективним рішенням є використання модуляції однієї несучої, часове та просторове розділення каналів, яке може реалізовуватися у багатопроменевих широкосмугових антенних решітках з високим динамічним діапазоном. Тому розуміння особливостей просторових та часових завмирань (англ. fading) багатопроменевих амплітуд, оцінки втрат та шумів сигналів ММД є важливим для проектування та реалізації майбутніх телекомунікаційних систем [1].

Основні моделі, розроблені дослідницькими групами (5GCM, mmMAGIC, METIS, 3GPP TR 38.901,…) для діапазону 0.5-100 GHz можна розділити на два типи: ймовірнісні моделі LOS Probability, що не залежать від частоти, та моделі, наближені для втрат у вільному просторі, що визначаються формулою Фріїса, – CI (Close-in Model) [1]. В роботі [1] вказано, що нові моделі поширення для MMR повинні наближатися до фізичних. Для малих розмірів стільників 30-150 м, які будуть застосовуватися для мобільних технологій 5 G [1], а також всередині приміщень, потрібно враховувати, наприклад, окремі дифракції та відбивання, а також точну геометрію забудови. Також важливим є те, що на відміну від, наприклад від дециметрового діапазону, основним механізмом поширення MMW є не дифракція, а відбивання, поглинання та розсіювання. Довжина MMW 1-10 мм та вузька ширина променів зменшують розміри

випромінюючих та приймаючих елементів фазованої антенної решітки (ФАР), а також розміри масиву ФАР [2].

При квазіоптичному підході до аналізу енергетичного бюджету та втрат радіосистем ММД можливо використання конусоподібної моделі випромінювання антени, яка використовується для розрахунку оптичних відкритих систем:

$$P_{\text{TX}} = P_{\text{RX}} \frac{4\pi d^2 PL_{atm}(f_c, d)}{D_{\text{TX}} A_{\text{RX}}} \tag{1}$$

де $P_{\text{TX}}, P_{\text{RX}}$ - потужність передавача та прийнятого сигналу відповідно, A_{RX} — площа плоскої апертури використання поверхні; D_{TX} коефіцієнт спрямованої дії, пов'язаний з коефіцієнтом підсилення співвідношенням (k - апертурний коефіцієнт), $D_{\text{TX}} = G_{\text{TX}}/k$; $PL_{atm}(f, d)$ - поглинання сигналу в атмосфері, що залежить від частоти несучої, гідро метеорів і відстані між передавачем та приймачем.

Такий підхід вважається найбільш реалістичним для визначення спрямованості випромінювання антен ММД, в якому передбачається використання ФАР з великою кількістю випромінюючих елементів. Також формулу (1) можна використовувати і для багатопроменевої моделі [3]:

$$P_{\text{RX}} = \frac{P_{\text{TX}} D_{\text{TX}} A_{\text{RX}}}{4\pi r^2} \times \sum_j \left(\prod_m p_m(\theta_j) \frac{\left|\Gamma_m(\theta_{mj})\right|^2}{\rho_m} \prod_n p_n(\theta_j) \left|\text{T}_n(\theta_{nj})\right|^2 \prod_l p_l(\theta_j) \frac{\left|D(\theta_{lj})\right|^2}{\rho_l} \right), \tag{2}$$

де ρ_m, ρ_l > 1 - коефіцієнти, що визначають надлишок шляху променів при відбиваннях і дифракції; $p(\theta_j)$ – ймовірність відповідного процесу для певних умов; Г, T, D– коефіцієнти відбивання, пропускання та дифракції відповідно.

Для аналізу бюджету радіосистем потрібно визначити необхідну потужність сигналу у приймачі, тобто чутливість приймача: $P_{\text{RX-sens}} = P_{\text{S}}(N_{\text{int}} + N_{\text{TX}} + N_{\text{RX}})/N$, де P_{S}/N означає необхідне відношення несучої до шуму для демодуляції. N_{RX} - втрати сигналу у приймачі, N_{int} - інтерференційні завади, які визначаються як сума шумів, пов’язаних із завадами від інших каналів зв’язку N_{K}, шумів, пов’язаних з молекулярним розсіюванням у атмосфері та розсіюванням на неоднорідностях (турбулентності) в атмосфері N_{scatt}, втрати (підсилення) сигналу, пов’язані з явищами дифракції та відбивання на перешкодах (властивих, наприклад, міській забудові) N_{NLOS}. N_{TX} - шум джерела сигналів, який враховує не тільки тепловий шум, але й інші складові, пов’язані зі способом генерації сигналів. Так, для реалізації систем ММД, передбачається використання інтеграції радіо та оптичних технологій. Такі системи називають радіоефірними системами (англ. Radio over fiber, RoF) [4]. Системи RoF мають переваги у порівнянні з електронними системами за способом формування та модуляції інформаційних сигналів (конвертації міліметрових хвиль в оптичному діапазоні, формуванню діаграм спрямованості фотонними методами у ФАР,

частотне мультиплексування радіоканалів та передача сигналів через оптичне волокно на великі відстані (десятки кілометрів) до віддаленої Базової станції або Дата-центру (рис.1).

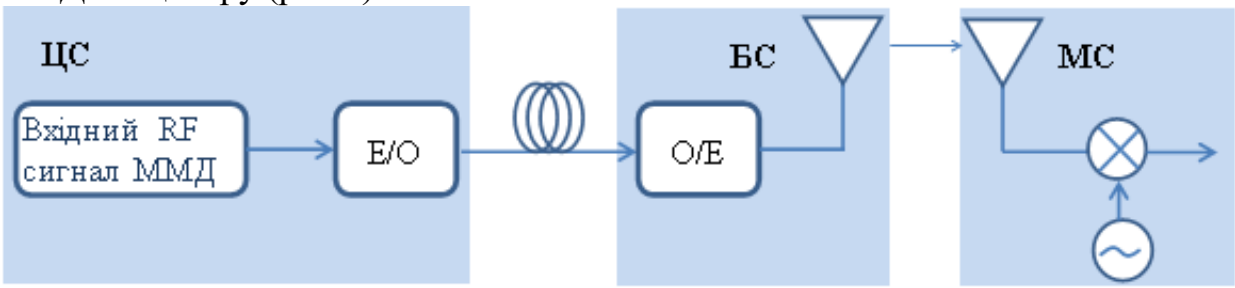


Рис.1. Структура радіоканалу ММД для мобільної системи з використанням технології RoF; ЦС- центральна станція, БС - базова станція, МС - мобільна станція

Основні складові компоненти RoF: волоконно-оптичні лінії, лазери, модулятори, локальні низькочастотні генератори, підсилювачі, фотодетектори, що працюють у певних діапазонах частот (смугах), характеризуються потужністю корисного сигналу та характерних шумів : $\sigma^2_{\text{noise}} = \sigma^2_{\text{thermal}} + \sigma^2_{\text{shot}} + \sigma^2_{\text{RIN}} + \sigma^2_{\text{sig-ASE}} + \sigma^2_{\text{ASE-ASE}}$ ($\sigma_{\text{thermal}}, \sigma_{\text{shot}}$ - тепловий та дробовий шуми відповідно; σ_{RIN} - флуктуації оптичної інтенсивності лазера; $\sigma_{\text{sig-ASE}}$ та $\sigma_{\text{ASE-ASE}}$ - шуми оптичного підсилювача, в якому крім шуму підсиленого сигналу також присутній підсилений шум спонтанного випромінювання, який генерується всередині самого підсилювача.

Інтерференційним завадам присвячено багато теоретичних досліджень. Проте шуми джерела сигналів σ^2_{noise} ММД можуть бути порівняні з інтерференційними завадами. Тому аналіз показників шумів та відношення сигнал/шум потребує подальшого вивчення.

Фотонні методи формування, передачі та розподілу сигналів ММД є перспективним рішенням для телекомунікаційних систем 5G та наступних поколінь. Для проектування та реалізації телекомунікаційних систем ММД, можливо, потрібні нові підходи у розрахунках, наближені до фундаментальних фізичних особливостей поширення, випромінювання та формування сигналів.

Література

1. Overview of millimeter wave communications for fifth-generation (5G) wireless networks-with a focus on propagation models/T. S. Rappaportat, et. al.// IEEE Transactions on Antennas and Propagation, Ukraine, Kyiv, 2017, 18 ст.
2. Хансен Р.С. Фазированные антенные решетки / Р.С. Хансен– М: Техносфера, 2012. – 560 с.
3. Quasi-optical approach to the analysis of the energy model of millimeter wave propagation and antenna characteristics/ Y.A Kremenetskaya., I.O. Liskovskiy, E.R. Zhukova // presented at the IEEE XI International Conference on Antenna Theory and Techniques, 2017, 4 ст.
4. Urick V.J. Fundamentals of Microwave Photonics / V.J. Urick, K.J. Williams, J.D. McKinney. - NJ, USA, NJ: Wiley, 2015 – 488 с.

УДК 621.396.1

ЙМОВІРНІСТЬ ПЕРЕРИВАННЯ ЗВ'ЯЗКУ В ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ НА БАЗІ АЕРОПЛАТФОРМИ ІЗ ЗАДІЯННЯМ МІЖПЛАТФОРМЕННОГО ОПТИЧНОГО КАНАЛУ У ВІЛЬНОМУ ПРОСТОРІ

Кравчук С.О., Кравчук І.М.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

Outage probability of communication in the telecommunication system based aeroplatfom with the employment of cross-platform optical channel in free space

The new architecture of the network of HAPS, which aims at providing broadband radio-access system (BRAS) services over long distances, is presented, using interplatform optical communication lines with possibility of routing in several ways. Stations HAPS act as base stations and combine the total traffic of the terrestrial BRAS network from the area they cover. The HAPS stations have transponders that convert BRAS signals to optical signals and vice versa.

Розвиток телекомунікаційних систем на базі аероплатформ (ТСВА) неможливий без задіяння міжплатформенних ліній зв'язку, причому, найбільш перспективними з точки зору підвищення пропускної здатності таких ліній є застосування оптичних систем у вільному просторі [1-5]. Метою даної роботи є дослідження наскрізного каналу передачі даних між наземними користувацькими терміналами через ряд аероплатформ, з'єднаних через оптичні канали у вільному просторі.

Розглянемо сценарій типової гетерогенної мережі ТСВА із міжплатформенним оптичним каналом у вільному просторі (рис. 1). Для даного сценарію типові значення міжплатформенних відстаней становлять 100…200 км, а висота зависання аероплатформи – 24 км. При цьому приймемо наявність дисперсії Ритова, яка є показником вираженості турбулентності, досить мала, і тому сцинтиляційні ефекти мають незначний ефект і можуть бути проігноровані.

Джерело на станції висотної аероплатформи (СВА) зв'язується з СВА-призначення через R_i (i = 1; 2;…; N – 1) оптичних приймально-передавальних пристроїв, що діють як ретранслятори в рівновіддаленості один від одного d_O, створюючи при цьому ланцюг із N з'єднань типу точка-точка. Кожен проміжний вузол в мережі з великою кількістю ретрансляцій діє як маршрутизатор, який направляє трафік до місця призначення. Такий підхід

також може бути запропонований для посилення наземної оптичної безпроводової передачі шляхом пом'якшення різноманітних порушень, таких як турбулентність. У даному дослідженні ми розглядаємо *N*-1 прольотів, де кожен має знання стану каналу попереднього прольоту. Прийнято використання ретрансляції типу прямого підсилення AF (amplify-and-forward) без декодування сигналу.

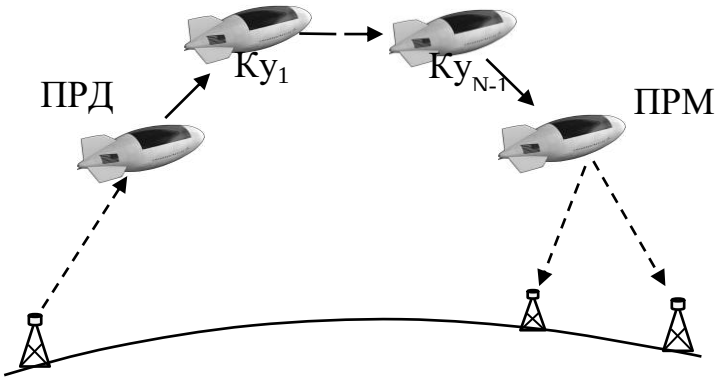


Рис. 1. Сценарій гетерогенної безпроводової мережі ТСВА на базі міжплатформенного оптичного каналу у вільному просторі

Для модуляції оптичної інтенсивності лазерного діоду використовується високочастотний сигнал $s_{OFDM}(t)$. Зауважимо, що нелінійна характеристика діода створює інтермодуляційні перекручення, які впливають на продуктивність системи.

В найпростішому випадку однопрольотної ретрансляції джерело розглядаємого ланцюга ретрансляцій приймає OFDM системи широкосмугового радіодоступу (СШР) WiMAX трафік від наземної станції. OFDM-сигнал із НВЧ-домену після перетворення на піднесучі *S* можна математично виразити [6]:

$$s_{\mathrm{OFDM}}(t) = \sum_{n=0}^{S-1} x_n \exp\left[j2\pi\left(\frac{n}{T_s} + f_c\right)t\right], \qquad 0 \le tT_s. \quad , \tag{1}$$

де f_c - частота високочастотної несучої; T_s - тривалість OFDM-символу. Встановивши захисний інтервал рівний нулю, тривалість T_s дорівнює вікну аналізу Фур'є [7].

Ймовірність переривання зв’язку на піднесучу між аероплатформами може бути визначена наступним чином

$$P_{out1,n}(SNR_{th}) = P_r(SNR < SNR_п) = (SNR_п/k)^{\beta/2}, \quad (2)$$

де $k = \alpha/\theta^4$; $\beta = \theta^2 / (4\sigma^2)$; $SNR_п$ - порогове значення SNR ($k >= SNR_п >= 0$); $\alpha = SNR\ \theta^4 / \Im^2$; θ - кут розсіювання половинного випромінювання лазеру; $\Im$ - оптична інтенсивність; σ^2 - дисперсія джиттера на оптичному приймачі.

Слід зазначити, що коли кількість піднесучих є великою, тому загальна ймовірність переривання зв'язку по всьому діапазону OFDM можна отримати шляхом залучення закону великих чисел $P_{out,1}(SNR) = 1/S \sum_{i=0}^{S-1} P_{out,1.i}(SNR_п)$.

Тоді можна провести математичне моделювання однопролітного сценарію з метою визначення необхідної точності позиціонування оптичної системи фокусування (в якості якого може бути оптичний телескоп) ТСВА.

На рис. 2 наведено результати моделювання у вигляді залежності P_{out} з кінця в кінець від відстані прольоту ретрансляції між станціями ТСВА для різної кількості ретрансляцій N. Можна бачити, що P_{out} зростає як збільшується відстань міжплатформенного прольоту (зберігаючи кількість ретрансляцій постійною) або кількості транзитних прольотів (зберігаючи постійну відстань між аероплатформами).

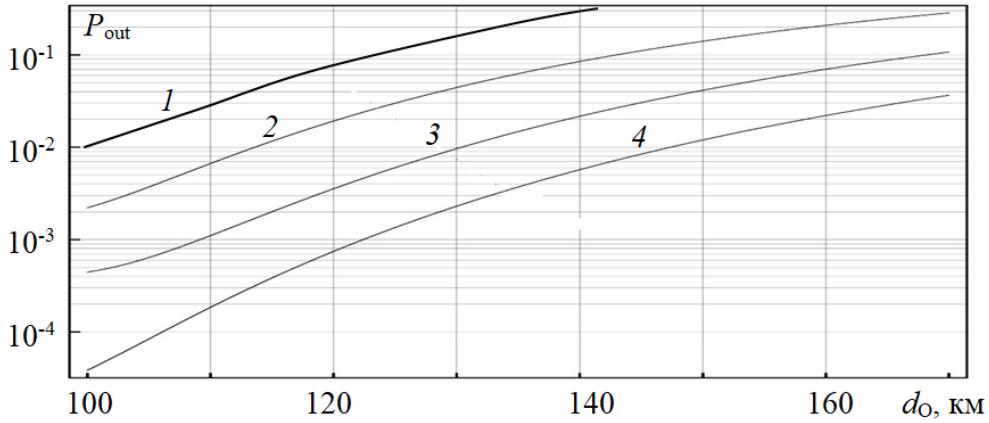


Рис. 2. Залежність P_{out} з кінця в кінець на вході приймача наземної станції від відстані прольоту ретрансляції для різної кількості ретрансляцій: *1* – 5; *2* – 4; *3* – 3; *4* – 2

Із отриманих результатів моделювання також виявлено, що ймовірність переривання зв'язку P_{out} зводиться до мінімуму для конкретного значення кута розходження променів (приблизно 70 мкрад) незалежно від значення вказівного джиттера. Це також демонструє домінуючий ефект джиттерування, наприклад, приріст від 8 до 10 мкрад, призводить до

серйозної деградації P_{out} з 10^{-9} до 2×10^{-6} для заданого значення дивергенції пучка 70 мкрад.

Таким чином, представлено нову архітектуру мережі ТСВА, яка спрямована на надання послуг СШР на далеких відстанях, використовуючи міжплатформенні оптичні лінії зв'язку з можливістю маршрутизації за декількома шляхами. Станції ТСВА виконують роль базових станцій і об'єднують загальний трафік наземної мережі СШР із зони, яку вони покривають. Станції ТСВА мають транспондери, які перетворять сигнали СШР в оптичні сигнали і навпаки.

У такій архітектурі якість обслуговування СШР (QoS) визначається/підтримується шляхом мінімізування ймовірності переривання зв'язку в конфігурації мережі. Ймовірності переривання зв'язку в даному сценарії визначається як ймовірність того, що прийнятий рівень потужності неприйнятно низький протягом певного часу. Загальна ефективність мережі визначається за допомогою розробленої математичної моделі каналу, яка включає в себе втрати лазерного променя та можливі ефекти наведення помилок.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Кравчук С.О. Принципи створення портативних тропосферних радіорелейних станцій // Матер. 9-ї міжнар. наук.-техн. конф. "Проблеми телекомунікацій", 21–25 квітня, 2015 р. – К.: НТУУ «КПІ», 2015. – С. 254–256.
3. Ильченко М.Е., Кравчук С.А. Телекоммуникационные системы на основе высотных аэроплатформ. – К.: Наукова думка, 2008. – 580 с.
4. Prospects of using of aerial stratospheric telecommunication systems / M. Zgurovsky, M. Ilchenko, S. Kravchuk, V. Kotovskyi, T. Narytnik, L. Cybulskyi // Proceedings of the 2016 IEEE International Scientific Conference "RadioElectronics & InfoCommunications" (UkrMiCo'2016), 11-16 September 2016, Kyiv, Ukraine. IEEE Conference Publications, 2016. – P. 20-23.
5. Кузьміч М.Ю., Кравчук С.О. Дослідження мобільної mesh-мережі безпілотних літальних апаратів з урахуванням затримки між вузлами // Матер. 11-ї міжнар. наук.-техн. конф. "Проблеми телекомунікацій", 18–21 квітня, 2017 р. – К.: Хімджест, 2017. – С. 196–198.
6. Transmission analysis of OFDM-based wireless services over turbulent radio-on-FSO links modeled by gamma-gamma distribution / A. Bekkali, C. B. Naila, K. Kazaura, K. Wakamori, and M. Matsumoto // IEEE Photon. J. – 2010. - vol. 2, no. 3. - P. 510–520.
7. Shieh W., Djordjevic I. OFDM for Optical Communications. Academic, 2010.

УДК 621.39

АРХІТЕКТУРА ПРОГРАМНО-ВИЗНАЧУВАНИХ РАДІОСИСТЕМ ДЛЯ РОЗРОБКИ РАДІООБЛАДНАННЯ

Кайденко М.М. Роскошний Д.В.
Науково-дослідний інститут телекомунікацій КПІ імені Ігоря Сікорського, Україна, Київ
E-mail: kkk610@ukr.net

Software Defined Radio Architecture for Develop Radio Equipment

This article presents Software Defined Radio Architecture, built on the basis of Software Communications Architecture and is intended for use in the creation of new generation radio systems.

В даній статті представлена архітектура, яка побудована на базі Software Communications Architecture та призначена для застосування при створенні радіосистем нового покоління

Програмно-визначувані радіосистеми (SDR - Software-Defined Radio) поєднують в собі передові технології для забезпечення гнучкості при створенні радіосистем. До цих технологій відносяться широкосмугові технології, радіочастотні компоненти, програмовані радіочастотні компоненти, технології цифрової обробки сигналів, аналогово-цифрові та цифро-аналогові перетворювачі, синтезатори частоти, технології побудови системи на кристалі (SoC - System-on-chip), технології обробки інформації. Завдяки передовим технологіям SDR надають можливість покращувати використання спектру, відкривати нові ринки телекомунікацій та розширювати перелік доступних послуг. Внаслідок гнучкості SDR технологій виникає ряд проблем при конфігуруванні та управлінні системою: збірка в єдине ціле обладнання та програмних компонент різних платформ в працюючу радіосистему; управління радіосистемою під час її роботи; робота радіосистеми у умовах фізичних та нормативних обмежень регулюючих органів різних країн; програмна самоконфігурація радіокомпонентів та адаптація; визначення загальних інтерфейсів для додатків та програмного забезпечення управління; використання бібліотек компонентів та радіоконфігурацій для різних апаратних та програмних платформ (переносимість).

Архітектура програмного забезпечення SDR, яка розглядається, базується на архітектурі комунікаційного програмного забезпечення (SCA - Software Communications Architecture) [1], яка була розроблена в рамках програми Department of Defense Joint Tactical Radio Systems (JTRS) [2]. SCA була призвана забезпечити відкриту архітектуру, яка дозволяє розробникам радіозасобів поєднувати апаратні та програмні компоненти в одній системі. По суті SCA в деякому сенсі є «операційною системою», яка визначає взаємодію програмних компонентів SDR. Однак SCA рухається до SDR від програмного забезпечення, а не від реалізації радіосистеми та перспектив її життєвого циклу. Хоча підхід SCA забезпечує гнучкість для програмних компонент, однак перехід від програмних компонент до робочої радіосистеми не є однозначним. Архітектура, яка представлена в даній доповіді і схематично зображена на рисунку 1, дозволить вирішити ці проблеми.

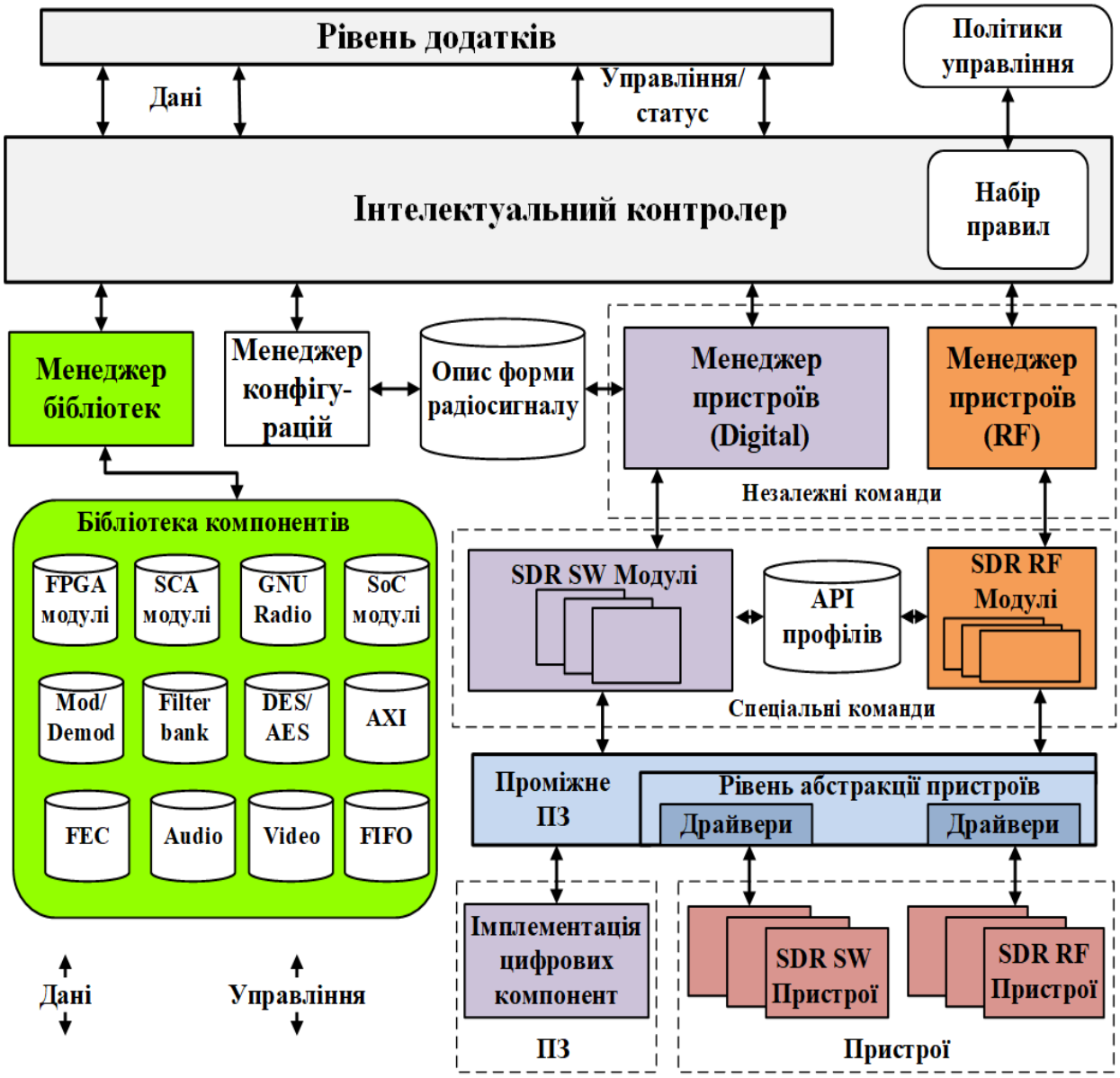


Рис.1 Модель архітектури програмно-визначуваної радіосистеми для розробки радіомодемного обладнання

Запропонована архітектура побудована на основі SCA специфікації і використовується для виявлення необхідних компонентів при реалізації реальної когнітивної радіосистеми [3,4]. Одним із основних компонентів, який використовується в цій моделі, є менеджер бібліотек для забезпечення організованого адміністрування компонент для безлічі файлів, що необхідні для програми SCA. Модель також демонструє використання класифікації компонентів, зокрема відповідних програмних інтерфейсів додатків (API - Application Programming Interface). API описує компонент для проекту таким чином, щоб дозволити компоненту інтерфейс з загальною архітектурою. Це покращує самосвідомість системи, яка в свою чергу покращує когнітивні здібності системи, дозволяючи радіосистемі визначати, які послуги надає доступний компонент і як отримати доступ до них просто знаючи тип класифікації.

Архітектура використовує Інтелектуальний контролер для зв’язку з рівнем

додатків, до його складу входить також менеджер, що визначає набір правил для визначених політик управління. Політики та правила генеруються для визначеного призначення радіозасобу в межах доступних для його реалізації компонентів. Інтелектуальний контролер визначає, які функції доступні і які компоненти активні, або які потрібно активізувати. Додатково Інтелектуальний контролер повинен містити модуль перевірки рівня доступу до додатків для забезпечення захисту від несанкціонованого доступу.

В архітектурі передбачено два менеджера пристроїв окремо для управління цифровими пристроями та радіочастотними пристроями. Це дозволяє забезпечити незалежне керування пристроями та покращити переносимість з платформи на платформу. Менеджери пристроїв створюють оперативну радіосистему інформація про яку знаходиться в описі програмного додатку (SAD - software application description). Динамічні радіосистеми можуть містити кілька SAD, які дозволять системі бути сумісними з різними стандартами та різними профілями передачі для одного стандарту. Після аналізу SAD цифрові пристрої та радіочастотні пристрої налаштовуються за допомогою менеджера пристроїв у відповідності до опису. Інформація для налаштування пристроїв (профілі) знаходиться в бібліотеці компонентів. Ця бібліотека зберігає зареєстровані компоненти, що доступні для радіосистеми, і керується менеджером бібліотек, який відповідає за внесення компонентів до бібліотеки, їх вилучення та підключення. Бібліотека компонентів використовується не тільки для забезпечення роботи радіосистеми і для покращення організаційного структура програмного забезпечення радіо, а й для поліпшення її автономності. У випадку конгнітивного радіо під керуванням Інтелектуального контролера визначається найбільш оптимальний варіант для побудови радіосистеми у відповідності до поставленої задачі.

Логічні пристрої контролюють свої апаратні пристрої через відповідний інтерфейс. Використовуючи класифікацію API, логічний пристрій має лише знати тип пристрою, надаючи доступ до відповідної базової функції. Це дозволяє логічному пристрою, що представляє наприклад підсилювач, керувати ним до тих пір, доки він використовується драйвером пристрою. Для конкретного компонента логічний пристрій - це простий шаблон, який не буде потрібним для створення системи в режимі реального часу.

Література

1. Software Communications Architecture Specification. FINAL / 15 May 2006 Version 2.2.2 - Режим доступу: http://www.public.navy.mil/jtnc/SCA/SCAv2_2_2/SCA_version_2_2_2.pdf
2. Joint Tactical Radio Systems. - Режим доступу: http://jtrs.army.mil
3. S. Kravchuk, M. Kaidenko, “Modem equipment for the new generation compact troposcatter stations”, Information and Telecommunication Sciences, No.1, pp. 5-12, 2016.
4. S. Kravchuk, M. Kaidenko, “Features of creation of modem equipment for the new generation compact troposcatter stations”, 2016 International Conference Radio Electronics & Info Communications (UkrMiCo) IEEE Conference Publications Pages:1-4, DOI: 10.1109/UkrMiCo.2016.7739634

УДК 621.396.1

РОЗПОДІЛ РЕСУРСІВ З ПІДТРИМКОЮ ЗАДАНОЇ ЯКОСТІ ОБСЛУГОВУВАННЯ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ АЕРОПЛАТФОРМ

Кравчук С.О., Афанасьєва Л.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

Resources distribution for the telecommunication systems based on aero-platform

The mechanisms of optimal planning and distribution of resources for maintenance of the cluster chairman (CC)-UAV are proposed, provided that minimization of the transmission power of the CC and the satisfaction of the requirements for the speed of the transmission of ground equipment is proposed. The minimum number of UAVs and their service time circuit, which provide speed stability queues packets.

Подальший розвиток телекомунікаційних систем на базі аероплатформ (ТСВА) потребує нових високоефективних механізмів розподілу ресурсів при збереженні необхідного рівня якості обслуговування [1-6].

В системному сценарію дослідження розглянуто ряд малогабаритних наземних терміналів (НТ), розподілених в певній географічній зоні. Дані НТ утворюють набір (множину) кластерів $\mathcal{G} = \|G1, G2, ..., G_{|\mathcal{G}|}\|$. В кожному кластері обирається один НТ в якості кластерного головуючого (КЗ), який несе відповідальність за відправку пакетів даних від усіх своїх членів кластера, використовуючи лінії передачі висхідної лінії зв'язку. Приймемо, що $\mathfrak{I}$ є множина показників (індексів) КЗ. Розмір кожного пакету даних по відношенню до КЗ є D_g ($g \in \mathfrak{I}$). В заданій географічній зоні використовується множина безпілотних літальних апаратів (БЛА) в якості літаючих базових станцій для об'єднання пакетів даних (їх прийому) від КЗ. Приймемо через множину $\mathcal{U}$ кількість U доступних БЛА. Останні повинні динамічно рухатись і зависати над КЗ, щоб об'єднувати дані каналу вверх. Зрозуміло, що час затримки (обслуговування) кожного БЛА залежить від кількості пакетів, які КЗ хоче передати. Для випадку багатостанційного доступу розглянемо схему OFDMA (orthogonal frequency division multiple access) із Z ресурсними блоками (РБ), кожен з яких займає ширину смуги Δf_z. Припустимо, що z_u це кількість РБ, що асоціюється з заданими БЛА u. Для кожного БЛА u визначається вектор $\boldsymbol{d}_u = [d^g{}_u]_{|\mathcal{G}|\times 1}$ причому кожен елемент являє собою час обслуговування БЛА, необхідний для покриття КЗ g протягом T. Також визначимо $P_{g,z}$ як потужність, що передається, що КЗ g необхідний для надійної передачі даних більше РБ z.

В кожному кластері черга пакетів даних на КЗ вміщує усі пакетів даних від членів кластеру (ЧК). В кожному часовому слоті ЧК передає до КЗ свій пакет даних з ймовірністю p. Приймемо, що $a_{g,t}$ є процесом надходження таких пакетів даних до КЗ, де g - кластер G_g протягом часового слоту t. При цьому пакети даних від кожного ЧК буде негайно запускати процес

надходження пакету даних до КЗ. Протягом кожного часового слоту $a_{g,t}$ може змінюватись від 0, який вказує на відсутність ЧК в даних G_g, що передаються, до $|G_g|$, який вказує, що усі НТ в G_g передають пакети даних до БЛА.

Для того, щоб гарантувати, що довжина черги КЗ не стане нескінченною, кількість БЛА та їх час обслуговування КЗ повинні бути достатніми. Тому спочатку визначається мінімальна кількість БЛА та їх час обслуговування КЗ, які забезпечують стабільність швидкості черги. Потім для встановлення успішної передачі по висхідній лінії зв'язку КЗ, визначається оптимальна кількість ресурсних блоків і мінімальна потужність, що передається, для кожного КЗ. В цьому випадку необхідно вирішити проблему оптимального розподілу ресурсів для енергозберігаючих комунікацій КЗ-БЛА.

Тривалість часу, необхідна для збору пакетів з кожного КЗ повинна бути досить довгою, щоб гарантувати стабільність швидкості черги. Теорема про стійкість швидкості вводить наступне правило для стабілізації мережі з багатьма чергами: приймати рішення на планування таким чином, щоб середній час обслуговування і швидкість прибуття задовольняли для середніх значень $a_{g,t} \leq d_{g,t}$ для кожної черги g. Визначимо матрицю $\boldsymbol{D} = [\boldsymbol{d}_u]_{|\mathcal{G}|\times U}$, де з кожним стовпцем - вектор $\boldsymbol{d}_u$.

Виходячи з визначення множини планувальних рішень за час обслуговування БЛА Λ, мінімальна кількість безпілотних літальних апаратів - це число, для якого Λ не є порожнім для заданої швидкості прибуття.

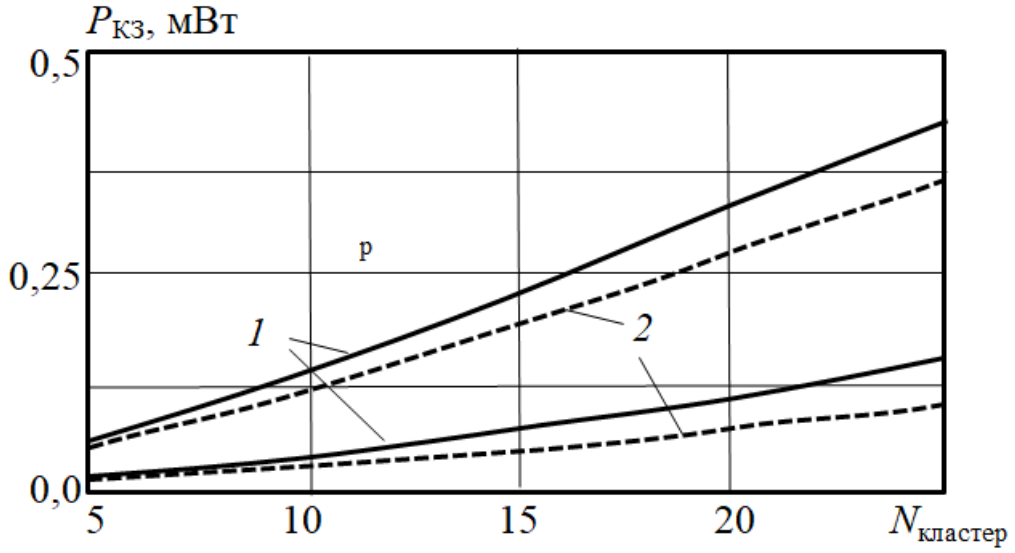
Далі, для кожного КЗ знаходимо оптимальну кількість блоків ресурсів і мінімальну потужність передачі, необхідну для успішної та енергоефективної передачі у висхідній лінії зв'язку. У нашій моделі системні ресурси включають блоки ресурсів, призначені для БЛА, і потужність передачі кожного КЗ. Кожен КЗ повинен передавати свої пакети з мінімальною потужністю, використовуючи призначені блоки ресурсів. Проблема розподілу блоків спільного ресурсу та оптимізації керування потужністю, яка мінімізує загальне споживання енергії КЗ, дається як

$$\min_{\boldsymbol{P},\boldsymbol{z}} \sum_{g} \sum_{u} d_g^u \sum_{z_u} P_{g,z}^u,$$

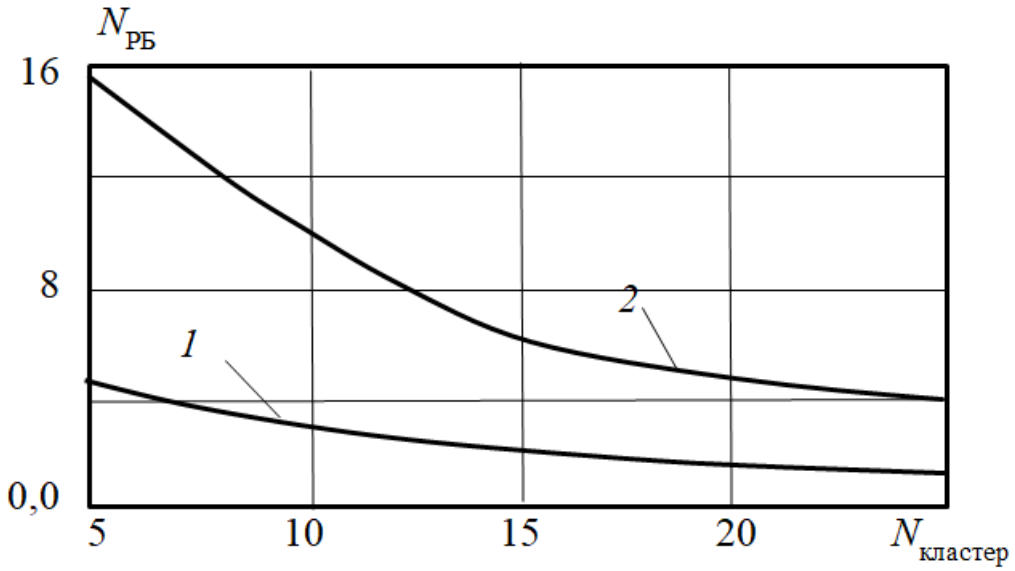
де $P^u{}_{g,z}$ – потужність, що передається, від кожного КЗ g по субканалу z, коли КЗ g обслуговується БЛА u ($0 < \sum_z P_{g,z}^u \leq P_g^{max}$);

На рис. 1, *а* представлено середню потужність передачі КЗ від кількості кластерів для двох сценаріїв. У першому сценарії, використовуються ряд БЛА як повітряні базові станції, а в другому сценарії - численні наземні базові станції (рівні кількості БЛА), які рівномірно розміщені для обслуговування КЗ. Як видно з рис. 1, *а* використання повітряних базових станцій призводить приблизно до 60% зниження потужності КЗ у порівнянні з тільки наземними базовими станціями. Наприклад, для 15 кластерів та 5 РБ, потужність передачі КЗ зменшується з 0,24 мВт до 0,06 мВт за допомогою БЛА замість наземних базових станцій. На практиці БЛА можуть ефективно рухатись у напрямках КЗ і значно зменшувати ефекти блокування та

затінення. Отже, КЗ можуть використовувати більш низьку потужність передачі для передачі своїх даних на БЛА, ніж до наземних базових станцій.



а)



б)

Рис. 1. Залежності середньої потужності передачі КЗ (*а*) і середньої кількості РБ на БЛА (*б*) від кількості кластерів для двох сценаріїв обслуговування КЗ за допомогою БЛА (неперервна крива) і наземних БС (пунктирна крива): *1* – РБ = 5; *2* – РБ = 20.

З рис. 1, *а* видно, що середня потужність передачі на КЗ зростає, коли кількість кластерів збільшується. Це пов'язано з тим, що, коли кількість КЗ збільшується, середній час, який кожний безпілотник може витратити для збирання даних з кожного КЗ, зменшиться. Таким чином, КЗ повинен відправити свій пакет з мінімальною тривалістю часу. Отже, КЗ збільшує свою потужність передачі, щоб відповідати швидкості слідування пакетів протягом заданого короткого часу.

На рис. 1, *б* представлено вплив кількості кластерів на середню кількість блоків ресурсів, які необхідно призначити для кожного безпілотника. З рис.

1, *б* видно, що середня кількість блоків ресурсів на БЛА нижче для більшої кількості кластерів. Це пов'язано з тим, що із збільшенням кількості кластерів мінімальна кількість необхідних БПЛ буде збільшуватися. Отже, кількість РБ на один БЛА відповідно зменшується. Наприклад, як показано на рис. 1, *б*, коли кількість кластерів збільшується з 10 до 20, середня кількість РБ на одиницю БЛА зменшується з 10 до 4 при загальній сумі 20 РБ.

Таким чином, Запропоновано механізми оптимального планування і розподілу ресурсів для підтримання зв'язку КЗ-БЛА при умові зведення до мінімуму потужності передачі КЗ і задоволенні вимог до швидкості передачі наземних пристроїв. Визначено мінімальну кількість БЛА та їх час обслуговування КЗ, які забезпечують стабільність швидкості черги пакетів. Для встановлення успішної передачі по висхідній лінії зв'язку КЗ, визначено оптимальну кількість ресурсних блоків і мінімальну потужність, що передається, для кожного КЗ. Розв’язано проблему оптимального розподілу ресурсів для енергозберігаючих комунікацій КЗ-БЛА.

Результати моделювання показують, що, оскільки вірогідність передачі пакетів наземних терміналів збільшується, також значно збільшується мінімальна кількість БЛА, необхідних для забезпечення стабільності швидкості слідування черги в кластерних головуючих. Визначено, що використання повітряних базових станцій на БЛА призводить приблизно до 60% зниження середньої потужності кластерних головуючих у порівнянні з тільки наземними базовими станціями.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Ильченко М.Е., Кравчук С.А. Телекоммуникационные системы на основе высотных аэроплатформ. – К.: Наукова думка, 2008. – 580 с.
3. Prospects of using of aerial stratospheric telecommunication systems / M. Zgurovsky, M. Ilchenko, S. Kravchuk, V. Kotovskyi, T. Narytnik, L. Cybulskyi // Proceedings of the 2016 IEEE International Scientific Conference "RadioElectronics & InfoCommunications" (UkrMiCo’2016), 11-16 September 2016, Kyiv, Ukraine. IEEE Conference Publications, 2016. – P. 20-23.
4. Кузьміч М.Ю., Кравчук С.О. Дослідження мобільної mesh-мережі безпілотних літальних апаратів з урахуванням затримки між вузлами // Матер. 11-ї міжнар. наук.-техн. конф. “Проблеми телекомунікацій”, 18–21 квітня, 2017 р. – К.: Хімджест, 2017. – С. 196–198.
5. Афанасьєва Л.О., Кравчук С.О., Міночкін Д.А. Ймовірність переривання зв’язку у безпроводовій системі з багатоантенною кооперативною ретрансляцією // Зб. наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 51. – С. 19-26.
6. Рижко А.В., Кравчук С.О. Дослідження можливості підвищення якості обслуговування для мереж багатопрольотної ретрансляції стандарту IEEE 802.16j // Матер. 11-ї міжнар. наук.-техн. конф. “Проблеми телекомунікацій”, 18–21 квітня, 2017 р. – К.: Хімджест, 2017. – С. 163–165.

УДК 621.39

АРХИТЕКТУРА И ВЫБОР КОМПОНЕНТОВ ДЛЯ ПРИЛОЖЕНИЙ SDR

Кайденко Н.Н., Роскошный Д.В.
Научно-исследовательский институт телекоммуникаций
КПИ имени Игоря Сикорского, Украина, Киев
E-mail: ккк610@ukrl.net

Architecture and components selecting for SDR applications

The general requirements for SDR systems and methods for their implementation on the Intel SoC platform and radio modules of Analog Devices using software of manufacturing companies.

Концепция программно-определямых радиосистем (SDR) предполагает, что в аналоговой части радиосистемы присутствуют только АЦП и ЦАП, а вся обработка сигналов, включающая в себя модуляцию, помехоустойчивое кодирование, реализацию адаптивных алгоритмов и т.д., производится программным способом [1].

Это позволяет использовать одну и ту же аппаратную платформу для реализации нескольких видов радиосистем.

В общем случае, требования к платформе, связанные со стоимостью, размерами и энергопотреблением, являются компромиссными, особенно в случае разработки систем, ориентированных на питание от батарей.

Хотя эти требования и являются компромиссными, тем не менее существует обобщенная архитектура программно-определямых радиосистем.

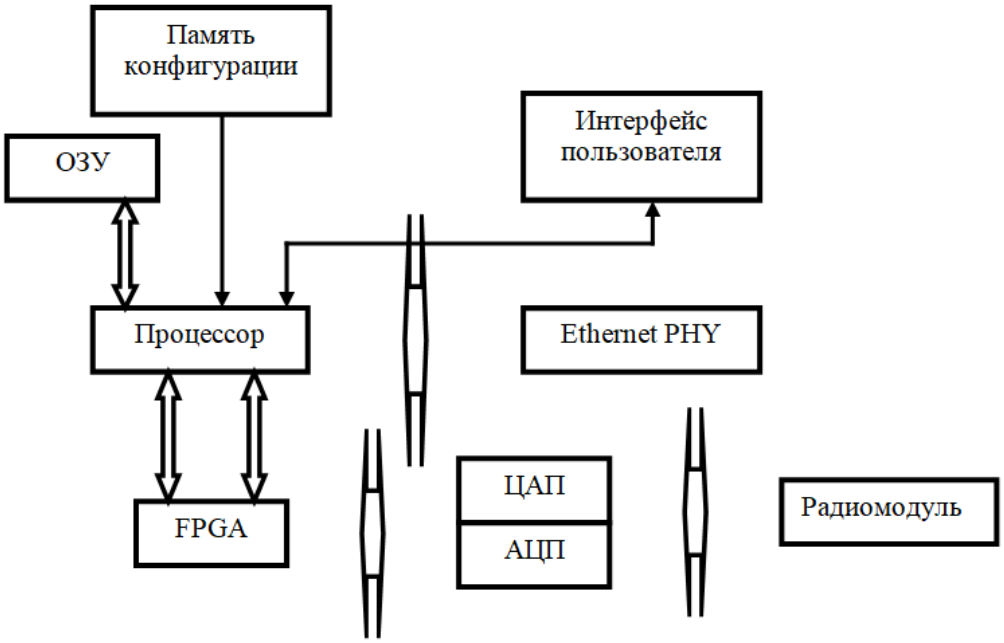


Рис.1. Упрощенная структурная схема программно-определяемой радиосистемы

Общими требованиями к системам SDR являются низкое энергопотребление (особенно в режиме ожидания), реконфигурируемость с достаточными ресурсами для обработки различных типов сигналов, таких как частотная манипуляция (FSK), квадратурная амплитудная модуляция (QAM), множественный доступ с кодовым разделением каналов (CDMA) и мультиплексирование с ортогональным частотным разделением (OFDM).

Также необходимо наличие внешних интерфейсов, например Ethernet.

Компания Analog Devices представила решение радиомодуля для программно-определяемых радиосистем. Разработанная для применения в различных областях, таких как военная электроника, измерительное оборудование и коммуникационная инфраструктура, микросхема приемопередатчика AD9364 сочетает в себе высокую степень интеграции, широкий диапазон рабочих частот и гибкость в управлении [2].

Применение тких настраиваемых однокристальных широкополосных радиочастотных модулей облегчает разработку аналоговой части SDR в диапазоне частот от 70 МГц до 6.0 ГГц.

AD9364 включает в себя входные и выходные каскады, блок аналого-цифровой обработки сигналов, синтезатор частот и цифровую схему управления, Всё это позволяет легко разработать программно-определяемую систему с внешним процессором.

Поддержка AD9364 осуществляется обширным набором вспомогательных ресурсов, что позволяет создавать программное обеспечение радиосистем с минимальными затратами времени [3].

В настоящее время в качестве внешних процессоров широко используются системы-на-кристалле (SoC). В общем случае SoC являются дальнейшим развитием технологии FPGA и представляют собой интегрированные в одном кристалле одно или несколько процессорных ядер, блок программируемой логической матрицы FPGA, а также аппаратно- или программно-реализованные модули управления периферийными устройствами.

В линейке SoC корпорации Intel (семейства Cyclone и Arria) в качестве процессорных ядер могут использоваться программные процессоры NIOS или интегрированные ядра ARM A9, что позволяет разрабатывать как чистые bare-metal приложения, так и приложения, работающие под управлением операционной системы Linux.

В последнем случае существенно упрощается обеспечение взаимодействия с внешними устройствами за счет использования существующих драйверов.

Блок программируемой логической матрицы FPGA используется в качестве реконфигурируемого аппаратного ускорителя при выполнении операций, связанных с цифровой обработкой сигналов – фильтрации, помехоустойчивого кодирования и т.д.

Системное проектирование на ПЛИС Altera проводится в приложении QSYS [4,5,6]. Это приложение упрощает процесс проектирования благодаря поднятию уровня абстракции при создании проекта (рис. 2).

Обмен данными между процессорным ядром и FPGA обычно осуществляется с использованием стеков типа FIFO (рис. 2), что позволяет обеспечивать обработку данных с разными тактовыми частотами.

Реконфигурация FPGA в зависимости от выбранного режима работы устройства проводится процессором путем подачи соответствующих команд, либо путем загрузки нового конфигурационного файла из соответствующей области памяти.

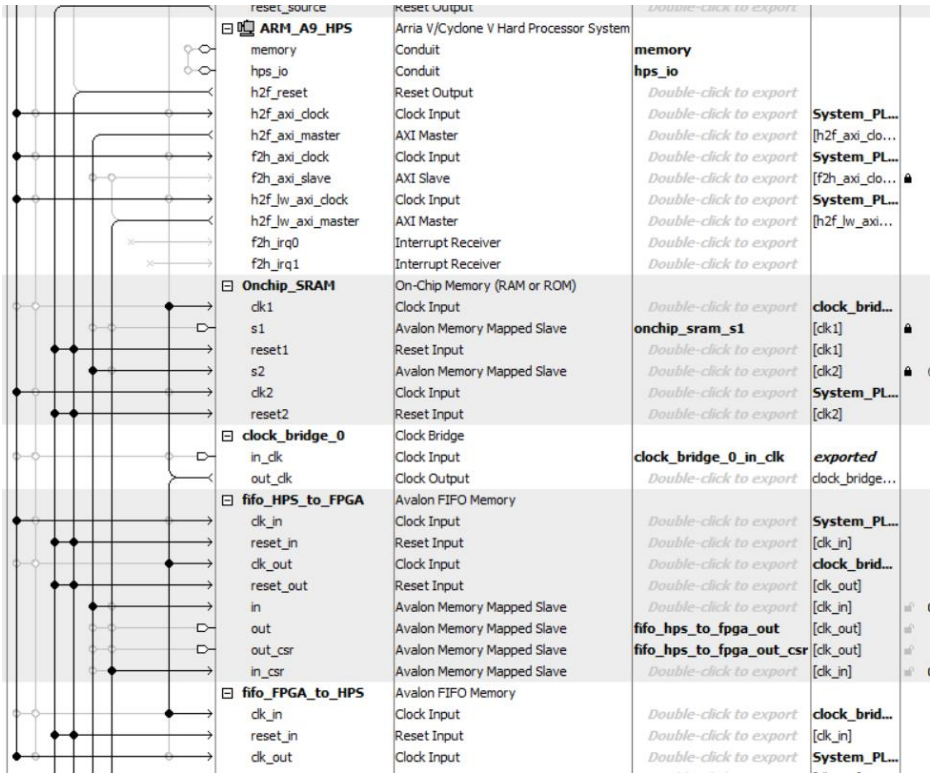


Рис. 2. Фрагмент приложения QSYS

Таким образом, алгоритмы обработки радиосигналов могут быть реализованы следующим образом: алгоритмически сложные, но менее скоростные задачи решаются с помощью процессора, а задачи с высокими требованиями к скорости обработки должны быть реализованы в FPGA.

Литература

1. Кайденко В.Н., Кайденко Н.Н., Крылач О.Ф., Роскошный Д.В. Организация взаимодействия между HPS и FPGA на базе SoC технологий при создании телекоммуникационных устройств. Проблеми телекомунікацій : 10-а Міжнар. наук.-техн. конф., 19-22 квіт. 2016р. : матеріали конф. – К., 2016. – С. 254–256.
2. https://wiki.analog.com/resources/eval/user-guides/ad-fmcomms2-ebz/ad9361
3. http://www.altera.com/literature/lit-cyclone-v.jsp
4. www.rocketboards.org
5. Altera Cyclone V Device Handbook, Volume 3: Hard Processor System Technical Reference Manual.
6. Altera SoC Embedded Design Suite User Guide.

УДК 621.396.2

СИНТЕЗ OFDM-АЛГОРИТМУ БЕЗПРОВОДОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Макаренко А.О.
Державний університет телекомунікацій
E-mail: makarenkoa@ukr.net

Synthesis of OFDM-algorithm wireless of the telecommunication systems

Conducted development of algorithms of control program of direct and reverse rapid transformation of Fourier for the off-wire modem of communication of data on 1024 input-output counting out. Hardware representation of modem is oriented to application of modern and powerful digital alarm processors, that allows considerably to decrease time of calculation of operations and rev up communication of data of the off-wire system.

Важливим інструментом для підвищення фізичної швидкості та вірогідності передачі даних у безпровідних мережах є розширення смуги пропускання спектральних каналів. В [1 - 3] показано, що найбільша ефективність передачі даних здійснюється в каналах з ортогональним частотним мультиплексуванням (ОЧМ;OFDM).

В представленій доповіді показано розробку алгоритмів ОЧМ-модуляторів/демодуляторів із застосуванням сучасних та потужних цифрових сигнальних процесорів (ЦСП) серії ADSP-21160 фірми Analog Devices. Запропоновані алгоритми дозволяють значно зменшити час обчислення операцій, смугу частот, що займає сигнал та збільшити швидкість передачі даних в безпровідних системах орієнтованих в першу чергу для передачі даних. Для створення керуючої програми модему використано програмне середовище Analog Devices VisualDSP++ [2, 4 - 6], яке призначене для розробки і відладки цифрових сигнальних процесорів серії ADSP-21160.

Блок-схема безпровідного OFDM-модему на основі ОЧМ із використанням прямого (ШПФ) та зворотного (ЗШПФ) швидкого перетворення Фур’є представлена в [1, 2, 8].

Спосіб ОЧМ характеризується рядом переваг, а саме [3]:

• велика спектральна ефективність модуляції завдяки максимально близькому розташуванню субканалів;

• висока завадостійкість інформаційного сигналу завдяки використанню великої кількості несучих в широкому діапазоні частот;

• можливість реалізації повністю цифрових високоефективних алгоритмів модуляції-демодуляції, основаних на використанні дискретного перетворення Фур’є (ДПФ).

Всі вищенаведені переваги ОЧМ стали можливими завдяки апаратній реалізації ЗШПФ та ШПФ. Переваги системи ОЧМ проявляються при великій кількості несучих. Без такого кроку неможлива реалізація ОЧМ, адже в іншому випадку пряме апаратне формування ОЧМ-сигналу вимагало б величезних схемотехнічних витрат у вигляді тисяч генераторів і модуляторів в передавачі і такого ж числа детекторів в приймачі. Маловірогідно, що така схема була б реалізована.

Реалізація ЗШПФ та ШПФ [1, 5] базується на формулах (1) і (2), відповідно:

$$x(n) = \frac{1}{N}\sum_{m=0}^{N-1} X(m) e^{j2\pi nm/N}, \quad (1)$$

$$X(m) = \frac{1}{N}\sum_{n=0}^{N-1} x(n) e^{-j2\pi nm/N}, \quad (2)$$

де m – індекс ДПФ в частотній області; n – індекс ДПФ в часовій області; N – кількість вхідних/вихідних відліків ДПФ.

Однак, оскільки значення $e^{j2\pi/N}$ з (1) та $e^{-j2\pi/N}$ з (2) є постійними для заданого числа N, то вираз $X(m) = \sum_{n=0}^{(N/2)-1} x(2n)\left(W_{N/2}\right)^{nm} + \left(W_N\right)^m \sum_{n=0}^{(N/2)-1} x(2n+1)\left(W_{N/2}\right)^{nm}$ можна обчислити і використовувати готові значення при створенні програмного забезпечення конкретного MIMO-модему передачі даних ($W_N = e^{j2\pi/N}$). Використання даної можливості та розбиття N вхідних/вихідних відліків ДПФ на дві та більше частини дозволяє зменшити кількість обчислювальних операцій до $(N/2)\log_2 N$ [7].

У загальному випадку, вимоги по використовуваній пам’яті для N-точкового ШПФ такі: N комірок для дійсних та N комірок для уявних даних і N комірок для коефіцієнтів повороту.

Для забезпечення функціонування в реальному часі повний розрахунок ШПФ повинен виконуватися в проміжку, що відповідає часу накопичення одного пакету даних. Передбачається, що, поки робиться обчислення ШПФ поточного пакету даних, ЦСП накопичує дані для наступного пакету. Безперервне отримання даних полегшується завдяки можливостям гнучкої адресації даних в ЦСП у поєднанні з використанням різних каналів прямого доступу до пам’яті.

Розглянемо ЦСП процесор ADSP-21160, який обчислює 1024-точкове 32-розрядне комплексне ШПФ з плаваючою точкою за 90 мкс. Очевидно, що максимальна частота дискретизації дорівнює 11,38 Мо/с. Тут сигнал має ширину смуги частот менше 5,7 МГц. Також передбачається, що немає додаткових витрат процесорного часу, пов’язаних з ШПФ, або обмежень, пов’язаних з передачею даних.

Наведений приклад дає оцінку максимальної ширини смуги сигналу, який може бути оброблений даним ЦСП з урахуванням характеристик реалізованого на ньому ШПФ. Число точок ШПФ також визначає мінімальний рівень шуму ШПФ відносно рівня широкосмугового шуму, і це також має бути враховано при виборі числа точок ШПФ.

Як вже говорилося вище, інтегроване середовище VisualDSP++ є основним засобом розробки і відладки додатків для процесорів компанії Analog Devices і підтримує процесори типу TigerSHARC, SHARC і Blackfin. Середовище VisualDSP++ може бути завантажене з веб-сайту компанії та після закінчення реєстрації користувачеві висилається серійний номер, що дає можливість працювати з пакетом в тестовому режимі впродовж 90 днів [4].

В доповіді показано удосконалення алгоритму функціонування безпровідного модему передачі даних на 64 відліки [3, 8], а саме: розроблено підпрограму реалізації ЗШПФ та ШПФ з кількістю вхідних/вихідних відліків, рівною 1024. В якості пристрою обробки даних застосовано ЦСП ADSP-21160, що має кращі характеристики в порівняні з мікроконтролером ATmega128. Частотний діапазон, який займають сигнали згідно виразів (1) і (2) складає 8 МГц. Ця смуга частот найбільш наближена до параметрів стандарту передачі даних 802.16е. Тому дослідження проводились в цій смузі частот і показали ефективність обраного шляху реалізації програмного забезпечення та схемотехнічних рішень.

Література

1. Dahlman E., Parkvall S., Skold J. 4G: LTE/LTE-Advanced for Mobile Broadband. - London: ELSEVIER, 2010. - 431 p.
2. Jeffrey G. A., Arunabha G., Rias M. Fundamentals of WiMAX: Understanding Broadband Wireless Networking. - Washington: Pearson Education, Inc., 2007. - 478 p.
3. Макаренко А. О. Багатоканальна телекомунікаційна система на основі мережі електроживлення: дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.12.02 – Телекомунікаційні системи та мережі / А. О. Макаренко. - К., 2011. - 156 с.
4. VisualDSP++ Development Software Release 5.0 [Електронний ресурс] // – Режим доступу : http://www.analog.com
5. Проектирование с использованием процессоров Analog Devices [Електронний ресурс] // - Режим доступу : http://kit-e.ru
6. Вальпа О. Д. Разработка устройств на основе цифровых сигнальных процессоров фирмы Analog Devices с использованием Visual DSP++ / О. Д. Вальпа. – М.: Горячая линия-Телеком, 2007. – 270 с.
7. Лайонс Р. Цифровая обработка сигналов / Р. Лайонс ; пер. с англ. ; [2-е изд.]. – М.: ООО «Бином-Пресс», 2006 г. – 656 с.
8. Гринкевич, Г.О., Макаренко, А. О. Розробка імітаційної моделі та алгоритмів функціонування MIMO-системи / Г. О. Гринкевич // Зв'язок. - 2012. - №2. - С. 29-33.

УДК 621.396.1

СХЕМА КОДОВАНОЇ КООПЕРАЦІЇ

Афанасьєва Л. О., Кравчук С.О., Шевченко І.І., Рисцова К.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
Компания «Инфопульс Украина»
E-mail: liana.afanasyeva@gmail.com

Coded cooperation scheme

Cooperative diversity - a method based on the combined use of multiple antennas to increase bandwidth for a given set of frequency bands. This paper provides an overview of the coded cooperation scheme. Coded cooperation separates the code words of each mobile device and transmits portions of each codeword through independent channels.

Існує великий інтерес до розробки різних кооперативних стратегій для підвищення надійності каналу безпроводового зв’язку за допомогою просторового рознесення [1-4]. Основні протоколи amplify-and-forward (AF), decode-and-forward (DF) прості в реалізації, базуються на повторюваності [5-6], але не ефективні щодо використання ширини смуги. Тому, метою роботи є дослідження схеми кодованої кооперації (coded cooperation- CC) для покращення спектральної ефективності.

В схемі кодованої кооперації, кооперація сигналів здійснюється на рівні підсистеми кодування каналів. Допоміжний вузол ретрансляції (ДВР) посилає інкрементну надмірність, яка при об'єднанні в цільовому приймачі (ЦП) з кодовим словом, відправленим джерелом сигналу (ДС), приводить до кодового слова з більшою надмірністю.

Надмірність в кодовому слові використовується в ЦП для збільшення можливостей відновлення вихідної інформації, якщо помилки були введені під час процесу передачі. У схемі CC кодове слово передається в двох частинах, кожне з яких використовує інший шлях або канал. На рис. 1 представлено один цикл передачі інформації для схеми з кодовою кооперацією. Основні етапи процесу послідовно позначені круговими номерами. Цикл починається з блоку інформаційних символів N_1, який вводиться в CRC-енкодер на ДС (етап 1). Результуючий сигнал CRC-енкодера потім вводиться на FEC-енкодер (етап 2), що приводить до кодового слова з N_1 символів, тобто зі швидкістю $R_1 = N_1 / N_I$. Це кодове слово потім передається ЦП та також підслуховується допоміжним вузлом, обраним для кооперативної ретрансляції з ДС (етап 3). Після отримання передачі джерела допоміжний вузол ретрансляції (ДВР) декодує коди FEC і CRC (крок 4). Якщо CRC не виявив помилки в декодованому повідомленні (етап 5), то отримані інформаційні символи N_I в ДВР знову подаються в

CRC-енкодер. Потім вихідний сигнал CRC-енкодера обробляється через FEC-енкодер, що приводить до кодового слова символів $N > N_1$ (етап 6), тобто швидкість кодування каналу в ДВР дорівнює $R = N/ N_I < R_1$.

Загальний результат обробки у вузлі ретрансляції являє собою кодове слово, згенероване тим же способом, що й кодове слово, передане джерелом сигналу, але містять $N_2 = N - N_1$ додаткових символу парності, які відділені від решти символів (етап 7). Під час другої фази процесу комунікації додаткові N_2-символи відправляються вузлом ретрансляції до цільового приймача (етап 8). У ЦП символи N_2 від ДВР об'єднуються з символами N_1 з ДВР для відновлення кодового слова з N символами і швидкістю R (етап 9). Потім це кодове слово декодується (етап 10), та вихідне повідомлення відновлюється, якщо FEC код зміг виправити всі помилки, введені під час зв'язку (етап 11).

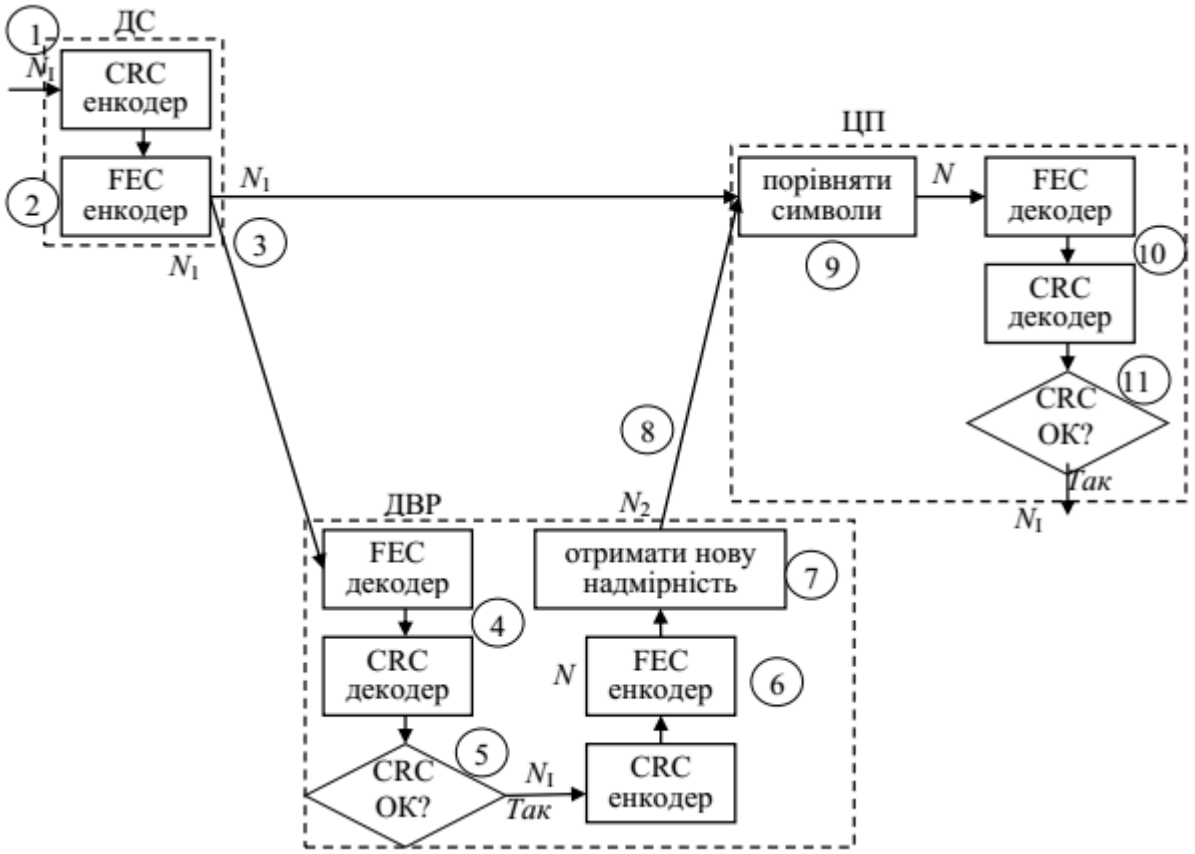


Рис. 1. Цикл передачі в схемі кодованої кооперації

Весь процес також можна розглядати так, як якщо вихідний вузол також виконує канальне кодування зі швидкістю R, а передане кодове слово з символами N_1 генерується шляхом пунктурування (видалення) символів N_2 з кодового слова з N символами. Незалежно від того, як генеруються задіяні коди каналів, кодове слово, передане вихідним вузлом, належить слабшому коду, ніж використовуваному в ЦП. Код в цільовому приймачі посилюється від коду на ДС шляхом об'єднання символів парності N_2, отриманих від

вузла-ретранслятора. Крім того, важливо відзначити, що ДВР і ДС працюють на ортогональних каналах так, що в той же час, коли ДС передає своє кодове слово, ДВР виконує ту ж операцію зі своїми власними даними. Більш того, в той час як ДВР допомагає ДС, відправляючи символи парності N_2, ДС взаємно допомагає вузлу ретрансляції таким же чином.

Операція кодованої кооперації передбачає, що ДВР може успішно декодувати вихідне повідомлення (яке він знає після перевірки CRC). В іншому випадку, допоміжний вузол ретрансляції не може генерувати додаткові символи парності N_2 для джерела, і замість цього він генерує і передає символи парності N_2 зі своїх власних даних. Через це більш слабке кодове слово, передане ДС, повинне бути дійсним кодовим словом, яке може бути розшифровано, коли ДВР не посилає додаткових символів парності N_2.

Оскільки при кодованій кооперації операція ДС та ДВР повністю симетрична, будемо позначати в подальшому два взаємодіючих вузла як вузол 1 і вузол 2. Існує чотири можливих кооперативних випадки для передачі символів:

1. Обидва вузла успішно декодують канальний код (слабший) один одного.
2. Обидва вузла не можуть декодувати канальний код (слабший) один одного.
3. Вузол 1 успішно декодує канальний код від вузла 2, але вузол 2 не може декодувати канальний код від вузла 1.
4. Вузол 1 успішно декодує канальний код від вузла 2, але вузол 2 не може декодувати канальний код від вузла 1. У цьому випадку обидва вузла відправляють додаткові символи парності для вузла 2, які можуть бути об'єднані в приймачі, використовуючи, наприклад, метод MRC .

Внаслідок цієї динаміки з чотирма подіями ймовірність відмови в схемі кодованої кооперації визначається середньою ймовірністю відмов серед чотирьох подій.

Література

1. Ільченко М.Ю. , Кравчук С.О. Телекомунікаційні системи. – Київ: Наукова думка, 2017. – 730 с.
2. Афанасьєва Л.О., Кравчук С.О., Міночкін Д.А. Ймовірність переривання зв’язку у безпроводовій системі з багатоантенною кооперативною ретрансляцією // Зб. наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 51. – С. 19-26.
3. Афанасьєва Л.О., Кравчук І.М., Кравчук С.О. Метод кооперативного рознесення // Матер. 10-ї міжнар. наук.-техн. конф. “Проблеми телекомунікацій”, 19–22 квітня, 2016 р. – К.: Хімджест, 2016. – С. 257–259.
4. Афанасьєва Л.О., Кравчук І.М., Кравчук С.О. Модель багатостільникової мережі з MIMO-кооперацією // Матер. 10-ї міжнар. наук.-техн. конф. “Проблеми телекомунікацій”, 19–22 квітня, 2016 р. – К.: Хімджест, 2016. – С. 263–265.
5. Laneman J. N., Tse D., Wornell G. Cooperative diversity in wireless networks: Efficient protocols and outage behaviour // IEEE Trans. on Information Theory. – 2004. – Vol. 50, № 12. – P. 3062–3080.
6. Hunter T., Nosratinia A. Cooperation diversity through coding // Proc. of IEEE Int. Symposium on Information Theory, July 2002. – New York, 2002. – P. 220–224.

УДК 621.391

КОДОВАНЕ КЕШУВАННЯ

Малецький Д.В., Міночкін Д.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dmytro.maletskiy@gmail.com

CODED CACHING

The decentralized coded caching scheme is considered as solution to the asynchronous user requests and as the key element in handling online and nonuniform demands.

Протягом останнього десятиліття спостерігається тенденція зміщення стільникового трафіку від передачі голосу до передачі даних. На відміну від голосу, який генерується в реальному часі безпосередньо перед передачею, контент зазвичай створюється завчасно. Така особливість контенту дозволяє розподіляти його по мережі та кешувати (в базових станціях або безпосередньо в мобільних телефонах користувачів) в періоди низької завантаженості мережі. У періоди високого рівня експлуатації мережі, кешований контент може бути використаний для зменшення навантаження мережі. Очікується, що кешування контенту стане ключовим компонентом архітектури майбутніх стільникових мереж.

Основні обмеження продуктивності систем з одним кеш-сховищем були дослідженні в області комп'ютерних наук переважно в 1980-х і 90-х роках. Основним покращенням, що надає кешування, в таких системах є локальна доставка контенту з внутрішнього кешу. Проте ця теорія не може бути застосована до систем з декількома кеш-сховищами (кеш-мереж). Саме такі кеш-мережі, будуть актуальні в контексті стільникових систем наступного покоління.

Окрім покращення, що надає локальна доставка контенту, яка є можливою в системах з одним кеш-сховищем, кеш-мережі уможливлюють отримання глобального покращення від кешування. Це покращення досягається за рахунок багатоадресної передачі від сервера, що є одночасно корисною для декількох користувачів. На відміну від локального покращення, це глобальне покращення, масштабується з кількістю кеш-сховищ в мережі. Теоретичні докази показують, що немає інших переваг кешування, що масштабуються з параметрами системи. Таким чином, це глобальне покращення є базовою властивістю звичайної кеш-мережі, а кодована багатоадресна передача являється основною технікою для таких мереж.

Ці результати свідчать про те, що кодування відіграє ключову роль в оптимальному функціонуванні кеш-мереж. Проте, в основу їх отримання покладений ряд стилізованих припущень (наприклад, одночасні запити користувачів, рівномірна популярність контенту, офлайн оновлення кеш-сховищ і т.п.). В [1] розглянуто, як ці припущення можуть бути спростовані. На основі гнучкого децентралізованого підходу до кодованого кешування,

що дозволяє незалежно розподіляти кеш між сховищами, показано, як опрацьовувати сценарії з асинхронними запитами користувачів, неоднорідною популярністю контенту та онлайн оновленням кешу.

Децентралізоване кодоване кешування полягає у тому, що на етапі розміщення контенту, коли рівень трафіку в мережі є низьким, кожен користувач випадковим чином кешує MF/N, де N – кількість файлів, що зберігається на сервері, F – розмір кожного файлу в бітах та M – деяке дійсне число $M\epsilon[0, N]$, біт кожного файлу незалежно від інших кеш-сховищ. Щоб розглянути етап доставки контенту припускається, що $K = N = 3$, де K – кількість користувачів. Таким чином, розглядається загальний кортеж запитів користувачів один, два та три, що роблять запит на файли A, B та C, відповідно. Файл A розділяється на вісім частин $A = (A_\emptyset, A_1, A_2, A_3, A_{12}, A_{13}, A_{23}, A_{123})$, де A_s позначає біти файлу A, які зберігаються виключно у користувачів у наборі S. Файли B та C розбиваються аналогічним чином. На основі цього поділу вміст кожного кешу може бути виражений, як показано на рис. 1. Спочатку, сервер надсилає кодований пакет $A_{23} \oplus B_{13} \oplus C_{12}$, який є одночасно корисним для усіх трьох користувачів (що легко побачити, перевіривши вміст кеш-сховищ). Потім він надсилає кодовані пакети, які корисні для двох користувачів, $A_2 \oplus B_1$ для першого та другого користувачів, $A_3 \oplus C_1$ для користувачів один та три та $B_3 \oplus C_2$ для користувачів два та три. Нарешті, сервер надсилає $A_\emptyset$, $B_\emptyset$ та $C_\emptyset$, кожен корисний лише одному користувачеві.

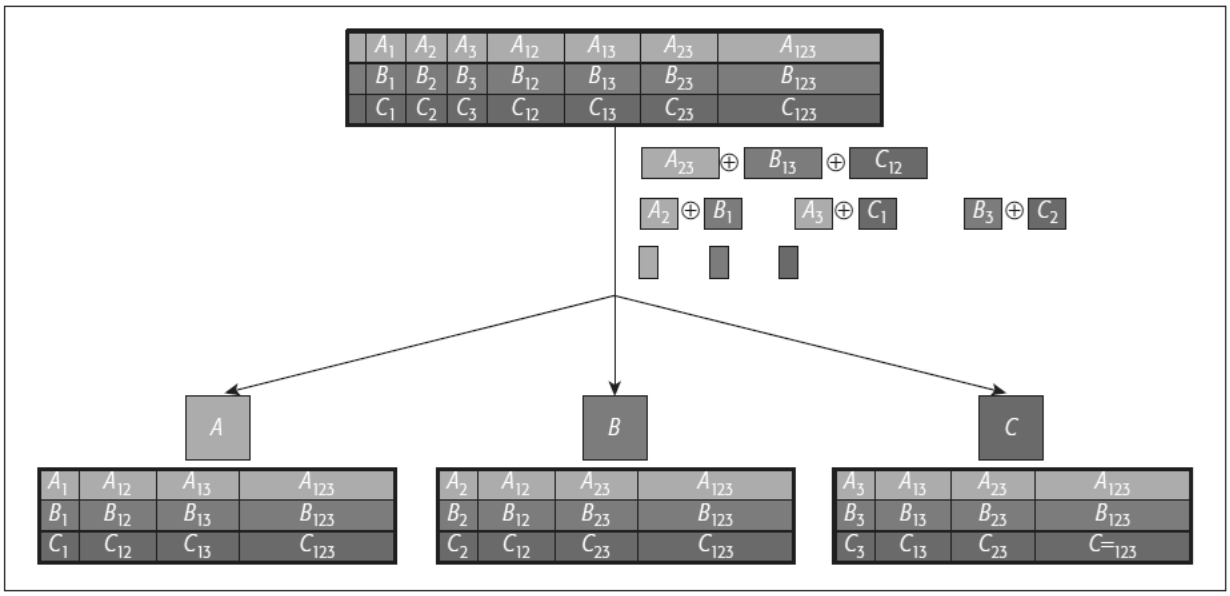


Рис.1 Схема децентралізованого кодованого кешування для *K=3* користувачів, *N=3* файлів та розміром кешу *M*.

Децентралізована схема кешування володіє властивістю універсальності, що є ключем для вирішення проблеми асинхронних та неоднорідних користувацьких запитів, а також проблеми онлайн обробки контенту.

Асинхронні запити та динамічні мережі. Зазвичай користувацькі запити є асинхронними, особливо це проявляється в стільникових мережах, де користувачі можуть переміщуватися від однієї «мережі» (стільника) до

іншої. В наслідок цього, кількість та ідентичність користувачів, що використовують спільний канал зв'язку, постійно змінюється. Децентралізована схема кодованого кешування дозволяє ефективно обробляти подібні ситуації. Перед відправкою контенту, сервер визначає сукупність активних користувачів, а потім використовуючи децентралізовану схему кодованого кешування надсилає контент.

Неоднорідні запити. Децентралізована схема кодованого кешування є приблизно оптимальною для контента з рівномірною популярністю. Проте, на практиці, файли контенту часто мають популярність, що коливається в межах кількох порядків. Для таких неоднорідних розподілів [2] пропонується розділити набір файлів на кілька груп з однаковою популярністю в кожній групі. Після цього, для кожної групи виділяється частка пам'яті у кеш-сховищах. Таким чином фази розміщення та передачі контенту проходять окремо для кожної групи файлів. Кількість користувачів, які надсилають запити на файли з певної групи файлів, є випадковою та не відомою під час фази розміщення. Незважаючи на це схема децентралізованого кодування гарантує ефективість данного групового підходу.

Онлайн оновлення кеш-сховищ. Окрім того, що контент відрізняється за популярністю, кожен набір популярних файлів постійно змінюється. Для забезпечення ефектвності, контент кеш-сховищ має постійно апаптуватися відповідно до цих змін. Зазвичай це робиться шляхом використання схем онлайн кешування, у яких контент кеш-сховищ оновлюється у кінці фази доставки. Згідно з [3] LRU алгоритм, що є оптимальним правилом для оновлення кешу в системі з одним кеш-сховищем, він не є оптимальним для кеш-мереж. В [3] пропонується альтернативний підхід, у якому сервер має два режими доставки. Для запитуваних файлів, які вже частково кешовані у сховищі, він використовує кодовану доставку. В свою чергу для не кешованих файлів сервер застосовує не кодовану доставку. Завдяки використанню не кодованої доставки, з кожного кеш-сховища вилучаються частини деяких старих файлів, що потім замінюються фрагментами нещодавно отриманих файлів. Оскільки кількість запитів до кешованих файлів є величиною випадковою, тут знову використовується універсальність децентралізованого кодованого кешування.

Таким чином, підтвердженно, що використання децентралізованої схеми кодованого кешування є ключем у вирішені проблем асинхронних запитів користувачів. Також представлена децентралізована схема являється ключовим елементом в обробці неоднорідних користувацьких запитів та онлайн оновлені вмісту кеш-сховищ.

Література

1. Maddah-Ali M. Coding for Caching: Fundamental Limits and Practical Challenges / M. Maddah-Ali, U. Niesen. // IEEE Communications Magazine. – 2016. – №54. – С. 23–29.
2. Niesen U. Coded Caching with Nonuniform Demands / U. Niesen, M. Maddah-Ali. // IEEE INFOCOM. – 2014. – С. 221–226.
3. Pedarsani R. Online Coded Caching / R. Pedarsani, M. Maddah-Ali, U. Niesen. // IEEE ICC. – 2015. – С. 1878–1883.

УДК 621.391.6

ПЕРСПЕКТИВЫ РАЗВИТИЯ INTERNET OF THINGS С ИСПОЛЬЗОВАНИЕМ СЕТЕЙ 5G

Шнурков В.О., Міночкін Д.А.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: shnurkov1997@ukr.net

Prospects for the development of Internet of Things using 5G networks

A review of the current state, prospects for the development of the Internet of things(IoT) - a new trend in the modern world. Smart devices will be able to penetrate almost every sphere of our life, but to realize this we need a new standard of mobile communication, which will be used as a basis for IoT. A review of the requirements that are advanced to the next generation network.

Интернет вещей (Internet of Things, IoT) – это глобальная сеть подключенных к Интернету физических устройств – «вещей», оснащенных сенсорами, датчиками и устройствами передачи информации. Эти устройства объединены посредством подключения к центрам контроля, управления и обработки информации.

Ценность продуктов из IoT-сферы заключается не в технологии или в интернет-подключении как таковом. Ценность составляет информация, которую собирают «умные» устройства, превращая данные в сведения и в руководство к действию для индивидуальных владельцев или групп людей. [1]

Для передачи данных от «умных» устройств сегодня существует несколько специализированных стандартов. Стандарт eMTC (enhanced Machine-Type Communication) разворачивается на основе мобильных сетей LTE, а EC-GSM-IoT (Extended Coverage – GSM – Internet of Things) работает поверх сети GSM. Но наиболее популярный – стандарт NB-IoT (Narrowband IoT). Его особенность состоит в том, что он может быть развернут, как в сетях GSM или LTE, так и независимо, отдельной сетью. [2]

По данным Ericsson Mobility Report, сегодня в мире насчитывается более 16 млрд подключенных устройств. По прогнозам, к 2020 году будут развернуты около 50 миллиардов подключенных устройств. Соотношение связанных вещей с людьми оценивается в 7: 1 к 2020 году. Хотя не все соединения будут осуществляться через сотовую сеть, ожидается, что они будут составлять 22% сотовых соединений к 2022 году. [3]

В связи с таким прогнозом возникают требования к новому стандарту

для соединения устройств. Появление технологии 5G вызвано необходимостью преодоления вызовов мобильного рынка. Предшествующие поколения технологии подвижной связи не способны решить следующие проблемы:

•взрывной рост мобильного трафика передачи данных — как абонентского, так и служебного;

- переход от соединений, сосредоточенных на задачах обеспечения связи в цепочке «человек-человек» (H2H) или «человек-машина (сервер)» (H2M), к соединениям, нацеленным на обеспечение связи в цепочке «машина-машина» (M2M);

- необходимость сократить капитальные затраты на развертывание сетей по сравнению с инвестициями, вкладываемыми в сети предыдущего поколения, и минимизировать операционные затраты для повышения их экономической эффективности.

Как считают ведущие мировые вендоры, сети 5G должны обеспечивать:

- возможность роста объема передаваемых данных более чем в 1000 раз в каждой области обслуживания за счет повышения спектральной эффективности, использования новых радиочастотных диапазонов и гетерогенных сетей;

- увеличение от 10 до 100 раз количества присоединенных абонентских устройств (до 300 тыс. на узел доступа; в настоящее время технология LTE обеспечивает работу до 200 абонентов в соте со скоростями 100/50 кбит/с в линиях вниз/вверх соответственно);

- увеличение от 10 до 100 раз типовых скоростей передачи данных на стороне пользователя;

- удлинение в 10 раз срока службы батарей для абонентских устройств с низкой мощностью;

- снижение в 10 раз задержки (менее 1 мс против 10 мс в LTE). [4]

Для обеспечения данных требований будет использоваться технология Massive MIMO - эволюция уже существующей технологии MIMO, которая используется в сетях 4G/LTE. Концепция реализации Massive MIMO предполагает использование многоэлементных фазированных антенных решеток с количеством элементов, превышающим 128. Это позволит обслуживать огромное количество устройств в пределах одной соты и добиться повышения спектральной эффективности.

Это, в свою очередь, позволит «перевернуть» многие традиционные

сферы применения беспроводных сетей, внедрив сотни миллионов онлайн-объектов, выполняющих самые различные функции. Собственно, 5G станет неким каркасом, вокруг которого начнет формироваться облик новой, цифровой экономики, активно использующей технологию IoT умножая уже известные преимущества последней и приближая ее широкое распространение.

Наибольший выигрыш от внедрения 5G и IoT смогут получить промышленная, транспортная, финансовая, энергетическая, медицинская сферы, а также сферы безопасности и развлечений. Малая задержка распространения сигнала в 5G дает ряд уникальных возможностей для применения при управлении беспилотниками или контроля движения самоуправляемых автомобилей. Совмещая данные из различных источников и устройств, можно получать бесконечный поток информации, используя его в разных сферах — от телемедицины и научных исследований до управления городским транспортом и добычи ископаемых.

5G приведет к революционным изменениям в тех сегментах IoT, где объекты сильно удалены, или необходима быстрая реакция. Как пример, можно привести АПК (мониторинг полей, управление сельхозтехникой) или промышленность (быстродействующие промышленные роботы и т.п.). [5]

Таким образом, в данной работе были рассмотрены актуальные на сегодняшний день тренды беспроводных систем связи, а именно:

- Концепция Internet of Things;
- Ценность данных, собираемых и обрабатываемых «умными» устройствами и возможности их использования в разных сферах жизни;
- Требования к новому стандарту сотовой связи 5G и важность их реализации для успешного развития IoT;
- Перспективы развития IoT.

Литература

1. Перспективы развития «интернет вещей» до 2020 года http://1234g.ru/novosti/internet-veshchej-k-2020-godu.
2. Что такое интернет вещей и зачем он нужен? https://nv.ua/science/lectures/chto-takoe-internet-veshchej-1326653.html.
3. Toward 5G: Applications, Requirements & Candidate Technologies, edited by Rath Vannithamby and Shilpa Talwar. ISBN: 978-1-1- 8-97983-9, John Wiley & Sons, 2017.
4. ISSN 0013-5771. «ЭЛЕКТРОСВЯЗЬ», № 10, 2013.
5. Интернет вещей и 5G, https://geektimes.ru/company/unet/blog/293017.

УДК 621.396.1

ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ СТІЛЬНИКІВ У МЕРЕЖАХ П'ЯТОГО ПОКОЛІННЯ 5G

Казачінер К.А., Кравчук С.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kazachinerkiril@gmail.com

Technologies of the Virtual Small Cells in 5G-Networks

Proposed an approach for the virtual small cell formation in 5G networks. Provided the mathematical algorithm for using virtual cells by which the overall network capacity can be significantly increased.

Для задоволення потреб користувачів та подолання викликів, висунутих у системі 5G, необхідна суттєва зміна стратегії проектування безпроводової стільникової архітектури мережі 5G. Одною з перспективних технологій розвитку мереж п’ятого покоління – є впровадження технології віртуалізації на мережевому рівні, рівні додатків, а також й віртуалізації стільників. В даній роботі запропоновано новий підхід до формування віртуальних малих стільників для мереж 5G, в якому підмножина кваліфікованих користувачів обирається як базові станції віртуальних малих стільників, що зв'язують інших користувачів з базовою станцією макросоти [1].

Ущільнення малих стільників є перспективною технікою у п'ятому поколінні (5G) мобільних мереж для підтримки очікуваного різкого збільшення швидкості передачі даних. У цій техніці макросота або гаряча точка з дуже високим попитом на трафік поділяються на менші стільники, в яких користувальницьке обладнання (UE), замість підключення до підмножини БС макросоти, підключені до підмножини БС малих стільників, яка обслуговує менше UE, з меншою відстані, ніж у підмножини БС макросоти. Використовуючи цей підхід, доступна смуга пропускання може бути повторно використана для внутрішніх повідомлень малих стільників. Цей результат у поєднанні зі збільшенням співвідношення сигнал/шум на рівні зв'язку може призвести до суттєвого збільшення загальної ємності мережі.

В даному дослідження ми припускаємо, що кожен UE, незалежно від інших UE, переходить до режиму БС малих стільників з певною вірогідністю α.

Підмножина БС малих стільників та обслуговуючі UE у режимі користувача складають два незалежних процеси Пуасона з щільністю:

$\lambda_b = \alpha\lambda$ та

$\lambda_u = (1- \alpha)\lambda$

Нормалізована щільність підключених UE через підмножину БС малих стільників, порівняно з імовірністю вибору режиму БС, α для різних значень $\overline{n}$ зображено на рис.1. Де n - середня кількість підключених користувачів до малого стільника.

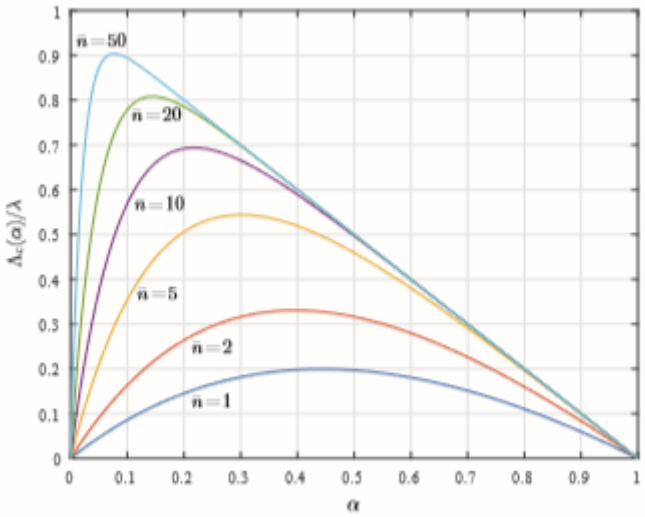


Рис. 1. Порівняння щільності підключення UE через підмножину БС малих стільників до ймовірності вибору режиму БС

На рисунку 2 показані точні та приблизні оптимальні ймовірності вибору режиму БС з точки зору середньої кількості підключених UE до кожної БС малого стільника. Як показано на рисунку, приблизна величина дуже точна для $\overline{n} \geq 5$. Крім того, на рисунку 2 показана оптимальна нормалізована щільність сполучених користувачів через підмножину БС малих стільників.

Область Пуассона підмножини БС малих стільників, в якій кожна БС пов'язана з незалежною випадковою зоною покриття з середньою площею $\overline{A}$, може розглядатися як процес покриття. У цьому випадку, UE у користувацькому режимі може бути підключено, принаймні, до однієї БС малого стільника з ймовірністю:

$$P_{con}(\alpha) = 1 - e^{-\lambda_b \overline{A}} = 1 - \exp(-\alpha\lambda\pi \mathrm{M}\{R_m^2\})$$

де M – це це математичне очікування, а R – відстань між UE та БС.

Використовуючи ймовірність вибору оптимального режиму для щільної мережі ($\overline{n} \gg 1$), при якій щільність малих стільників дорівнює щільності підмножини БС малих стільників, отримуємо:

$$\lambda_{b.opt} = \alpha_{opt}\lambda = \frac{\ln(\overline{n}+1)}{\overline{n}+1}\lambda \cong \frac{\ln(1+\lambda\pi \mathrm{E}\{R_m^2\})}{\pi \mathrm{E}\{R_m^2\}}.$$

Це означає, що, асимптотично, кількість малих стільників логарифмічно зростає з щільністю користувачів. Оскільки ізольовані UE з'єднуються безпосередньо з підмножиною БС макросоти, а кожен малий стільник підключений до макросоти з зовнішньою лінією, то щільність необхідних ліній до підмножини БС макросоти для того, щоб усі користувачі були пов’язані, розраховується:

$$\lambda_\iota = \lambda_{b.opt} + \left(\lambda - \lambda_{b.opt} - \Lambda_c(\alpha_{opt})\right) =$$

$$= \left[\frac{\ln(\overline{n}+1)}{\overline{n}+1} + \frac{1 - \frac{\ln(\overline{n}+1)}{\overline{n}+1}}{(\overline{n}+1)^{\frac{\overline{n}}{\overline{n}+1}}}\right]\lambda \cong \frac{1 + \ln(1+\lambda\pi \mathrm{E}\{R_m^2\})}{\pi \mathrm{E}\{R_m^2\}}$$

для $\overline{n} \gg 1$. Отже, коли кількість з'єднань до БС макросоти пропорційна λ без використання технології віртуальних малих стільників, це число пропорційне логарифму λ у високо щільних мережах, при використанні технології малих віртуальних стільників [2].

Було розглянуто метод формування віртуальних стільників, в якому група окремих UE може відігравати роль підмножини БС малих стільників для інших UE. Для цієї схеми була отримана оптимальна щільність малих стільників, при якій кількість з'єднань зв'язку з підмножиною БС макросоти для підключення всіх користувачів безпосередньо або через малі стільники мінімізується, і було показано, що це значення асимптотично пропорційне логарифму щільність мережі.

Література

1. A Survey of 5G Network: Architecture and Emerging Technologies - Akhil Gupta, Rakesh Kumar Jha.
2. Virtual Small Cells Formation in 5G Networks - Aydin Behnad, Xianbin Wang.

УДК 621.396.9

КОНЦЕПЦИЯ СОЗДАНИЯ АРХИТЕКТУРЫ «РАСПРЕДЕЛЕННОГО СПУТНИКА» ДЛЯ НИЗКООРБИТАЛЬНЫХ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ГРУППИРОВКИ МИКРО- И НАНО-СПУТНИКОВ

Ильченко М.Е.[1], Нарытник Т.Н.[1], Рассамакин Б.М.[1], Присяжный В.И.[2], Капштык С.В.[2]

[1] КПИ им. Игоря Сикорского

[2] Национальный центр управления и испытаний космических средств

E-mail: director@mitris.com

The concept of creating a "distributed satellite" architecture for low-orbit information and telecommunications systems based on the grouping of micro and nano satellites

For low-orbit information and telecommunication systems for various purposes, the concept of creating a "distributed satellite" architecture is proposed, which is based on the use of satellite platforms of the micro satellite and nano satellite and the distribution of functional blocks of the composite payload of higher-class satellites (mini satellite and small satellite) connected satellites.

Растущий интерес к использованию низких околоземных орбит (высотой до 1500 км) обусловлен многими факторами[1-8]. К ним относятся:

-перспективы внедрения и развития в ближайшее десятилетие Интернета вещей (Internet of Thongs - IoT) и, построенных с использованием родственных технологий, промышленного интернета вещей (Industrial Internet of Thongs - IIoT) и интернета вещей для удаленных районов (Remote Internet of Things - RIoT), что обуславливает дальнейшее развитие телекоммуникационных систем для передачи возрастающего трафика этих услуг;

-задачи исследования Земли из космоса для целей научных исследований и экономического использования природных ресурсов, контроля развития и функционирования инфраструктурных проектов, функционирования территориально распределенных промышленных производств, транспортной инфраструктуры всех видов транспорта[1.2],

Фактором, существенно ограничивающим дальнейшее внедрение микро и нано спутников, является их ограниченные возможности по размещению, адаптации, обеспечению электроснабжения и отвода тепла сложной полезной нагрузки. Разрешить это противоречие можно на основе размещения сложной полезной нагрузки на нескольких спутниках, находящихся на одной орбите в непосредственной близости один от другого и функционирующих совместно. Такой подход названо концепцией создания архитектуры «распределенного спутника». В качестве примера в докладе рассмотрены возможные варианты применения архитектуры «распределенного спутника» в двух сегментах рынка космических информационных систем: дистанционное зондирование Земли и телекоммуникационные системы. Применение «распределенного спутника» в радиолокационных системах с синтезированной апертурой (SAR-система) рассмотрено с учетом требования операторов спутниковых SAR-систем и потребителей их информации о необходимости увеличивать информационное

содержание в изображениях SAR, улучшать разрешения по дальности, по азимуту и временные показатели (частота повторной съемки одной и той же области), а также обеспечивать наблюдение под различными углами (интерферометрия и томография) [4]. Использование архитектуры «распределенного спутника» в SAR-системах позволяет также реализовать технологию мультистатической радиолокации с «мягкой» интерференционной базой (от 200 м до 1 км) [3]. На рис.1. представлена схема организации и взаимодействия «распределенного спутника». В состав «распределенного спутника» входят: спутник-передатчик на платформе микро спутника, который является ядром спутникового кластера, и нескольких спутников-приемников на платформе куб-сат. Подробно рассмотрены функции, которые должны выполнять спутник-передатчик, межспутниковая радиолиния и спутник-приемник. Межспутниковая радиолиния, которая организуется отдельно к каждому спутнику-приемнику, обеспечивает измерение наклонной дальности и определение углов (угол места и азимут в плоскости местного горизонта) на основе моноимпульсного метода слежения.

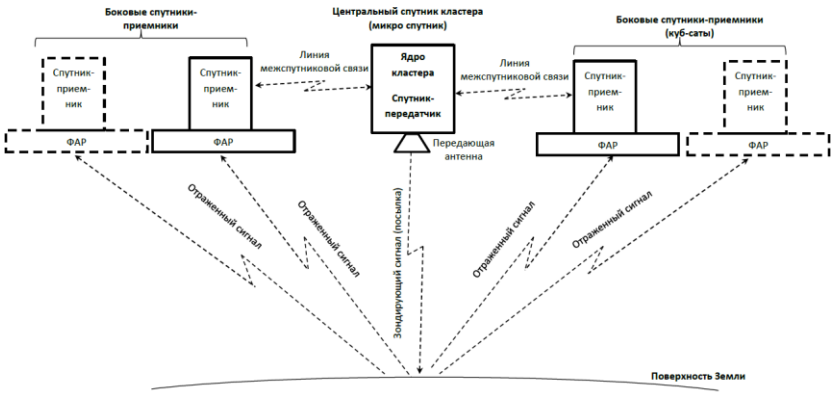


Рис. 1. Применение концепции «распределенного спутника» для задач дистанционного зондирования с синтезированной апертурой.

Работа «распределенного спутника» поясняется рис.2, на котором представлена структурная схема SAR-системы дистанционного зондирования Земли .

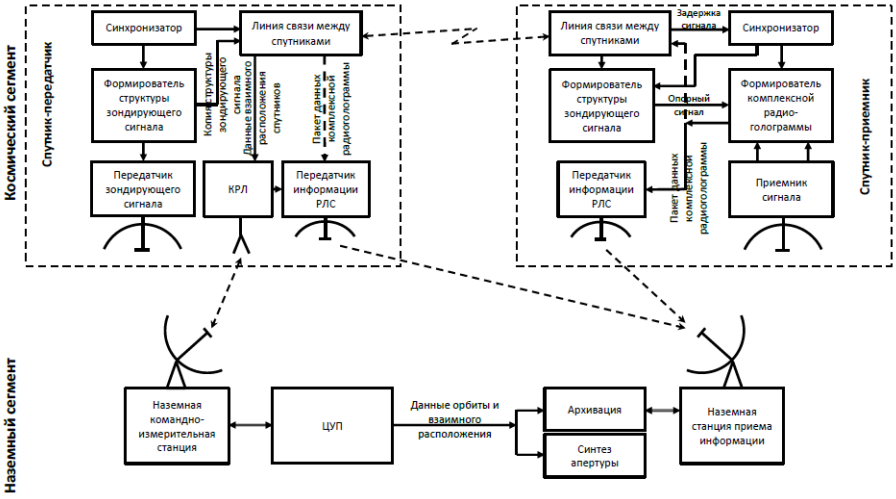


Рис. 2. Структурная схема SAR-системы дистанционного зондирования Земли

Применение «распределенного спутника», в состав которого входят корневой спутник и спутники-ретрансляторы. в телекоммуникационных системах иллюстрируется рис.3, на котором представлен вариант архитектуры низкоорбитальной системы спутниковой связи.

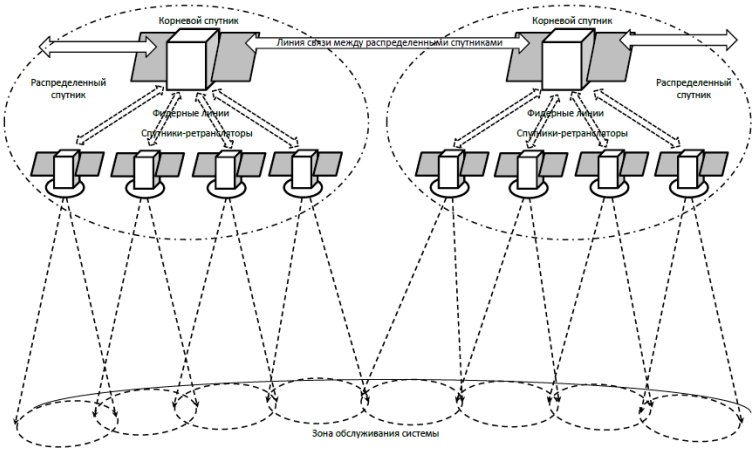


Рис. 3. Вариант архитектуры низкоорбитальной системы спутниковой связи

Концепция «распределенного спутника» с использованием только спутников форм-фактора куб-сат, которая может быть применена при построении спутниковой системы для предоставления услуг IoT, представлена на рис.4.

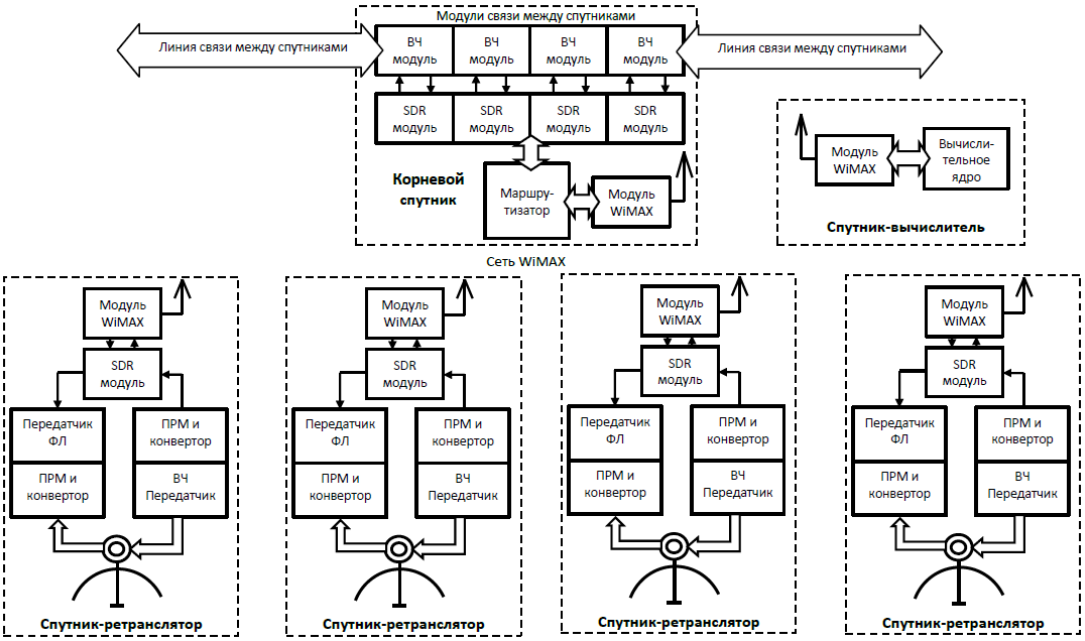


Рис.4. Вариант «распределенного спутника» для
LEO-системы IoT с использованием куб-сат

В этой схеме спутники-ретрансляторы обеспечивают передачу в лучах пользователей транспортного потока DVB-S2, DVB-S2x, и прием потоков DVB-RCS/2, WiMAX от пользователей. Архитектура «распределенного спутника» позволяет реализовать в космическом сегменте LEO-системы FC-архитектуру.

В заключение отметим, что архитектура «распределенного спутника» позволяет эффективно использовать спутники класса микро спутник и нано спутник (куб-сат) для создания сложных информационно-телекоммуникационных систем космического базирования, в частности систем дистанционного зондирования земли радиолокационного типа с синтезированной апертурой, систем связи и широкополосного доступа, в том числе систем Интернета вещей. Использование платформ микро спутников массой до 100 кг и нано спутников массой до 10 кг создает условия для снижения стоимости низкоорбитальной информационно-телекоммуникационной системы, а разнесение функциональных элементов целевой полезной нагрузки системы по нескольким физически обособленным элементам позволяет упросить восстановление работоспособности системы и создать условия для совершенствования системы в процессе эксплуатации.

Литература

1. Prospects for the Small Satellite Market. A Euroconsult Executive Report. March 2015.
2. Iceye raises $13 million for radar microsatellites. by Jeff Foust - August 24, 2017 http://spacenews.com/iceye-raises-13-million-for-radar-microsatellites.
3. Верба В.С., Неронский Л.Б., Осипов И.Г., Турук В.Э. Радиолокационные системы землеобзора космического базирования/ Под ред. В.С. Вербы. – М.: Радиотехника. 2010 – 680с.: ил.
4. A Tutorial on Synthetic Aperture Radar. Alberto Moreira, Pau Prats-Iraola, Marwan Younis, Gerhard Krieger, Irena Hajnsek, and Konstantinos P. Papathanassiou. Microwaves and Radar Institute of the German Aerospace Center (DLR), Germany. IEEE Geoscience and Remote Sensing Magazine. March 2013.
5. LEO Vantage 1 - Gunter's Space Page. http://space.skyrocket.de/doc_sdat/leo-vantage-1.htm.
6. LEO Vantage 2 Satellite. http://spaceflight101.com/meteor-m-2-1/leo-vantage-2.
7. OpenFog Reference Architecture for Fog Computing. Produced by the OpenFog Consortium Architecture Working Group. February 2017. OPFRA001.020817.

УДК 621.396

ПОКРАЩЕНИЙ АЛГОРИТМ ВЕРТИКАЛЬНОЇ СИНХРОНІЗАЦІЇ МІЖ WIMAX ТА WIFI

Немченко К.В., Міночкін Д.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: knemchenko@srs.kpi.ua

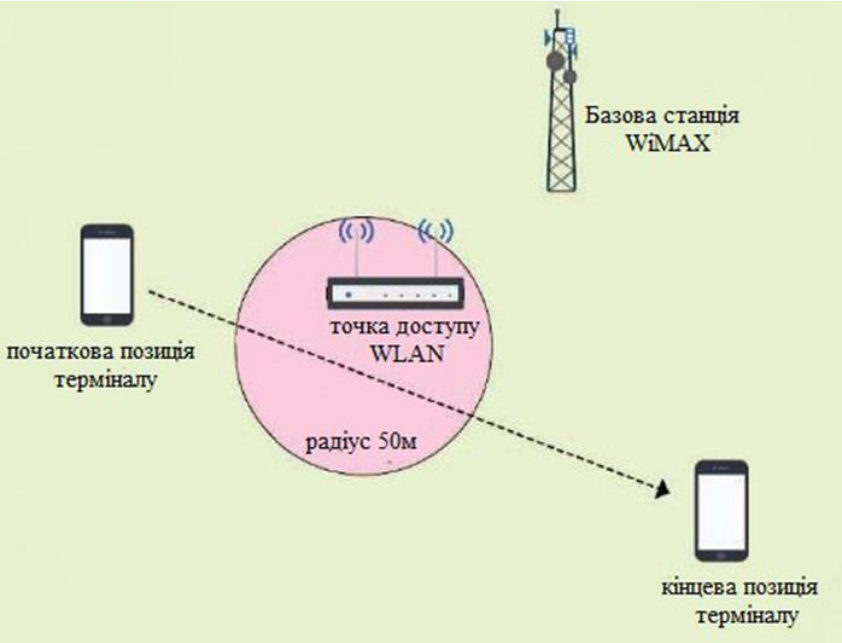
Improved algorithm of the vertical synchronization of the WIiMAX and WiFi

This publication about improving the decision algorithm during vertical handover between WLAN and WiMAX. The improvements include proposing new algorithm for vertical handover the two networks the service for the users. The proposed algorithm is based on the WLAN overload, which is dedicated while providing good quality of service.

На сьогодні використання портативних приладів збільшується щоденно. Тому у населення виникає потреба у високоякісному обслуговуванні операторами зв'язку. На сьогодні одне з головних завдань інженерів телекомунікацій полягає у забезпечені користувачів мережі постійним якісним зв'язком.

Для територіально розподілених систем, ефективним технічним рішення є можливість підтримки терміналів відносно точок доступу, що їх обслуговують. Передача обслуговування передбачає передачу поточного з'єднання з однієї станції обслуговування до іншої. Передача відбувається в процесі руху абонента між базовою станцією, яка його обслуговує та іншими базовими станціями територіально розподіленої системи [1].

Типовим прикладом є передача обслуговування між WiMAX та WiFi мережами (рисунок 1).



Рис, 1. Схема мережі з вертикальною передачею обслуговування між WiMAX та WiFI

Згідно стандарту IEEE 802.21 для вертикальної передачі обслуговування між WiMAX та WLAN на сьогодні використовується алгоритм зазначений на рисунку 2.

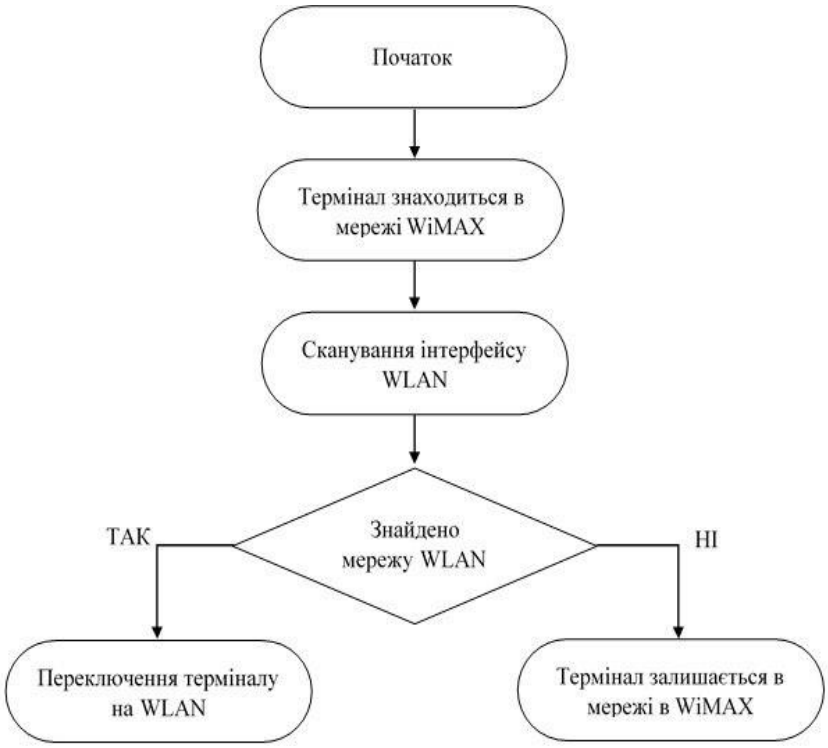


Рис. 2. Схема існуючого алгоритму вертикальної передачі обслуговування у стандарті IEEE 802.21

Такий алгоритм ініціює переключення терміналу з мережі WiMAX на WLAN у випадку якщо мережа WLAN є доступною до підключення. Весь час термінал сканує інтерфейс WLAN і якщо мережа є доступною він ініціює процес передачі обслуговування [2].

Однак у реальних системах виникають ситуації коли після підключення до мережі WLAN якість з'єднання стає гіршою ніж при підключенні по мережі WiMAX. Зазвичай така проблема виникає через перенавантаження, збій програмного забезпечення та відсутність з'єднання [3].

Для вирішення даної проблеми слід аналізувати стан мережі WLAN. Якщо навантаження на мережу WLAN або у системі присутні інші вищезазначені проблеми, то переключення не відбувається. У випадку, якщо мережа WLAN може прийняти нових абонентів — виконується передача обслуговування. Алгоритм схематично зображено на рисунку 3.

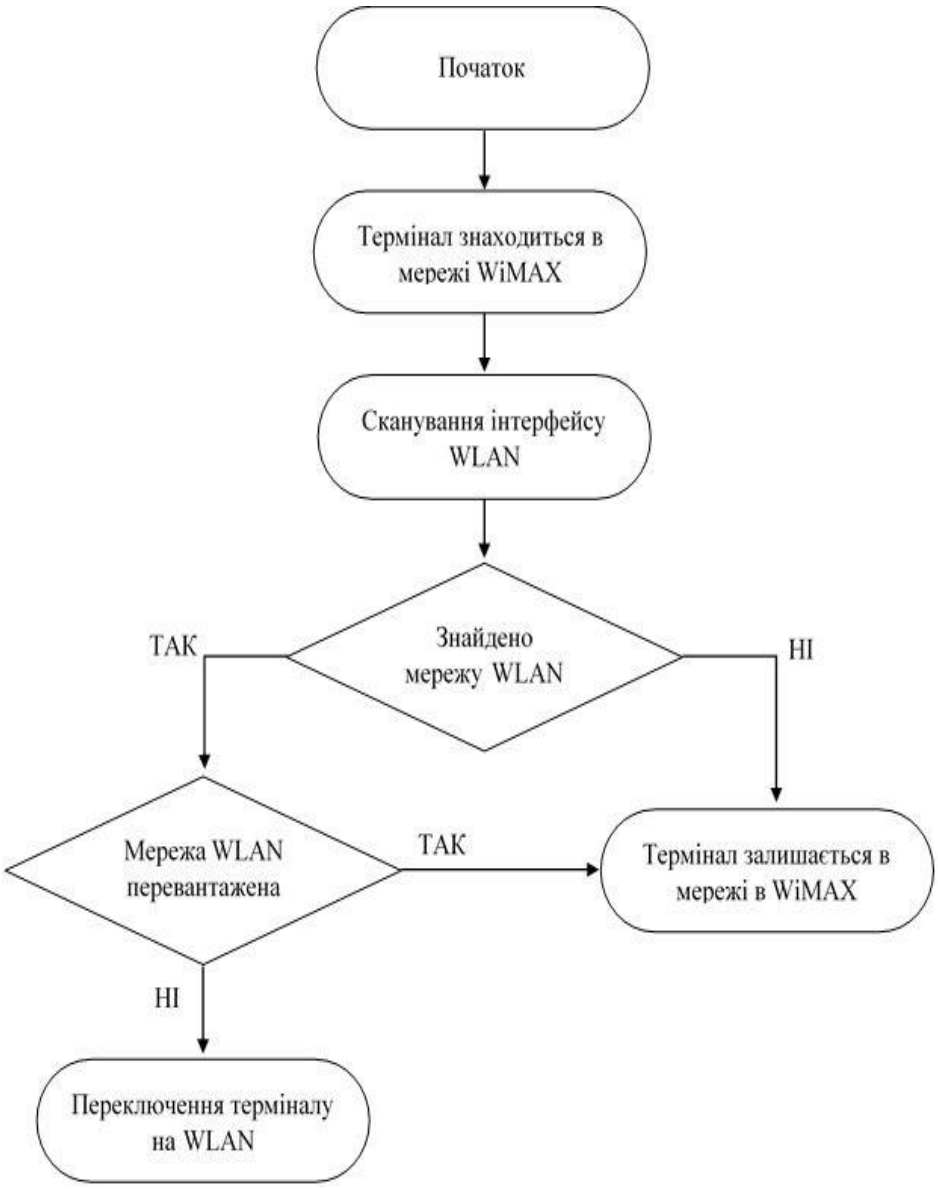


Рис. 3. Схема покращеного алгоритму вертикальної передачі обслуговування на базі існуючого

Таким чином, запропонований алгоритм ні в якому разі не погіршить якість обслуговування при виконанні вертикальної передачі обслуговування між WiMAX та WLAN.

Література

1. С.О, Кравчук, Д.А. Міночкін, “Класифікаця методів вертикальної передачі обслуговування”, Національний технічний університет України “Київський політехнічний інститут”.
2. Z. Dai, R. Fracchia, J. Gosteau, P. Pellati and G. Vivier, “Vertical Handover Criteria and Algorithm in IEEE 802.11 and 802.16 Hybrid Networks”, Communications 2008, IEEE International Conference, (2008) May 19-23.
3. M. Kassar, B. Kervella and G. Pujolle, “An Overview of vertical handover decision strategies in heterogeneous wireless networks”, Computer Communications, vol. 31, (2008), pp. 2607-2620.

УДК 621.391

АВТОМАТИЗАЦІЯ ФОРМУВАННЯ РІВНЯННЯ БАЛАНСУ МАРКІВСЬКОГО ПРОЦЕСУ

Пустовий Б.Л., Князєва Н.О.
Інститут холоду, кріотехнологій та екоенергетики імені В. С. Мартиновського Одеської національної академії харчових технологій, Україна
E-mail: b.pustoviy@gmail.com

The automation of the equation balance modeling of the Markov process

The software was developed during this work. It is intended to automate the calculation of probable states of the system and to construct the transition graph of the Markov process. Also this program can create system of equations to determine stationary probabilities.

У зв'язку зі збільшенням попиту на сучасні інтелектуальні сервіси (ІС) виникає необхідність в дослідженні методів підвищення якості їх надання, що обумовлює необхідність оцінки ефективності управління наданням ІС.

Для оцінки ефективності управління наданням ІС необхідно виконати аналіз архітектури мережі, принцип побудови системи управління і розробку результуючого критерію ефективності управління наданням ІС. Питання, пов’язані з дослідженням методів оцінки ефективності управління ІС були розглянуті в роботах Л.Н. Беркман [4], Н.О. Князевої, С.В. Шестопалова [2] та інших науковців.

Згідно рекомендацій МСЕ [3] для визначення ефективності управління наданням ІС необхідно розрахувати технічні показники роботи мережі, такі як час знаходження в мережі заявки на ІС, ймовірність втрати заявки, кількість заявок, котрі очікують обслуговування. Для розрахунку технічних показників в роботах [1, 2] пропонується використовувати аналітичну модель системи управління ІС. Майже всі моделі дискретних систем із стохастичним характером функціонування розробляються на основі СМО, процеси в яких є випадковими і, у багатьох випадках, марківськими або деяким чином пов'язані з марківськими процесами. Тому при вирішенні завдань теорії масового обслуговування може використовуватися математичний апарат теорії марківських процесів. Застосування марківських процесів особливо ефективне і результативне при дослідженні СМО та мереж масового обслуговування (МеМО) з накопичувачами обмеженої ємкості [1].

Однак використання марківських процесів, при ручному розрахунку стає неможливим у великих системах через дуже велику кількість станів системи. У системі з одним управляючим приладом (УП) і трьома класами заявок кількість станів становить 40, але вже при збільшенні кількості УП до трьох і кількості класів заявок до трьох, кількість можливих станів зростає до 64 тис., що робить абсолютно неможливим вручну побудувати граф переходів і систему рівнянь для розрахунку показників.

В даній роботі запропоновано програмне забезпечення (ПЗ) для автоматизації розрахунку ймовірних станів системи, побудови графу переходів марківського процесу та формування системи рівнянь для визначення стаціонарних ймовірностей.

ПЗ написане на скриптовій мові програмування JavaScript з використанням відкритої бібліотеки React JS, що дозволяє запускати його у будь-якому браузері. Максимальна кількість станів для розрахунку СМО (МеМО) залежить від технічних характеристик комп'ютера.

При розробці ПЗ були прийняті деякі допущення:

- одночасно УП може обслуговувати лише один клас заявок;
- черга на обслуговування будується за дисципліною FIFO;
- система функціонує без втрати заявок.

Вхідними даними розробленого ПЗ є:

- кількість УП;
- максимальна довжина черги на обслуговування;
- кількість класів заявок та їх пріоритет.

На основі введених вхідних даних ПЗ кодує всі можливі стани марківського процесу для заданої системи. Кодування відбувається наступним чином:

$$E_n = (\text{П}_1\text{Ч}_1 \,/\, \text{П}_2\text{Ч}_2 \,/\, \ldots \,/\, \text{П}_i\text{Ч}_i / .. / \text{П}_N\text{Ч}_N), \qquad (1)$$

де: - E_n – стан марківського процесу, n – номер стану;

- $\text{П}_i = \overline{0,\ m}$ – стан обслуговуючого приладу, одночасно в котрому на обслуговуванні може знаходитись лише одна заявка певного класу («0» - прилад вільний, «m» – на обслуговуванні знаходиться заявка класу «m»), «i» – номер приладу, «N» – кількість УП;

- $\text{Ч}_i = \underbrace{\overline{0,\ m \ldots m}}_{k}$ – стан черги на обслуговування («0» - черга порожня, «m» – в черзі на обслуговуванні знаходиться заявка класу «m»), «k» - кількість місць в черзі на обслуговування.

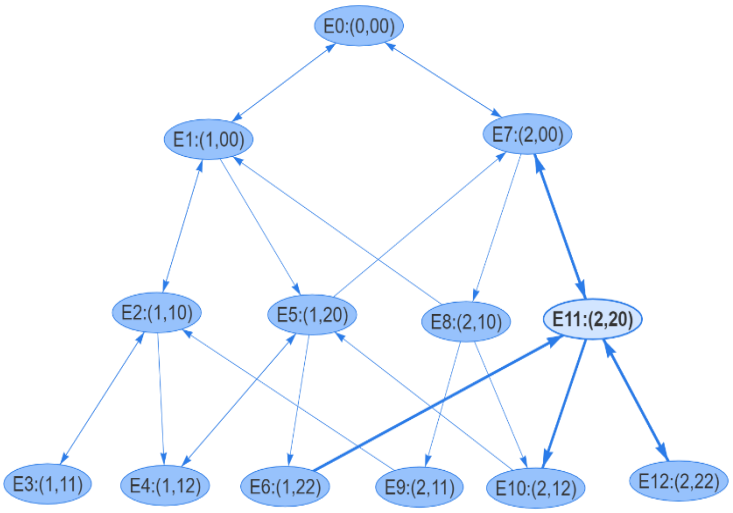


Рис. 2. Розмічений граф переходів марківського процесу

Використовуючи закодовані стани, ПЗ будує розмічений граф марківських процесів. На рис. 2 наведено приклад побудови графу переходів марківського процесу в системі з одним УП, максимальною довжиною черги у дві заявки з різним пріоритетом.

На основі сформованого графу переходів ПЗ складає систему рівнянь для визначення стаціонарних ймовірностей:

$$
\begin{cases}
p0 \cdot \lambda 1 + p0 \cdot \lambda 2 = p1 \cdot \mu 1 + p7 \cdot \mu 2 \\
p1 \cdot \mu 1 + p1 \cdot \lambda 1 + p1 \cdot \lambda 2 = p0 \cdot \lambda 1 + p2 \cdot \mu 1 + p5 \cdot \mu 1 \\
p2 \cdot \mu 1 + p2 \cdot \lambda 1 + p2 \cdot \lambda 2 = p1 \cdot \lambda 1 + p3 \cdot \mu 1 + p4 \cdot \mu 1 \\
p3 \cdot \mu 1 = p2 \cdot \lambda 1 \\
p4 \cdot \mu 1 + p4 \cdot \mu 1 = p5 \cdot \lambda 1 \\
p5 \cdot \mu 1 + p5 \cdot \lambda 1 + p5 \cdot \lambda 2 = p4 \cdot \mu 1 + p6 \cdot \mu 1 + p7 \cdot \lambda 1 \\
p6 \cdot \mu 1 = p11 \cdot \lambda 1 \\
p7 \cdot \mu 2 + p7 \cdot \lambda 1 + p7 \cdot \lambda 2 = p0 \cdot \lambda 2 + p8 \cdot \mu 2 + p11 \cdot \mu 2 \\
p8 \cdot \mu 2 = p1 \cdot \lambda 2 + p9 \cdot \mu 2 + p10 \cdot \mu 2 \\
p9 \cdot \mu 2 = p2 \cdot \lambda 2 \\
p10 \cdot \mu 2 + p10 \cdot \mu 2 = p5 \cdot \lambda 2 \\
p11 \cdot \lambda 1 + p11 \cdot \mu 2 + p11 \cdot \lambda 2 = p7 \cdot \lambda 2 + p10 \cdot \mu 2 + p12 \cdot \mu 2 \\
p12 \cdot \mu 2 = p11 \cdot \lambda 2 \\
\sum_{k=0}^{12} p_k = 1
\end{cases}
\qquad (2)
$$

де λ – інтенсивність надходження заявок, μ – інтенсивність обслуговування заявок.

Для запропонованої СМО при знайдених значеннях стаціонарних ймовірностей станів випадкового процесу ПЗ будує вирази для розрахунку технічних показників [1]:

Середнє число заявок в черзі:

$$L = 1p_2 + 2p_3 + 2p_4 + 1p_5 + 2p_6 + 1p_8 + 2p_9 + 2p_{10} + 1p_{11} + 2p_{12} \qquad (3)$$

Середнє число заявок в системі:

$$M=1p_1 + 2p_2 + 3p_3 + 3p_4 + 2p_5 + 3p_6 + 1p_7 + 2p_8 + 3p_9 + 3p_{10} + 2p_{11} + 3p_{12} \qquad (4)$$

Ймовірність втрати заявок:

$$P = p_3 + p_4 + p_6 + p_9 + p_{10} + p_{12} \qquad (5)$$

В даному прикладі представлені вирази для розрахунку технічних показників для СМО, в котрій наявний лише один управляючий прилад, але ПЗ дозволяє розраховувати показників і для МеМО з багатьма управляючими приладами.

Автоматизація процесів формування рівняння балансу марківських процесів дозволяє розраховувати технічні показники для великих систем, що зменшує похибку при дослідженні ефективності управління ІС та суттєво полегшує розрахунок технічних показників мережі.

Література

1. Алиев Т.И. Основы моделирования дискретных систем. СПб: СПбГУ ИТМО, 2009. 363
2. Князєва Н.О. Управління інтелектуальними сервісами в мережах наступного покоління: монографія / Н.О. Князєва, С.В. Шестопалов – Одеса: Бондаренко М.О., 2017. – 268 с.
3. “Международный союз электросвязи (ITU)”, официальное Интернет-представительство. — Режим доступа: http://www.itu.int (дата обращения 20.03.2015 г).
4. Беркман Л. Н. Інваріантність систем управління конвергентних мереж в режимі надзвичайних ситуацій / Л. Н. Беркман, Л. О. Комарова, І. А. Бойко // Наукові записки Українського науково-дослідного інституту зв'язку. - 2014. - № 1. - С. 11-15. - Режим доступу: http://nbuv.gov.ua/UJRN/Nzundiz_2014_1_4.

УДК 004.056.5:004.75

МЕТОД РОЗШИФРОВКИ ТРАФІКУ TLS ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ ЗАГРОЗ

Радівілова Т.А., Тавалбех М.Х.
Харківський національний університет радіоелектроніки
E-mail: tamara.radivilova@gmail.com, tavalbeh@icloud.com

DECRYPTING TLS TRAFFIC METHOD FOR HIDDEN THREATS DETECTION

The analysis of the basic methods of decrypting the TLS traffic was conducted on this work. The methods and technologies for detecting malicious activity in encrypted traffic used by leading companies are presented. Also developed, tested and offered a method of interception and decryption of traffic transmitted through TLS. The developed method was automated and can be used for remote listening to the network, which will allow decoding data transmitted in real-time mode.

В даний час існує тренд збільшення частки шифрованого трафіку. За оцінками Cisco, 60% трафіку в інтернет зашифровано, а за прогнозами Gartner до 2019-го вже 80% трафіку буде таким. Шифрування потрібне для забезпечення приватності громадян, для збереження таємниці в секреті, для виконання вимог законодавства. Але зловмисники також використовують шифрування для обходу механізмів детектування їх несанкціонованої активності, приховуючи взаємодію з командними серверами шкідливих програм і для інших завдань [1].

Існує багато ситуацій, коли адміністратори IT повинні використовувати перевірку пакетів, наприклад за допомогою Wireshark. Однак, коли дані зашифровуються, це стає більш складним завданням. Зазвичай найпростішим способом дешифрування даних є використання закритого ключа для відповідного відкритого ключа. Wireshark надає ще один засіб для дешифрування даних, а також з використанням пре-мастер ключа. Ponemon Institute попросив респондентів оцінити ймовірність виникнення атак і здатність протистояти цим атакам, які показано в таблиці 1 [2].

Пропонований в даній роботі підхід представляє собою метод розшифровки TLS-трафіку, який передбачає наявність у зловмисника доступу до комп'ютера або мережі, або ж зловмисник міг занести на комп'ютер жертви закладки, які можуть збирати дані про сесії. Такі умови потрібні для формування файлів сесійних ключів, які будуть використовуватися разом з відповідним перехопленим трафіком. Перехопити трафік жертви можна, перебуваючи в будь-якій ділянці мережі між сервером і об'єктом нападу.

Нижче наведено опис реалізації запропонованого методу розшифровки TLS-трафіку. В реалізації використовувався аналізатор трафіку Wireshark,

який допомагає провести аналіз роботи мережі, діагностувати проблеми, а також має багато інших корисних можливостей.

Таблиця 1. Напади та ймовірність протистояння ним.

	Ймовірність	
	нападу	***Протистояння нападу***
1. Зловмисник робить фішингові загрози ще більш законними, і навіть інформовані одержувачі вважають, що використання TLS гарантує їм безпеку. Однак, натиснувши на посилання, зловмисник надсилає користувачів до сервера SSL, завантаженого зловмисним програмним забезпеченням, яке заражає клієнта, оскільки трафік зловмисного програмного забезпечення зашифрований і не розпізнається системами виявлення вторгнень.	79%	17%
2. Зловмисник надсилає зашифрований потік захищених, чутливих та інших критичних даних, що надходять через брандмауер через "звичайні" порти (443,80 та ін.), які брандмауер налаштований прийняти, оскільки вони є затвердженими портами.	78%	30%
3. Ряд зловмисників використовує шифрування, щоб приховати інформацію про мережу, включаючи паролі та конфіденційні дані, які вони надсилають на сервери SSL. Шифрування засліпило системи моніторингу/інспектування для цієї внутрішньої мережі.	74%	16%
4. Зловмисник заважає комунікаціям із шкідливим програмним забезпеченням, коли хробак, вірус або ботнет «телефонує додому», щоб відправити вкрадені дані до головного комп'ютера або завантажити інструкції або більше шкідливих кодів.	66%	26%
5. За допомогою міжсайтового скриптингу зловмисники викрадають файли cookie, які можуть використовуватися для захоплення облікового запису або сеансу, зміни налаштувань користувача, отруєння cookie і/або неправдивої реклами. Все це можна виконати, ховаючись в SSL/TLS трафіку.	62%	19%

Нижче наведено опис реалізації запропонованого методу розшифровки TLS-трафіку. В реалізації використовувався аналізатор трафіку Wireshark, який допомагає провести аналіз роботи мережі, діагностувати проблеми, а також має багато інших корисних можливостей.

1. Робимо закладку на комп’ютер жертви (вірус, e-mail, та ін.). Використовуємо лог-файли сесійних ключів для отримання ключів, які використовуються для шифрування та дешифрування трафіку. Отримання таких лог-файлів за допомогою закладок не є трудомістким (браузери, бібліотеки NSS, java-додатки, відладні записи Java Virtual Machines).
2. Аналізуючи отримані варіанти ключ записів ключей, складаємо NSS-файл з відповідним форматом. Цей формат використовується Wireshark'ом, щоб розшифрувати TLS-записи, зашифровані відповідними ключами. Для цього потрібно мати лог-файл із записами сесійних ключів в NSS-форматі і аналізатором трафіку Wireshark. Wireshark дуже чутливий до формату NSS-файлу, тому краще ретельно перевірити, чи збігається кількість байт у кожному елементі рядка, відсутність зайвих пропусків та інше.
3. Захоплюємо трафік аналізатором трафіку після того, як буде розпочато запис ключів до лог-файлу, так як в іншому випадку нам не вдасться мати сесійні ключі, які відповідають захопленим TLS-записам. Треба пам’ятати, що ключі є дійсними тільки для однієї TLS-сесії і не підходять для дешифрування трафіку іншого сеансу.
4. Відкидаємо непотрібні пакети, що проходять через інтерфейс, що прослуховується, для чого використовуємо відстеження обміну трафіком з визначеним хостом і фільтрації за потрібним протоколом.
5. Після того, як вдалося сформувати файл із сесійними ключами, прив'язуємо файл до Wireshark'у.
6. Тепер у вмісті пакету з'явилася вкладка «Розшифровані дані SSL/TLS» і можна побачити текст запиту. Також можна обрати будь-який пакет протоколу TLS і в його контекстному меню обрати функцію «Follow SSL/TLS Stream» і, незважаючи на зашифровану передачу HTTPS, ми бачимо трафік, що передається, і можемо його експортувати для подальшого аналізу.

Особливістю описаного методу є те, що не обов'язково захоплювати трафік на комп'ютер, який генерує TLS-трафік, його можна перехватити просто будучи в мережі і прослухавши її. А добити файл із сесійними ключами можна, встановивши на комп'ютер жертви закладку або просто скопіювати його, маючи доступ до комп'ютера.

ВИСНОВОК. В процесі роботи розроблено метод дешифрування трафіку TLS, який можна застосувати навіть при віддаленому прослуховуванні мережі. Даний метод автоматизовано і дозволяє розшифровувати дані практично в режимі онлайн.

Література

1. White paper. Cisco public. Encrypted Traffic Analytics. 2018 Cisco.
2. Hidden Threats in Encrypted Traffic: A Study of North America & EMEA. Independently conducted by Ponemon Institute LLC. 2016.

УДК 681.513

ТОЧНЫЕ И ГРАНИЧНЫЕ ОЦЕНКИ СТАЦИОНАРНОЙ ВЕРОЯТНОСТИ ДОСТУПНОСТИ СЕТЕВОЙ УСЛУГИ

Зайченко Ю.П., Васильев В.И., Вишталь Д.М., Любашенко Н.Д.
КПИ им. Игоря Сикорского, Украина
E-mail: d.vishtal@kpi.ua

Accurate and interval estimates of the stationary probability of network service availability

The problems of obtaining accurate estimates of the probability of network service availability for arbitrary pairs of nodes are considered. Estimations of minimax borders of probability of the node pair availability for networks of large dimension with a complex structural organization are constructed.

В последние десятилетия проблемы надежности сетевых структур принадлежат к приоритетным направлениям исследований в теории надежности. Формально сеть связи интерпретируется как связный граф без петель. Граф может быть как неориентированным, частично ориентированным, так и полностью ориентированным. Динамическая модель сети представлена стохастическим графом, элементы которого взвешены весовыми параметрами. Обычно весовые значения присваиваются ребрам, считая при этом узлы абсолютно надежными. При необходимости можно присвоить веса и узлам. Для сетей с восстановлением роль весовых параметров играют коэффициенты готовности элементов сети. Отказы элементов обусловлены техническими неполадками и внешними воздействиями. Для практики важно знать, что, несмотря на отказы элементов, любая пара абонентов сети может получить соединение (доступность сетевой услуги).

Под доступностью сетевой услуги понимается возможность предоставления связи для любого пользователя в любой момент времени. Можно дать несколько формальных определений свойства доступности сетевой услуги:

1. Сеть обладает свойством (s-t) доступности в момент времени *t*, если из узла s в узел t существует, по крайней мере, один простой путь;
2. Сеть обладает свойством полнодоступности в момент времени *t*, если для любой пары узлов сети существует, по крайней мере, один простой путь;
3. Сеть обладает свойством полнодоступности в момент времени *t*, если существует, по крайней мере, одно основное дерево сети;
4. Сеть обладает свойством полнодоступности в момент времени *t*, если в каждом из разрезающих множеств сети существует, по крайней мере, один доступный элемент.

Разумеется, определения [2-4] эквивалентны, но по-разному представляют структуру свойства связности сети. Вероятность доступности сетевой услуги позволяет объективно ответить на вопрос, какая из сравниваемых сетей лучше соответствует своему назначению. Мониторинг этой характеристики дает возможность своевременно вносить необходимые коррективы в эксплуатацию и развитие сети. Задача оценки доступности сетевой услуги относится к классу так называемых “трудновычислимых” задач комбинаторной логики свойств и классов. По этой причине получение точной оценки доступности сетевой услуги для очень больших сетей не всегда возможно и приходится ограничиваться оценками “снизу” и “сверху”. Для решения рассматриваемой задачи осуществляется перевод понятий доступности сетевой услуги на язык булевых алгебр [1]. Этой цели служат алгоритмы поиска путей, разрезающих множеств сети, алгоритмы декомпозиции структурной функции.

В работе рассмотрена задача оценки стационарной вероятности парной связности сети.

Бинарная стохастическая модель системы

1. Пусть C={1,2,…,*n*} - проиндексированное конечное множество элементов системы. Число $|C|$ называют порядком системы. Бинарность означает, что элементы и система в целом принимают значения в множестве B_2={0,1}.

Эволюция *i*-го элемента во времени моделируется соответствующим альтернирующим процессом восстановления $x_i(t)$, *i*=1,2,…,*n*.

$$x_i(t) = \begin{cases} 1, \text{ если в момент времени } t \ i-\text{й элемент работоспособен;} \\ 0, \text{ в противном случае.} \end{cases}$$

Нам потребуются некоторые результаты теории восстановления в удобной для нас интерпретации.

Вероятность застать *i*-й элемент в момент времени *t* в доступном состоянии называется нестационарным коэффициентом готовности и обозначается

$$P\{x_i(t)=1\} = P_i(t), i = 1,2.\text{K}, n.$$

С ростом *t* нестационарный коэффициент готовности стремится к постоянному значению – стационарному коэффициенту готовности *i*-го элемента. Его значение определяется как отношение средней длины интервала доступности *i*-го элемента к средней длине цикла *i*-го альтернирующего процесса:

$$\lim_{t\to\infty} P\{x_i(t)=1\} = \frac{M[\theta_{x_i}]}{M[\theta_{x_i}]+M[\xi_{x_i}]} = P_i, i = 1,2.\text{K}, n.$$

2. Пусть вектор состояния элементов $X(t) = (x_1(t),\text{K}, x_n(t))$ однозначно определяет состояние системы. Соответствующую функцию (двузначный предикат) называют структурной функцией системы:

$$\varphi(x_1(t),\text{K } x_n(t)) = \begin{cases} 1, \text{ если в момент времени } t \text{ система работоспособна;} \\ 0, \text{ в противном случае.} \end{cases}$$

Формально, роль множества истинности (ложности) может выполнять любая функция алгебры логики, за исключением функций-констант.

Большинство систем обладают свойством монотонности, поэтому ограничимся случаем, когда структурная функция $\varphi(x_1(t),\text{K } x_n(t))$ монотонна.

Постановка задачи

Задано:

- $G(Y, X)$ - структура сети;
- $Y = \{y_1,\text{K}, y_l\}$ – множество узлов сети;
- $X = \{x_1,\text{K}, x_n\}$ – множество каналов сети;
- $s, t \in Y$ - две произвольные вершины сети;
- θ_{x_i} - случайные интервалы времени доступности *i*-го канала сети,
- ξ_{x_i} - случайные интервалы времени недоступности *i*-го канала сети.
- $p_i = \dfrac{M[\theta_{x_i}]}{M[\theta_{x_i}]+M[\xi_{x_i}]}$ - коэффициент стационарной готовности *i*-го канала сети.

$$\overline{p}_i = 1 - p_i = q_i$$

- С целью упрощения будем считать все узлы абсолютно надежными.

Принятые предположения:

1. Зависимостью случайных величин $\left\{\theta_{x_i}\right\}$ и $\left\{\xi_{x_i}\right\}$, $i=\overline{1...n}$ можно пренебречь. $\exists M\left[\theta_{x_i}\right]<\infty,\ \exists M\left[\xi_{x_i}\right]<\infty.$

2. Вектор состояния элементов сети однозначно определяет (s-t) связность ((s-t) доступность) сети.

3. Сеть рассматривается как восстанавливаемая система с полнодоступным восстановлением.

4. При заданном режиме информационной нагрузки на сеть (малая, средняя, большая) устанавливается стационарный режим.

5. Состояние сети относительно $\varphi_{s,t}$-доступности (недоступности) определяется ресурсным состоянием ее элементов при заданной нагрузке на сеть.

Требуется найти:

$P\left\{\varphi_{s,t}\left(x_1,\text{К},x_n\right)=1\right\}$ - стационарную вероятность (s-t) связности сети.

Для решения поставленной задачи были использованы следующие алгоритмы:

- алгоритм поиска всех кратчайших (s-t) путей сети;
- алгоритм поиска всех минимальных (s-t) сечений (разрезов) сети;
- алгоритм ортогонализации функции связности в ее наиболее компактном представлении (декомпозиция Шеннона).

В результате ортогонализации получаем вычислительную схему для оценки вероятности (s-t) связности, минимальную с точки зрения вычислительной трудоемкости. Присвоив в ортогонализованной МДНФ $\varphi_{s,t}\left(x_1,\text{К},x_n\right)$ переменным x_i значения p_i, а переменным с отрицаниями $\overline{x}_i$ значения q_i, получим представление вероятности (s-t) связности как функцию готовности элементов сети.

Выводы. Использованный подход, основанный на изоморфизме булевой алгебры свойств и булевой алгебры классов и порядковых соображений, может быть применен не только для оценки вероятности (s-t) доступности, но и для оценки вероятности полносвязности сетей связи большой размерности. Найденная вероятность парной и полной связности позволяют анализировать свойства доступности с изменением сетевой нагрузки.

Для сравнительного анализа надежности сетевых структур необходимо уметь вычислять вероятности их полносвязности. Та из структур, которая обладает большей вероятностью полносвязности, является более предпочтительной.

В случае сетей чрезмерно большой размерности, когда точная оценка невозможна, конструируются оценки «снизу» и «сверху [2].

В дальнейшем этот подход может использоваться:

- для решения задач синтеза сетей с заданными свойствами;
- для оценки точного или приближенного среднего стационарного времени пребывания сети в состоянии доступности сетевой услуги;
- для оценки важности элементов [3].

Литература

1. Р. Сикорский. Булевы алгебры. - М.: Мир - 1969.- 375 с.
2. К. Райншке, И. Ушаков “Оценка надежности систем с использованием графов”, М., “Радио и связь”, 1988г. – 208 стр.
3. Р. Барлоу, Ф. Прошан “Статистическая теория надежности и испытания на безотказность” М., “Наука”, 1984 г. – 327 стр.

УДК 004.72:621.39

АНАЛІЗ МЕТОДІВ ПАРАЛЕЛЬНОЇ ОБРОБКИ ДАНИХ

Могильний С.Б., Котик І.В.
Інститут телекомунікаційних систем КПІ імені Ігоря Сікорського
E-mail: kotik.iv@gmail.com

ANALYSIS OF PARALLEL DATA PROCESSING METHODS

The current task is to increase the bandwidth of communication channels, including through the parallel processing of data when compressed, encrypted, etc. In this work we explore the possibilities of multi-core data processing by combining, in our case, several microcomputers into a cluster.

Актуальною є задача збільшення пропускної здатності каналів зв’язку в тому числі за рахунок паралельного оброблення даних при їх стисненні, шифруванні тощо. В даній роботі досліджується можливості багатоядерної обробки даних за допомогою об’єднання, в нашому випадку, кількох мікрокомп’ютерів в кластер.

Паралельні обчислення — спосіб організації комп'ютерних обчислень, при якому програми розробляються як набір взаємодіючих обчислювальних процесів, які працюють паралельно і в архітектурі комп'ютерів реалізуються в основному у формі багатоядерних процесорів.

Ідея розпаралелювання обчислень ґрунтується на тому, що громісткі завдання можуть бути розділені на набір менших завдань, які можуть бути вирішені одночасно.

- Задача розбивається на підзадачі, які можуть виконуватися у один і той самий момент часу.
- Кожна підзадача в свою чергу розбивається на послідовність інструкцій.
- Інструкції кожної підзадачі виконуються одночасно на різних процесорах.
- У процесі обчислень використовується загальний механізм контролю-координації.

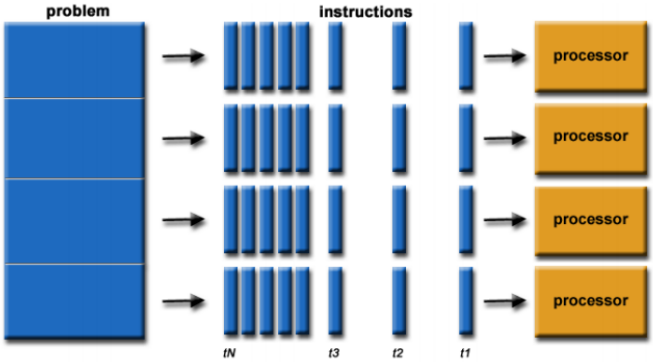


Рис. 1. Схема паралельних обчислень

Обчислювальна задача має:

- Допускати розбиття на незалежні підзадачі, які можна виконувати

одночасно.

- З використанням численних обчислювальних ресурсів розв’язуватися за коротший проміжок часу, ніж з використанням одного процесора.

Паралельні обчислення існують таких форм:

- паралельність на рівні інструкцій,
- паралельність даних,
- паралельність завдань.

Паралельність на рівні інструкцій.

Комп'ютерна програма — це потік інструкцій, що виконуються процесором. Даний потік інструкцій можна розділити на групи, які виконуватимуться паралельно, можна змінювати порядок даних інструкцій і це не вплине на результат роботи всієї програми. Такий прийом відомий як паралельність на рівні інструкцій. Просування в розвитку паралельності на рівні інструкцій в архітектурі комп'ютерів відбувалося з середини 1980-х до середини 1990-х.

Паралельність даних.

Основна ідея підходу, заснованого на паралельності даних, полягає в тому, що одна операція виконується відразу над всіма елементами масиву даних. Різні фрагменти такого масиву обробляються на векторному процесорі або на різних процесорах паралельної машини. Розподілом даних між процесорами займається програма. Векторизація або розпаралелювання в цьому випадку найчастіше виконується вже на етапі компіляції – перевід вихідного тексту програми в машинні команди. Роль програміста в цьому випадку зазвичай зводиться до задання налаштувань векторної або паралельної оптимізації компілятору, директив паралельної компіляції, використання спеціалізованих мов для паралельних обчислень.

Паралельність завдань (багатопоточність).

Стиль програмування, заснований на паралельності завдань, має на увазі, що обчислювальне завдання розбивається на декілька відносно самостійних підзадач і кожен процесор завантажується своєю власною підзадачею.

Засоби для здійснення паралельних обчислень.

Засоби, які дають змогу втілити парадигму паралелізму, можна класифікувати наступним чином:

* апаратні
  + засоби для проведення обчислень (обчислювальна техніка)
    - обчислювальна техніка, зібрана з стандартних комплектуючих;
    - обчислювальна техніка, зібрана з спеціальних комплектуючих;
  + засоби візуалізації;
  + засоби для зберігання і обробки даних;

* програмні

+ програмні засоби загального призначення (операційні системи, стандартні бібліотеки, мови програмування, компілятори, профайлери, дебагери і т.п.);

+ спеціальні програмні засоби: бібліотеки (PVM, MPI); засоби

об’єднання ресурсів (Dynamite, Globus та інші).

Паралельні комп’ютери поділяються на:

* Сучасні автономні комп’ютери. Вони є паралельними з точки зору їх внутрішньої будови:

+ Наявність численних функціональних модулів (L1-кеш, L2-кеш, пристрої попереджувального вибору команд (prefetch), decode, floating-point, графічні процесори (GPU), модулі для цілої та дійсної арифметики і т.д.);

+ Багатоядерність чи багатопроцесорність (Multiple execution units/cores);

+ Підтримка використання потоків (Multiple hardware threads) Будова обчислювального чіпу IBM BG/Q з 18 ядрами (PU) та 16 кеш-модулями 2-го рівня (L2).

* Кластери, які складаються із кількох робочих станцій, з’єднаних мережею (див рис. 2).

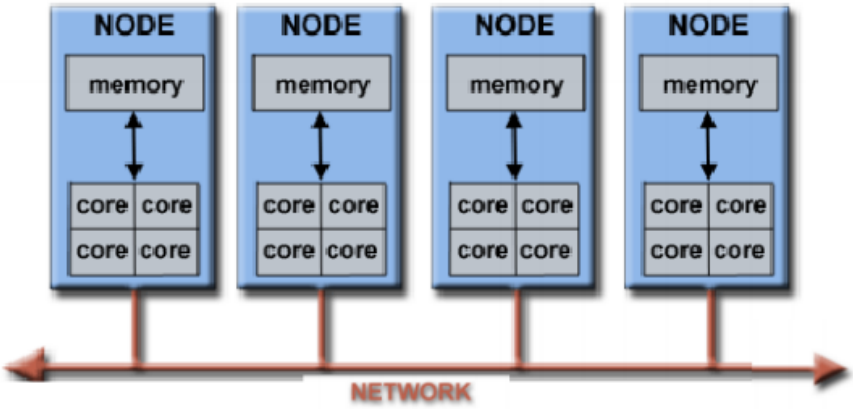


Рис. 2. Схема кластера

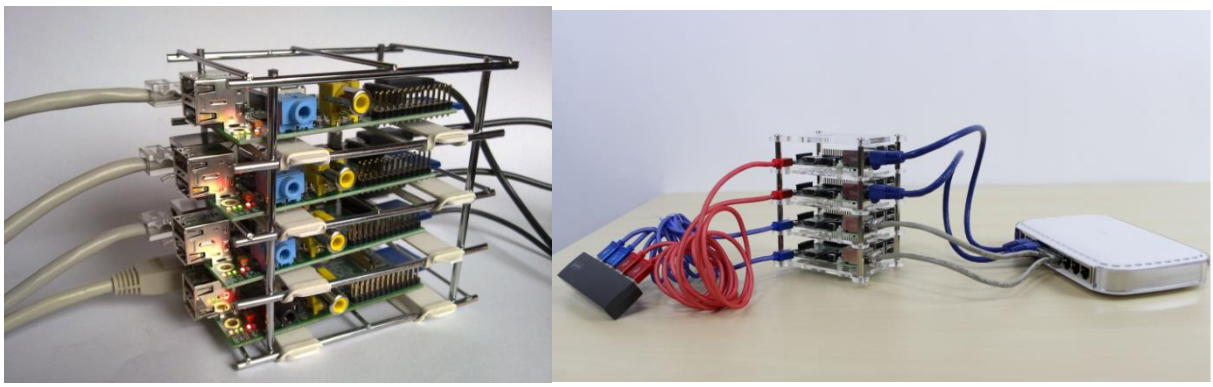


Рис. 3. Кластери з 4-х Raspberry Pi

Висновки. Виконано дослідження дозволяє збільшити ефективність стиснення та шифрування даних при підготовці їх для передачі в каналах зв’язку.

Література

1. Хокні Р., Джессхоуп К. Паралельні ЕОМ. Архітектура, програмування та алгоритми. М.: Радіо і зв'язок. 1986. 392 с.
2. Головкін Б.А. Паралельні обчислювальні системи. М.: Наука. 1980. 520 с.

УДК 621.396

ВОССТАНОВЛЕНИЕ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Правило В.В., Белоха Д.К.
Институт телекоммуникационных систем КПИ им. Игоря Сикорского, Украина
E-mail: valeriy_pravilo@ukr.net, belohadk97@gmail.com

Restoring transfer messages based on network traffic analysis

In this paper, have been described the possibilities of restoring transfer messages based on network traffic analysis. Also, have researched the problems of the transmission protocols, the variety of possibilities saving them and creation of the automation system of providing information of the data.

На сегодняшний день существует задача восстановления и анализа информации, передаваемой в сети. Восстановление и обработку инорфмации можно проводить на разных уровнях. Чтобы собрать данные, нужно понимать протоколы передачи этих данных, как они работают и как с ними работать.

Протокол передачи данных − набор соглашений интерфейса логического уровня, которые определяют обмен данными между различными программами. Эти соглашения задают единообразный способ передачи сообщений и обработки ошибок при взаимодействии программного обеспечения разнесённой в пространстве аппаратуры, соединённой тем или иным интерфейсом.

Стек протоколов TCP/IP содержит 4 уровня:

- канальный уровень,
- сетевой уровень,
- транспортный уровень,
- прикладной уровень.

Наиболее известные протоколы, используемые в сети Интернет:

- HTTP (Hyper Text Transfer Protocol) − это протокол передачи гипертекста;
- FTP (File Transfer Protocol) − это протокол передачи файлов со специального файлового сервера на компьютер пользовател;
- POP3 (Post Office Protocol) − это стандартный протокол почтового соединени;
- SMTP (Simple Mail Transfer Protocol) − протокол, который задает набор правил для передачи почт;
- TELNET − это протокол удаленного доступа. TELNET дает возможность абоненту работать на любой ЭВМ находящейся с ним в одной

сети, как на своей собственной, то есть запускать программы, менять режим работы.

При передаче данных от прикладного уровня к транспортному, затем через уровень сетевой взаимосвязи, каждый из протоколов, по которым проходят данные, выполняет свою личную логику для этих данных и конечный результат этой логики прикрепляет к началу заголовка.

На рис.1 представлены результаты обработки данных и формирования таких заголовков пакета в сети TCP\IP.

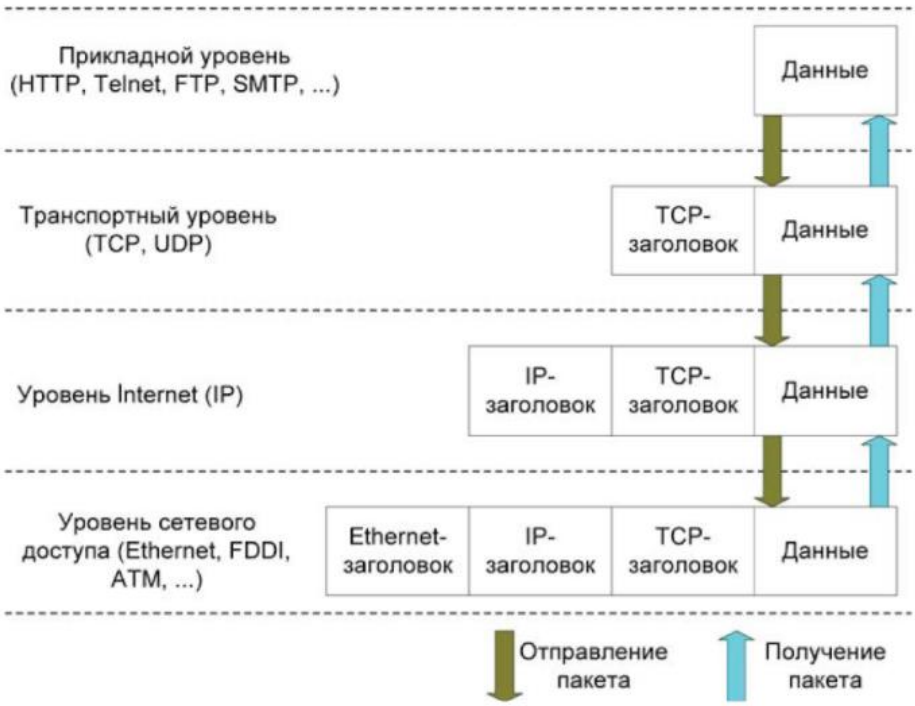


Рис. 1. Процесс обработки данных и формирования заголовков пакета в сети TCP\IP

На приемной стороне эти заголовки удаляются в ходе того, как выполняются и проходят некоторые из этих протоколов.

Таким образом, получаем легкость и гибкость в настройке протоколов, ведь ни один из них не должен знать и не знает о существовании другого.

Рассмотрим методы перехвата данных сети:

1. Програмное обеспечение Wireshark,
2. Командная строка dumpcap,
3. TShark,
4. Использование устаревшего центра передачи,
5. Настройка порта на передатчик,
6. Использование сетевого контакта,
7. «Хакинг» ARP протокола.

Кроме того, необходимо сохранять принятые данные на диск. В этом случае наиболее целесообразно воспользоваться командной утилитой dumcap. Это решение, которое не имеет пользовательского интерфейса, что является несомненым плюсом, в условиях того, что обрабатывается трафик

сети, иначе обрабатывающие устройство могло бы не выдерживать то количество трафика, которое проходит через сеть. Решение поддерживает сбор всех типов данных. Фильтрование данных предлагается проводить на следующих этапах.

После сбора данных понадобиться их анализ и обработка. Есть несколько различных способов этой прорцедуры. Но на данный момент рассмотривается способ обработки данных с помощью NetworkMiner.

NetworkMiner – програмное обеспечение, с помощью которого возможно получить доступ к файлам данных, которые были приняты ранее. При чем не важно – были эти данные в открытом или закрытом доступе. С помощью этой программы возможно извлечь ифнормацию из принятых данных, как показано на рис.2.

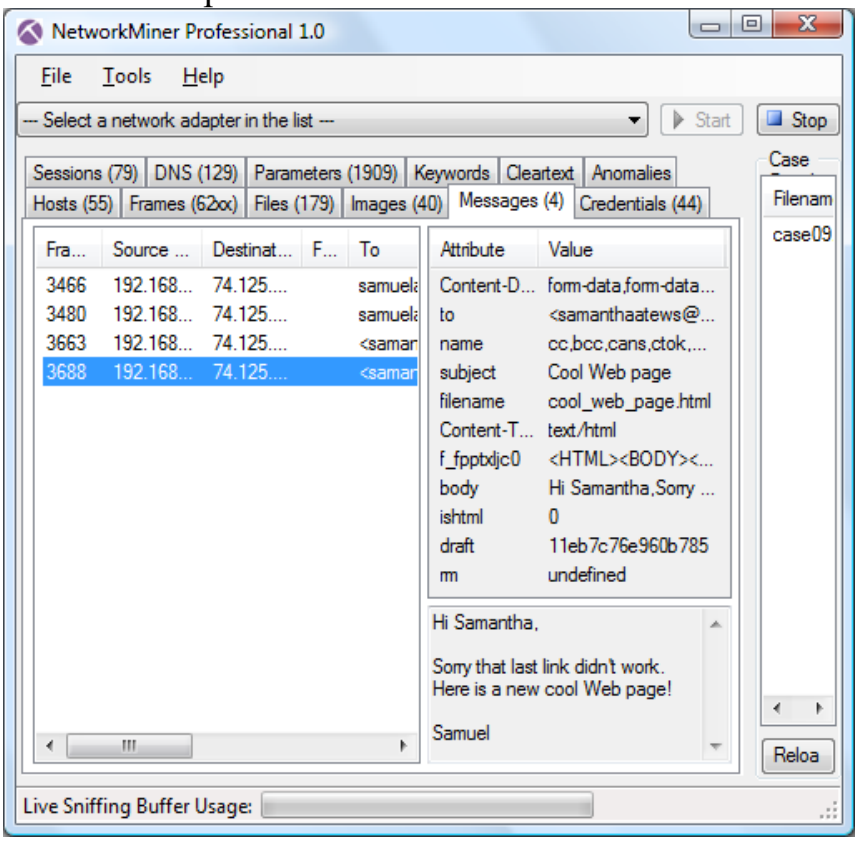


Рис. 2. Пример работы программы NetworkMiner по извлечению информации

Как результат, при желании, найдя нужный кусок информации, можно с ним работать: удалять, изменять и т.д.

Литература

1. Erik Hjelmvik, http://netres.ec/?b=113EA66, 11 March 2011.
2. V. Shaniagin, Information Security, pp 362 – 365, Litres, 2017.
3. Erik Hjelmvik., http://netres.ec/?b=11100F0, 15 January 2011.

УДК 621.391+004.7

МЕТОД КОМПОЗИЦІЇ ВЕБ-СЕРВІСІВ

Колюкаєва В.О., Новогрудська Р.Л.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
E-mail: vkolyukaeva@gmail.com, rinan@ukr.net

THE METHOD OF WEB SERVICES COMPOSITION

In this paper we consider the method of composition of web services, which allows to increase the efficiency and transparency of the composition of web services. The method takes into account the requirements for criteria based on the division of web services into classes of sensitivity. The following describes the steps of the method.

В даній роботі розглядається метод композиції веб-сервісів, який дозволяє підвищити ефективність та прозорість композиції веб-сервісів. Метод враховує вимоги до критеріїв на основі поділу веб-сервісів на класи чутливості. Наведено опис етапів методу.

На сьогоднішній день існує велика кількість різнотипних веб-сервісів, які пропонують користувачам однакові функції. З точки зору користувача не є важливим яку саме службу (веб-сервіс) буде використано. Також, користувач може висувати певні вимоги до веб-сервісів (системна швидкість, надійність тощо). Такі вимоги можуть виступати в якості критеріїв для вибору необхідного веб-сервісу. Таким чином, існує проблема раціонального вибору веб-сервісів для їх композиції у складну веб-службу яка виконує конкретне завдання кінцевого користувача.

Для вирішення описаної проблеми пропонується метод композиції веб-сервісів на основі класів чутливості.

Розглянемо етапи методу вибору веб-сервісів, які дозволяють реалізувати раціональний вибір веб-сервісів з метою їх подальшої композиції:

1. Формування вибірки веб-сервісів;
2. Введення опису ряду ознак, що характеризують чутливість веб-сервісів;
3. Обчислення значень характеристик веб-сервісів в залежності від навантаження;
4. Побудова матриці «об'єкт-ознака»;
5. Пошук відповідності у значеннях характеристик веб-сервісів на основі матриці;
6. Формування класів чутливості;
7. Формування множини міток приналежності веб-сервісів до певних класів чутливості;
8. Вибір найкращого веб-сервісу за показниками (для виконання поставленої задачі).

Пункт 7 при досить великому обсязі вибірки є вкрай трудомістким, тому доцільно автоматизувати цей процес, провівши кластеризацію даних з

числом кластерів, що дорівнює кількості класів чутливості. Також результати кластеризації можуть слугувати індикатором правильності евристичного поділу на класи: якщо отримані кластери досить відокремлені один від одного, то класи обрані вірно.

Отримавши матрицю «об'єкт-ознака» і множину відповідних класів, можливо навчити і оцінити алгоритм класифікації «з учителем». В якості такого алгоритму в запропонованому методі використовується метод опорних векторів.

Для обчислення ознак необхідно провести збір необхідних даних за допомогою тестування вибірки веб-сервісів. В процесі тестування здійснюється послідовне виконання ітерацій. Одна ітерація триває 1 секунду. Кількість запитів, що відправляються протягом однієї ітерації, залежить від її номеру. Запити рівномірно розподілені в рамках секунди. В середньому один тест триває 15-25 хвилин в залежності від швидкості відповіді на запити веб-сервісом. Кожен веб-сервіс тестується 3 рази з різницею між тестами в 9 годин, результати проведених тестів усереднюються. Такий підхід до тестування дозволяє знизити розкид значень, що виникає через різну завантаженості веб-сервісів протягом дня.

Матриця «об'єкт-ознака» формується на основі результатів тестів веб-сервісів.

По кожному веб-сервісу спочатку обчислюється середній час обробки запитів, стандартне відхилення і число необроблених запитів по ітераціям. Далі з метою усунення обмеження на однозначний план тесту (крок тесту і максимальне число запитів в секунду) і мінімізації опису характеристики чутливості веб-сервісу виконується апроксимація значень ознак по ітераціям поліномом першого ступеня за допомогою алгоритму лінійної регресії. Значення коефіцієнтів отриманої регресійної моделі, а також сумарна квадратична помилка використовується в якості ознак, що характеризують чутливість веб-сервісу.

У подальших обчисленнях середнього часу обробки і стандартного відхилення виключаються помилкові запити, тобто такі запити, що не були оброблені протягом 30 секунд або веб-сервіс повернув у відповіді на запит HTTP-код, відмінний від «200 - OK».

Експертом проводиться аналіз отриманих даних та виноситься рішення, який веб-сервіс буде використовуватися. Існує кілька методів, які можуть бути використані на цьому етапі. Турнірні методи і метод малих сум можуть застосовуватися, у тому випадку, коли особа, що приймає рішення (ОПР) може задати пріоритети критеріїв по важливості. Метод трьох-градаційних ранжировок використовується для ситуацій, в яких пріоритетною є вимога відсутності низьких оцінок за критеріями.

Для задачі вибору веб-сервісу в більшості випадків всі критерії є неоднорідними, тобто мають різні шкали вимірювання. Пропонується використовувати підхід, який дозволяє вирішити проблему вибору при наявності кількісної інформації про важливість критеріїв, не нормалізуючи і не приводячи неоднорідні критерії до єдиної порядкової шкали (ЄПШ).

Використання такого підходу є аргументованим, оскільки при переводі до ЄПШ може бути втрачена частина інформації. При виборі веб-сервісу вводиться єдина функція, яка є сумою критеріїв, помножених на відповідні коефіцієнти важливості. При цьому важливість кожного критерію описується різними значеннями коефіцієнтів. Чим важливіший критерій, тим більше значення приймає відповідний коефіцієнт. Така функція буде мати вигляд:

$$\Phi = \alpha_1 K_1 + \alpha_2 K_2 + \ldots + \alpha_n K_n .$$

При використанні даного підходу, результат вибору є досить прозорим та зрозумілим. Обмеженням для використання підходу є необхідність наявності кількісних шкал для всіх критеріїв.

Варто зазначити, що існує два основних підходи до постановки задачі вибору:

1. Пошук кращої композиції веб-сервісів з урахуванням структури завдання. При цьому вводяться 4 базові структури об'єднання веб-сервісів (послідовна, циклічна, умовна і паралельна), для кожного можливого поєднання реалізацій підзадач веб-сервісами розраховується інтегральне значення критеріїв порівняння (цей процес, як правило, оптимізується) і вибирається варіант композиції з найкращими інтегральними оцінками значень критеріїв;

2. Пошук кращої композиції без урахування структури завдання. При цьому загальна задача пошуку кращої композиції веб-сервісів в рамках окремого завдання розглядається як пошук кращих рішень для окремих підзадач.

Запропонований метод використовує другий підхід, оскільки, по-перше, в більшості випадків виконується умова незалежності веб-сервісів і, по-друге, цей підхід дозволяє наочно представляти результати вибору з урахуванням відносної важливості критеріїв.

Таким чином, за рахунок введення нового критерію для оцінки веб-сервісів, було досягнене підвищення ефективності при збереженні прозорості дій, що дозволить при розробці програм зекономити на кваліфікованих кадрах.

Література

1. Климов В.В. Модели, алгоритмы и программные средства поиска и композиции веб-сервисов с использованием семантических описаний: Дисс. кандидата наук / В.В. Климов ; МИФИ.— 2012.— С. 22.
2. Воронцов К.В. Комбинаторный подход к оценке качества обучаемых алгоритмов // Математические вопросы кибернетики / Под ред. О.Б. Лупанов.— Москва : Физматлит, 2014.— Т. 13.— С. 5–36.
3. Bergstra James, Bengio Yoshua. Random Search for Hyper-Parameter Optimization // J. Mach. Learn. Res.— 2012.— Vol. 13.— P. 281–305.
4. Душкин Д.Н., Душкин Н.Д. О проблеме выбора оптимальной по предпочтениям композиции сервисов // Сборник научных трудов Первой Международной научно-практической конференции «Радиоинфоком – 2013».— Т. 2.— Москва: МГТУ МИРЭА, 2013.— С. 62–66.
5. Бабошин А.А. Подход к организации взаимодействия веб-сервисов на основе модели потока работ / А.А. Бабошин, А.М. Кашевник // Труды СПИИРАН.- 2013.- С. 247-254.

УДК 004.89

ПІДХІД ДО ОБРОБКИ ТА ЗБЕРІГАННЯ РЕЗУЛЬТАТІВ ОЦІНКИ ПСИХОФІЗІОЛОГІЧНОГО СТАНУ ЛЮДИНИ

Кущ В.С., Штогріна О.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vetalkushch13@gmail.com

Approach to the processing and storage the results of assessment the psychophysiological state of human

This article describes loading of colors of the environment on the psychophysiological state of human. Consequently, a new software program is offered, which allows you to store and process data, as well as count pictures for adjusting the person's psychophysical state.

Зараз вчені вважають, що люди переживають інформаційну епоху, ознакою якої є перенасичення людини інформацією, як корисною, так і шкідливою, небажаною [1]. З кожним роком швидкими темпами розвивається поліграфічна галузь, вдосконалюються мультимедійні пристрої, збільшується кількість відео та зображень і спрощується доступ до них. В результаті щоденно використовуються технології, які здатні передавати, штучно створені, різноманітні відтінки кольорів, яких в природі раніше не було. У зв’язку з цим, формується нове кольорове середовище, яке оточує людину в повсякденному житті і неможливо уникнути його впливу знаходячись у місті. В протилежній ситуації знаходяться антарктичні зимівники, які довгий час проживають в Антарктиді. На цьому материку переважають однотипні, неяскраві, кольори. Перенасичення або нестача кольорів в середовищі може мати вплив на психофізіологічний стан людини.

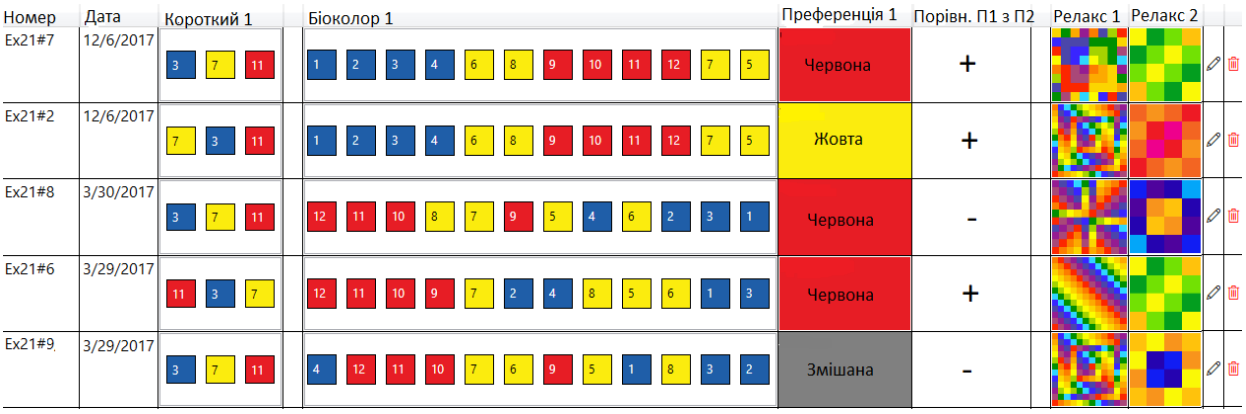
Психологи досліджують теорію впливу кольорів на людський стан, та запропонували методи коригування його за допомогою кольорових релаксуючих зображень [2]. Спочатку проводиться базовий тест, який передбачає вибір різнокольорових карток в послідовності. За результатами такого тесту обираються певні релаксуючі зображення, перегляд яких коригує стан людини. Безпосередньо процес зберігання і обробки результатів тесту, дуже громіздкий, також може супроводжуватися похибками підрахунків, які викликані людським фактором при довготривалій роботі над однотипними даними. Таким чином, актуальним є завдання розробки підходу до визначення кольорової преференції [3] людини, а в рамках нього розробки програмного забезпечення (ПЗ), яке б дозволило зберігати та обробляти дані про стан людини, виявляти критичні ситуації та підбирати релаксуючі зображення.

Вищезгадані тести проводяться в рамках дослідження стану зимівників на українській антарктичній станції «Академік Вернадський», що здійснюється Національним антарктичним науковим центром Міністерства освіти і науки України. Обстеження зимівників проводиться для всіх членів

експедиції до відправки, а також під час перебування на антарктичній станції, визначені показники фіксуються та передаються в НАНЦ України. На основі отриманих від експертів знань про методи оцінки стану людини, були розроблені відповідні алгоритми, що покладені в основу розробленого ПЗ. Дане ПЗ дає можливість наочно побачити результати проходження тесту зимівником, його результуючу преференцію та призначене йому релаксуюче зображення для коригування його стану. Надається можливість додавати нові результати тестів та редагувати вже внесені дані. Також для можливості пошуку залежностей в ручному режимі та дослідження припущень психологів розроблено можливість фільтрування даних по різним критеріям.

Всі дані подані у вигляді таблиці, що зручно для порівняння декількох результатів тестів. На рис. 1 представлена частина інтерфейсу користувача розробленого ПЗ. На ньому продемонстровані результати проходження тесту, який складається з двох частин: короткий та біоколор, у зазначену дату. Картки, які були обрані зимівником, представленні у вигляді рядка та позначені відповідним кольором та номером. В кінці рядка зазначається обчислена результуюча преференція. Також, можна побачити яке саме релаксуюче зображення для коригування стану зимівника застосовувалося в той період. В кінці кожного із рядків є кнопки, що дозволяють відредагувати данні тесту або видалити його, ця можливість доступна тільки користувачу з відповідними правами доступу.

Вручну, співставлення декількох результатів тестів та визначення по ним релаксуючих зображень дуже громіздкий та складний процес. Автоматизація порівняння результатів всіх тестів для досліджуваного в зазначений час використовуються для виявлення випадків не співпадіння, що сигналізує або про некоректне проведення тесту, або про критичний стан досліджуваного. Для більшої наочності в інтерфейс були додані стовпці, в яких відображаються зазначені порівняння.



Номер	Дата	Короткий 1	Біоколор 1	Преференція 1	Порівн. П1 з П2	Релакс 1	Релакс 2
Ex21#7	12/6/2017	3 7 11	1 2 3 4 6 8 9 10 11 12 7 5	Червона	+		
Ex21#2	12/6/2017	7 3 11	1 2 3 4 6 8 9 10 11 12 7 5	Жовта	+		
Ex21#8	3/30/2017	3 7 11	12 11 10 8 7 9 5 4 6 2 3 1	Червона	-		
Ex21#6	3/29/2017	11 3 7	12 11 10 9 7 2 4 8 5 6 1 3	Червона	+		
Ex21#9	3/29/2017	3 7 11	4 12 11 10 7 6 9 5 1 8 3 2	Змішана	-		

Рис. 1. Приклад частини інтерфейсу користувача:
результати проходження тестів та релаксуючі зображення

На рис. 2 зображено діаграму преференцій зимівників по одному із можливих критеріїв фільтрування, що дає змогу відслідковувати динаміку зміни психофізіологічного стану за досліджуваний проміжок часу. Використання діаграм та графіків для демонстрації обраних даних дає змогу

наочно представляти загальну картину психофізіологічного стану людини, робити подальші прогнози, щоб мати можливість попередити небажані наслідки.

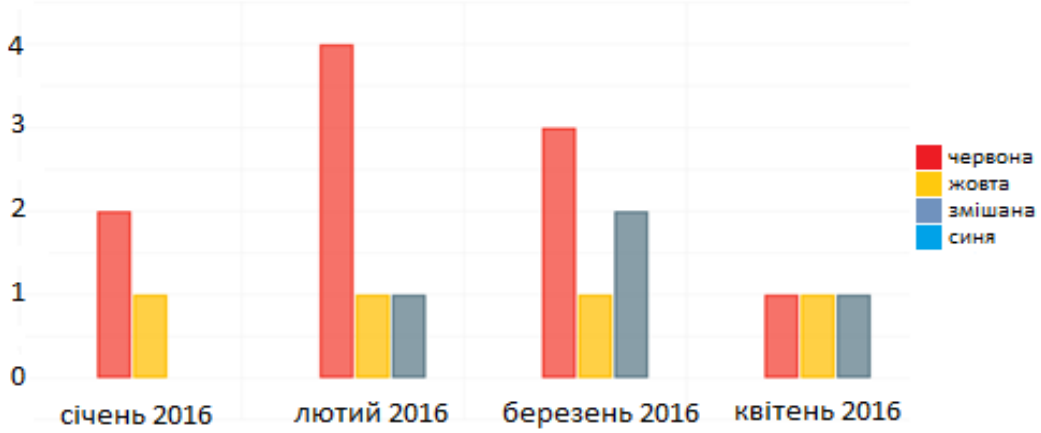


Рис. 2. Приклад частини інтерфейсу користувача:
діаграма результатів тестів одного зимівника, за обраний проміжок часу

Для розробки ПЗ, була обрана платформа .NET, використано мову програмування C#. Для зберігання результатів використовується СУБД MS SQL. Для можливості автономної роботи був розроблений програмний модуль, який є WPF додатком, таке рішення дає можливість використовувати ПЗ без підключення до інтернету. Також були реалізовані можливості для імпорту та експорту даних в різні формати, наприклад, xls. Це може знадобитися для супутніх завдань, таких як передача даних із антарктичної станції в умовах обмеженого доступу до інтернету або для збереження резервної копії зібраних даних про зимівників.

Для реалізації підходу до обробки та зберігання результатів оцінки психофізіологічного стану людини реалізоване ПЗ, яке надає можливість діагностувати та аналізувати стан людини спираючись на результати проходження тестів, застосовані релаксуючі зображення. При розробці ПЗ особливу увагу було приділено інтерфейсу користувача, за допомогою якого психологи, медики та співробітники НАНЦ мають можливість наочно відстежувати та аналізувати стан зимівників та робити відповідні висновки. Розроблене ПЗ базується на клієнт-серверній архітектурі, всі результати обстеження зимівників зберігаються в базі даних НАНЦ, тому доступ до них забезпечується з будь якого місця, при наявності мережі.

Література

1. Кастельс Мануель. Информационная епоха: экономика, общество и культура / Пер. С англ., под науч. ред. О.И. Шкаратана. - М., 2000. - С. 27.
2. Мадяр А.Й. Спосіб корекції психофізіологічного стану людини. / А.Й. Мадяр, О.Е. Ковалевська, В.В. Арбатов, В.Н. Бережанський, М.В. Луцюк, Є.В. Моісенко, С.В. Чорний // Патент на корисну модель №28058 від 26 листопада 2007 року.
3. Мадяр С. - А. И. Инновационные методы исследований в психофизиологии цветового восприятия: Методическое пособие / С. - А. И. Мадяр, Е. В. Моисеенко, Е. Э. Ковалевская // – К., 2015. – с. 1 – 30.

УДК 621.391

ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ ЗАДАНИХ ПОКАЗНИКІВ ЯКОСТІ ОБСЛУГОВУВАННЯ В МЕРЕЖАХ SDN

Ряба Н.М., Правило В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: natasha.ryaba19@gmail.com

ENFORCEMENT OF PRE-DEFINED SERVICE QUALITY INDICATORS IN SDN NETWORKS

Considering the current state of the Internet, the available approaches to providing Quality of Service (QoS) for single services or specific tenants are limited and inflexible. Providers need a better solution that is scalable and that allows fine-grained tuning of network traffic. Recently, different SDN enabled QoS frameworks have emerged, offering a lot of possibilities for network reconfiguration and high level definition of policies.

На сьогоднішній день мережа в класичному вигляді являє собою набір різноманітних протоколів, кількість яких постійно зростає. При цьому протоколи призначені для вирішення передбачених проблем, це ускладнює мережу і стає на заваді забезпеченню якості обслуговування. Через це використовуються статичні мережі, в яких всі поставлені задачі вирішуються на окремих пристроях передачі. Це шкодить якості обслуговування, тому що адміністраторам постійно доводиться налаштовувати устаткування різних постачальників окремо, змінюючи параметри (наприклад, пропускну здатність) для виконання вже визначених правил і політик. Проте вимоги користувачів постійно змінюються і для задоволення їх потреб необхідне динамічне вирішення.

Програмно-конфігуровані мережі(ПКМ) – це нова технологія, суть якої полягає в розділенні рівня управління та пристроїв передачі даних. Вона використовує стандартний протокол OpenFlow. Архітектура ПКМ передбачає централізацію рівня управління трафіком, відділивши управління від трафіку і централізацію управління пристроями. В результаті функція управління переходить до спеціального пристрою, що називається контролером SDN.

Контролер являє собою «мозок мережі», він дозволяє спростити управління мережею, при цьому збільшуючи її масштабованість та гнучкість. Він управляє спеціальними комутаторами, що виконують передачу по протоколу OpenFlow. Комутатори працюють на основі таблиць потоків, які формуються контролером. Записи в таблиці потоків складаються з полів, де вказані характеристики потоків(1). Потоки перевіряються на відповідність записів в таблиці, якщо записи збігаються, то з пакетом виконується дія, що записана в наступному стовпці таблиці. В разі не виконання умов пакет переходить до обробки контролером.

Центральний контролер знає все про структуру і топологію мережі. Він реагує на запити комутаторів, якщо виникає проблема і на основі отриманої інформації вносить потрібні зміни в таблицю комутації. Це дає змогу

покращити мережу і в подальшому не налаштовувати її вручну. Кожен контролер маю свою унікальну таблицю потоків, яка формується з зібраної інформації з центрального контролера. Отже, за допомогою протоколу OpenFlow контролер може додавати, видаляти та змінювати записи з таблиць.

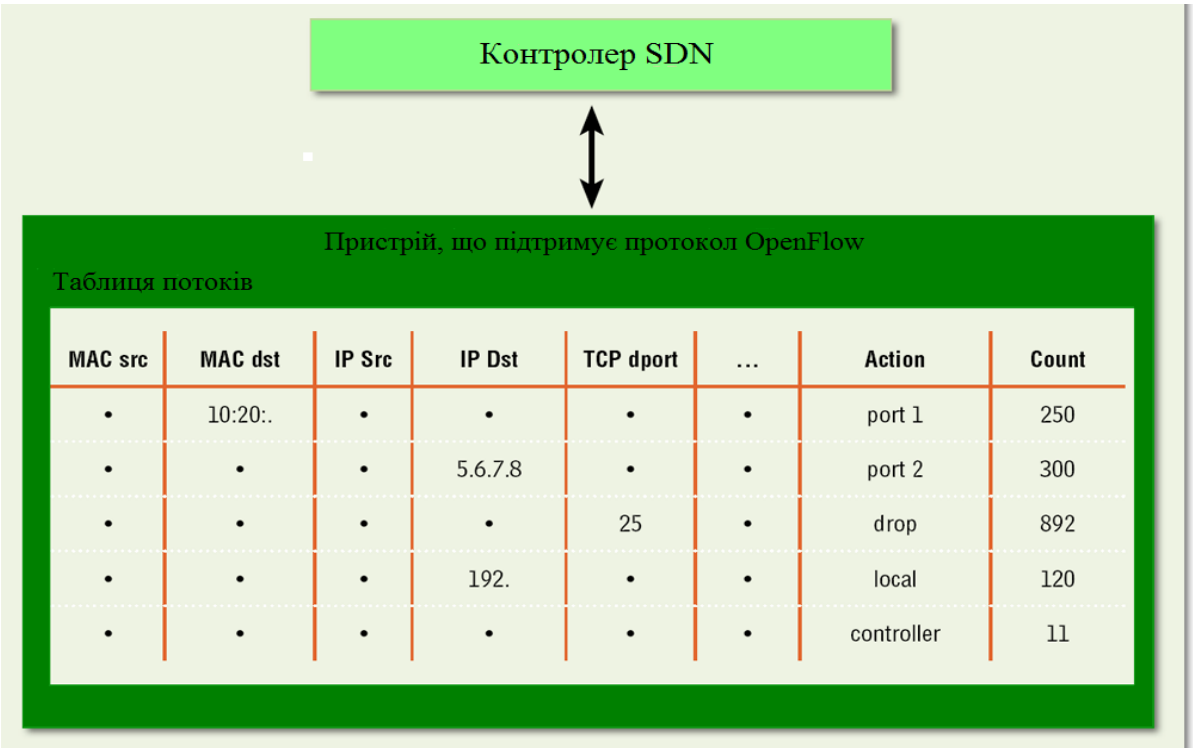


Рис1. Таблиця потоків на мережевому пристрої

Важливою частиною мереж є загальна ефективність зв'язку, яка називається якістю обслуговування(QoS). QoS містить вимоги щодо всіх основних аспектів передачі даних, таких як пропускна спроможність, час відгуку, джиттер, переривання, та ін. Для забезпечення QoS потоки додатків повинні бути розділеними, оскільки вони конкурують за пропускну здатність. Тоді мережеві ресурси повинні бути виділені так, щоб забезпечити перевагу більш пріоритетному трафіку. Це дозволяє використовувати відповідний розподіл мережевих ресурсів. Цей процес часто вимагає знання поточного стану мережі, коли можна прийняти правильні рішення щодо переадресації пакетів. Ось чому моніторинг мережі є важливим аспектом QoS. У кінцевому підсумку, метою є також забезпечення зближення мереж, що означає, що мережні ресурси повинні використовуватися як можна більш рівномірно.

Якщо не враховувати доступні методи SDN, QoS спирається на кінцеві угоди між хостами та Угодами про рівень послуг (SLA) між постачальником та користувачем. Незважаючи на те, що цей підхід є надійним, він підходить для надання найкращих послуг. З іншого боку, мультимедійні потоки та потоки VoIP потребують своєчасної доставки за надійність і повинні оброблятися окремо. Поточну архітектуру Інтернету іноді важко

контролювати, головним чином через багато різних вендор-специфічних програмних продуктів під час використання. Не існує стандартного способу встановлення політики високого рівня контролю трафіку та обмежень щодо глибини розділення трафіку.

Найпоширенішим способом забезпечення QoS являється так зване віртуальне розрізання доступної пропускної здатності. Це можна класифікувати як резервування ресурсів, де кожному потоку потрапляє певна частина загальної потужності передачі. На відміну від цього, поточна динамічна маршрутизація пропонується як альтернатива, яка безпосередньо не призначає жодного ресурсу для потоку.

Дуже багато з'являється нових варіантів оптимізації параметрів мережі з використанням концепції SDN. До них належать, наприклад, створення нового протоколу маршрутизації. Розроблений протокол працює на основі алгоритму Дейкстри, проте використовує комплексну метрику на основі функцій корисності. Цей підхід дозволяє враховувати тип трафіку (VoIP, Video, Internet) і, в залежності від нього, розраховувати власне функцію корисності, знаючи показники затримки передачі, пропускної спроможності і долі втрат пакетів.

Протоколи маршрутизації з метою задоволення зростаючих вимог щодо якості обслуговування розширюють свої класичні функції в напрямку підтримки додаткових можливостей. Новим підходом являється балансування навантаження по каналах ТКС з реалізацією багатопотокової стратегії маршрутизації. Забезпечення балансування навантаження на практиці дозволяє оптимізувати рішення завдання маршрутизації і ефективно використовувати ресурси мережі, в результаті чого поліпшуються значення ключових показників QoS.

Технологія SDN може значно покращити конфігурування мережі і для цього не потрібні нові мережні протоколи і стандарти. З допомогою цієї технології оптимізується трафік, підвищиться надійність і безпека за рахунок актуальної інформації про мережу. Кількість пристроїв зменшиться, що підвищить ефективність розгортання мережевого обладнання та покращить управління мережею. За допомогою технології SDN можна керувати різними мережевими параметрами і при цьому не користуватись якимось додатковим устаткуванням. Збільшення продуктивності, зменшення затримок за рахунок централізованого управління. Всі ці механізми виявляються корисними для якості обслуговування.

Література

1. Softw are-Defined Networking: The New Norm for Networks [Electronic resource] / ONF. – 2012.
2. Орлов Є. В. Програмно-конфігуровані мережі: архітектура, міжнародна стандартизація.
3. М.Б. Лурджан, А.А. Воропаева (канд. Техн. Наук), Г.В. Ступак. Исследование возможностей внедрения алгоритмов маршрутизации в программно-конфигурируемых сетях (sdn).
4. А.В. Лемешко, Т.В. Вавенко. Разработка и исследование потоковой модели адаптивной маршрутизации в программно-конфигурируемых сетях с балансировкой нагрузки.

УДК 621.391: 004.72

ВИКЛИКИ ТА ПРОБЛЕМАТИКА В ПРОМИСЛОВОМУ «ІНТЕРНЕТІ РЕЧЕЙ»

Давидюк А.М., Курдеча В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: mr.wokawoka@gmail.com

CHALLENGES AND PROBLEMS IN THE INDUSTRIAL "INTERNET OF THINGS"

To solve the problem of the Industrial "Internet of Thing" nowadays we have two the most popular ways. Each one has their own pluses and minuses. The main are cheap energy consuming, flexible scalability, opportunity of maintain the great number of connected devices, independence from fast Internet connection. The result shows that the most effective and cheaper way of solving this problem is to use the LP-WAN technology for Industrial IoT.

Причина виникнення проблеми. З розвитком технологічного рівня суспільства та кількості сенсорних приладів, які використовуються на виробництві виникли потреби в побудові спеціальних систем, які будуть займатись контролем та збором інформації. Основні перешкоди пов'язані з: витратами на управління мережею, масштабованістю, розміром крайових вузлів та їх енергоефективністю.

Нині існують два полярних напрямки рішення цієї проблеми (рис.1). Перший, як і найдавніший - це реалізація за допомогою пристроїв з відносно коротким радіусом дії. Другий варіант - за допомогою пристроїв з великою зоною покриття.

Рис. 1. Порівняльна характеристика підходів до побудови мереж.

Підхід короткого радіусу дії. Мінусами цієї реалізації є великий рівень витрат на розгортку самої мережі та складність подальшого масштабування мережі відповідно до збільшення зони покриття чи вузлів самої мережі. Також тяжкою

задачею є забезпечення функціонування такої мережі та її адміністрування. Плюсом використання цього типу мережі є її енергоефективність при використанні правильного підходу побудови і використанні відповідних протоколів чи технології.

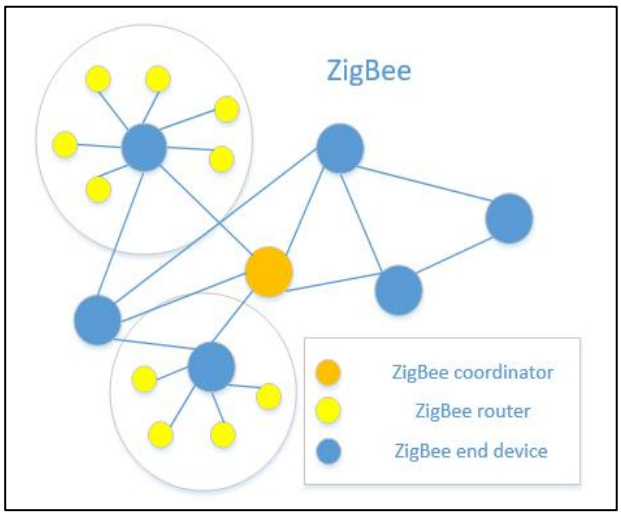


Рис. 2. Приклад побудови мережі типу ZigBee

Наприклад, для роботи з сенсорними мережами найбільш енергоефективним буде використання протоколу ZigBEE 802.15.4 на базі протоколів ZigBee та 6loWPAN (рис.2). Проте ріст даної мережі обмежений, оскільки зростає складність в управлінні та інтерференцією між самими вузлами в мережі. Однак ці мережі вимагають високошвидкісного інтернету, що часто не можливо в умовах сільської місцевості.

Підхід дальнього радіусу дії. Іншим варіантом були використані стільникові мережі

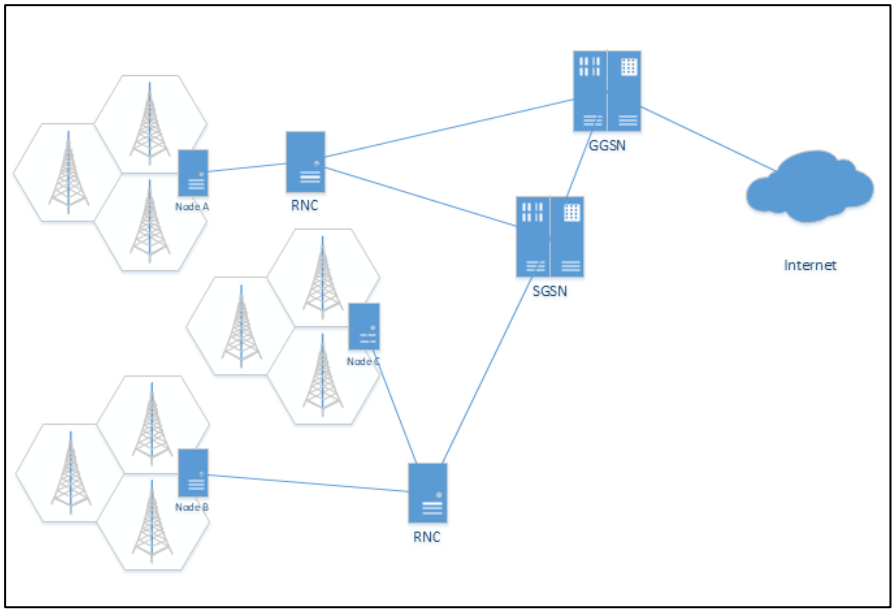


Рис. 3. Приклад побудови мережі на базі стільникових мереж

. Перевагами є широкий діапазон дії, що охоплює великі території, та використання існуючих стандартів, таких як GSM, GPRS, або 3G/4G (рис.3).

Основною проблемою цих систем є те, що вони були розроблені без урахування вимог Індустріального Інтернету речей.

В той час як в стільникових збільшується доступна смуга пропускання, в службах IIoT все навпаки. Сенсорна мережа вимагає підтримки величезної кількості пристроїв з низькою пропускною спроможністю, які надсилають короткі повідомлення лише один раз протягом певного часу. Тому використання поточних стільникових рішень явно неефективне з точки зору масштабованості та енергетичних витрат. Відповідно до масштабованості, то однією з можливих реалізацій організації та забезпечення зв'язності з незалежними системами є використання фемтосот або пікосот, що підвищує вартість мережі. Щодо енергоефективності, стільникові мережі потребують квазі-постійного зв'язку між кінцевими вузлами та базовою станцією, що має надзвичайно негативний вплив на час роботи акумулятора.

Новий підхід з використанням LP-WAN. Підхід з використанням LP-WAN забезпечує покриття значних територій та низьке енергоспоживання.

Як показано на рис.4, LP-WAN використовує топологію зірки, де всі кінцеві вузли безпосередньо підключені до базової станції. Отже, LP-WAN модем безпосередньо встановлюється на цих пристроях. У деяких випадках концентратори/шлюзи можуть бути використані для підключення кластера вузлів до базової станції (топологія зірки зірок).

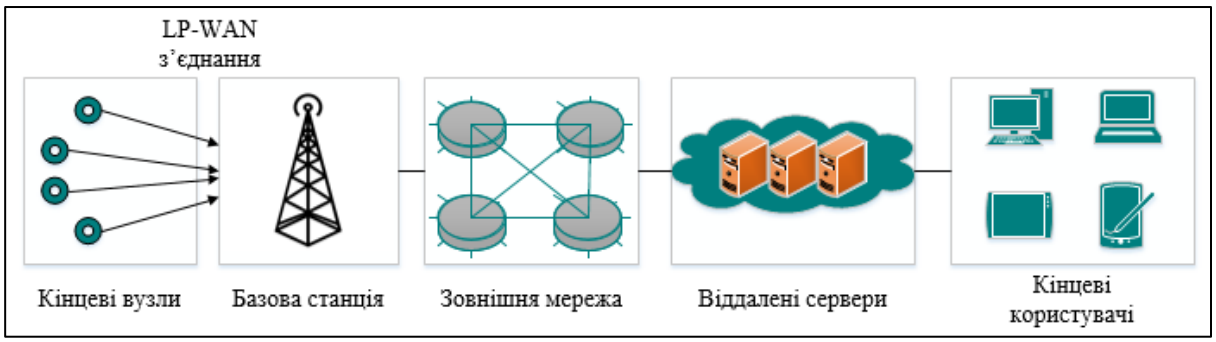


Рис. 4. Загальний підхід до побудови LP-WAN мережі

У порівнянні з діапазоном 2,4 ГГц, передача в низькочастотній смузі призводить до більш глибокого огинання перешкод на величини покриття, що є суттєво важливими характеристиками для забезпечення внутрішнього підключення.

З метою зниження енерговитрат, більшість рішень фокусуються на підключенні до висхідної лінії зв'язку; таким чином, низхідна лінія суттєво обмежується, отже час «очікування», необхідний для отримання даних - зменшується.

Таким чином, основними перевагами LP-WAN платформ, являються: високий рівень масштабованості, широкий діапазон покриття, необхідний рівень «відклику» мережі, заощадження роумінгу, знижений рівень енергоспоживання.

Висновки. Отже, виходячи з запропонованих рішень проблеми стабільного, дешевого та якісного впровадження промислового інтернету речей, найбільш вигідним являється використання LP-WAN мереж, які в свою чергу даю якісну перевагу над своїми конкурентами. Основним недоліком таких мереж є використання нових або мало поширених стандартів, що в свою чергу веде до певних труднощів в провадженні і використанні таких рішень.

Література

1. Gonzalo PajaresMartinsanz,State of the Art in LP-WAN Solutions for Industrial IoT Services; http://www.mdpi.com/1424-8220/16/5/708/htm,Departamento de Tecnologías de la Información y las Comunicaciones, Universidad Politécnica de Cartagena, Cartagena 30202, Spain, May 2016
2. Anton-Haro, C.; Dohler, M. Machine-to-Machine (M2M) Communications. Architecture, Performance and Applications; Elsevier: Waltham, MA, USA, 2015.
3. A Reconfigurable Smart Sensor Interface for Industrial WSN in IoT Environment Qingping Chi, Hairong Yan, Chuan Zhang, Zhibo Pang, and Li Da Xu, Senior Member, IEEE, vol. 10, no 1, pp. 3-6.
4. M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications", *IEEE J. Emerg. Sel. TopicsCircuitsSyst.*, IEEE, vol. 3, no. 1, pp. 45-54, Mar. 2013.

УДК 004.72

БЕЗПЕКА IOT СИСТЕМ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Вергун А.І., Курдеча В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: xhc044x@gmail.com

IOT SYSTEMS SECURITY USING BLOCKCHAIN TECHNOLOGY

Currently, the Internet of things is still a lot of problems related to safety and scalability. All these problems are solved with huge losses on the scale and the acquisition of certificates is also urgent security problem associated with centralization devices Internet of things. Solving these problems is possible through the application of technology for decentralized blokcheynu.

Інтернет речей (IoT) швидко увійшов в життя мільярдів людей по всьому світу. Однак зростання кількості підключених пристроїв веде до збільшення ризиків безпеки: від заподіяння фізичної шкоди людям до простоїв і пошкодження обладнання. Оскільки велика кількість об’єктів і систем IoT вже піддавалися нападу і було завдано значний збиток, забезпечення їх захисту виходить на перший план.

Безпека IoT систем можна розділити на чотири основні шари [1]: фізичний рівень захисту, мережевий рівень захисту, рівень захисту хмарного обчислення та программного коду IoT системи, рівень захисту додатку.

Рис. 1. Архітектура рівнів безпеки IoT системи

Основними невирішеними загрозами є:

- Атаки Сивіли (порушення конфіденційності, ненадійна передача данних);
- Аутентифікація та безпечне спілкування (Порушення конфіденційності);
- Проблеми розподілу ключів довіри та розподілення адрес для пристроїв;
- Проблема відстеження правопорушень.

Для вирішення деяких з обговорених загроз є відмінні бібліотеки з відкритим вихідним кодом, які виконують шифрування навіть в пристроях IoT з обмеженими обчислювальними ресурсами. Всі взаємодії вимагають надійної перевірки автентичності і взаємної довіри, отже економити на сертифікатах не можна. У більшості випадків сертифікатами можна легко керувати віддалено (OTA) за допомогою стандартних протоколів, таких як SCEP, EST і OCSP. Завдяки надійному центру сертифікації, який надає можливість обробляти сертифікати, ключі та облікові дані, фактичну перевірку справжності можна робити за допомогою потужних стандартів TLS і DTLS. За допомогою TLS/DTLS вирішується проблема підслуховування в мережі, дві кінцеві точки можуть обмінюватися ключами шифрування або отримувати їх для обміну даними, які

неможливо розшифрувати іншим пристроям. Однак проблему досі залишається проблема вірогідності що треті сторони та центри сертифікації можуть бути зламані або скомпрометовані.

Вирішення цих проблем можна забезпечити за допомогою технології децентралізованого блокчейну. Блокчейн є децентралізованим, розподіленим, спільним та незмінним базою даних, який зберігає реєстр активів та транзакцій через P2P мережу. Блокчейн використовує хешування SHA-256 для забезпечення сильного криптографічного підтвердження для автентифікації та цілісності даних. По суті, дані блоку містять список всіх транзакцій та хешу попереднього блоку. Блокчейн має повну історію всіх транзакцій і забезпечує транскордонну глобальну розподілену довіру.

В представленій нижче архітектурі мережі Інтернету речей з застосуванням технології Блокчейн [2] можна виділити декілька основних компонентів з яких вона складається:

- Блокчейн вузол (Node) - записує всі транзакційні блоки. Містить інформацію про керування пристрою користувачами, іншим пристроєм, керуванням, які виконує адміністратор та білінгом.

- Адміністратор (Admin) - особа, яка реєструє користувачів, шлюзи та пристрої в блокчейні та надає доступ для них.

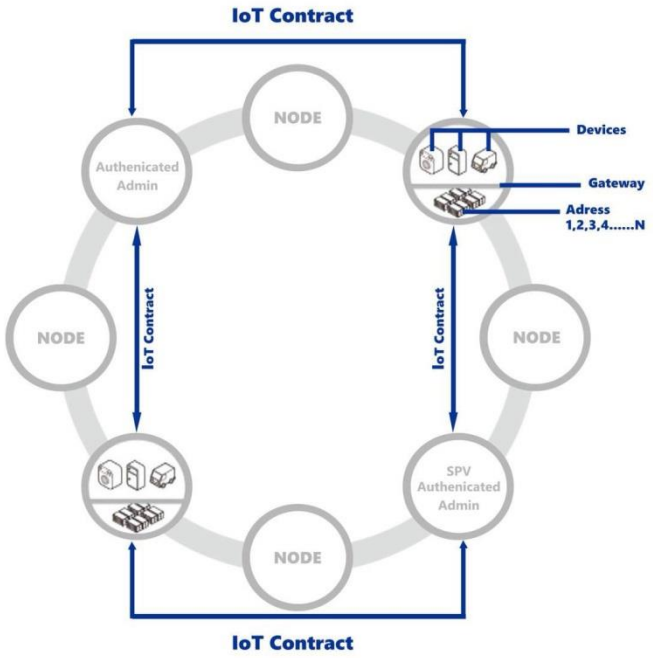


Рис. 2. Архітектура мережі Інтернету речей на базі технології Блокчейн

Ці налаштування безпечно зберігаються у вузлі блокчейна та передаються іншим користувачам, шлюзам та пристроям через мережу. Тому кожен користувач та пристрій підтримує останні пов'язані з ними налаштування.

- Шлюз (Gateway) - як такий, пристрій використовується для управління пристроями або датчиками. Він може аналізувати деталі контракту IoT, а потім передавати до пристроїв або датчиків. Надає кожному пристрою або датчику індивідуальну адресу.

- Пристрій (Device) - як такий, пристрій, підключений до шлюзу.

Блокчейн має 160-розрядний адресний простір, на відміну від адресного простору IPv6, який має 128-розрядний адресний простір. Адреса блоку становить 20 байт або 160-бітовий хеш відкритого ключа, створеного ECDSA (алгоритм цифрового підпису еліптичного кривизни). З 160-бітною адресою blockchain може створювати та розподіляти адреси в автономному режимі приблизно на 1,46 * 1048 IoT пристроїв. 21 Вірогідність зіткнення адрес становить приблизно 1048, що вважається достатньо захищеною, щоб забезпечити GUID (глобальний унікальний ідентифікатор), який не вимагає перевірки реєстрації або унікальності під час призначення та розподілу адреси на пристрої IoT.

Надійні треті сторони або централізовані органи та служби можуть бути порушені, скомпрометовані або зламані. Для того щоб забезпечити можливість єдиної та багатопартійної автентифікації на пристрої IoT за допомогою технології блокчейн можна надавати децентралізовані правила і логіку автентифікації. Крім того, smart-контракти [2][3] можуть забезпечити більш ефективні правила доступу до авторизації для підключених пристроїв IoT з меншою складністю порівняно з традиційними протоколами авторизації, такими як RBAC, OAuth 2.0, OpenID, OMA DM і LWM2M. Ці протоколи сьогодні широко використовуються для ідентифікації, авторизації та керування пристроєм IoT. Більш того, конфіденційність даних також може бути забезпечена шляхом використання smart-контрактів [2][3], які встановлюють правила доступу, умови та час для того, щоб певна особа або група користувачів або машин могли володіти, контролювати або мати доступ до даних.

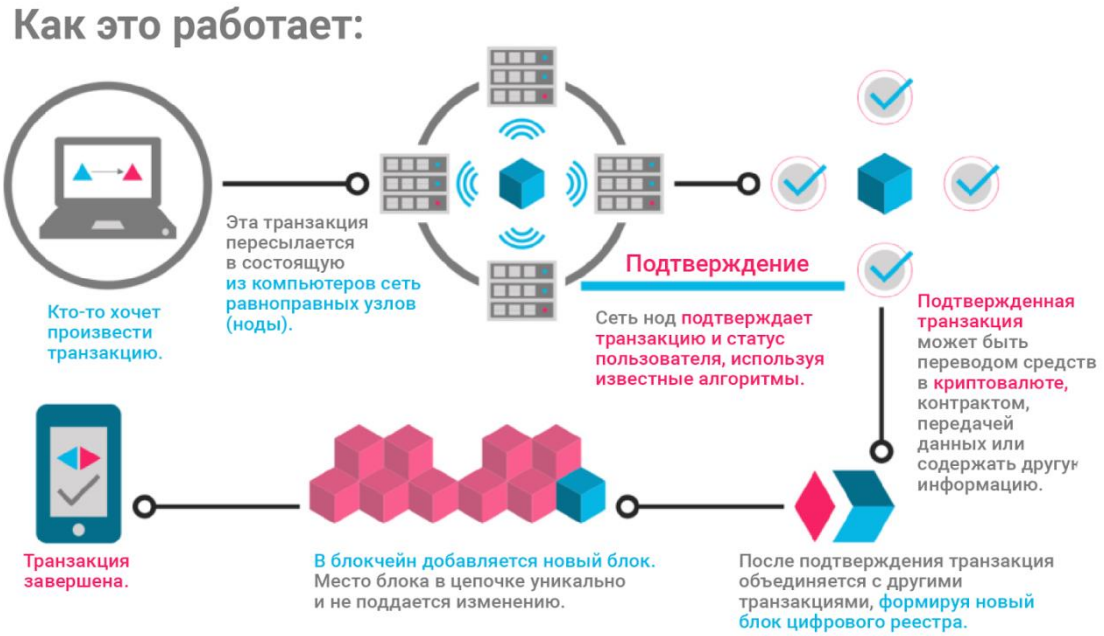


Рис. 3. Як працюють смарт-контракти

За допомогою технології блокчейну, управління і розподіл ключів довіри повністю усуваються, оскільки кожен пристрій IoT матиме власну унікальний ідентифікатор GUID та асиметричну ключову клавішу після встановлення та підключення до мережі. Це також призведе до значного спрощення інших протоколів захисту, таких як DTLS та TLS.

Висновок. Отже саме за домогою технології блокчейн можна вирішити проблеми конфіденційності передачі данних, проблему автентифікації, розподілення ключів довіри серед IoT пристроїв, проблему сертифікації та зниження коштів на неї шляхом її виключення, проблему відстеження правопорушень шляхом відстеження транзакцій.

Література

1. M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems (2017).
2. Why blockchain and iot are best friends from IBM blog https://www.ibm.com/blogs/blockchain/ 2018/01/why-blockchain-and-iot-are-best-friends/
3. Internet of Things: Security challenges for next generation networks http://ieeexplore.ieee.org/ document/7542301/

УДК 621.396.1

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ ОНТОЛОГІЧНИХ МОДЕЛЕЙ ТА БАЗ ДАНИХ

Коваленко В. Ю. Новогрудська Р.Л.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vladimir.kovalenko.y@gmail.com

COMPARATIVE ANALYSIS OF ONTOLOGIES AND RELATIONAL DATABASES

The article gives a comparative analysis of information representation using ontologies and relational databases. The analysis was conducted on four levels: conceptualization of information, data representation, data modeling, and efficiency.

Стаття наводить порівняльний аналіз способів представлення інформації з використанням онтологій та баз даних. Аналіз проведено на наступних умовних рівнях: концептуалізація інформації, представлення даних, моделювання даних, ефективність.

Незважаючи на те, що область моделювання знань налічує значну кількість моделей представлення, жодна з них не була популяризована так само, як онтології протягом останнього десятиліття. Онтології почали активно розвиватися в області обчислювальної техніки та науки, зокрема, в області штучного інтелекту та баз даних (БД). Саме БД найчастіше використовуються для представлення інформації про реальний світ, але вони накладають кілька обмежень для забезпечення ефективного доступу до даних та управління ними.

У даний час відбувається дискусія про те, чи можна вважати онтологією базу даних. Наукова спільнота, в більшості, вважає онтології найкращим способом відображення реальності завдяки їх властивості моделювати семантичні терміни. Онтологія використовує для представлення даних специфічні елементи: класи, властивості, екземпляри, агреговані відносини, узагальнені відносини, а також аксіоми, представлені логічними мовами (дескриптивна логіка або логіка першого порядку) щоб додати семантику до моделей. Але онтологія не описує конкретні представлення комп'ютерних даних і, отже, не залежить від реалізації. Варто відзначити, що досить легко знайти прямі зв'язки між онтологією та базою даних. Клас може відповідати таблиці бази даних, властивість реляційним атрибутам, узагальнюючі відносини або обмеження аксіомам тощо. Проте таке порівняння не таке тривіальне, як це здається на перший погляд.

Пропонується провести порівняльний аналіз підходів до побудови онтологічних моделей та баз даних на чотирьох рівнях: Концептуалізація інформації; Представлення даних; Моделювання даних; Ефективність.

Рівень концептуалізація інформації. Бази даних можна розглядати як спрощенні онтології [2], оскільки в БД відсутні аксіоми, що описують реальність. Схема бази даних являє собою механізм представлення, який розроблений в основному для задоволення вимог конкретного застосування або користувача, тому, коли ці вимоги змінюються, необхідно також змінити точку огляду і схему БД. На противагу, онтології вважаються незалежними від тексту і реалізації і, як такі, працюють на більш високому рівні абстракції. Що стосується визначення

онтології, то згідно з [3] онтології представляють лише узагальнені знання, а їх предметна область зазвичай узгоджена і залежить від рівня та мети використання. Таким чином, ті сукупності концептів які використовуються (або розробляються) тільки для конкретного додатка, не розглядаються як онтології. Крім того, при використанні онтологічної моделі немає необхідності розрізняти базові або складні типи даних і, більш того, їх властивості мають набагато більше семантики, ніж типи даних БД, оскільки онтології не потрібно нормалізувати.

Рівень представлення даних. Інформація, представлена в онтології, змішує поняття специфікації схеми з даними. На відмінно від БД, яка чітко диференціює схему та дані. При використанні онтології, екземпляри класів можуть повторюватися. Проте така функція не завжди може вважатися недоліком, оскільки, за рахунок наявності в онтології семантичних зв'язків, вона дозволяє підвищити ефективність при пошуку по онтології. Якщо розглядати процес ініціалізації даних, варто зауважити, що для онтологічної моделі немає специфічних вимог які регламентують цей процес. При додаванні нового екземпляру не накладаються жодні обмеження. В противагу для БД кортеж не може бути вставлений в базу даних, якщо він не задовольняє всі семантичні обмеження схеми, такі як первинні ключі або зовнішні ключі, нульові перевірки, тощо. Отже, для реляційної бази даних такий факт може бути обмеженням на внесення даних в порівнянні з онтологією.

З іншого боку, онтології використовують семантичний механізм міркувань (СММ) для вирішення проблем ініціалізації даних. Саме він визначає, чи екземпляр належить онтології чи ні, в залежності від виконання усіх накладених обмежень. Наприклад, чи узгоджені усі визначені аксіоми, правила успадкування, тощо. У результаті кожного разу, коли потрібна перевірка, викликається СММ. Онтології мають власний механізм для вилучення інформації зі сховища онтології. Такий механізм працює аналогічно механізмам мов запитів, таких як SQL. Розглянемо основну відмінність такого механізму від аналогічних механізмів БД. СММ можуть вибрати нову інформацію, незалежно від того, чи містяться дані в онтології. Для запитів по простору даних онтології використовуються такі мови як SPARQL або SERQL. Ці мови повертають інформацію про відношення між термінами онтології з використанням предикатів, властивих структурі графів, тоді як мова SQL (мова запитів БД) представляє плоску та табличну структуру інформації, що зберігається в словнику.

Рівень моделювання даних. На відміну від онтологій, концептуальна модель, яка використовується для представлення даних в БД, є семантично багатшою, ніж дескриптивні логічні моделі, які використовуються для представлення більшості онтологій [1,4,5]. Проте концептуальні моделі пропонують занадто низький рівень виразності. Онтології не можуть розглядатися як концептуальні моделі, оскільки вони є багаторазовими, тоді як концептуальні моделі можуть бути багаторазово доступними лише на нижчому рівні.

Необхідно також враховувати відмінності між різними моделями баз даних (в контексті різниці між моделями на різних рівнях проектування: концептуальна модель, логічна модель, фізична модель). Логічне представлення бази даних не визначає той самий рівень семантики, що концептуальна модель тієї ж БД. Обмеження моделі даних призводять до семантичних втрат у представленні

інформації. Наприклад, нехай розширена схема сутність-зв'язок або діаграма UML представляє відношення IS-A. Воно може зникнути, коли схема не була належним чином перетворена в відповідну реляційну логічну модель, наприклад за допомогою SQL. Однак, більшість подібних перетворень не змінюють семантики інформації, представленої у сховищі.

Така ж проблема актуальна і для онтологій. Їх семантика залежить від мови представлення. Отже, онтологія, представлена за допомогою конкретної мови, такої як KIF, RDF, OWL або конкретного інструменту (Protege, WebOde, WebOnto, тощо) має власні семантичні обмеження. Тим не менше, переходи між цими мовами можуть призвести до семантичних втрат або навіть до деяких несумісностей. Такі недоліки не є актуальними для баз даних.

Мови опису онтології є набагато виразнішими в сенсі вираження семантичних концепцій, ніж бази даних, оскільки в БД містяться лише конструкції для визначення або вибору даних, а в онтологіях присутні також конструкції для опису семантичних відношень та зв'язків між даними. Крім того, онтологічні мови забезпечують більш коректну та точнішу концепцію домену.

Рівень ефективності використання. Бази даних є більш ефективними ніж онтології, коли мова йде про рівень підтримкиу даних. Для баз даних наявний широкий спектр інструментів для їх налаштування. При великих об'ємах баз даних не втрачається впорядкованість даних. Але вони однозначно програють при необхідності розвивати модель і вносити зміни.

Висновки. В роботі було проаналізовано підходи до побудови онтологічних моделей та баз даних. Порівняння БД та онтологічних моделей проведено по чотирьом умовним рівням: рівень концептуалізації інформації, рівень представлення даних, рівень моделювання даних, рівень ефективності використання. Подальші дослідження буде спрямовано на опис підходу до інтеграції базових понять БД та онтологічних моделей з метою спрощення та автоматизації процесу представлення даних з онтологічних моделях за допомогою БД.

Література

1. Meersman R Ontologies and databases: More than a fleeting resemblance. In: Proceedings of inter-national workshop on open enterprise solutions: systems, experiences, and organizations (OES-SEO),Luiss Publications Rome (2001).
2. K Gómez-Pérez A, Férnandez-López M, Corcho-García O (2003a) Metodologies, tools and languages for building ontologies. where is their meeting point? In: Data knowledge engineering, vol 46. Elsevier Science Publishers B.V. Amsterdam, The Netherlands, pp 41–64.
3. Dillon T, Chang E, Hadzic M, Wongthongtham P (2008) Differentiating conceptual modelling from data modelling, knowledge modelling and ontology modelling and a notation for ontology modelling. In: APCCM '08: proceedings of the fifth on Asia-Pacific conference on conceptual modelling. Australian Computer Society Inc., Darlinghurst, Australia, pp 7–17.
4. Cullot N, Parent C, Spaccapietra S, Vangenot C (2003) Ontologies: a contribution to the dl/db debate. In: Proceedings of the first international workshop on semantic web and databases (VLDB workshop).
5. Ruiz F, Hilera JR (2006) Using ontologies in software engineering and technology ontologies for software engineering and software technology. Springer, Berlin 49–102.

УДК 004.89

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ОБРОБКИ ДАНИХ В РОЗПОДІЛЕНОМУ ДАТА ЦЕНТРІ

Прокопець В.А., Глоба Л.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vprokopets95@gmail.com

Experimental research of energy-efficient data processing in distributed data-center

In this study, the effectiveness of the method of dynamic allocation of resources in the virtualized network of mobile operator of Ukraine with increasing energy efficiency of data processing has been analyzed.

Сучасні телекомунікаційні системи складаються з великої кількості вузькоспеціалізованого фірмового обладнання, яке, як правило, може виконувати невеликий обсяг конкретних операцій.

1. Кожен постачальник мережевого обладнання спеціалізується на деяких функціях, обмежених визначеною ділянкою мережевої топології (наприклад, виступає виробником обладнання для мережі доступу, або ядра мережі). Зазвичай, більшість вендорів не має задовільних технічних рішень для інших частин мережевої топології.

2. Практично будь-яке вузькоспеціалізоване обладнання, задля якомога кращого виконання своїх функцій має складну і специфічну структуру, яка не достатньо уніфікована з іншим обладнанням навіть того ж самого виробника.

Ці фактори спричинюють необхідність підтримки гетерогенних мультивендорних мереж операторами зв’язку, які експлуатують подібні мережі.

Підхід використання хмарних обчислень в бізнесі є наслідком переходу від продукто-орієнтованого виробництва до сервіс-орієнтованого надання послуг. Головна ідея – оренда послуг замість купівлі обладнання.

З цього випливає основний принцип хмарних обчислень - користувач платить лише за ті ресурси, які йому потрібні і отримує їх за запитом у короткий термін. У зв’язку з цим, постає проблема динамічного визначення необхідної кількості орендованих ресурсів у постачальників хмарних сервісів для зменшення вартості обчислень за рахунок відсутності надлишкових ресурсів, що не використовуються із забезпеченням необхідних показників QoS. У зв’язку з цим потрібно визначитись, наскільки часто переглядати обсяг виділених ресурсів та змінювати його для недопущення порушення вимог до якості обслуговування та надлишкового використання ресурсів.

Для вирішення даної проблеми у дослідженні запропоновано метод динамічного розподілу ресурсів для визначення оптимального обсягу ресурсів для віртуалізованих вузлів мережі мобільного зв’язку. Метод дозволяє з’ясувати обсяги потрібних ресурсів для забезпечення високого рівня обслуговування користувачів, уникнути надлишковості ресурсів та, як наслідок, їх простою. Крім того метод дозволяє з’ясувати моменти часу, що є оптимальними для перерахунку обсягів ресурсів.

У даному дослідженні ефективність методу перевіряється шляхом його застосування у віртуалізованому ядрі мобільної мережі України.

Опис запропонованого підходу

Експериментальне дослідження проводиться засобами імітаційного моделювання середовища Matlab за таким планом:

Підготовчі кроки:

Крок 1. Визначення розподілу трафіку в мережі

Крок 2. Побудова топології мережі

Крок 3. Моделювання добової кривої навантаження

Крок 4. Визначення реального навантаження на мережах LTE кожного міста

Крок 5. Визначення навантаження на елементах мережі

Основні кроки:

Крок 6. Обчислення контрольних інтервалів для проведення зміни кількості орендованих ресурсів в дата-центрі

Крок 7. Визначення енергетичної кривої для ЦОД

Крок 8. Оцінка енергоспоживання для усієї мережі з використанням підходу PCPB

Крок 9. Загальна оцінка кількості споживаних ресурсів

В моделі для спрощення топології допущено, що мережа LTE розгорнута в 5 найбільших містах в різних частинах України.

Результаті імітаційного моделювання.

Згідно описаного підходу основною задачею підготовчого етапу є визначення величини та розподілу навантаження по мережевим елементам. Після цього обчислюються контрольні інтервали для зміни кількості орендованих ресурсів та відповідно кількість ресурсів. Останнім етапом оцінюється ефективність роботи методу.

Таблиця 1. Оцінка енергоспоживання із використанням запропонованого алгоритму.

Сумарне енергоспоживання в мережі, МВт	Максимально можливе енергоспоживання, МВт	% від максимального
1,3306	1,633	81,5%

Таблиця 2. Результат динамічного розподілу ресурсів у ядрі EPC мобільної мережі

City	Resource pool	Average amount of free resources per day	Average % of free resources per day
Kyiv	33	13,34	40,41%
Kharkiv	30	11,52	38,40%
Dnipro	24	10,05	41,89%
Lviv	14	6,35	46,43%
Odesa	20	9,29	45,39%
In total	**120**	**50,55**	**41,78%**

На рис.1 зображено результат роботи методу динамічного розподілу ресурсів у віртуалізованому ядрі мобільної мережі для міста Києва у графічному вигляді. Червона лінія ілюструє випадок статичного розподілу ресурсів. Зелена крива показує трафік протягом дня. Синя крива показує обсяг ресурсів, розподілених відповідно до запропонованого методу динамічно.

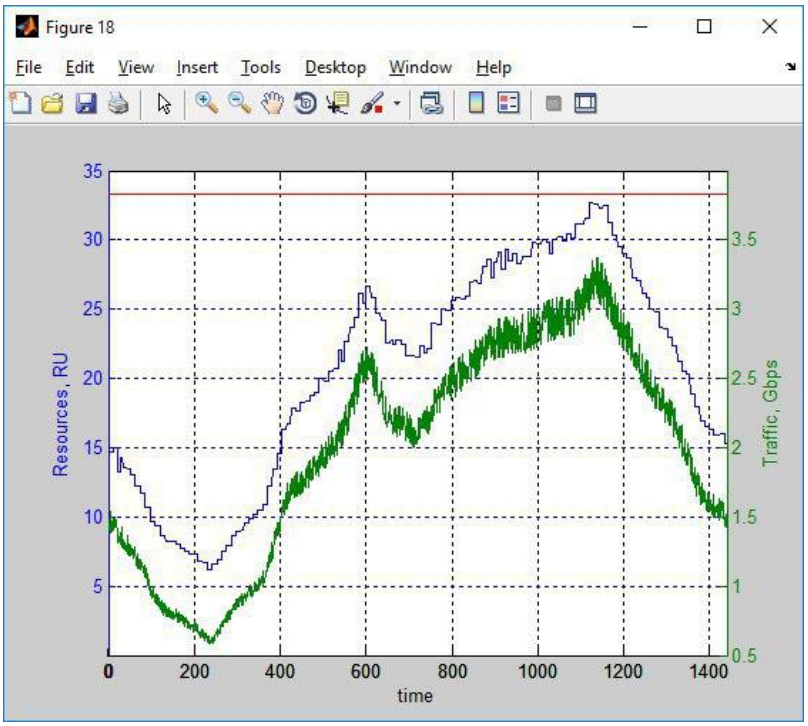


Рис.1. Результат роботи методу динамічного розподілу ресурсів у віртуалізованому ядрі мобільної мережі для міста Києва

Результати дослідження показали, що комбінація запропонованих підходів дозволяє досягти економії обчислювальних ресурсів на 41,78% завдяки застосуванню методу динамічного розподілу ресурсів та підвищити енергоефективність обчислень на 35,78% завдяки застосуванню підходу PCPB.

Література

1. Abid H. A novel scheme for node failure recovery in virtualized networks / H. Abid; N. Samaan // 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013). – Ghent, Belgium, 2013. – P. 1154-1160.
2. Skulysh M. Model for Efficient Allocation of Network Functions in Hybrid Environment / M. Skulysh, L. Globa, S. Sulima // Information and Telecommunication Sciences. 2016. № 1. P. 39–45.
3. Alexander Schill, Larysa Globa, Oleksandr Stepurin, Nataliia Gvozdetska, Volodymyr Prokopets “Power Consumption and Performance Balance (PCPB) scheduling algorithm for computer cluster”, // UkrMiCo’2017, 11-15 September 2017, Odesa, Ukraine, pp. 1-8.

УДК 621.396

АНАЛИЗ МЕТОДОВ ПРОГНОЗИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

Запорожец Д.Б., Скулиш М.А.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: zaporozhetsdb@gmail.com

Analysis of Forecasting Methods using Neural Networks

Was analyzed forecast of Internet traffic as an important issue that has received few attentions from the computer networks field. By improving this task, efficient traffic engineering and anomaly detection tools can be created, resulting in economic gains from better resource management. This paper presents a Neural Network Ensemble (NNE) for the prediction of TCP/IP traffic using a Time Series Forecasting (TSF) point of view. Several experiments were devised by considering real-world data from two large Internet Service Providers. In addition, different time scales (e.g. every five minutes and hourly) and forecasting horizons were analyzed. Overall, the NNE approach is competitive when compared with other TSF methods (e.g. Holt-Winters and ARIMA).

Прогнозирование трафика TCP / IP является важной задачей для любого среднего или крупного сетевого провайдера [1]. Несколько провайдеров интернет-услуг (ISP) используют Multiprotocol Label Switching (MPLS) для реализации инфраструктуры трафика путем создания полной сетки виртуальных сетей MPLS между всеми парами маршрутизаторов в сети [2]. Теоретически это позволит оптимизировать ресурсы полосы пропускания в сети, что позволит повысить качество обслуживания в целом. В случаях, когда MPLS не используется, традиционное распределение весов протокола маршрутизации может быть сделано гораздо более эффективно, зная будущую матрицу трафика спроса между всеми конечными точками сети. Следовательно, нужно предусмотреть автоматические средства разработки трафика, которые адаптируются к будущим условиям сети на основе точных алгоритмов прогнозирования трафика.

Прогнозирование трафика также может помочь обнаружить аномалии в сетях [3]. Атаки безопасности, такие как отказ в обслуживании, вирусы или даже нерегулярное количество СПАМ, могут быть обнаружены путем сравнения реального трафика со значениями, предсказанными алгоритмами прогнозирования.

В настоящее время эта задача часто решается интуитивно опытными сетевыми администраторами с помощью маркетинговой информации о будущем количестве клиентов и их обычном поведении [1]. Но это не дает точную картину о том, как будет выглядеть трафик, мало используемого для серьезного ежедневного сетевого администрирования. С другой стороны, вклад из областей оперативных исследований, статистики и аналитики привели к более точным методам прогнозирования, которые заменили основанные на

интуиции. В частности, поле прогнозирования временных рядов (TSF), также называемое одномерным прогнозированием, имеет дело с предсказанием хронологически упорядоченной переменной [5], [6]. Цель TSF - моделировать сложную систему как «черный ящик», предсказывая ее поведение, основанное на исторических данных, а не как это работает.

Из-за его важности было предложено несколько методов TSF, таких как Holt-Winters [7], методология ARIMA [8] и нейронные сети [9]. Holt-Winters была разработана для серий с трендовыми и сезонными факторами. Совсем недавно была предложена двойная сезонная версия. ARIMA является более сложным подходом, требующим таких шагов, как идентификация модели, оценка и валидация. Каждая модель ARIMA основана на линейной комбинации прошлых значений и / или ошибок. Нейронные сети - это модели подключений, вдохновленные поведением центральной нервной системы, и, в отличие от предыдущих методов, они могут прогнозировать нелинейные ряды. В прошлом несколько исследований доказали предсказуемость сетевого трафика с использованием аналогичных методов, таких как HoltWinters и ARIMA [3]. Следуя свидетельствам нелинейного сетевого трафика, также были предложены NN [4].

Данный подход использует уже имеющуюся информацию, предоставленную Simple Network Management Protocol (SNMP), которая с достаточной точностью оценивает трафик, проходящий через каждый сетевой интерфейс. SNMP широко используется каждым интернет-провайдером, поэтому сбор этих данных не вызывает дополнительного трафика в сети.

Naive Benchmark Method. Наиболее часто используемым методом наивного прогнозирования является прогнозирование будущего. Тем не менее, этот метод будет плохо работать в сезонных данных. Таким образом, лучшей альтернативой является использование сезонной версии, где прогноз будет определяться наблюдаемым значением за тот же период, связанный с предыдущим сезонным циклом.

B. Holt-Winters. Важный метод прогнозирования из семейства методов экспоненциального сглаживания. Прогностическая модель основана на некоторых основных шаблонах (например, трендовых и сезонных), которые отличаются от случайных шумов путем усреднения исторических значений [7]. Его популярность обусловлена такими преимуществами, как простота использования, сокращенный спрос на вычислительные ресурсы и точность прогнозов, особенно при совместном использовании с сезонными сериями.

C. ARIMA Methodology. Основное преимущество этого метода зависит от точности над более широкой областью рядов. Глобальная модель основана на линейной комбинации прошлых значений и ошибок, называемой AutoRegressive Integrated Moving-Average (ARIMA).

D. Artificial Neural Networks. Нейронные модели являются врожденными кандидатами на прогнозирование из-за их нелинейных и помехоустойчивых

возможностей. Основная идея – обучить нейронные сети прошлым данным, а затем использовать эту сеть для прогнозирования будущих значений.

В этой работе было рассмотрено нескольких подходов к прогнозированию при применении к трафику TCP / IP. К ним относятся три метода прогнозирования временных рядов (TSF): Holt-Winters, методология ARIMA и подход нейронной сети (NNE).

Анализ преимуществ и недостатков приведенных алгоритмов показал, что следует методы прогнозирования с использованием нейронных сетей к активным сценариям измерения, в которых информация уровня пакета в реальном времени подается в механизм прогнозирования или рекомендуем применять методы прогнозирования для требований к трафику, связанных с конкретными интернет-приложениями, поскольку это может принести пользу некоторым управленческим операциям, выполняемым интернет-провайдерами, таким как приоритизация трафика и распределение сетевых ресурсов. Кроме того, для улучшения этапа выбора модели в тестируемых моделях TSF можно использовать ряд методов оптимизации. В этом случае оптимизация модели может проводиться параллельно с использованием модели прогнозирования в режиме реального времени, выполняя замену модели, когда ожидаются лучшие результаты.

Література

1. K. Papagiannaki, N. Taft, Z. Zhang, and C. Diot, “Long-Term Forecasting of Internet Backbone Traffic,” IEEE Transactions on Neural Networks, vol. 16, no. 5, pp. 1110–1124, Sept. 2005.
2. B. Davie and Y. Rekhter, MPLS: Multiprotocol Label Switching Technology and Applications. USA: Morgan Kaufmann, 2000
3. B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen, “Sketch-based Change Detection: Methods, Evaluation, and Applications,” in Proceedings of Internet Measurment Conference (IMC’03). Miami, USA: ACM, Oct. 2003.
4. J. Jiang and S. Papavassiliou, “Detecting Network Attacks in the Internet via Statistical Network Traffic Normality Prediction,” Journal of Network and Systems Management, vol. 12, pp. 51–72, 2004.
5. J. Hanke and A. Reitsch, Business Forecasting. Allyn and Bancon Publishing, Massachussetts, USA, 1989.
6. S. Makridakis, S. Weelwright, and R. Hyndman, Forecasting: Methods and Applications. John Wiley & Sons, New York, USA, 1998.
7. P. R. Winters, “Forecasting sales by exponentially weighted moving averages,” Management Science, vol. 6, pp. 324–342, 1960.
8. G. Box and G. Jenkins, Time Series Analysis: Forecasting and Control. Holden Day, San Francisco, USA, 1976.
9. A. Lapedes and R. Farber, “Non-Linear Signal Processing Using Neural Networks: Prediction and System Modelling,” Los Alamos National Laboratory, USA, Technical Report LA-UR-87-2662, 1987.

УДК 004, 372.862, 377.169.3

ВПРОВАДЖЕННЯ ОСВІТНІХ ЕЛЕКТРОННИХ ЗАСТОСУВАНЬ В НАВЧАЛЬНИЙ ПРОЦЕС

Чічіков А.О., Штогріна О.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: tonychichikov@gmail.com

Implementation of educational application into the learning process

The abstract describes the benefits of using educational applications in the learning process. And the process of developing such programs for training. Possibilities for development of such programs for various educational subjects are obtained. The main idea of application is to create a resource for preparation for laboratory work. Students were able to review the theoretical knowledge necessary for preparation for laboratory work. Students could consider and practice a phased procedure of laboratory work.

Національна програма інформатизації в Україні визначає побудову інформаційного суспільства в Україні однією з найактуальніших задач сьогодення. Інформаційне суспільство — це соціологічна концепція, яка стверджує, що в основі розвитку суспільства лежить виробництво, обробка, використання науково-технічної й іншої інформації. Основу концепції інформаційного суспільства поклали З. Бжезінський, Д. Белл [1].

Для розвитку інформаційного суспільства національною доктриною розвитку освіти визначено пріоритетні заходи, що спрямовані на реалізацію державної політики у сфері освіти. Здійснення цих заходів, забезпечить удосконалення навчально-виховного процесу, доступність та ефективність освіти, створить умови для приведення рівня і якості освітнього рівня у відповідність з вимогами кадрового забезпечення та інноваційного розвитку України [2].

Державне агентство з питань електронного урядування для реалізації національної програми інформатизації за мету визначає підвищення рівня комп’ютерної та інформаційної грамотності населення, впровадження нових методів навчання із застосуванням сучасних ІТ технологій [1].

Покращення підготовки спеціалістів галузі та напряму підготовки «Телекомунікації», можливе завдяки збільшенню обсягів та покращенню якості навчальних матеріалів у електронному вигляді.

Метою роботи є дослідження можливості створення електронного навчального застосування з використанням комбінованих методів навчання. Дослідження можливості створення навчальних застосувань для різних навчальних дисциплін. Та дослідження якісного впливу навчальних застосувань на навчальний процес.

В ході даної роботи створено подібне навчальне застосування на прикладі курсу технічної електродинаміки, та на його прикладі розглянуто

особливості створення навчальних застосувань для інших навчальних дисциплін.

У процесі створення навчального застосування та проведення дослідження були застосовані методи гейміфікації навчального застосування.

Процес створення електронного навчального середовища викликає необхідність приведення навчальних матеріалів до такої форми, щоб ними було зручно користуватися в електронному форматі [3]. Тому доречним є також і докорінна зміна або переробка цих матеріалів відповідно до сучасних вимог. Такою зміною і є застосування для курсу технічної електродинаміки. Воно включає в себе можливість наочно здійснювати ознайомлення студентів з процесом і послідовністю проведення лабораторної роботи. Що дозволяє студентам мати чітке розуміння і уявлення про завдання, цілі та сутність експерименту. Зосереджувати увагу на змісті експерименту, не витрачаючи увагу на орієнтацію в повністю незнайомій обстановці та на знайомстві з обладнанням і складом установки. Безпосередньо перший етап знайомства таким чином виноситься за рамки лабораторної роботи та здійснюється при попередній підготовці до лабораторної роботи.

З урахуванням перспективності використання електронних засобів освіти [4], було створено навчальне застосування освітнього характеру для курсу технічної електродинаміки з використанням комбінованих методів навчання. Навчальне застосування є електронною імітацією лабораторних робіт курсу технічної електродинаміки. Навчальне застосування містить деякі теоретичні відомості з курсу технічної електродинаміки, що допомагають студентові зорієнтуватися і чіткіше зрозуміти зміст роботи та її головну мету. Також застосування містить елементи практичного характеру які вимагають від студента інтерактивної взаємодії та дають змогу отримати практичні навички підготовчого характеру. Ці інтерактивні елементи являють собою завдання з налаштування апаратури, де студенту необхідно правильно налаштувати пристрої перед початком роботи. Також наявні завдання де необхідно провести вимірювання фізичних величин, що також є тренуванням корисних навичок студента перед лабораторною роботою. Таким чином у сукупності ці види завдань, що присутні у застосуванні допомагають студенту зрозуміти сутність, практичну значущість та проблематику пов’язану з професійною сферою, що закладена в лабораторних роботах. Завдання, їх зміст та послідовність скомбіновані в застосуванні таким чином, щоб сформувати в свідомості студента чіткий портрет дисципліни, проблематику та методологію рішення прикладних завдань. Дати чітке усвідомлення ходу та змісту лабораторної роботи та структурувати навчальний матеріал. Розроблене застосування дозволяє ознайомитися з пристроєм і порядком складання лабораторної установки, а також віртуально виконувати практичні вправи з лабораторної роботи. У цьому застосуванні використовуються макети лабораторних установок з предмету технічна електродинаміка та поширення радіохвиль. Ці тривимірні моделі розроблені в рамках даної роботи спеціально для використання в рамках електронного навчального застосування. Застосування дозволяє

збирати установки з набору блоків. Залежно від положення блоків в установці можливо змоделювати різні фізичні процеси і отримати необхідні вихідні результати. Тому для отримання правильних результатів відповідно до завдання лабораторної роботи важливою частиною є порядок складання установки. При знятті показань з вимірювальних пристроїв установки, в ході проведення лабораторної роботи, проводиться заміна деяких її складових. Різні варіанти збірки дозволяють студентам побачити роботу установки з заданими фізичними залежностями і тим самим застосувати теоретичні знання на практиці.

Для розробки застосування була обрана платформа розробки ігор Unity 3D з використанням тривимірних моделей окремих блоків лабораторних установок. Тривимірні моделі складових блоків лабораторних установок були змодельовані в пакеті створення тривимірної графіки Blender 3D.

В рамках застосування віртуальні установки володіють нескінченним ресурсом, не вимагають ремонту і заміни деталей на відміну від їхніх матеріальних прототипів. Застосування з віртуальними установками знижує експлуатацію установок в лабораторії, що дозволяє продовжити термін їх майбутньої служби.

В ході дослідження розглянуто можливість створення електронного навчального застосування з використанням комбінованих методів навчання. Використання електронних навчальних застосувань в навчальному процесі має ряд переваг, котрі розглянуто в даній роботі. Виявлено можливість створення електронних навчальних застосувань для різних навчальних дисциплін та виявлено високу ефективність їх використання. Результати дослідження показали позитивний вплив використання навчальних застосувань на навчальний процес. В ході дослідження створено навчальне застосування для курсу технічної електродинаміки, та на його прикладі розглянуто особливості створення навчальних застосувань для інших навчальних дисциплін.

Література

1. Brzezinski Z. Between Two Ages. America's Role in the Technetronic Era / Z. Brzezinski. The Viking Press, 1970, P.123.
2. Державне агентство з питань електронного урядування України [Електронний ресурс] – режим доступу: http://www.e.gov.ua/content/dovidkovo , вільний.
3. Ковалинська І. Використання електронного навчального простору [Електронний ресурс]/ І. Ковалинська //Український науковий журнал "ОСВІТА РЕГІОНУ", №4 2012, с. 239 – режим доступу: http://social-science.com.ua/article/931, вільний.
4. Ившина Г. В. Разработка электронных образовательных ресурсов: мониторинг качества и внедрение Часть1. Учебно-методическое пособие по направлению «Электронные образовательные ресурсы» / Казанский государственный университет им. В.И. Ульянова-Ленина; Автор-сост.: Г. В. Ившина - Казань: КГУ, 2008.

УДК 004.724.4

ВПРОВАДЖЕННЯ ВІРТУАЛІЗАЦІЇ МЕРЕЖЕВИХ ФУНКЦІЙ НА МЕРЕЖІ ПЛАТФОРМИ ПЕРЕДАЧІ SMS - ПОВІДОМЛЕНЬ

Чиж В.В. , Скулиш М.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vasyachyzh1996@gmail.com

Network functions virtualization

The article highlights the main architectural elements of the concept of network function virtualization (NFV), which allows to increase the efficiency of investments and the overall flexibility of the network architecture by avoiding hardware implementations towards software implementation of network services. The concept of NFV technology was formed due to the desire to reduce the cost of creating, maintaining and operating networks, and also because of the desire to make independent life cycles of software and hardware from each other.

Мережа будь-якої системи передачі даних складається з різноманітних типізованих технічних пристроїв. Запуск будь-якого нового мережевого сервісу передбачає додавання все нових наборів обладнання, котрі вимагають місця в апаратних кімнатах, нових джерел живлення. Це веде до зростання вартості споживаної енергії, капітальних та операційних витрат, а також необхідності найму персоналу, що володіє все більш різноманітною кваліфікацією і профілізацією. Крім того, фізичне мережеве спорядження швидко застаріває, а також вимагає все більш частих ітерацій циклу закупівля - проектування - інтеграція - розгортання. Причому, на прибутку компанії це найчастіше позначається скільки-небудь негативно. Для уникнення підвищенню витрат необхідні дещо нові підходи до розвитку бізнесу операторів і сервіс-провайдерів. Одним з таких підходів є віртуалізація мережевих функцій (Network Functions Virtualization) – NFV [1].

Це технологія віртуалізації фізичних мережевих елементів телекомунікаційного зв’язку, коли мережеві функції виконуються програмними компонентами, що працюють на стандартних серверах (найчастіше x86) і віртуальних машинах (VM) в них. Ці програмні модулі можуть взаємодіяти між собою для надання послуг обміну інформації, чим раніше займалися апаратні платформи.

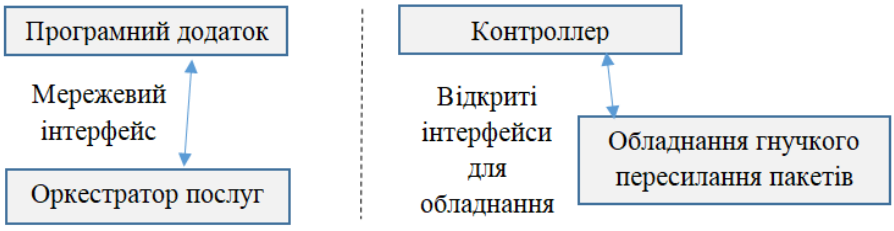


Рис. 1. Загальна структура NFV

Розглянемо архітектуру NFV для нової SMS-платформи.

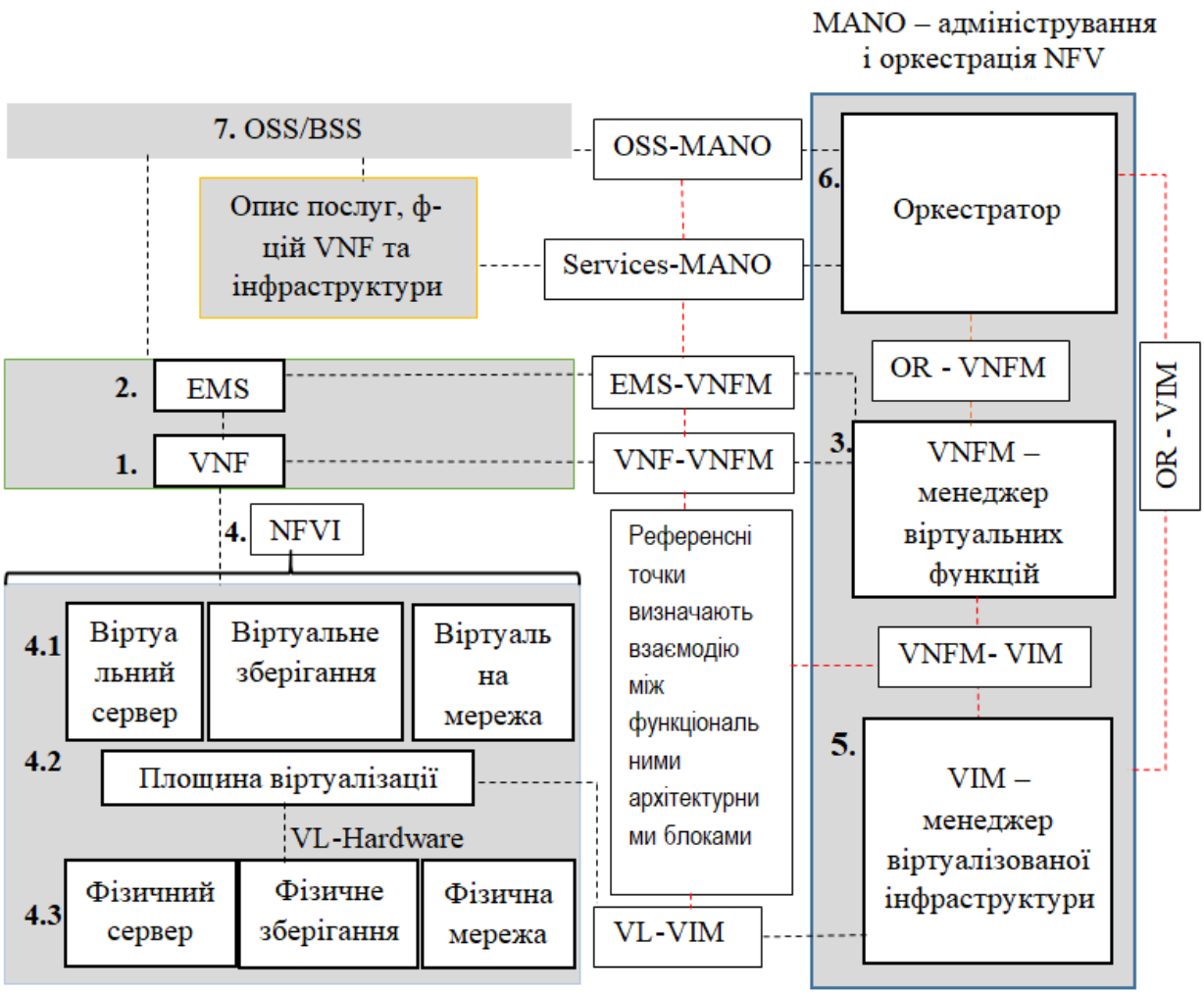


Рис. 2. Архітектура NFV для SMS-сервісу

Головна особливість запропонованої схеми - виділення віртуальних ресурсів тим чи іншим задачам, що поступають по запиту. При цьому досягається найбільш оптимальне використання ресурсів устаткування: серверів, зберігання і мережі. Для цього в архітектурі NFV передбачений компонент адміністрування і оркестрації MANO [2] (Management and Orchestration), який створює комплексні послуги серед різних VNF (які можуть управлятися від різних VNFM). MANO має безліч референсних точок, наприклад Or-Vi(orchestration- VIM), NF-Vi (network virtualization - VIM), Or-Vnfm (orchestration - VNFM) та ін. Чому вони називаються саме «референсними точками», а не інтерфейсами? Інтерфейс означає двосторонній обмін сигнальними повідомленнями між об'єктами, які являють собою закінчені або фізичні, або програмні об'єкти. Референсна точка, на відміну від інтерфейсу, визначає взаємодію між функціональними архітектурними блоками, які самі складаються із закінчених програмно-апаратних об'єктів. А в концепції MANO ми оперуємо саме функціональними блоками, а не об'єктами.

Розглянемо роботу системи NFV і її окремих елементів для сервісу передачі SMS повідомлень (Рис. 2).

1. Блок віртуальної мережевої функції VNF (Virtual Network Function):

Віртуальні мережеві функції VNF для SMS-платформи - основа архітектури NFV. Це і є віртуалізовані функції мережевих елементів. Наприклад, це може бути маршрутизатор (Router VNF), базова станція (BS VNF), комутатор (Switch VNF). VNF може представляти також одну з підфункцій мережевого елемента, наприклад, пересилання пакетів (forwarding) в маршрутизаторі. Тоді кілька VNF будуть відповідати одному фізичному мережевому елементу

2. Система адміністрування елементів EMS (Element Management System):

Система адміністрування елементів EMS керує роботою VNF. Вона відповідає за задання параметрів, тобто адміністрування (Management) операцій VNF, точно також, як фізичні мережеві компоненти керуються системами управління мережею NMS (Network Management System). Наприклад, це може бути управління при відмовах (fault management), управління продуктивністю (performance management). Однією VNF може відповідати одна EMS, або одна EMS може керувати кількома VNF. Крім того, сама EMS також може являти собою VNF, керовану від іншої EMS.

3. Менеджер VNFM (VNF Manager):

Менеджер VNFM управляє роботою однієї або декількох VNF. Наприклад, він контролює життєвий цикл функцій VNF, тобто, запускає, обслуговує, і зупиняє роботу VNF. VNFM може виконувати ті ж функції, що і EMS, але через референсну точку VeNf-Vnfm.

4. Інфраструктура NFVI (Network Function Virtualization Infrastructure):

Це середовище (інфраструктура), в якій працюють VNF. Ця інфраструктура включає:

4.1. Ресурси фізичного обладнання(обчислювальні сервери, комутатори та ін.)

4.2. Рівень віртуалізації відповідає за абстрагування фізичних ресурсів у вигляді віртуальних ресурсів. На цьому рівні знаходиться спеціальна програмна платформа Hypervisor, яка розділяє програмні засоби від апаратних, тобто дає можливість запускати програми незалежно від обраного обладнання. Наприклад, операційна система може працювати на будь-якому фізичному сервері, який призначається для цієї цілі в даний момент.

4.3. Віртуальні ресурси (обчислювальні, мережеві та ресурси зберігання) – це віртуальна частина інфраструктури головного блоку NFVI. Фізичні ресурси абстрагуються в віртуальні ресурси, які використовуються для роботи функцій VNF. Припустимо, що площина віртуалізації відсутня(**Virtualization Layer**). В принципі, VNF можуть працювати безпосередньо на виділених матеріальних ресурсах і бути жорстко до них прив'язані. Однак, при цьому ми не можемо називати їх віртуальними мережевими функціями NVF, в такому випадку, їх слід назвати PNF (Physical Network Functions). Це теж можливо. Однак, в цьому випадку перенесення віртуальної машини з одного фізичного сервера на інший (що часто буває необхідно, наприклад, при зміні місця розташування користувача віртуальної машини VM) потрібно буде виконувати вручну, а це складно, довго і затратно.

5. Менеджер віртуалізованої інфраструктури VIM (Virtualized Infrastructure Manager):

Це система адміністрування інфраструктури NFVI. Вона відповідає за управління ресурсів NFVI всередині одного домену інфраструктури сервісу. Вона також відповідає за збір результатів вимірювань продуктивності і подій.

6. Оркестратор NFV (NFV Orchestrator):

Оркестратор NFV генерує, обслуговує і припиняє роботу мережевих сервісів (функцій) VNF, а також ініціює створення закінченої послуги з багатьох VNF. Оркестратор NFV також відповідає за адміністрування глобальних ресурсів NFVI. Наприклад, він адмініструє ресурси обчислень, зберігання і мережі на кількох менеджерах VIM на мережі. Оркестратор не взаємодіє безпосередньо з VNF, а тільки через VNFM і VIM. Наприклад, є кілька функцій VNF, з яких створена комплексна послуга. Наприклад, це може бути віртуальна базова станція або віртуальний домен опорної мережі EPC(Evolved Packet Core). На мережі ці елементи можуть бути представлені обладнанням або від одного, або від різних вендорів. Тоді потрібно створити комплексну (end to end) послугу з використанням декількох VNF. При цьому потрібен оркестратор послуг для комунікації з усіма VNF і створення комплексної послуги.

В EPC, що є останньою архітектурою базової мережі для стільникової системи,

приклади мережевих функцій, котрі можуть бути віртуалізовані, включають MME (Mobility Management Entity), S/P-GW (Serving/Packet Gateway) та інші.

7. Система підтримки операцій і бізнесу OSS / BSS (Operation Support System / Business Support System):

Це фізична система OSS / BSS платформи передачі повідомлень. OSS займається управлінням мережею (network management), управлінням при відмовах (fault management), управлінням конфігурацією (configuration management) і управлінням послугами (service management). BSS відповідає за управління клієнтами (customer management), управління продуктами (product management), управління замовленнями (order management) та ін. В архітектурі NFV, наявна BSS / OSS платформи може бути інтегрована з системою NFV MANO, за допомогою стандартних інтерфейсів.

У чому переваги та вигоди від застосування даної моделі для SMS-сервісу? Можна вказати лише основні з них:

1. Оперативність виведення нових послуг на ринок. Замість того, щоб проводити маркетингові дослідження, будувати нову апаратну платформу для нових сервісів, проводити загальне тестування, запускати пілотні проекти, на що зазвичай йдуть місяці, за допомогою запропонованої архітектури можна програмно конструювати нові послуги, в дата-центрах, там їх тестувати і швидко виводити на ринок. У разі невдачі або безперспективності нової послуги (що іноді трапляється при прорахунках маркетингу) ціна невдачі буде мінімальною.

2. Скорочення капітальних витрат. Реалізація мережевих елементів на стандартних (commodity) серверах в дата-центрах при масовому розгортанні буде обходитися значно дешевше ніж на виділеному обладнанні.

3. Скорочення операційних витрат. Обслуговування стандартних серверів в дата-центрах проводиться сертифікованим IT-персоналом, якому для роботи з NFV лише потрібно пройти курси підвищення кваліфікації. Крім того, чисельність необхідного персоналу також скорочується, з тих же причин.

4. Гнучкість використання ресурсів. При невеликому трафіку викликів задіюється мінімальну кількість віртуальних машин на серверах, при зростанні трафіку, автоматично підключаються нові віртуальні машини, на яких працюють VNF для емуляції функцій мережевого обладнання. У разі апаратної реалізації, ресурси обладнання будуть використовуватися нераціонально, оскільки ресурси завжди розраховуються на максимальний трафік в мережі, а такі ситуації трапляються лише в години максимального навантаження. В інший час обладнання (в разі апаратної реалізації) залишається недовантаженим.

Основна проблема, яка тут буде виникати - наявність власних дата-центрів у вендерів, або доступність дата-центрів у хмарних провайдерів для аутсорсингу ресурсів стандартних серверів і систем зберігання, обробки і аналізу даних.

Література

1. “NFV виртуализация сетевых функций” [URL: https://habrahabr.ru/company/ua-hosting/blog/247431] Osaul 19.09.2015.
2. “Management and Orchestration” [URL: http://network-functions-virtualization.com/mano.html].
3. Skulysh M., Method of LTE functional units organization with evolved packet core virtualization. Skulysh M., Klimovych O. // Information and Telecommunication Sciences. — 2015. — No. 4. — P. 38–45.

УДК 621.396.1

ОСНОВНІ ХАРАКТЕРИСТИКИ СИСТЕМ INTERNET OF THINGS

Новогрудська Р. Л., Миніч М. А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: rinan@ukr.net, marinka43753@gmail.com

MAIN CHARACTERISTICS OF SYSTEMS INTERNET OF THINGS

The research devotes to the review of systems Internet of things. The main characteristics and features of IoT systems, potential areas of use of such systems are presented, as well as a list of problems associated with their implementation.

Наведене дослідження присвячено огляду систем Internet of Things. Наведено основні характеристики та особливості систем IoT, потенційні сфери використання таких систем, а також перелік проблем, пов’язаних з їх впровадженням.

На сьогоднішній день Internet of Things (IoT) широко використовується в різних сферах. Наприклад, транспортування, охорона здоров'я, комунальні послуги, логістика, фармацевтика та інші. У майбутньому, майже всі активні пристрої матимуть інтернет-інтерфейс. Компанії і вчені звертають увагу на забезпечення рішення для двох проблем: опрацювання великих об'ємів інформації, що надходить з пристроїв і розпізнавання необроблених даних. Парадигма IoT охоплює величезну кількість різних областей і здатна атакувати різні існуючі і майбутні проблеми, пов’язані з апаратним забезпеченням, потужністю, безпекою, надійністю, сумісністю та проблеми обміну даними [1]. Тому, на даний момент ці проблеми є актуальними, так як технологія IoT застосовуватиметься в найближчому майбутньому.

IoT поєднує всі види речей, пов’язаних з інтернетом. Ці «речі» включають все, починаючи від сенсорів руху, пристроїв, що вимірюють температуру та закінчуючи різними типами смарт речей, таких як, смартфони, автономні автомобілі, будівлі та ін. Всі ці пристрої в майбутньому будуть збирати дані, ділитися інформацією і функціонувати раціональним шляхом, тому наше життя стане легшим і гармонійним.

Для кращого розуміння технологій IoT досліджено пов’язані сфери, такі як всепроникаючий комп’ютинг, інтегрований інтелект, розумні будинки та міста, зв’язок від машини до машини (M2M), бездротові сенсорні мережі, семантичні сенсорні мережі, семантика та великі дані, машинне навчання.

Потенційні домени додатків IoT. IoT має величезний ринковий потенціал в останні роки. У 2014 році було 1,5 мільярди інтернет-ком’ютерів і 1 мільярд мобільних телефонів з підтримкою інтернету. До 2020 року кількість IoT пристроїв, підключених до інтернету, становитиме близько 50-100 мільярдів [2]. IoT використовується в найрізноманітніших доменах додатків. Для прикладу: авіація, навчання, енергія, розваги і спорт, екологія, фінанси, влада, розумні будинки, логістика, важка індустрія та багато інших.

Характеристики та особливості IoT. У світі IoT існує мільярди пристроїв. Деякі з них мають високорівневі архітектури з великими можливостями пам'яті, високою швидкістю процесора (наприклад, мобільними

телефонами). Тим часом деякі з них, навпаки, мають архітектуру низького рівня, обмежену пам'ять та обчислювальні можливості (наприклад, датчики температури). Взаємозв'язок між цими пристроями робить IoT дуже складною системою взагалі.

Хмарні обчислення грають важливу роль в екосистемі IoT. За допомогою хмарних обчислень можуть бути збільшені обчислювальні ємності і обсяги для зберігання. Крім того, датчики можуть використовуватися скрізь, і дані з них можуть опрацьовуватись через служби хмарних обчислень.

Питання безпеки і конфіденційності піднімаються через велику кількість пристроїв і відсутність уніфікованої стандартизації вивчення безпеки IoT. Кожен пристрій, що підключений до інтернету може викликати проблеми з безпекою. Тому, такі дослідження не повинні ігноруватись. Дослідження і реалізація безпеки IoT в останні роки стає передовим питанням через атаки DoS (відмова в обслуговуванні). Згідно з опитуванням Мохамеда [3] щодо різних загроз, пов’язаних з IoT, визначено такі категорії: відмова в обслуговуванні, фізичні атаки, підслуховування та пасивний моніторинг, аналіз трафіку та виведення даних. Також розглянуті питання безпеки та конфіденційності в IoT належать до конфіденційності користувачів та захисту даних, аутентифікація та управління ідентифікацією, політика інтеграції, авторизації та контролю доступу, надійні рішення для атак.

Проблеми впровадження IoT. Зрозуміло, що у наступні роки буде проведено багато розробок IoT, але також необхідне проведення досліджень та аналізів у майбутньому. Нижче наведені основні напрями розвитку IoT та проблеми його впровадження.

1. Підвищення IoT стандартів

За підтримки компаній та дослідницьких груп за останні роки прикладено багато зусиль для стандартизації IoT. Хоча, все ще не вистачає стандартизації в реалізації машинного навчання і у великих структурах обробки даних. Зрозуміло, що при впровадженні нової технології формування загальноприйнятої стандартизації займає деякий час. Протягом процесу стандартизації, різні вендори та компанії лише з декількох спроб реалізують свої системи.

2. Приватність та безпека IoT

Зростає турбота про проблеми безпеки та конфіденційності, які потребують розділеного доступу, високошвидкісний потік даних, автономне прийняття рішень тощо. Зі зростанням складності таких мереж, стає набагато складніше підтримувати загальну безпеку та конфіденційність. Кібербезпека стала однією з найважливіших областей завдяки вищезгаданим проблемам у світі IoT. Збільшення заходів безпеки може погіршити продуктивність обробки даних IoT. Мабуть, це одне з головних відкритих питань.

3. Використання семантики в світі IoT

Семантичний веб використовується в нижніх шарах розробки IoT, наприклад, онтологія SSN, опис датчиків і датчики даних. Оскільки, неоднорідність і розмір світового IoT розширюється, то сумісність між пристроями, фреймфорками та системами стане ще важчою. M2M стандарт намагається подолати це, використовуючи семантичні технології абстракції і

сумісність.

4. Розробка систем навчання для IoT

Декілька років тому були розроблені навчальні системи та рішення з особливостями контекстної обізнаності. Вони в основному розроблені логічно, правильно і з використанням різноманітних алгоритмів. Нейронні мережі можуть використовуватись більш широко з великими даними IoT, що швидко накопичуються, а отже рішення побудови IoT систем можуть вдосконалитися. Нові навчальні фреймворки для більших IoT розробок зі значно більшим трафіком даних можуть бути розроблені з новими великими аналітичними даними та рішеннями.

5. Впровадження та розробка методів глибокого навчання

Однією з основних характеристик глибокого навчання є використання низькорівневих функцій (або навіть самих вихідних даних) і перетворення їх у змістовні, висококласні функції в межах моделі шляхом застосування неконтрольованого та контрольованого навчання за допомогою каскадних шарів. Для успішної реалізації глибокого навчання загалом потрібні великі набори даних, де модель вивчає приховані функції високого рівня. Це добре підходить для великих даних та концепції IoT.

6. Підвищення автономії та впровадження самоорганізованого IoT

Структури програм IoT можуть бути розширені та розроблені з повністю автоматизованим зв'язком M2M, автоматичними міркуваннями та системами навчання. Не надаючи інформацію та повідомлення людям для взаємодії та прийняття рішень, пристрої зможуть сприймати, навчитися, взаємодіяти та вирішувати різні питання, використовуючи системи та рішення IoT. Цифрові персональні помічники, які керують усіма навколишніми пристроями, і спілкуються з іншими рішеннями з особистої допомоги, можуть бути додатково розроблені. Розроблені знання структур IoT можуть бути вдосконалені. Розумні міста, які керують усіма пристроями IoT та спілкуються з іншими розумними містами, автономними транспортними засобами, розумними дорожними системами, інтелектуальними мережами та системами виробництва енергії, а також більш розумною планетою, можуть бути майбутніми проектами та ініціативами з використанням рішень IoT.

Проаналізувавши інформацію щодо IoT, впевнено можна сказати, що проблем і невирішених питань досить багато і вони потребують зусиль для вирішення. Тому дослідження і розробки передових компаній та розробників спрямовані на покращення функціонування цієї передової технології IoT.

Література

1. Internet of Things Global Standards Initiative. Internet of Things Global Standards Initiative. 2015. URL: www.itu.int.
2. Charith Perera et al. “Semantic-Driven Configuration of Internet of Things Middleware”. In: 9th International Conference on Semantics, Knowledge and Grids. IEEE, 2013, pp. 66–73.
3. Mohamed Abomhara and Geir M. Koien. “Security and privacy in the Internet of Things: Current status and open issues”. In: 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS). IEEE, May 2014, pp. 1–8.

УДК 621.396

ПЛАНУВАННЯ РЕСУРСІВ ГЕТЕРОГЕННОГО ТЕЛЕКОМУНІКАЦІЙНОГО СЕРЕДОВИЩА НА БАЗІ АНАЛІЗУ СТАТИСТИЧНИХ ДАНИХ

Белокур Б.В., Скулиш М.А.
Інститут телекомунікаційних систем,
КПІ імені Ігоря Сікорського, Україна
E-mail: belokur.bv@gmail.com

Planning resources of heterogeneous telecommunication environment on the basis of statistical data analysis

The development of modern telecommunication industry requires the modernization of existing networks in automated control systems based on methods for forecasting the main parameters. The main difference between software-configurable networks is remote control logic from routers and switches, the emergence of logically structured network management. To ensure the requirements of rapid exchange of information was proposed criterion of choosing the most efficient network protocol according on network resources. It can be used in the development of adaptive control methods for heterogeneous networks.

Сучасні мережі не завжди відповідають зростаючим вимогам по швидкості введення в експлуатацію та швидкості внесення змін в конфігурацію мережі. Поява програмно-конфігурованих мереж (Software-defined network) має змінити стан речей. Головною відмінністю таких мереж є видалення керуючої логіки з маршрутизаторів і світчей, поява логічно централізованого управління мережею, а також можливість програмування мережі [1].

Часто основні переваги сучасних систем управління — універсальність і багатофункціональність - стають в спеціалізованих системах і їх основними недоліками. Це пов'язано з необхідністю врахувати специфіку роботи системи, яка вимагає відповідних налаштувань мережі та методів управління її роботою. Тому класичні методи проектування мережі, що враховують, усереднені показники продуктивності, не можуть забезпечити ефективне використання мережевих ресурсів [2].

Для оцінки ефективності функціонування мережі, прийнято використовувати такі показники [3, 4]: середній час затримки при передачі інформаційних повідомлень, середній час перебування повідомлень в мережі, середня завантаженість мережі, середня продуктивність мережі, показники надійності та ін.

Функція оцінки ефективності є багатопараметричною, тому для її розрахунку береться мінімально необхідна кількість найбільш важливих показників.

Нехай $M^{(i)} = \left\{M_1^{(i)}, \dots, M_J^{(i)}\right\}$ — безліч таких показників, $\dim M = I$ кожен з яких, в свою чергу, визначається сукупністю часткових показників.

Визначимо функцію оцінки ефективності функціонування мережевого протоколу на підмножині показників:

$$L = L(M_0), M_0 \subset M$$

Для гетерогенної мережі критичними є тимчасові показники, і крім цього необхідно враховувати вимоги до: надійності, захищеності, пропускної здатності, стійкості до перешкод і т.д. Визначимо множину М наступним чином:

$$M = \{M_1, M_2, M_3, M_4\}$$

де M_1 — час затримки повідомлення; M_2 — час комутації; M_3 — розмір повідомлення; M_4 — пропускна спроможність ліній зв'язку.

Розглянемо процес обробки інформаційних повідомлень. Для n-го інформаційного повідомлення, що обробляється m-м каналом мережі введемо булеву функцію:

$$B(n,m) = \begin{cases} 1, & \text{якщо канал обслуговує повідомлення } n \\ 0, & \text{якщо канал не обслуговує повідомлення } n \end{cases}$$

Нехай:

$$M_1 = \{t^3_{n,m}\},\ M_2 = \left\{t^{(k)}_{n,m}\right\},\ M_3 = \{V_n\},\ M_4 = \{\mathrm{C}_{n,m}\}\ ,$$

де $t^{(k)}_{n,m}$ – час комутації пакета, що залежить від мережевого пристрою і визначається його технічними характеристиками; Cn,m —пропускна здатність каналу передачі даних; Vn — об'єм пакетних даних.

Визначимо обмеження на час доставки пакета — T_n і доступну пропускну здатність мережі — F_m.

Звідси сумарний час обробки інформаційних повідомлень на фіксованому часовому інтервалі — узагальнений показник ефективності, який можна визначити наступним чином:

$$L(M_0) = \sum_{m=1}^{M} \sum_{n=1}^{N} B(n,m) \left(t^3_{n,m} + t^{(k)}_{n,m} + \frac{V_n}{\mathrm{C}_{n,m}} \right)$$

Критерієм вибору найбільш ефективного мережевого протоколу S гетерогенної мережі є вимога мінімізації узагальненого показника ефективності — сумарного часу обробки інформаційних повідомлень на фіксованому часовому інтервалі.

При обмеженнях, які накладаються характеристиками мережі:

$$\sum_{n=1}^{N} B(n,m)\, \mathrm{C}_{n,m}(S) \le F_n, m = \overline{1, M}$$

При обмеженнях, накладених тактико-технічними характеристиками:

$$\sum_{n=1}^{N} B(n,m)\, \mathrm{C}_{n,m} \left(t^3_{n,m}(S) + t^{(k)}_{n,m}(S) + \frac{V_n}{\mathrm{C}_{n,m}(S)} \right) \le T_n, n = \overline{1, N}$$

Таким чином, визначено критерій вибору найкращого мережевого протоколу в якості якого виступає вимога щодо мінімізації узагальненого показника ефективності - сумарного часу обробки інформаційних повідомлень на фіксованому часовому інтервалі при обмеженнях на час доставки і на доступну пропускну здатність мережі, накладених згідно характеристикам телекомунікаційної мережі. Сформульована оптимізаційна задача вибору найбільш ефективного мережевого протоколу:

$$L_k = L_k(M_0, M_{\text{нп}}), k = \overline{1, K}\ ;\ L(M_0) \to sup\ ,$$

де M_0 — підмножина показників, критичних при функціонуванні мережі, $M_{\text{нп}}$ = M\M0 — підмножина некритичних показників.

Оцінки некритичних показників з $M_{\text{нп}}$ визначюать обмеження відповідної оптимізаційної задачі:

$$L_k(M_0, M_{\text{нп}})\ \aleph\ F_k\ , k = \overline{1, K}$$

де $\aleph$ - відношення, яке може бути як строгого, так і нестрогого порядку, F_k – гранична оцінка для k-го некритичного показника.

У свою чергу, застосування запропонованих моделей в програмно-конфігурованих мережах дозволить забезпечити виконання вимог до продуктивності мережі і надійності обслуговування абонентів за рахунок ефективного функціонування мережі без виділення надлишкових ресурсів.

Разом з тим слід зазначити, що практичне застосування запропонованої моделі вимагає деяких додаткових досліджень. Зокрема, при розробці методів адаптивного управління необхідно приділити увагу формуванню безлічі критичних і некритичних показників, які використовуються при формулюванні узагальненого критерію ефективності.

Результати роботи можуть застосовуватися при розробці методів адаптивного управління для гетерогенних мереж з високими вимогами по оперативності.

Література

1. Логвинов С.С. Об уровнях управления программно-конфигурируемой сети (SDN) // T-Comm: Телекоммуникации и транспорт. 2017. Ст. 50-55.
2. Косенко В.В., Бугас Д.Н. Анализ эффективности использования ресурсов мультисервисной информационно-телекоммуникационной сети // Технологический аудит и резервы производства — № 5/2(25), 2015. Ст. 17-22.
3. Rodrigues, C. An ontology for managing network services quality / C. Rodrigues, S. R. Lima, L. M. lvarez Sabucedo, P. Carvalho // Expert Systems with Applications. - 2012. Pp.107-117.
4. De Assis, M. V. O. A seven-dimensional flow analysis to help autonomous network management / M. V. O. de Assis, J. J. P. C. Rodrigues // Information Sciences. - 2014. Pp.120-125.

УДК 621.39

ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ АРХІТЕКТУРНИХ РІШЕНЬ ДЛЯ ПОБУДОВИ МАСШТАБОВАНИХ ПРОГРАМНИХ ПРОДУКТІВ

Дуля О.О., Міночкін Д.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: sasa97973@gmail.com

THE COMPARATIVE STUDY OF ARCHITECTURAL SOLUTIONS FOR MAKING SCALABLE SOFTWARE PRODUCTS

This work about researching architectures serverless and microservices. It shows the difference between these architectures. The report reveals the biggest advantages and disadvantages of serverless and microservices.

Сервіс-орієнтована архітектура (*service-oriented architecture,* SOA) придумана в кінці 1980-х. Вона бере свій початок в ідеях, викладених в CORBA (*Common Object Request Broker Architecture* — загальна архітектура брокера об'єктних запитів), DCOM (*Distributed Component Object Model* - розподілена модель компонентних об’єктів), DCE (*Data Communication Equipment* - Апаратура передачі даних) і інших документах [3]. Про SOA написано багато, є кілька її реалізацій. Але, по суті, SOA можна звести до кількох ідей, причому архітектура не диктує способи їх реалізації:

- Сполучуваність додатків, орієнтованих на користувачів.
- Багаторазове використання бізнес-сервісів.
- Незалежність від набору технологій.
- Автономність (незалежні еволюція, масштабованість і швидке розгортання).

SOA - це набір архітектурних принципів, що не залежать від технологій і продуктів, зовсім як поліморфізм або інкапсуляція.

В основі мікросервісної архітектури лежать концепції SOA. Призначення у неї: створити єдиний загальний корпоративний додаток з декількох спеціалізованих додатків бізнес-доменів [4].

Мікросервісна архітектура створювалася в контексті швидко і постійно мінливих бізнесів, які (в основному) з нуля створюють власні хмарні додатки. У випадку з мікросервісамі ми повністю контролюємо додатки (при цьому в системі можуть використовуватися і сторонні веб-сервіси).

Характер побудови / проектування мікросервісів не вимагає глибокої інтеграції. Мікросервіси повинні відповідати бізнес-концепції, обмеженому контексту. Вони повинні зберігати свій стан, бути незалежними від інших мікросервісів, і тому вони менше потребують інтеграції. Тобто низька

взаємозалежність і висока зв'язність привели до побічного ефекту - зменшення потреби в інтеграції.

Тобто, мікросервіси - це маленькі автономні сервіси, що працюють разом і спроектовані навколо бізнес-домену.

Оскільки не обов'язково володіти серверами як фізичними машинами, в більшості випадків, розробник не повинен думати про сервери і масштабування, він має можливість зосередитися лише на бізнес-логіці.

Serverless дає змогу використовувати кожен з «мікросервісів» вашої програми, будь то платежі, управління користувачами, новинний бюлетень, як повністю незалежну функцію, яка може «впасти», не пошкодивши додаток цілком [1]. Кожна з цих служб може масштабуватися незалежно. Тобто якщо ніхто не використовує генерацію PDF-файлів, ця служба не доступна, але якщо багато користувачів вирішили скористатися цим сервісом, вона миттєво масштабується для його підтримки.

Також, ще однією перевагою є потрібність платити тільки за ті послуги, які використовуються, і тільки за час, коли вони дійсно використовувалися. Це і є Serverless [2].

Зазначу, що для Serverless потрібно трохи інша архітектура наших додатків. Вони повинні мати подієву структуру і не використовувати інформацію про стан (stateless).

Serverless і Мікросервіси мають спільні характеристики, але вони сильно відрізняються тим, як вони забезпечують хмарні обчислення.

Ціноутворення - це найперша відмінна риса. Serverless - це pay-as-you-go (плата, якщо використовується), що робить його привабливим варінтом для додатків, що мають незначну кількість запитів, або для стартап-організацій. Це також зменшує експлуатаційні витрати за рахунок того, що інфраструктура та віртуальні машини оброблюються постачальниками послуг, а не безпосередньо на власному обладнанні, IaaS (інфраструктура, як послуга) чи PaaS (платформа, як послуга).

Масштабування - це також перевага архітектури serverless. За своєю природою serverless може краще справитись з піковими навантаженнями і може автоматично, швидко керуватися. Єдиний недолік - це максимальна кількість запитів, які можуть бути оброблені, що робить її непридатною для високонавантажених систем.

Serverless ще більш детальна за мікросервіси і надає значно більшу степінь функціональності. Але зворотна сторона цього - це робить її більш складною. Serverless має також інші недоліки, такі як обмеження кількості запитів, обмежений час операції та підтримує меншу кількість мов програмування.

Його компонентами є часто конкретними постачальникам хмарних послуг, які може бути важко змінити. Функції мають бути stateless (без запам'ятовування стану), а керування станом відбуватися виключно, за границями функції - це означає, що більше ніякої кеш-пам'яті.

Окрім цього, функції в serverless можуть використовуватися, як планові задачі, чи обробники подій, а не лише в якості послуг.

Хоча мікросервіси все ще забезпечують ґрунтовний підхід до сервіс-орієнтованої архітектури, serverless розвивається в напрямку архітектури заснованої на подіях (event-based) і очевидно має переваги з точки зору часу до виходу на ринок, гнучкого ціноутворення та знижених експлуатаційних витрат.

Малоймовірно, що serverless зараз підійде до кожної системи. Зараз, найкращим рішенням буде поєднання цих двох архітектурних рішень, для того, щоб донести і використати переваги хмарних технологій для себе і ваших клієнтів.

Таким чином, в роботі проведено порівняльний аналіз архітектурних рішень (serverless та мікросервісів), з чого випливає наступне:

1. Головна різниця serverless та мікросервісів в тому, як вони забезпечують хмарні обчислення.

2. Масштабованість та ціноутверення - головні переваги Serverless.

3. Мікросервіси не мають обмеженої кількості запитів та обмеженого часу операції, на відміну від Serverless.

4. Всі функції в serverless мають бути stateless (без запам'ятовування стану).

5. Мікросервіси забезпечують грунтовний підхід до сервіс-орієнтованої архітектури, а serverless розвивається в напрямку архітектури заснованої на подіях (event-based).

6. Найкращим варіантом, на сьогодні, є метод комбінування цих архітектурних рішень, для отримання максимальної вигоди.

Література

1. Roberts, Mike (25 July 2016). "Serverless Architectures". *MartinFowler.com*. Retrieved 30 July 2016.
2. "Creating full-stack Serverless applications on the AWS platform". *Serverless-Stack.com*. Retrieved 5 April 2017.
3. S. Newman, Building Microservices – Designing Fine-Grained Systems, O'Reilly, 2015.
4. E. Wolff, Microservices: Flexible Software Architecture, Addison-Wesley, 2016.

УДК 004.93

ПІДХІД ДО МАРКУВАННЯ ЗОБРАЖЕНЬ

Остапенко М.С., Штогріна О.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: mak7.ostapenko@gmail.com

Approach to marking images

In this paper propose the method to speed up labeling of the image for creating new datasets. We need datasets for training convolutional neural networks that solve the various task of computer vision for example: image classification, object detection, and localization..

Із розвитком технологій та зростанням потреб людства, постає необхідність збільшення автономності виконання виробничих процесів у всіх галузях народного господарства: від охорони здоров'я до транспорту і зв'язку. Для виконання більшості дій, що виконуються людиною, необхідне візуальне сприйняття світу. Тому не можливо повністю автоматизувати виробничі процеси без використання алгоритмів комп'ютерного зору. На даний момент вже існують алгоритми по розпізнанню об'єктів на зображеннях, що мають більшу точність від людини не залежно від критеріїв оцінювання. Їх використовують у системах автоматичного керування транспортними засобами, аутентифікації, аналізу емоційного стану людини, первинної діагностики хвороб.

Найбільш ефективними алгоритмами комп'ютерного зору для розпізнавання об'єктів є алгоритми, що базуються на штучних нейронних мережах (НМ). Проблема використання таких алгоритмів, полягає в необхідності мати велику кількість зображень для їх навчання. Людині достатньо один раз показати об'єкт і після цього вона зможе його з високою точністю розпізнавати незалежно від освітлення, кута зору, кольору та інших умов. Для навчання НМ потрібно подавати на вхід сотні варіантів одного й того ж або схожих зображень зроблених в різноманітних умовах. Після такого навчання НМ знаходить приховані залежності між зображеннями, та набуває можливості здійснювати бінарну класифікацію, тобто відрізняти об'єкт, на який вона була навчена, від усіх інших. Для покращення процесу навчання використовуються розмічені зображення, в яких окрім самого зображення, присутня інформація з описом об'єкта.

Існуючі програмні інструменти забезпечують зручний процес маркування вмісту зображень: об'єктів, їхнього розміщення та взаємодії між собою. Опис виконується в залежності від поставленої задачі, яку потрібно вирішити, це може бути розпізнавання, локалізація, класифікація, сегментація. Разом розмічені зображення будуть являти собою набір даних, що складається із самих зображень та файлу опису вмісту кожного зображення.

Серед розробників найбільш широко використовуються два засоби маркування зображень Sloth [1] та LabelImg [2]. Sloth надає гнучкі можливості опису вмісту зображень, за рахунок налаштування процесу

маркування кожним окремим користувачем. Він підтримує всі формати зображень і дозволяє представляти файл опису зображення у форматах XML, JSON, CSV. LabelImg є зручним у використанні, але у порівнянні із Sloth не надає можливості індивідуального налаштування процесу маркування і опис зображення формує тільки у форматі XML.

На даний момент не існує достатньої кількості розмічених зображень для навчання НМ, за винятком, найбільш популярних та комерціалізованих областей використання. А вище описані інструменти надають можливість тільки ручного маркування. Здійснюваний людиною процес маркування є дуже повільним, що призводить до неможливості якісно розмітити потрібну кількість зображень. Отже актуальним завданням є розробка підходу до маркування зображень, який би включав попереднє автоматизоване маркування, з можливістю подальшого ручного корегування отриманої розмітки.

Для автоматизації процесу маркування зображень пропонується використовувати алгоритми, що виконують класифікацію, локалізацію об’єктів та описують їх взаємодію між собою на зображенні.

Для класифікації об’єктів на зображенні використана переднавчена нейронна мереже ResNet [3]. На відміну від задачі класифікації об’єктів, задача локалізації вимагає точного встановлення положення об’єкта на зображенні, отримання координат його центру, ширини та довжини обмежувального регіону. Для локалізації об’єктів на зображенні пропонується використовувати один із алгоритмів YOLO [4] або Faster R-CNN [5].

YOLO (You only look once) розділяє вхідне зображення на комірки. Для кожної комірки передбачує вірогідність, того що вона належить до певного класу і далі об’єднує комірки в обмежувальні блоки. Використання тільки однієї згорткової нейронної мережі, що виявляє всі об’єкти на зображенні лише за одне поширення зображення через мережу, надає значну перевагу у швидкості. За рахунок цього YOLO одночасно виконує задачу локалізації та класифікації. Його можна використовувати для обробки відео потоків та відстеження об’єктів. Але його недоліком є точність віднесення шуканого об’єкту до певного класу у випадках коли об’єкт займає відносно малу площу по відношенню до всього зображення.

Faster R-CNN для локалізації використовує детектор на основі вікна, що рухається (sliding window detector). Це допомагає переформулювати задачу локалізації в задачу класифікації в регіоні, що надає високу точність, але вимагає більше обчислювальних ресурсів. Faster R-CNN являє собою суму детектора та класифікатора. Алгоритм Faster R-CNN є точнішим за YOLO, але більш повільнішим, що не дає змоги працювати ефективно з відео потоком, а при роботі із зображеннями може виникати короткочасна затримка.

Описані алгоритми є доступними для загального використання. Їх можна завантажувати і для більшої точності дотреновувати нейронні мережі,

на яких вони базуються, на власних даних. Також алгоритми можна завантажити разом із навченими параметрами та зразу використовувати.

Запропонований підхід до маркування зображень складається із кроків:

1. Налаштування середовища маркування, для отримання необхідних інструментів та обрання алгоритму автоматизації, відповідно до заданих параметрів.

2. Автоматизоване маркування зображення, для отримання його первинного опису, що включає класи об’єктів, їх ключові точки та обмежувальні блоки.

3. Ручне корегування опису зображення, отриманого на попередньому кроці.

4. Збереження файлу опису зображення у зазначеному форматі.

Для налаштування середовища маркування, перед початком роботи, вказується тип задачі, що виконується, це може бути або класифікація, або локалізація. Тип задачі визначає вихідні параметрів. Для задачі класифікації вихідним параметром є лише назва класу до якого належить об’єкт, що знаходиться на зображенні. Для задачі локалізації вихідними параметрами є назва класу об’єкту, координати центру, ширина та довжина обмежувального блоку навколо об’єкта. Також вхідним параметром є множина назв класів можливих об’єктів, що можуть бути присутніми на зображеннях. Використовуючи назви класів алгоритми автоматизованого маркування будуть їх виділяти серед всіх інших об’єктів на зображенні. Для збереження вихідного файлу опису зображень потрібно вибрати його формат, який придатний для подальшого використання.

Запропонований підхід дозволяє підвищити швидкість маркування зображень, для подальшого їх використання при навчанні або тестуванні НМ.

Подальша робота буде полягати у підвищенні точності і швидкості класифікацій та локалізації об’єктів, за рахунок зміни кількості шарів НМ, використання технік зменшення розмірності або інших архітектур НМ. Також планується додати можливості маркування зображень, для задачі сегментації.

Література

1. Computer Vision for Human Computer Interaction Karlsruhe Institute of Technology. Sloth [Електронний ресурс] – режим доступу: http://sloth.readthedocs.io/en/latest/, вільний.
2. Tzu Ta Lin. LabelImg [Електронний ресурс] – режим доступу: https://github.com/tzutalin/labelImg, вільний.
3. K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition”, arXiv:1512.03385, 2015.
4. Joseph Redmon, Santosh Divvala, Ross Girshick, Ali Farhadi, “You Only Look Once: Unified, Real-Time Object Detection”, arXiv:1506.02640, 2015.
5. Shaoqing Ren, Kaiming He, Ross Girshick, Jian Sun, “Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks”, arXiv:1506.01497, 2015.

УДК 261.396

РЕАЛІЗАЦІЯ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ ДЛЯ ВІДЕО З ВИКОРИСТАННЯМ СИНГУЛЯРНОГО РОЗКЛАДАННЯ

Лісковський І.О., Кулик М.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: lisaknod@gmail.com, maryna.kulyk2015@gmail.com

Implementation of steganographic system for video using singular value decomposition

In this paper a video steganography methodology using singular value decomposition (SVD) and discrete wavelet transform (DWT) is presented. The final results have been plotted and compared between peak signal to noise ratio (PSNR) with embedding strength and mean square error (MSE) with embedding strength. Experimental results indicate that the proposed steganography method provides high level of imperceptibility and robustness against many existing methods.

У даній статті представлена методологія відео-стеганографії з використанням сингулярного розкладу (SVD) та дискретного вейвлет-перетворення (DWT). Отримані результати були представлені графіками та порівняні між піковим відношенням сигнал / шум (PSNR) з стійкістю вбудовування та середньоквадратною помилкою (MSE) з стійкістю вбудовування. Експериментальні результати показують, що запропонований метод з використанням сингулярного розкладу (SVD) та дискретного вейвлет-перетворення (DWT), забезпечує високий рівень непомітливості та стійкості на відміну від багатьох існуючих методів.

Спочатку оригінальний відео-файл було перетворено в групу з P-кадрів, після чого площини RGB були розділені і розкладені у різних діапазонах частот за допомогою дискретного вейвлет перетворення (ДВП). Для отримання трансформованого коефіцієнта застосовується дискретне косинусне перетворення (ДКП) на обраних частотних діапазонах, потім сингулярний розклад забезпечує сингулярні значення на наступному етапі.

Для отримання стего-фрейму використовується наступний вираз:

$$M(i, j) = So(i, j) + \alpha * Sw(i, j),$$

де M(i, j) - стего-фрейм; So(i, j) - сингулярні значення площини R, G, B кожного кадру в відео; Sw(i, j) - сингулярні значення площини R, G, B окремих водяних знаків; α - масштабний коефіцієнт.

Для вилучення вбудованого зображення застосовується зворотна процедура. Виділений файл можна отримати за допомогою наступного виразу:

$$Sw(i, j) = (M(i, j) – S0(i, j)) / \alpha .$$

Дослідження проводилося з використанням пакету Matlab R2012b. Щоб оцінити продуктивність, спочатку була проведена візуальна оцінка оригінального відео-файлу та файлу з вбудованим ЦВЗ. Але цей тест є чисто суб'єктивний за своїм характером і, отже, недостатнім. Тому для перевірки ефективності методу необхідні деякі раціональні методи.

Щоб оцінити продуктивність запропонованої методики були використані такі характеристики як пікове відношення сигналу до шуму (PSNR) і середньоквадратична помилка (MSE). Пікове відношення сигнал/шум необхідний для обчислення якості вилученого зображення у порівнянні з оригінальним прихованим зображенням. Пікове відношення сигнал/шум PSNR обчислюється за допомогою наступного виразу:

$$PSNR = 10 \log10 (2552 /MSE),$$

де MSE - середньоквадратична помилка між початковим зображенням І розміру M × N та виділеним зображенням оцінюється за формулою:

$$MSE = \frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - I_s(i,j)\right)^2\right].$$

Експериментальні значення MSE та PSNR стосовно вбудовування узагальнені в наступній таблиці.

Таблиця 1 Значення середньоквадратичної помилки та пікового відношення сигнал/шум

Embedding Strength	MSE	PSNR
0.1	.0161	152.13
1	0.161	129.10
2	0.3214	122.17
3	0.4821	118.12
4	0.6428	115.24
5	0.8035	113.01
6	0.9643	111.18
7	1.1250	109.6478
8	1.2857	108.3125
9	1.4464	107.1346
10	1.6071	106.0810

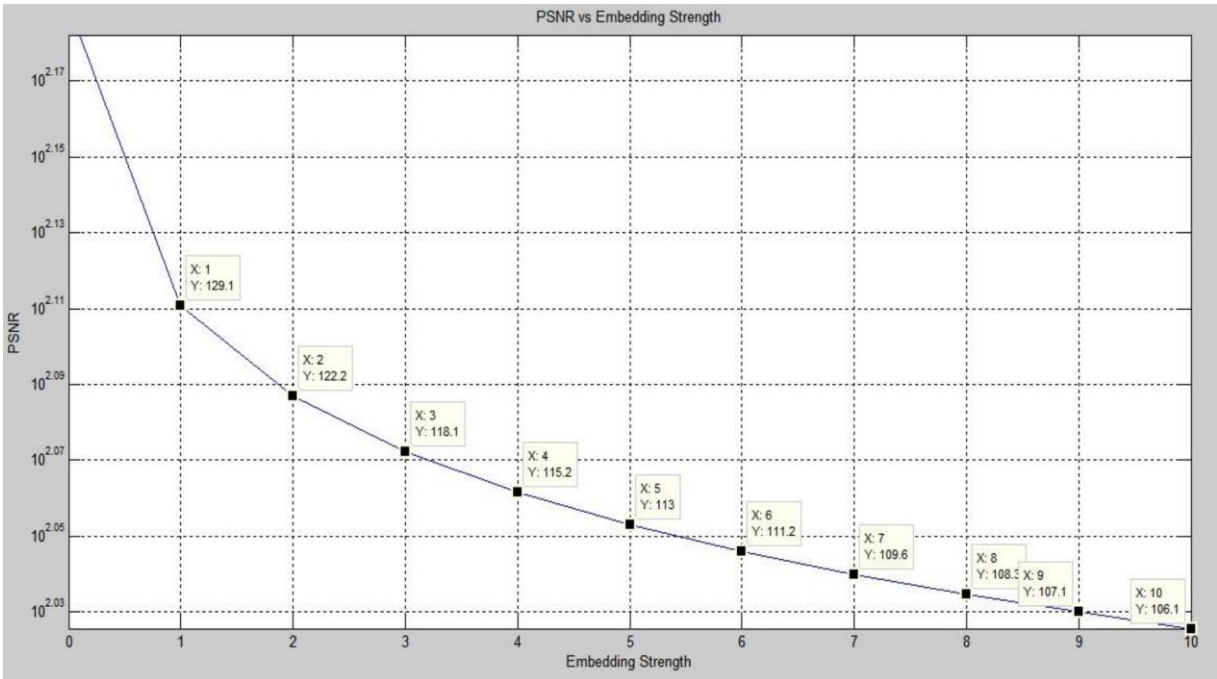


Рис. 1. Пікове відношення сигнал / шум та стійкість вбудовування

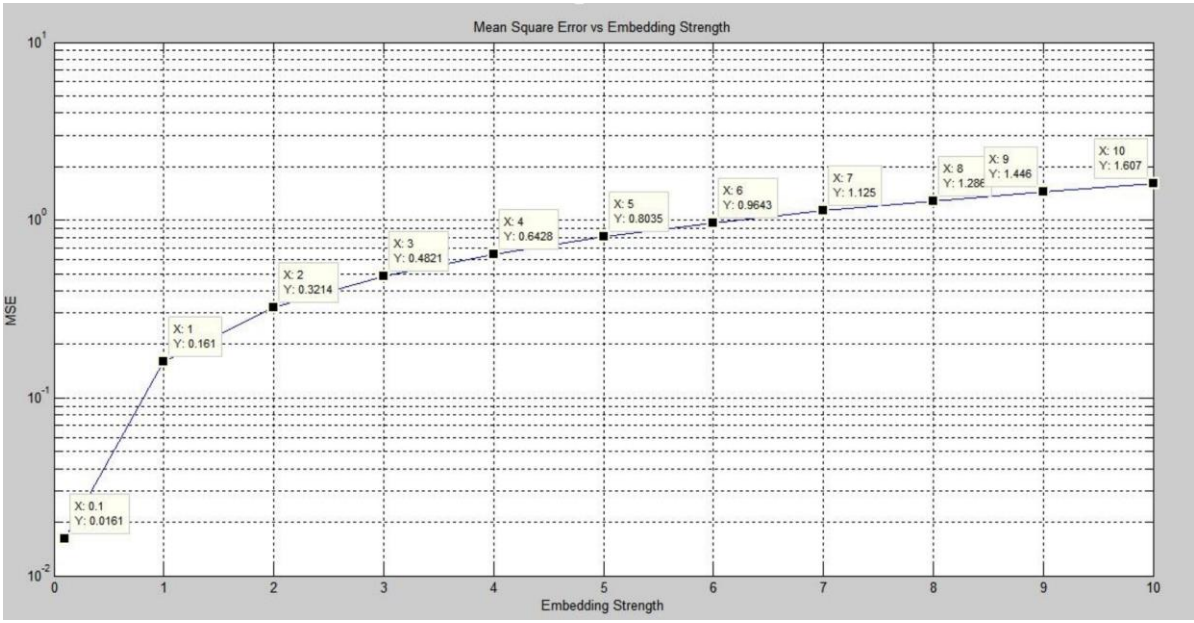


Рис. 2. Середньоквадратична помилка та стійкість вбудовування

З рисунків видно, що в міру збільшення стійкості вбудовування середньоквадратична помилка також збільшується, але пікове відношення сигнал / шум зменшується.

В статті представлений метод стеганографії відео на основі сингулярного розкладання, що використовує дискретне вейвлет-перетворення та дискретне косинусне перетворення. Це менш складний метод порівняно з багатьма іншими існуючими методами відео-стеганографії. Крім того, застосування дискретного вейвлет-перетворення робить наш метод обчислювально реальним. Результати експерименту вказують на те, що система на основі дискретного вейвлет-перетворення та сингулярного розкладу має більше непомітності, що призводить до підвищення рівня захищеності системи.

Література

1. Diljeet Singh, Navdeep Kanwal, “Dynamic Video Steganography Using LBP on CIELAB Based K-Means Clustering”. IEEE 2016.
2. Dhanya Job, Varghese Paul, “An Efficient Video Steganography Technique for Secured Data Transmission”. IEEE 2016.
3. Ramandeep Kaur, Pooja, Varsha, “A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques”. IEEE 2016.
4. Diksy M. Firmansyah, Tohari Ahmad, “An Improved Neighbouring Similarity Method for Video Steganography”.
5. Ramadhan J. Mstafa, Khaled M. Elleithy, “A Novel Video Steganography Algorithm in DCT Domain Based on Hamming and BCH Codes”. IEEE 2016.
6. Liyun Qian, Pei Zhou, Jian Chen, Zhitang Li, “An Improved Matrix Encoding Steganography Algorithm Based on H.264 Video”. IEEE 2016.

УДК 004.7

ОСОБЕННОСТИ ВНЕДРЕНИЯ ТЕХНОЛОГИИ WI-FI НА ОСНОВЕ СТАНДАРТА 802.11AX

Мындру М.А., Курдеча В.В.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: nick-myndru@yandex.ru

Features of the introduction of Wi-Fi technology based on the standard 802.11ax

The article briefly describes the features and benefits of the new wireless standard Wi-Fi 802.11ax, designed to increase the data transfer speed four times in places where users are crowded.

На сегодняшний день всё шире распространяются локальные беспроводные сети, использующие радиочастоты для передачи данных. Одно из основных преимуществ сетей WLAN, как следует из их названия, заключается в том, что они являются беспроводными. Однако беспроводная сеть имеет некоторые серьезные недостатки по сравнению с традиционным Ethernet.

В то время как 802.11ac теоретически поддерживает Ethernet-эквивалентную скорость одного гигабита в секунду или 1 Гбит / с, гораздо более популярный стандарт 802.11n поддерживает максимальную скорость 600 Мбит / с - чуть более половины скорости 802.11ac , В реальных приложениях беспроводная сеть значительно медленнее, чем проводная сеть при передаче файлов по локальной сети. Проблема становится еще более острой, если у вас оживленная сеть или уровень сигнала слабее оптимального.

Максимальная пропускная способность сети, доступная через единую точку беспроводного доступа в стандарте 802.11b / g, составляет 54 Мбит / с и используется всеми пользователями, подключенными к этой точке доступа. Стандартный проводной сетевой порт обеспечивает коммутируемую пропускную способность 100 Мбит / с.

Поскольку пользователи беспроводного доступа к сети имеют доступную пропускную способность, производительность сети может быть уменьшена по мере подключения дополнительных пользователей беспроводной связи к точке доступа. Приложения с интенсивной полосой пропускания уменьшают доступную общую пропускную способность для всех пользователей в зоне покрытия. Фактическая пропускная способность в зонах покрытия беспроводной сети будет варьироваться в зависимости от количества пользователей и типов приложений, используемых на клиентских компьютерах. Клиентские компьютеры, использующие только адаптеры 802.11b, значительно уменьшат доступную пропускную способность из-за того, как стандарт 802.11b/g был разработан для поддержки обратной совместимости. Как таковой, CSSD рекомендует, чтобы клиентский адаптер поддерживал 802.11b/g в качестве предпочтительного метода доступа. Беспроводные сетевые системы хорошо работают для работы с низкой пропускной способностью, таких как просмотр веб-страниц и электронная почта. Мероприятия с высокой пропускной способностью, включая потоковое видео, совместное использование MP3 и видеоконференции, скорее всего,

приведут к снижению производительности и должны быть обескуражены подразделениями университета до тех пор, пока отраслевые стандарты и оборудование не станут доступны для поддержки этих мероприятий. Текущая технология беспроводной сети позволяет 15-25 пользователям эффективно использовать единую точку беспроводного доступа (рис 1), несмотря на то, что поставщики утверждают, что гораздо большее число пользователей может связываться с одной точкой беспроводного доступа.

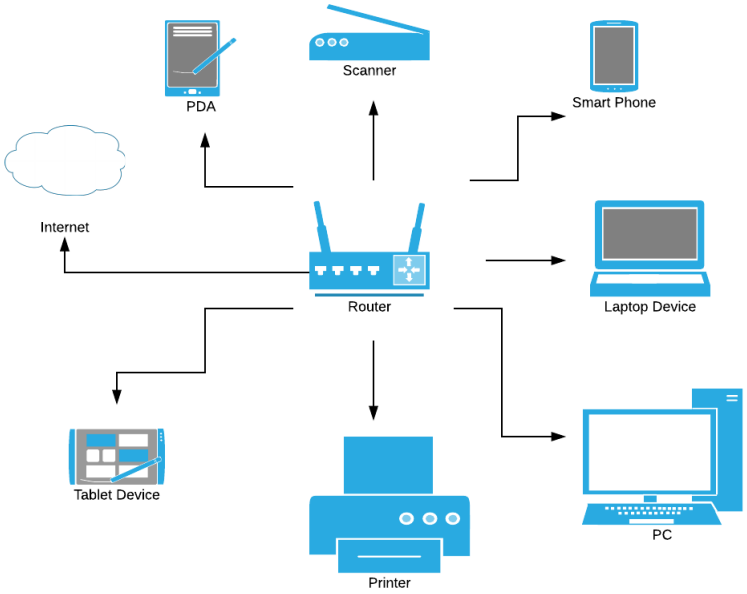


Рис. 1. Загруженность сети

Новый стандарт беспроводных сетей IEEE 802.11ax направлен на повышение скорости обмена данными в местах большого скопления пользователей (рис 2).

Рис. 2. Пример объекта с высокой плотностью пользователей

Помимо повышения скорости передачи данных новый стандарт реализует несколько механизмов для обслуживания большего количества пользователей и повышения надежности передачи данных в беспроводных сетях (рис 3). В стандарте 802.11ax применяется технология MU MIMO и для передачи в восходящем канале (Uplink Multi-user Multiple Input Multiple Output, UL MUMIMO), т.е. от пользователей к точке доступа. Кроме того, для того чтобы

более эффективно использовать широкий частотный диапазон и бороться с частотноселективными замираниями и интерференцией, впервые будет применяться множественный доступ с ортогональным частотным разделением (Orthogonal Frequency-Division Multiple Access – OFDMA)

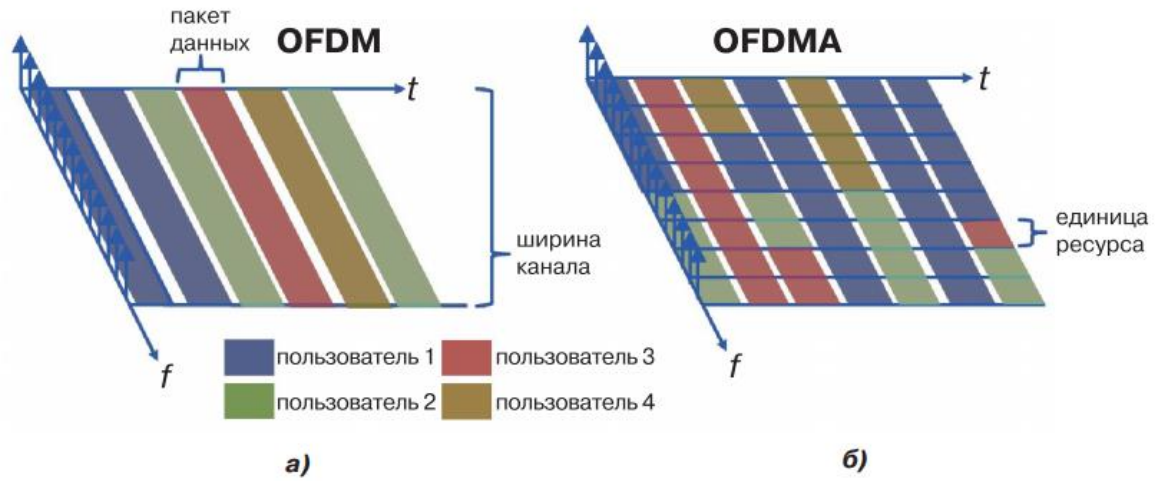


Рис. 2. Один пользователь, использующий канал с использованием OFDM (а) и мультиплексирование различных пользователей в одном канале с использованием OFDMA (б)

При планировании сетей 802.11ax предполагается наличие сильно неоднородного трафика, в то время как в предыдущих версиях Wi-Fi, как правило, учитывался только один тип трафика (например, видеотрансляция в режиме реального времени, загрузка файлов или просмотр веб-страниц). Еще одной особенностью IEEE 802.11ax является интенсивное использование восходящего канала в современных беспроводных сетях. Это объясняется многочисленными загрузками фото, видео и документов в социальные сети и облачные сервисы.

В следствии вышесказанного одной из основных целей разработчиков стандарта 802.11ax является увеличение пропускной способности для пользователей в 4 раза в местах с плотным размещением точек доступа. С этой целью все устройства 802.11ax поддерживают работу по нисходящей линии связи Uplink MU-MIMO и MUOFDMA для увеличения числа одновременно подключенных пользователей. Для повышения производительности сетей Wi-Fi с плотным размещением точек доступа стандарт 802.11ax содержит ряд методов, которые повышают эффективность использования канальных ресурсов сетями с перекрывающимися областями радиовидимости (Overlapped BSS – OBSS).

Литература

1. А.Г. Кирьянов, А. И. Ляхов, Д. А. Михлина, Е. М. Хоров, И.А. Щелкина Проблемы создания IEEE 802.11ax — нового поколения сетей Wi-Fi / Инфор- мационные процессы, Том 16, № 1, 2016, стр. 1–12.
2. Типы фреймов сети стандарта IEEE 802.11. – http://wi-life.ru/texnologii/wi-fi/wi-fi-frames-management-control-data.
3. Wi-Fi with 802.11ax means unprecedented capacity and better efficiency. – https://www.qualcomm.com/products/features/80211 ax

УДК 621.396.1

ОНТОЛОГІЧНА МОДЕЛЬ МОДЕЛЮЮЧОГО КОМПЛЕКСУ ДЛЯ ІДЕНТИФІКАЦІЇ МОРСЬКИХ ОБ'ЄКТІВ

Філімонов М. Ф.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: filimonovkolya97@gmail.com

В даній роботі розглядається один підхід до розробки інтелектуальної системи моделювання предметної області. Передбачається використання такої системи для ідентифікації, визначення типу об’єкта та частини його параметрів. В процесі моделювання використовується онтологічна модель, за допомогою якої можливо сформувати та розділити дані та представленні знання, описати більшість концептуальних проблем предметної області, та перевірити взаємозв’язки наявні в системі.

В сучасному світі існує велике різноманіття предметних областей, для автоматизації роботи з даними яких необхідно розробити спеціальні системи моделювання. Для розробки таких систем існує потреба в використанні не лише класичних математичних методів моделювання, а й специфічних засобів розробки експертних систем на основі глибшого використання знань. Такий підхід необхідно використовувати і при розробці моделюючої системи для ідентифікації та класифікації морських об’єктів.

Моделююча система для ідентифікації та класифікації морських об’єктів має вирішити реалізовувати автоматизовану роботу над дослідницьким процесом та його безпосереднє керування, а саме створення потрібних сцен та сценаріїв. Також, необхідно передбачити автоматизацію процесу моделювання функціонування гідроакустичних сигналів відповідно до водного простору та даних морського середовища.

У статті розглянуто підхід до створення систем моделювання з використанням онтології. Цей підхід передбачає:

- Розробку концептуальної моделі знань, відповідно до її специфіки.
- Формалізацію знань з використанням моделі, для ідентифікації та класифікації об’єктів.
- Реалізацію компонентів системи моделювання, для зменшення витрат за допомогою деяких готових рішень.

ОНТОЛОГІЧНА МОДЕЛЬ СИСТЕМИ МОДЕЛЮВАННЯ

Онтологічна модель використовує дані та знання , які збираються під час моделювання. Онтологія дозволяє формально описати будь які поняття, групи класів, відношення між об’єктами та типами, елементи класів та інше.

Формально онтологію можна описати наступною залежністю:

$$O = \{C, T, A, F, R\},$$

C – це набір класів, які описують нашу предметну область;

T – це сукупність стандартних типів та значень атрибутів;

A – це набір атрибутів, тих типів та об’єктів які знаходяться в нашій системі;

F – набір меж для наших атрибутів;

R – сукупність відносин в предметній області

Онтологічна модель предметної області для моделюючої системи для ідентифікації та класифікації морських об’єктів представлена на Рис. 1.

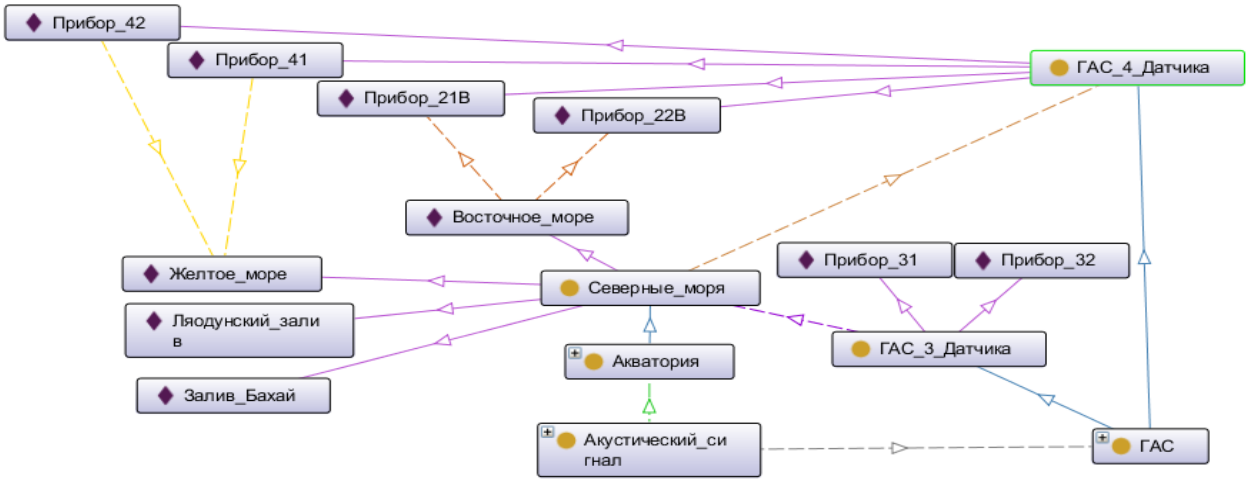


Рис. 1. Онтологічна модель предметної області

Опишемо елементи онтологічної моделі предметної області. Для онтологічної моделі визначено наступні класи та атрибути класів:

1. Акваторія – C_1 Клас має наступні атрибути:
   - тип – A_1,
   - рельєф – A_2.
2. Море – C_2 Клас має наступні атрибути:
   - тип – A_1,
   - рельєф – A_2.
3. Акустичний сигнал – C_3 Клас має наступні атрибути:
   - Амплітуда – A_1,
   - Час фіксації – A_2,
   - Тиск – A_3,
   - Фаза – A_4,
   - Частота – A_5.
4. ГАС – C_4
5. ГАС Датчик – C_5

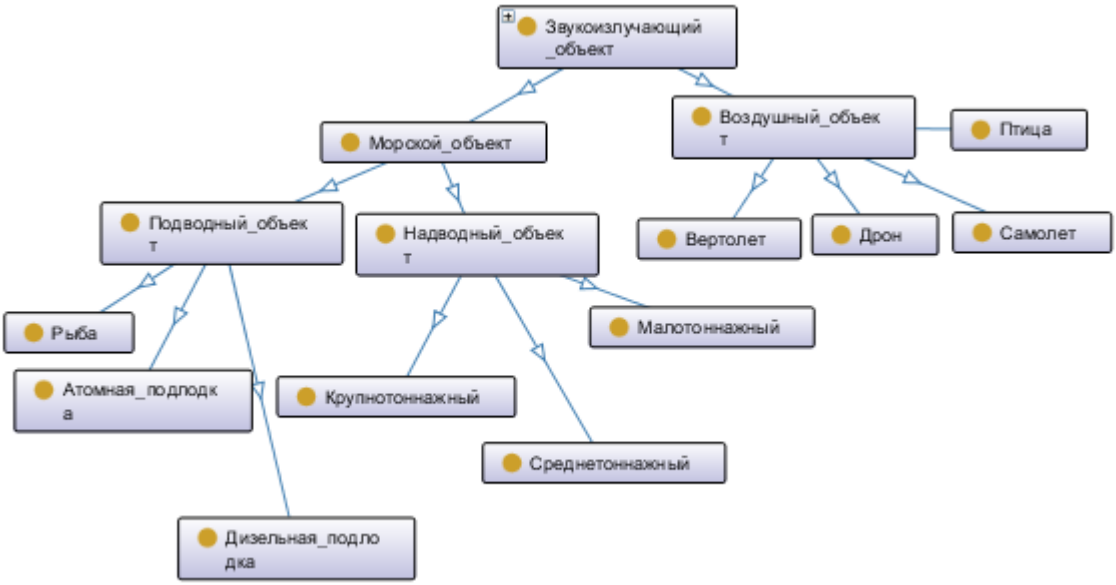


Рис. 2 – Онтологічна модель предметної області

6. Звуко-випромінюючий Об’єкт – C_8 Клас має наступні атрибути:
   - частота сигналу – A_1,
   - спектрально-енергетичні характеристики – A_2,
   - векторно-фазові характеристики – A_3,
   - відстань – A_4,
   - швидкість – A_5,
   - тиск – A_6,
   - напрямок руху – A_8.
7. Морський об’єкт – C_9
8. Повітряний об’єкт – C_{10}
9. Підводний об’єкт – C_{11}
10. Надводний об’єкт – C_{12}

Определенно следующее множество данных:

Для класса «Прибор» – C_5: прибор_1 – D_1, прибор_2 – D_2,…, прибор_n – D_n;

Для класса «Моря» – C_2: N – количество морей;

Определенно следующие виды отношений:

I. Отношение типа *“is-are” (класс-подкласс)* - R^{ia}

Отношением этого типа связаны класс «Объект» и его подклассы «Надводный объект», «Подводный объект», «Воздушный объект» - R^{ia}_1.

II. Отношение типа *“класс-данные”* - R^{cd}

Отношением этого типа связанны все классы и подклассы модели со своими данными.

III. Отношение *“установлен в”* типа – R^{in}

Это отношение связывает объект или класс с местом в котором оно размещено.

IV. Отношение типа *“Зафиксирован датчиком ”* R^d

V. Отношение типа *“Зафиксирован в акватории ”* R^{da}

Это отношение связывает датчик и снятый с ним сигнал с тем где он зафиксирован.

VI. Отношение типа *“Наблюдается ГАС”* R^{lg}

Розроблена онтологічна модель являє собою предметну область у термінах бази знань, що дає змогу описати суб’єкти предметної області в умовах концептів. Використовуючи відношення описані в онтології можна використовувати алгоритми описової логіки для обробки даних онтології.

ВИСНОВКИ. У роботі запропоновано підхід до розробки моделюючої системи для ідентифікації та класифікації морських об’єктів. Інтелектуальна система моделювання дозволяє класифікувати морські об'єкт для їх визначення на основі їх параметрів. Запропоновано онтологічну модель моделюючої системи, описано елементи онтології, такі як класи, атрибути, відношення різного типу та ін. Подальші дослідження будуть пов'язані організацію логічних висновків на основі онтології, для реалізації пошуку по моделюючій системі.

Література

1. Globa, L., Kurdecha, V., Ishchenko, I., Zakharchuk, A. An approach to the Internet of Things system with nomadic units developing. 2017. 14th International Conference The Experience of esigning and Application of CAD Systems in Microelectronics, CADSM 2017 - Proceedings 7916127, c. 248-250
2. V.R. Senchenko·O.V. Koval L.S. Globa·R.L. Novogrudska Intelligent modeling system based on cloud-technology, Prosedings of International Conference Radio Electronics & Info Communications" (UkrMiCo), DOI:10.1109/UkrMiC.2016.7739646, IEEE Digital Library, 2016
3. Y.A. Zagogulko, O.I. Borovikova The technology of ontologies constructing for the Internet portals of scientific knowledge // Jornal of NGU: Informational technologies. - 2007. – V. 5, issue 2. – P.12
4. L. Globa, R. Novogrudska, O. Oriekhov Method of heterogeneous information resources structuring and systematizing for Internet portals development, 978-1- 4673-2232-4/13/$31.00 ©2013, IEEE, EuroCon 2013, 1-4 July 2013, Zagreb, Croatia, p. 319-326
5. A. Koval, V/ Senchenko, A/ Gagarin, V. Gaydargu Gathering and processing of information on marine moving facilities – presentation, IEEE BlackSeaCom 2017 – International Black Sea Conference on Communications and Networking 5-8 JUNE 2017 // ISTANBUL, TURKEY
6. Namrata Rastogi, Dr. Parul Verma, Dr. Pankaj Kumar, Analyzing ontology editing tools for effective semantic information retrieval: International Journal of Engineering Sciences & Research Technology http: // www.ijesrt.com

УДК 621.391.3

СИСТЕМА РАННЬОГО РЕАГУВАННЯ З ХМАРНИМ СХОВИЩЕМ ДАНИХ

Пльотка Б.С., Курдеча В.В.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: bplotka.1996@gmail.com

WIRELESS CLOUD MONITORING SYSTEM

The article describes the early response system with a cloud data warehouse, and the ability to connect through the web interface. Describes the main software and hardware components of the system.

У статті наводиться опис системи раннього реагування з хмарним сховищем даних, та можливістю підключення через веб-інтерфейс. Описуються основні програмні та апаратні компоненти системи.

Система раннього виявлення - це система, що забезпечить попередження певного не стандартного стану середовища. Це дозволить власнику системи прийняти рішення щодо будь-якого вимірювання датчика ля того, щоб мінімізувати збиток або повністю уникнути катастрофи. Система здатна визначати та передбачати критичний стан. Перехід в критичний стан дасть лише грошовий збиток або психологічний збиток для особи чи організації. Система раннього виявлення здатна попередити чи звести шкоду до мінімуму.

Хмарні системи(ХС) та Інтернет речей (IoT) є двома поняттями, які з'явилися відносно нещодавно, і вони є основною інформаційною технологічна індустрією нового покоління. IT тісно пов'язаних з хмарними обчисленнями, таким чином, що IoT отримує потужний обчислювальні засоби через хмарні обчислення та хмарні обчислення знаходить найкращий практичний канал на основі IoT [1].

Моніторинг діяльності визначає зміни у навколишньому середовищі. Ці дані можуть зберігатися і використовуватися для кількох цілей. Розвивати нові розширені сервіси для інтелектуальних середовищ, збирати дані під час діяльності з моніторингу необхідно зберігати, обробляти та співвіднесені з різними відомостями, які характеризують або впливати на навколишнє середовище[2].

На рис 1 показана ілюстрація загальної системи архітектури хмарної системи моніторингу.

Опис потоку виглядає наступним чином:

1. Він починається з пристрою моніторингу, де всі підключені датчики. Всі дані зібрані з датчиків будуть групуватись.

2. Він буде передаватися на сервер бази даних за допомогою мереж.

3. Сервер бази даних буде служити як сховище, що зберігатиме дані, зібрані пристроєм моніторингу. Оскільки база даних знаходиться в Інтернеті, до неї можна отримати доступ з будь-якої точки світу і в будь-який час.

4. Веб-сайт був розроблений, щоб дати можливість оцінити та здійснювати моніторинг. Наявні інструменти для відображення здатні відображати всі дані зібрані у вигляді графів і таблиці. Графік може бути показаний для забезпечення поточного статусу району моніторингу.

Подібна архітектура не накладає обмежень на обмежень на жоден з ключових вузлів архітектури. Кожен вузол може бути замінений з мінімальними затратами ресурсів та модифікаціями інших вузлів системи.

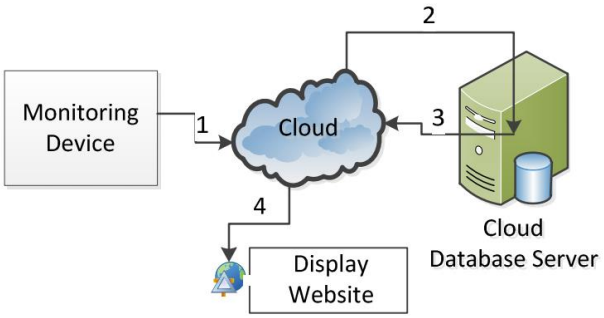


Рис.1 Загальна архітектура системи

З загальної архітектури системи існує два основних компоненти, необхідні для роботи системи. Компоненти - це апаратне та програмне забезпечення. Апаратна частина складається з модуля сенсора, модуль обробки та модуль передавача. Програмне забезпечення складається з програми для основної плати, програми на стороні сервера та програми на веб-сайті для відображення даних.

З рис. 1 показано, що апаратне забезпечення існує лише в пристрої моніторингу, інші частини більше стосуються впровадження програмного забезпечення.

Основні модулі

- модуль зондування, що включає в себе пристрій моніторингу;
- модуль обробки;
- модуль передачі.

Модуль зондування складається з декількох датчики та цифрова перетворювальна схема. Датчики використовуються для перетворення даних, зібраних у середовищі, та перетворює в аналогові дані, в той час як перетворювальна схема використовується для перетворення аналогових даних на цифрові дані.

Модуль обробки в основному є мікроконтролером з декількома вхідними та вихідними комунікаційними портами. Модуль обробки керує потоком даних від датчика до передавального модулю.

Модуль обробки повинен бути невеликим за розміром та використанням енергії, повинен також мати простий процес експлуатації.

Модуль передавача керує зв'язком між модулем обробки та базою даних. Він створює онлайн бази даних. Дані, що походять від модуля обробки та надсилає до бази даних і зберігає в конкретні таблиці. Ці таблиці пізніше використовуватиме клієнт для відображення візуальних графіків.

Модуль програмного забезпечення призначений для обробки потоку даних. Безшовний алгоритм щоб забезпечити безперебійну роботу системи без втручання людини протягом тривалого часу.

Порядок роботи системи описується наступним чином:

1. Модуль обробки отримає дані від датчики, коли запит модуля обробки.

2. Дані від датчика буде відформатовано на материнській платі в формі корисної інформації, і вона знаходиться у форматі HTTP-запиту.

3. Корисне навантаження буде упаковане разом із послідовним протоколом зв'язку і передається на модуль передачі інформації.

4. Передавальний модуль виділяє корисне навантаження і відправити його в онлайн базу даних.

5. Онлайн база даних, після отримання відформатованого корисного навантаження, зберігає його в своїй базі даних. Пізніше дані будуть оброблятися на основі конфігурація, визначена базою даних.

6. Сайт використовується для відображення всіх даних, що зберігаються в базі даних. Цей веб-сайт покаже всі дані, які обробляються базою даних. Це забезпечить легкий доступ до даних, і кінцевий користувач може аналізуйте дані за допомогою шаблону на веб-сайті відображення.

Висновок. В статті система раннього реагування з хмарним сховищем даних, та можливістю підключення через веб-інтерфейс. Описана архітектура, та основні апаратні та програмні елементи системи.

Запропонована архітектура забезпечує незалежність окремих модулів системи, простоту доступу до опрацьованих даних, що в свою чергу забезпечує більш швидке реагування на критичні чи потенційно критичні стани системи, для мінімізації шкоди від них.

Література

1 .Fan Tongke, “Smart Agriculture Based on Cloud Computing and IOT,” Journal of Convergence Information Technology (JCIT), vol8., issue2, no 2, pp. 1-5, Jan 2013.

2. A. Celesti, A. Puliafito, M. Villari, “Big Data Storage in the Cloud for Smart Environment Monitoring,” Procedia Computer Science, Elsevier, Vol 52, 2015, pp. 500-506.

УДК 621.391.3

ВИБІР АЛГОРИТМУ МАШИННОГО НАВЧАННЯ ДЛЯ ЗАСТОСУВАННЯ ПРИ ОБРОБЦІ ДАНИХ В ПІДМЕРЕЖІ IOT

Бугаєнко Ю.М., Курдеча В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yura.buhaenko@gmail.com

CHOICE OF MACHINE EDUCATION ALGORITHM FOR APPLICATION FOR DATA PROCESSING IN THE IOT NETWORK

The article describes the choice of machine learning algorithm for application in the proposed data processing method in the IoT subnet to further reduce the load on the information processing server.

У статті наводиться опис вибору алгоритму машинного навчання для застосування у запропонованому методі обробки даних в підмережі IoT для подальшого зменшення навантаження на сервер обробки інформації.

Сенсорні мережі і вузли IoT (Internet of Things) продукують величезні обсяги інформації, що генеруються з вбудованих або носимих розумних пристроїв і корпоративних банків даних. Отримати корисну інформацію з таких обсягів данних стає все важче, а проблема аналізу данних є однією із ключових на данному етапі розвитку інтернету речей. У деяких випадках, інтерактивне управління та обробка данних може знадобитися в реальному часі, наприклад в областях, що мають особливе значення, наприкад системи спостереження за здоров’ям чи в системи безпеки. Але в інших випадках це не є визначаючим фактором, тому використовуються різні методи для зменшення кількості оброблюваних данних задля зменшення навантаження на обчислювальну мережу.

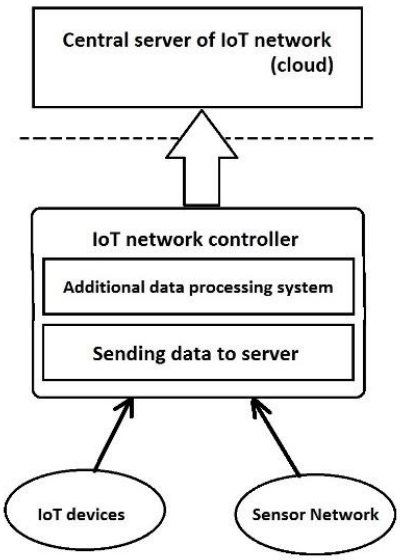


Рис. 1. Модифікована схема передачі і обробки даних в IoT

У попередній роботі [1] було запропоновано вирішувати данну проблему на стороні підмережі IoT і з застосуванням алгоритмів злиття даних. В новій роботі, для досягнення універсальності системи прийняття рішень а також покращення її якісних показників, було вирішено перенести її на алгоритми машинного навчання (Рис 1).

При виборі алгоритму який слугуватиме базою для даного способу обробки даних потрібно враховувати складність алгоритму. Оскільки в таких мережах, центральний вузол має не надто великі обчислювальні можливості, то вибраний алгоритм має бути максимально простим, але при цьому достатньо точно аналізувати різні параметри в даних що надходять[2]. Насправді, будь-які підходи до машинного навчання роблять одне і теж. У нас завжди є дві основні речі: По-перше, це набір гіпотез. Це може бути набір функцій, або набір ваг для нейронів нейронної мережі, або набір всіляких вирішальних дерев. Залежить від конкретного підходу. По-друге, у нас є набір навчальних даних. Наше завдання завжди зводиться до одного: визначити, яка ж з наших моделей найбільш адекватна нашим навчальних даних.

Після огляду і порівнянні деяких алгоритмів, для застосування його в данному способі обробки данних, був обраний Наївний баєсів класифікатор. Байєсівський підхід дає точний чисельний критерій для вирішення цього завдання.

Наївний байесовский алгоритм - це алгоритм класифікації, заснований на теоремі Байеса з припущенням про незалежність ознак. Моделі на основі НБА досить прості і вкрай корисні при роботі з дуже великими наборами даних. При своїй простоті НБА здатний перевершити навіть деякі складні алгоритми класифікації. Це і стало вирішальним фактором для вибору саме цього алгоритму. З точки зору машинного навчання теорему Байєса можна застосувати до машинного навчання таким чином: позначимо наші дані - D, а наші гіпотези - h. Тоді нам потрібно знайти вірогідність гіпотез наших даних p (h | D), яка за теорією Байеса рівна:

$$p(h|D) = \frac{p(D|h)\,p(h)}{p(D)}$$

Нас цікавить тільки співвідношення ймовірностей, тому ми можемо викинути з цього виразу p (D) (D не залежить від h) і p (h) (будемо вважати, що всі гіпотези різновірогідні; строго кажучи, це не завжди так, ми ще повернемося до цього питання, але в багатьох випадках це справедливо) [3]. Виходить, що нам треба знайти таку гіпотезу h, для якої максимально p (D | h). Говорячи математичною мовою, ми повинні для кожної гіпотези обчислити її апостеріорну ймовірність і вибрати гіпотезу, для якої ця ймовірність максимальна.

Розглянемо переваги і недоліки Байєсового класифікатора більш детально:

Позитивні сторони:

•Класифікація, в тому числі багатокласова, виконується легко і швидко. Це дозволяє прогнозувати ймовірність для безлічі значень цільової змінної.

•Коли допущення про незалежність виконується, НБА перевершує інші алгоритми, такі як логістична регресія (logistic regression), і при цьому вимагає менший обсяг навчальних даних.

•НБА краще працює з категорійними ознаками, ніж з безперервними. Для безперервних ознак передбачається нормальний розподіл, що є досить сильним допущенням.

•Класифікація в режимі реального часу. НБА дуже швидко навчається, тому його можна використовувати для обробки даних в режимі реального часу.

Негативні сторони:

•Якщо в тестовому наборі даних є певне значення категорійного ознаки, яке не зустрічалося в навчальному наборі даних, тоді модель присвоїть нульову ймовірність цього значення і не зможе зробити прогноз. Це явище відоме під назвою «нульова частота». Дану проблему можна вирішити за допомогою згладжування. Ще одним обмеженням НБА є припущення про незалежність ознак. В реальності набори повністю незалежних ознак зустрічаються вкрай рідко.

Висновки. В даній статті був запропонований спосіб обробки данних на стороні підмережі IoT який базується на Наівному байєсовському критерії. Даний спосіб має декілька вагомих переваг, головними з яких є зменшення, за рахунок його використання обсягів даних, що в свою чергу зменшуватиме навантаження на сервер обробки інформації, та безпровідну мережу. Також суттєвою перевагою даного способу є те, що його імплементація може проходити без додавання додаткових фізичних пристроїв до системи Internet of Things.

Література

1. Бугаєнко Ю.М., «Модифікована структура мережі IoT для зменшення навантаження на мережу», ст 32-38, Київ 2016
2. Fan Tongke, “Smart Agriculture Based on Cloud Computing and IOT,” Journal of Convergence Information Technology (JCIT), vol8., issue2, no 2, pp. 1-5, Jan 2013
3. Metechko I. Наивный байесовский классификатор [Електронний ресурс] / Igor Metechko – Режим доступу до ресурсу: https://sohabr.net/habr/post/262155/?version=109183.

УДК 621.396.1

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ НЕРЕЛЯЦИОННЫХ И РЕЛЯЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Новогрудская Р.Л., Добров Ю.А.
Институт телекоммуникационных систем КПИ им. Игоря Сикорского, Украина
E-mail: rinan@ukr.net, yuriydobrov@gmail.com

A benchmark comparison of NoSQL and SQL DBMS

The paper is devoted to comparing the performance of the most popular database management systems (DBMS) of nonrelational and relational data models. The big trend of Big Data has had a great impact on the development and spread of NoSQL databases. It is assumed that they are significantly ahead of traditional relational databases for performing data access operations. However, is it so? The purpose of this work is to perform benchmarks for measuring the time for create, read, update and delete (CRUD) operations for different volumes of data. As the results presents, just a few instances of NoSQL: MongoDB, Redis and Couchbase, really work faster than the traditional classical RDBMS MSSQL Server. CouchDB and RavenDB lost to the MSSQL Server in all tests. Cassandra and Hypertable were controversial in this comparison - they turned out to be slower than RDBMS with the exception of operations for writing large portions of data.

Потребность в хранении и обработке больших объёмов неструктурированных данных привела к созданию новых методик и технологий в области баз данных, такими являются NoSQL решения – системы управления базами данных (СУБД), которые отошли от традиционной реляционной модели данных, предложенной Эдгаром Коддом в 1969 году.

СУБД – это набор прикладных программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных.

На сегодняшний день можно выделить четыре основные категории NoSQL-хранилищ:

1. Key-value (ключ — значение). Является большой хеш-таблицей, в которой допустимы только операции записи и чтения данных по ключу.
2. Document-oriented (документо-ориентированные). Коллекции структурированных документов. Позволяют осуществлять выборку по различным полям документа, а также модификацию частей документа.
3. Column (колоночные). Таблицы с колонками и строками. Отличаются от SQL баз данных переменным количеством колонок для разных строк на уровне одного документа, каждая строка имеет уникальный ключ. Можно рассматривать данное решение как хеш-таблицу хеш-таблицы, первым ключом является ключ строки, вторым — имя колонки. При задании вторичных индексов возможны выборки по значению в колонке, а не только по ключу строки.

4. Graph (графовые). Данный тип БД специально предназначен для хранения математических графов: узлов и связей между ними.

Сравнительный анализ производительности нереляционных и реляционных СУБД проводился с целью оценки времени, необходимого для операций записи, чтения, изменения и удаления для разных объёмов данных. Для такой оценки было выполнено ряд тестов. Для замеров были взяты представители трёх вышеперечисленных категорий: MongoDB, RavenDb, CouchDB, Couchbase (документо-ориентированная), Cassandra, Hypertable (колоночные), Redis (ключ-значение). В качестве РСУБД был взят Microsoft SQL Server.

Реализация сравнения производительности была выполнена с использованием .NET, языка программирования C# и официальных драйверов для подключения к серверам тестируемых баз данных, взятые из NuGet Gallery. Для снятия показателей затраченного времени был использован .NET класс Stopwatch из пространства имён System.Diagnostics.

Тестовыми данными во всех базах являются автоматически сгенерированные строковые пары типа ключ-значения. Стоит отметить, что все результаты являются средним значением времени для трёх операций для каждой базы данных.

Результаты эксперимента показаны в сводных таблицах.

Табл. 1. Время на запись (мс)

База данных	Количество операций			
	10	100	10000	100000
MongoDB	58	76	2543	19876
RavenDb	566	1904	81290	738650
CouchDB	67	379	66478	912010
Couchbase	69	71	959	8382
Cassandra	120	238	9805	89341
Hypertable	56	198	10945	115321
Redis	34	65	980	13015
MSSQL Server	27	111	16732	219567

Табл. 2. Время на чтение (мс)

База данных	Количество операций			
	10	100	10000	100000
MongoDB	7	19	1020	9871
RavenDb	122	511	47200	423300
CouchDB	21	186	18670	17500
Couchbase	13	21	780	7000
Cassandra	111	318	19200	220190
Hypertable	56	102	3103	78450
Redis	5	46	439	4899
MSSQL Server	13	44	312	16749

Табл. 3. Время на обновление (мс)

База данных	Количество операций			
	10	100	10000	100000
MongoDB	76	83	3186	25963
RavenDb	614	2104	96790	836363
CouchDB	98	459	69783	110569
Couchbase	78	97	1460	9754
Cassandra	159	258	9976	94378
Hypertable	78	259	13875	167456
Redis	45	98	3950	50478
MSSQL Server	31	118	19678	317856

Табл. 4. Время на удаление (мс)

База данных	Количество операций			
	10	100	10000	100000
MongoDB	2	25	19655	17656
RavenDb	76	766	84904	776390
CouchDB	78	556	64789	704345
Couchbase	5	16	989	7493
Cassandra	33	97	13807	94778
Hypertable	17	106	10478	124569
Redis	6	9	9	56
MSSQL Server	9	45	2654	27690

Как показывают результаты экспериментов, реляционная база данных MSSQL Server по-прежнему является высокопроизводительным решением, которая уступает лишь немногим NoSQL СУБД в плане временных затрат на операции доступа к данным.

Литература

1. Yishan Li, Sathiamoorthy Manoharan, “Communications, Computers and Signal Processing”, August 2013.
2. Haleemunnisa Fatima, Kumud Wasnik, “International Journal of Advances in Electronics and Computer Science”, March 2016.
3. Abdullah Talha Kabakus, “Journal of King Saud University – Computer and Information Sciences”, 2 July 2016.

УДК 004.7

ПІДХІД ДО СИНХРОНІЗАЦІЇ ДАНИХ КОРИСТУВАЧІВ, ЩО ВЗАЄМОДІЮТЬ У РЕАЛЬНОМУ ЧАСІ

Шемшур Я. С., Штогріна О.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yaroslav.shemshur@gmail.com

An approach to synchronize customer data that interacts in real time

The article provides a possibility to synchronize program objects between of real-time interaction users. A way to optimize the volume of traffic when using mobile devices to transmit a large number of small messages is described.

Більшість сучасних інформаційних технологій базуються на клієнт-серверній архітектурі. В її основу був покладений принцип повного відділення реалізації виконуваних функцій від інтерфейсу для доступу до них. Використання серверу з відповідною функціональністю, як сполучної ланки між користувачами, забезпечило швидкий та безпечний обмін інформацією [1]. Проте, на сьогоднішній день все більше виникає потреба обміну інформацією між всіма користувачами певного застосування в реальному часі. Також необхідно враховувати, що зазвичай використовуються мобільні застосування, що накладає обмеження пов’язані з передачею даних по мобільній мережі. Синхронізація даних користувачів в реальному часі затребувана в таких сферах як робототехніка, медицина, архітектура, та в багатьох застосуваннях, які несуть науковий або розважальний характер у тому числі на основі доповненої чи віртуальної реальності. Прикладом такої взаємодії можуть бути проекти в яких є необхідність одночасної взаємодії фахівців однієї предметної області: розробка архітектури присадибної ділянки, будинку, чи навіть великого торгового комплексу, керування технікою різного рівня, проведення навчання оперування чи взаємодії з медицинською технікою, використання графічного редактору, та ін.

Враховуючи те, що клієнти повинні постійно обмінюватися великою кількістю повідомлень з сервером, постає проблема мінімізації об’єму трафіку, особливо при використанні мобільних пристроїв. Також особливу увагу необхідно приділити безпеці передачі повідомлень користувачів, та забезпечити можливість використання необхідного методу шифрування. Як приклад в ігровій індустрії на сьогоднішній день існують програмні рішення, які вирішують проблеми синхронізації даних користувачів в реальному часі, але вони не повністю відповідають все більш зростаючим вимогам до швидкодії, об’ємів трафіку та можливості вибору альтернативних способів

забезпечення безпеки. А саме: «Photon Server» (http://www.photonengine.com), «Smart Fox Server» (http://www.smartfoxserver.com) та «Unity network» (https://docs.unity3d.com/Manual/UNet.html). Ці програмні рішення мають жорстко встановлені правила серіалізації/десеріалізації та використовують стандартні протоколи з великим об'ємом «службових» даних [2].

Отже актуальним завданням є розробка підходу до синхронізації даних користувачів, що взаємодіють в реальному часі, що дозволить підвищити швидкість обміну повідомленнями, зменшити об'єм трафіку та обирати відповідний спосіб захисту повідомлень, що передаються.

Для вирішення поставленого завдання запропоновано зменшити об'єм трафіку за рахунок мінімізації об'єму повідомлення та використання більш легкого протоколу передачі даних.

Для мінімізації об'єму повідомлення розроблено спеціальний метод серіалізації/десеріалізації об'єкта, що дозволяє серіалізувати/десеріалізувати тільки частину об'єкта, що змінилась, або зазначати тільки ідентифікатор вже заздалегідь описаного стану. Як приклад, створюється список анімацій об'єкта, з відповідними ідентифікаторами, самі ж анімації зберігаються на пристрої користувача. Для зміни анімацій об'єкта, передається тільки ідентифікатор анімації, яку необхідно відтворити.

Після порівняння та дослідження протоколів передачі даних UDP та TCP було виявлено, що протокол UDP дозволяє зменшити об'єм трафіку при передачі невеликих повідомлень до 4х разів. Але, на відміну від TCP, він функціонує без підтвердження та гарантії доставки повідомлень. Тому запропоновано передавати дані по протоколу UDP та використовувати розроблений додатковий програмний модуль на сервері, який би відповідав за підтвердження прийому повідомлень.

Протокол UDP функціонує на транспортному рівні моделі OSI, а це означає, що він не може відповідати за шифрування даних. Тому було запропоновано розробити програмний модуль, який буде відповідати за захист при передачі повідомлень. В даному випадку програмний модуль дозволяє використовувати необхідні алгоритми шифрування в залежності від вимог, висунутих до безпеки застосування. Також цей модуль відповідає за генерацію та пересилку користувачу динамічних ключів шифрування, які постійно оновлюються при взаємодії з сервером.

Отже при реалізації запропонованого підходу до синхронізації даних користувачів, що взаємодіють в реальному часі були розроблені програмні модулі прийому/відправки та шифрування/дешифрування повідомлень, серіалізації/десеріалізації об'єкта та обробки даних. На рис. 1 продемонстрований обмін даними між користувачами у реальному часі при використанні запропонованого підходу.

Рішення запропоновані в рамках підходу дозволяють мінімізувати об’єм кожного повідомлення, що в сукупності з передачею по протоколу UDP, суттєво зменшує загальний об’єм трафіку. Також зменшення об’єму повідомлення, підвищує швидкість обміну даними, за рахунок зменшення часу та обчислювальних ресурсів на шифрування/дешифрування повідомлення.

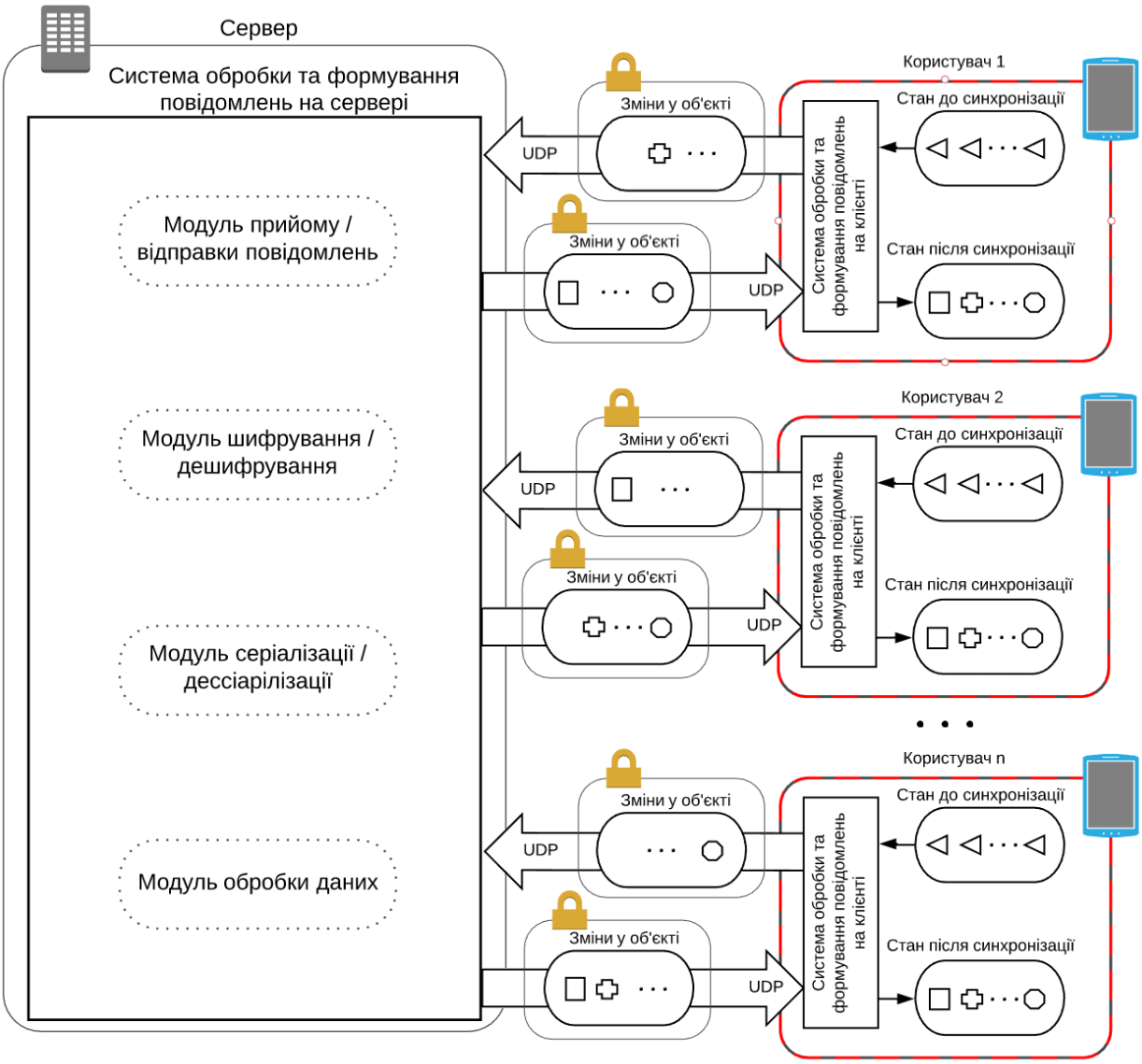


Рис. 1. Обмін даними між користувачами у реальному часі

Література

1. Alex Berson Client/server architecture : New York - McGraw-Hill, 1996 — 20с.
2. Jason Edelman Network Programmability and Automation: Skills for the Next-Generation Network Engineer / Jason Edelman, Scott S. Lowe, Matt Oswalt Virginia Wilson — 359с.

УДК 621.396

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ КРАТКОСРОЧНОГО ПРОГНОЗИРОВАНИЯ СЕТЕВОГО ТРАФИКА

Запорожец Д.Б., Скулиш М.А.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: zaporozhetsdb@gmail.com

Short-term Forecasting: Methods to Predict Network Traffic

We analyzed the ability of simple linear forecasting methods to predict short-term real network traffic behavior. To evaluate such ability we experimentally estimate forecasting accuracy of some basic methods operating time series based on a real network traffic.

Прогнозирование стохастического процесса является одной из наиболее общих прикладных научных проблем, поэтому в этой области были предложены многочисленные подходы и методы. Простые и в то же время надежные методы прогнозирования также имеют решающее значение для различных решений для сетевого трафика. Сегодня существуют два основных подхода к управлению сетью [1]: офлайн и онлайн. Оба этих метода нуждаются в прогнозировании поведения трафика. Разницу можно найти в длительности интервалов прогнозирования: автономные методы основаны на долгосрочном прогнозировании (часы и дни), в то время как онлайн-методы, основанные на быстрых изменениях в сети, работают с краткосрочными прогнозами (с секунд до десятков минут). Новизна этого исследования заключается в исследовании методов прогнозирования с использованием реальных временных рядов интенсивности сетевого трафика.

Примерами ранних подходов являются модели FARIMA [2] (авторегрессионная дробно интегрированная скользящая средняя) для долгосрочного прогнозирования интенсивности сетевого трафика. Еще одной примерной моделью является ARIMA [3] (авторегрессионная интегрированная скользящая средняя. Третий общий подход - использование нейронных сетей для прогнозирования [3].

Методы прогнозирования демонстрируют высокую точность даже для дальнего прогнозируемого горизонта. Но в то же время у них есть некоторые серьезные недостатки, когда применяются для управления онлайн-трафиком. Сначала для любой модели ARIMA / FARIMA требуется анализ временного ряда для оценки адекватных параметров модели. Нейронные сети свободны от таких ограничений, но им требуется сравнительно длительное время для обучения, в то время как реальное поведение трафика может быстро измениться, и такое изменение приведет к новому циклу обучения. И, наконец, такие методы довольно сложно реализовать в реальном сетевом

оборудовании из-за значительной вычислительной сложности, особенно в случае нейронных сетей.

Описанные выше долгосрочные методы прогнозирования являются излишними для краткосрочного прогнозирования. Основными требованиями здесь являются сравнительная простота, полная автоматизация процессов и способность быстро реагировать на произошедшие изменения. Линейные методы, отвечают всем этим требованиям.

В целом, наблюдаемые временные ряды могут быть представлены суммой нескольких ненаблюдаемых компонентов [4].

$$X(t) = \mu(t) + S(t) + e(t)$$

Здесь μ (t) - модель тренда, S (t) - сезонная составляющая, e (t) - стационарный остаток. В случае краткосрочного прогнозирования можем пренебрегать сезонной частью и концентрироваться на плавном тренде и остаточной центрированной случайной составляющей.

Далее будет рассмотрено некоторые классические методы линейного прогнозирования.

Полиномиальная аппроксимация. Метод, основанный на представлении сегмента временных рядов в форме заданного степенного полинома.

$$P_k(x_t) = a_0 + \sum_{i=1}^{k} a_i x_{t-i}^{i}$$

Здесь a_0, ..., a_n- коэффициенты, x_{t-1}, ..., x_{t-n} - n - значения сегмента временных рядов, k - полиномиальная мощность. Коэффициенты могут быть получены методом наименьших квадратов, сводя к минимуму кумулятивную квадратичную ошибку предсказания

Полиномиальная экстраполяция. Основная разница между полиномиальной экстраполяцией и аппроксимацией является необходимость точно соответствовать всем значениям сегмента. Следствием такого условия является жесткое ограничение для размера сегмента: оно должно быть ровно n = k + 1 балл.

Сглаживание с помощью формул Спенсера. Другими известными методами получения тренда по наблюдаемым данным являются формулы Спенсера [6]. В этой работе предоставлено формулы на основе 5- и 7-балльных формул, которые относятся к взвешенному движущемуся усредненному процессу. Исходные формулы Спенсера были модифицированы для экстраполяции значения тренда за пределами рассматриваемого сегмента временных рядов.

$$x_t[5] = \frac{1}{35}[-28x_{t-5} + 77x_{t-4} - 28x_{t-3} - 98x_{t-2} + 112x_{t-1}$$

$$x_t[7] = \frac{1}{21}[-12x_{t-7} + 18x_{t-6} + 12x_{t-5} - 9x_{t-4} - 24x_{t-3} - 12x_{t-2} + 48x_{t-1}$$

Здесь x_t [5] - прогноз на основе 5-точечной формулы и x_t [7] - следовательно, по 7-точечной формуле. Практически формулы Спенсера представляют

собой низкочастотные фильтры, отбрасывающие высокочастотный шум стационарного остатка.

Линейное предсказание. Метод авторегрессии, основанный на представлении случайного процесса как временной инвариантной линейной системы [5].

$$\hat{y}(n) = -\sum_{k=1}^{p} a_k y(n-k)$$

Здесь $\hat{y}(n)$ - предсказание n-го значения временных рядов. Весовые параметры a_1, ..., a_k могут быть получены путем минимизации кумулятивной ошибки предсказания квадрата на участке длины n.

$$\sum_{n} [y(n) - \hat{y}(n)]^2 \rightarrow \underset{\{a_k\}}{min}$$

Экспоненциальное сглаживание. Экспоненциальное сглаживание можно рассматривать как частный случай взвешенного среднего значения с учетом всех предыдущих значений ряда с экспоненциально убывающими коэффициентами. Существует множество экспоненциальных сглаживающих типов моделей.

Наиболее оптимальным методом автономного краткосрочного сетевого прогнозирования является экспоненциальное сглаживание. Он сочетает в себе универсальность и в то же время надежность, точность среди всех рассмотренных методов. Экспоненциальное сглаживание с параметром адаптивного сглаживания было признано лучшим методом прогнозирования.

Были оценены методы краткосрочного прогнозирования. Полученные результаты помогут исследователям и инженерам разрабатывать решения для управления сетью, особенно системы балансировки нагрузки, которые нуждаются в таких методах, выбирать наиболее подходящие. Статистический анализ используемых временных рядов интенсивности реального сетевого трафика можно рассматривать как дополнительный вклад в работу, раскрывая внутреннюю структуру процессов и лучше понимая присущие ему свойства и характеристики.

Литература

1. Awduche D. et al. Overview and principles of Internet traffic engeeniring. RFC 3272, may, 2002.
2. Shu Y. et al. Traffic prediction using FARIMA models In: Communications, 1999. ICC’99. 1999 IEEE International Conference on. IEEE, 1999. pp. 891-895.
3. Rutka G. Network Traffic Prediction using ARIMA and Neural Networks Models In: Electronics and Electrical Engineeging. 2008. pp. 47-52.
4. Koopman S. J., Shephard N. State space and unobserved component models. Cambridge University Press, 2004.
5. Makhoul J. Linear prediction: A tutorial review In: Proceedings of the IEEE. 1975. pp. 561-580.
6. Kendall, M. G., Stuart A.: The advanced theory of statistics. Vols. II and III. (1961).

УДК 004.724.4

АНАЛІЗ ЗАСОБІВ МОДЕЛЮВАННЯ ДЛЯ МЕРЕЖЕВОЇ СМО ІЗ ДИНАМІЧНО ЗМІНЮВАНИМИ ПАРАМЕТРАМИ ВУЗЛІВ ОБСЛУГОВУВАННЯ

Нездвецький В.С., Скулиш М.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vnezdd@gmail.com

MODELING ANALYSIS FOR THE NETWORK MASS-SERVICE SYSTEMS WITH DYNAMICALLY CHANGING PARAMETERS OF SERVICE NODES

For today's data transmission networks, the issue of streamlining data processing is increasingly being raised. With increasing downloads of the channel, packet loss occurs more often, which in turn leads to a deterioration in the quality of work and an increase in the response time of applications. Increasing the bandwidth of channels (own or leased) is often expensive and does not always help - the delay in the network still remains very large. Sometimes the problem can be solved (partially or completely) by applying priority service rules, changing application settings, or viewing the solution architecture. However, the solution based on the method of dynamically changing the parameters of service nodes remains insufficiently considered. The effectiveness of the method of dynamically changing the parameters of service nodes needs to be proved, therefore, it was decided to execute modeling of the system of mass maintenance of applications as much as the systems used in real life and to apply the above method on the simulated system.

Для сучасних мереж передачі даних все частіше постає питання оптимізації обробки потоків даних. При збільшенні завантаження каналу втрати пакетів відбуваються частіше, що, в свою чергу, веде до погіршення якості роботи і збільшення часу відгуку додатків. Нарощування пропускної здатності каналів (власних або орендованих) нерідко обходиться дорого і не завжди допомагає - затримка в мережі все одно залишається дуже великою. Іноді проблему вдається вирішити (частково або повністю) за рахунок застосування правил пріоритетного обслуговування (CoS / QoS), зміни налаштувань додатків або перегляду архітектури рішення. Проте рішення в основі якого лежить метод динамічної зміни параметрів вузлів обслуговування досі залишається недостатньо розглянутим.

Мережі передачі даних в більшості випадків складаються з багатьох автономних вузлів, незалежно від типу обладнання що діє в якості вузла

обслуговування. Параметри вузлів в більшості також підлягають зміні навіть безпосередньо під час процесу обробки заявок. Ефективність методу динамічної зміни параметрів вузлів обслуговування потребує доведення, тому було прийняте рішення виконати моделювання системи масового обслуговування заявок максимально подібної до систем що використовуються в реальному житті та застосувати вищевказаний метод на змодельованій системі.

Інженерний програмний пакет MATLAB включає в себе безліч засобів для побудови моделей в різних предметних областях. Одним з таких засобів є інструмент StateFlow, що входить до складу комплексу Simulink. Основне призначення якого побудова моделей реактивних систем (або кінцевих автоматів), що характеризуються великою кількістю станів, в які система переходить при настанні певних подій. Існують прийоми, що дозволяють успішно використовувати цей інструмент для моделювання СМО. Однак його застосування в цих цілях пов'язане з рядом труднощів, головними з яких є наступні факти:

• представлення СМО у вигляді кінцевого автомата не очевидно і не однозначно (зокрема, моделювання СМО з нескінченною чергою (абстракція), може стати неможливим);

• перехід кінцевого автомата зі стану в стан не передбачає передачі будь-якої інформації, в той час як майже всяка зміна в СМО супроводжується передачею певної інформації всередині системи;

• моделювання СМО як кінцевого автомата вимагає явного визначення безлічі подій і умов, що забезпечують зміну станів системи. Це істотно ускладнює процес опису моделі і загромаджує її графічне представлення.

У зв'язку з перерахованими труднощами для вирішення поставленого завдання був обраний інший інструмент, що також входить до складу Simulink - бібліотека SimEvents. Ця бібліотека є набором блоків Simulink, призначених для моделювання систем дискретних подій (Discrete Event

System, DES). Процес побудови моделей засобами SimEvents позбавлений недоліків, властивих StateFlow і перерахованих вище.

Крім того, ця бібліотека має низку корисних властивостей і функцій:

• до складу бібліотеки входять модулі, що описують черги з різними дисциплінами обслуговування (в т.ч. з керованими пріоритетами);

• є блоки для опису різних (в т.ч. множинних) каналів передачі даних;

• для опису заявок бібліотека передбачає особливий тип даних - сутності, які дозволяють не тільки розглядати кожну заявку як самостійний цілісний предмет інтересу, а й наділяти його особливими властивостями (атрибутами).

Перераховані особливості визначають вибір бібліотеки SimEvents в якості основного інструментального засобу (поряд з MATLAB і Simulink) для вирішення поставленої задачі.

Висновок. Інженерний програмний пакет MATLAB включає в себе інструментальні засоби, що дозволяють будувати, моделювати і відлаштовувати моделі СМО, котрі, в свою чергу, можуть бути використані для дослідження методів оптимізації мереж передачі даних. Ці засоби представлені комплексом Simulink і бібліотекою блоків SimEvents що входить до його складу.

Блоки бібліотек SimEvents є потужним, гнучким, але легким у розробці інструментом для опису моделей СМО.

Розроблені в цьому режимі моделі при належному тестуванні та віддачі можуть служити незамінним засобом вирішення реальних завдань масового обслуговування.

Література

1. Навколо форумів сайтів Exponenta.ru і Matlab.ru/Математика в додатках, №2 (6) 2004 г. - http://exponenta.ru/
2. Довідкові матеріали по пакету MATLAB R2008a (http://mathworks.com)/
3. Дослідження операцій. Завдання, принципи, методологія. Уч. посібник для студ/ Е. С. Вентцель. - 4-е вид., Стер. - М .: Вища. шк., 2007. - 208 с.
4. Теорія ймовірностей і математична статистика: Уч. посібник для вузів / В. Е. Гмурман. - 9-е вид., Стер. - М. Вища. шк., 2003. - 479 с.

УДК 621.396.946

ПРОЦЕДУРА ПОБУДОВИ ЕНЕРГОЗБЕРІГАЮЧОЇ ТОПОЛОГІЇ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ МОНІТОРИНГУ ЦІЛЕЙ

Новіков В.І., Алєксєєва І.В., Лисенко О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна E-mail: lysenko.a.i.1952@gmail.com

Procedure for formation the energy-saving layout topology of the wireless sensor circuit monitoring of the targets

Proposed a new mathematical model of procedure for formation the energy-saving layout topology of the wireless sensor network (WSN) monitoring of the targets. Construction of network topology is carried out by controlling the transmission power of nodes WSN.

Електроживлення вузлів безпроводових сенсорних мереж (БСМ) у більшості випадків здійснюється від батарей. У зв’язку з цим в системі управління БСМ виділена підсистема управління витратами енергоресурсу вузлів[1]. Метою її функціонування є мінімізація та перерозподіл витрат енергоресурсу вузлами для максимізації тривалості функціонування БСМ. Існуючі методи управління витратами енергоресурсів БСМ не враховують особливостей БСМ і тому не забезпечують максимізацію тривалості їх функціонування при виконанні вимог до якості інформаційного обміну. У зв’язку з цим, задача розробки нових та удосконалення існуючих методів управління витратами енергоресурсів для використання в БСМ є актуальною на сьогоднішньому етапі розвитку безпроводових телекомунікацій.

Управління витратами енергоресурсу вузлів БСМ може бути реалізоване за рівнями еталонної моделі OSI з використанням різних методів, які в загальному випадку можна поділити на дві групи: методи збереження енергії батарей і методи управління потужністю передачі.В роботі[2] було запропоновано новий енергозберігаючий метод моніторингу цілей у зонах спостереження сенсорів БСМ, який відноситься до першої групи методів і складається з трьох етапів:

1. Знаходження верхньої межі максимальної тривалості функціонування сенсорної мережі $T_{\Phi_{БСМ}}$ та матриці спостереження $|T|_{n\times m}$ (яка визначає інтервал часу, протягом якого сенсори спостерігають за цілямиу зонах спостереження).

2. Визначення сесій спостереження – розбиття матриці спостереження $|T|_{n\times m}$ в послідовність матриць (сесій) спостереження $T_{n\times m} = T_1 + T_2 +, ..., T_t$, які не зменшують отримане значення максимальної тривалості функціонування

сенсорної мережі та забезпечують виконання умови один сенсор – одна ціль.

3. Визначення маршрутів передачі зібраної інформації за сесіями спостереження.

Для підвищення ефективності енергозберігаючого методу моніторингу цілей пропонується використати в ньому нову енергозберігаючупроцедурупобудови топології мережішляхом управління потужністю передачі вузлів БСМ. Під топологією мережі розуміють сукупність вузлів на місцевості і каналів, що сполучають їх, у взаємному розташуванні. Топологія визначає потенційні можливості мережі з доставки даних між взаємодіючими вузлами. Передбачається, що кожен вузол може змінювати потужність передачі $p_i = [p_{i\min} ... p_{i\max}]$ з певним кроком дискретизації Δp.

Відповідно, під управлінням топологією БСМ розумітимемо управління $U_{\text{Т}}$, що змінює топологію БСМ в процесі її функціонування за рахунок перерозподілу потужностей передач вузлів p_i з метою забезпечення цільової функції Z_k, $k = \overline{1, K}$ [1, 2]:

Z_1 – мінімізація потужностей передачі вузлів ($\min p_i$) і загальної потужності сенсорної мережі $P_{\text{заг}}$ в цілому.

Z_2 – забезпечення зв'язності мережі (зв'язності між вузлами i та u – $cv_{iu} = 1$);

Z_3 – мінімізації часу затримки передачі повідомлень ($\min \overline{t}_{\text{з}}$);

Z_4 – максимізації пропускної спроможності мережі ($\max S$);

Для підвищення ефективності функціонування БСМ моніторингу цілей мережевий рівень еталонної моделі OSI (як складову частину системи управління) пропонується реалізувати на двох підрівнях: на верхньому рівні проводиться оперативне управління топологією мережі (створюються потенційні маршрути передачі інформації); на нижньому – управління побудовою і підтримкою маршрутів при отриманій топології (реалізується конкретний метод маршрутизації) [3].

Верхній і нижній рівні працюють в різних часових інтервалах. Цикл управління маршрутами значно менший за цикл управління топологією. Співвідношення циклів управління повинно бути таким, що на кожному кроці топологічних змін повинен відбуватися весь цикл управління маршрутами. Тільки в цьому випадку можливе досягнення ефективності реалізованої топології.

Розглянемо математичну модель процедури побудови топології БСМмоніторингу цілей.

Модель мережі.БСМ представляється у вигляді графа $G = (V, E)$ з множиною вершин $V = \{i\}$ і множиною ребер $E = \{(i, j) | \, p_{iu} \approx (d_{iu})^{-\alpha})\}$, що визначають матрицю зв'язності $\tilde{N}V = \|cv_{iu}\|$, де $cv_{iu} = \{0, 1\}$ – булева змінна, d_{iu} – відстань між вузлами i та u для $i \neq u$, $i = \overline{1, N}$, $u = \overline{1, N}$, p_{iu} – потужність

передачі вузла i, яка необхідна для забезпечення радіозв'язності з вузлом u, $0 \le p_{iu} \le p_{\text{пор}}$ для $0 \le i \le n$, α – параметр, що приймає значення між 2 та 4. $P(CV) = \sum_{i=1}^{n} p_i$ – загальна потужність передачі сенсорної мережі, що витрачається.

Параметри БСМ моніторингу цілей: кількість вузлів N; кожен вузол графа i у момент t описується сукупністю параметрів: координати розташування (x_i, y_i); потужність передачі p_i; ємність батареї $E_i^{\text{á}}$; маршрутна таблиця найкоротших шляхів $\Pi_i = \left\| l_\eta(\pi_{iu}^{(b)}) \right\|$, де $b \in D$, $(i,u) \in E$, $\pi_{iu}^{(b)} = \{0,1\}$ – маршрутна змінна, що визначає відсутність (наявність) маршруту від відправника i до адресата b через сусідній вузол $u \in N_i$, l_η – довжина найкоротшого маршруту, $\eta = \overline{1,\text{H}}$ – позитивні метрики (наявність радіозв'язності – η_1, енергія батарей вузлів – η_2, потужність передачі вузлів – η_3, відстань – η_4, затримка передачі – η_5, пропускна спроможність – η_6). Інтенсивність вхідних потоків визначається матрицею тяжіння $\mathbf{Q}^\xi = \left\| Q_{ab}{}^\xi \right\|$, $\sum_{a=1}^{N}\sum_{b=1}^{N} q^\xi{}_{ab} \le q_{\max}^\xi$, де $a \in S$ − відправник ; $b \in D$ − базова станція; $q_{iu}^\xi \le s_{\max}$ − пропускна спроможність радіоканалу $\forall (i,u) \in E$; радіозв'язність між вузлами мережі підтримується одним з детермінованих протоколів канального рівня.

Множина вимог до процедури побудови топології $\{\text{B}_q\}$, $q = \overline{1,4}$: мінімізація потужностей передач вузлів і загальної потужності сенсорної мережі в цілому; забезпечення зв'язності мережі; мінімізація часу затримки передачі повідомлень; максимізація пропускної спроможності мережі.

Необхідно: у режимі реального часу знайти матрицю зв'язності CV^* (визначити потужність передачі p_i для кожного вузла i, $0 \le i \le N$ що забезпечує виконання цільової функції Z_k, $k = \overline{1,K}$:

$$C_k^* = \arg \underset{U_{\text{т}} \in \Omega_{\text{т}}}{opt}\, Z_k(CV), \tag{1}$$

при виконанні обмежень на множину управляючих впливів, і ресурси мережі $\Omega_{\text{ò}}$

$$\Omega_{\text{т}} : \left\{ \begin{array}{l} t_{\text{з}}^\xi(m_{ab}) \le t_{\text{здоп}}^\xi \, (l_{ab}^\xi(m_{ab}) \le l_{\text{доп}}^\xi), \\ q_{iu}^\xi \le s_{\text{доп}}(cv_{iu}), \\ p_i \le p_{\text{пор}}, \\ E_i^{\text{б}} \le E_{i\max}^{\text{б}}, \text{для } i \in C - D \end{array} \right\} \tag{2}$$

де $t_{\text{ç}}^\xi$ – затримка передачі трафіка ξ- го типу, q_{iu}^ξ – інтенсивність потоків пакетів, що поступають за всіма маршрутами m_{ab}, які проходять через даний

вузол i – $q_{iu}^{\xi} = \sum_{a=1}^{N} \sum_{b=1}^{N} \gamma_{ab}$; $(i,u) \in m_{ab}$ – маршрут з відправником у вузлі a і одержувачем b; a, b, i, $u \in V$, p_i – потужність передачі i-го вузла відповідно до прийнятих маршрутних рішень Π_i; $s(cv_{iu})$ – пропускна спроможність радіоканалу; l_{ab}^{ξ} – кількість ретрансляцій для пари вузлів (a,b) повідомлень по маршруту m_{ab}; $p(m_{ab}) = \sum_{(i,u)\in m_{ab}} (k_1 d_{ij}^{-\alpha} + k_2)$, $a = 2...4$, k_1 і k_2 – константи; $p_{\text{пор}}$, $t_{\text{з доп}}$, $l_{\text{доп}}$ – допустимі значення вищеназваних параметрів.

Основне завдання при побудові топології БСМ полягає в отриманні зв'язної топології та задоволенні показників якості обслуговування потоків даних при мінімізації загальної потужності передачі вузлів у сенсорній мережі.

В цьому випадку цільова функція приймає вигляд

$$CV^* = \left\| cv_{iu}^* \right\| = \arg\min_{U_{\text{т}} \in \Omega_{\text{т}}} P(CV) = \arg\min_{U_{\text{т}} \in \Omega_{\text{т}}} \sum_{m=1}^{M} \sum_{a=1}^{N} \sum_{b=1}^{N} p(m_{ab}(CV)), \qquad (3)$$

де $P(CV)$ – загальна потужність передачі вузлів сенсорної мережі; a, b, i, $u \in V$; при виконанні обмежень (2).

Завдання пошуку матриці зв'язності CV^* (1) відноситься до класу NP-повних. Застосування для його вирішення класичних методів приводить до експоненціальної складності. Отримання точного рішення для мережі, яка налічує десятки (сотні) вузлів, пов'язане із значними часовими витратами. Тому для скорочення перебору топології в подальших дослідженнях планується розробити множину правил, об'єднаних в базу знань, що змінюють зв'язність мережі для поліпшення її параметрів [4]. Це дозволяє отримати в реальному масштабі часу близькі до оптимальних рішення і використовувати методику для побудови топології БСМ моніторингу цілей. Критерієм визначення моменту перебудови топології мережі є невиконання однієї з умов обмеження $\Omega_{\text{т}}$.

Література

1. Лисенко О. І. Функціональна модель системи управління безпроводовою сенсорною мережею із самоорганізацією для моніторингу параметрів навколишнього середовища / О. І. Лисенко, К. С. Козелкова, В. І. Новіков, Т. О. Прищепа, А. В. Романюк // Системи обробки інформації. - 2015. - Вип. 10. - С. 222-225
2. Новіков В. І. Метод збільшення часу життя безпровідної сенсорної мережі з надлишковою кількістю вузлів під час стеження за цілями моніторингу / В. І. Новіков // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. - 2017. - Том 28 (67) № 2 - С. 38-43.
3. Романюк В.А. Активная маршрутизация в мобильных радиосетях / Романюк В.А. // Зв'язок. – № 3. – 2002. – С. 21 – 25.
4. Романюк В.А. Підходи до розробки нової архітектури системи управління неоднорідними безпроводовими сенсорними мережами. / В.А. Романюк, О.І. Лисенко, І.В. Алєксєєва, А.В. Романюк, В.І. Новіков // Математичні машини і системи, 2017, № 2. С. 15-23.

УДК 621.382

ИССЛЕДОВАНИЕ МОБИЛЬНОСТИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Прищепа Т.А., Лисенко А.И.
Институт телекоммуникационных КПИ им. Игоря Сикорского, Украина
E-mail: its_tk@ukr.net

Mobility Research in Wireless Sensor Networks

The article analyzes the impact of mobility on performance indicators of the wireless sensor network, such as delaying the meeting between the sensor and the node and delaying the delivery of large messages.

Сейчас мобильность в БСМ является преимуществом, а не проблемой. Результаты [1-4] показывают, что мобильность не только повышает время функционирования сети, но и позволяет решить вопрос задержки при передаче.

Как известно, традиционное определение для БСМ описывает гомогенную сеть с одноуровневой архитектурой, где все узлы кроме стока и шлюза имеют одинаковый ресурс батареи и возможности оборудования. Однако, такой подход с "плоской" архитектурой неотвратимо приводит к осложнениям в контексте множественного доступа, маршрутизации, сохранения энергии узлов и управления сетью. Мобильность стоков может рассматриваться как проявление гетерогенности, что позволяет реализовать сетевую иерархию и кластеризацию, которые могут быть использованы для улучшения масштабируемости сети и времени ее функционирования.

На первый взгляд, повышение скорости узла v должно повышать эффективность системы, поскольку при равных промежутках времени сток может установить контакт с большим количеством узлов и собрать больше информации по сенсорам. Однако, мы должны внимательно выбирать этот параметр учитывая следующие факторы. С одной стороны, чем больше скорость стока, тем выше вероятность для статического узла установить передачу данных. С другой, если мобильный сток движется через эффективную зону связи с сенсором слишком быстро, существует высокая вероятность что продолжительность контакта, будет недостаточной для передачи потенциально долгого пакета. Иными словами, при увеличении скорости стока возрастает вероятность потерь переданных пакетов. Таким образом, выбор скорости мобильного стока превращается в компромисс между минимизацией задержки передачи данных от сенсоров и минимизации вероятности потерь переданных пакетов.

Задержка встречи между сенсором и узлом.

Пусть сеть состоит из мобильных стоков m и статических сенсоров n в кругу единичного радиуса. Сток и сенсор имеют одинаковый радиус передачи r. Шаблон перемещения мобильного стока $M_i (i = 1,..., m)$ соответствует модели перемещения со случайными направлениями, однако, с

постоянной скоростью v. Траектория стока определяется последовательностью эпох. В течение каждой эпохи скорость движения v для M_i и направление движения является постоянным и не зависящим от позиции стока. Определим Q_i как продолжительность эпохи для M_i, определяемой как временной интервал между начальной и конечной точками M_i. Q_i - случайная величина с экспоненциальное распределение. Распределение различных $Q_i(i=1,...,m)$ независимый и одинаково распределен - случайные величины с равным среднему значению. Согласно продолжительность эпохи для различных L_i также случайные величины с равным средним значением $\overline{L}=\overline{Q}\upsilon$.

Предположим, что распределение мобильных стоков стационарно. Иными словами, вероятность подхода независимых мобильных стоков до определенного статического узла с разных сторон одинакова. Определим, что факт встречи статического сенсора $N_j(1,...,n)$ и одного мобильного стока M_i, соответствует ситуации, когда M_i покрывает N_j в течение эпохи. Поскольку M_i покрывает площадь $\pi r^2+2rL_{i,k}$ в течение k-ї эпохи, тогда количество эпох X_i, которая необходима для первой встречи сенсора и стока геометрически распределена величина [5] с функцией распределения:

$$F_{x_i}(x)=\sum_{x_k\le x}p(1-p)^{k-1} \tag{1}$$

В случае количества мобильных стоков более 1 задержка встречи сенсора и стока рассчитывается как задержка до момента, когда первый мобильный сток установил контакт с узлом. Таким образом, количество эпох, которая необходима для встречи, составляет минимумом для всех $X_i(i=1,...,m)$ с функцией распределения:

$$F_x(x)=1-\left[1-F_{x_i}(x)\right]^m\cong\sum_{x_k\le x}mp(1-p)^{k-1} \tag{2}$$

Взяв $\overline{X}$ как среднее значение для X, ожидаемая задержка встречи узла и стока:

$$\overline{D_1}=\overline{X}\cdot\frac{\overline{L}}{\upsilon} \tag{3}$$

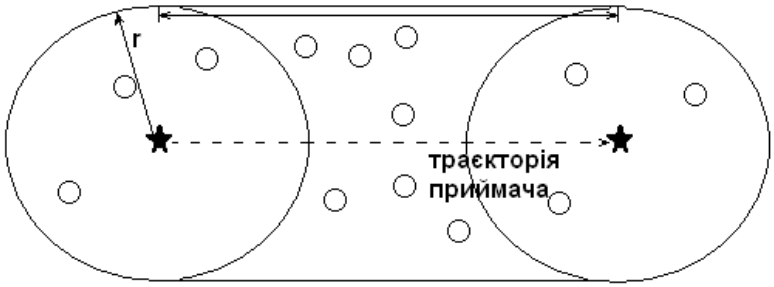


Рис. 1. Иллюстрация к расчету функции распределения задержки встречи сенсора и стока

Эти результаты дают некоторое представление о способе выбора параметров для минимизации задержки встречи сенсора и стока. Если увеличить радиус радиопередачи r, или увеличить число мобильных стоков m или скорость стока v, задержка может быть уменьшена. Однако, приведенный анализ не учитывает время, необходимое для передачи данных при каждой встрече стока и сенсора. Если длина сообщения не является относительно малой, сообщение может быть разделено на несколько частей и направлено в несколько стоков.

Выводы. Цель мобильных беспроводных сенсорных систем (МБСМ) - реализация масштабного сбора информации через беспроводные сети и мобильные устройства сбора информации (стоки). Теоретический анализ показал, что при наличии сведений об особенностях движения мобильных стоков, многоуровневая схема кластеризации может обеспечить доставку пакетов от сенсора к стоку за ограниченное время и с достаточной энергетической эффективностью. Ослабление ограничений предельного времени доставки пакетов позволяет дальше повышать экономию энергетических ресурсов. Было определено, что мобильность стоков может снизить уровень потребления энергии и, таким образом, продлить время функционирования сети. С другой стороны, негативным эффектом в таком случае является рост задержки доставки сообщений и вероятность потери сообщения. Аналогичные проблемы возникают при выборе плотности размещения мобильных стоков (количество стоков и радиус их действия).

Литература

1. Прищепа Т.О. Порівняльний аналіз форматів передачі інформації у безпроводових сенсорних системах на безпомилковість /Прищепа Т.О. // Науковий вісник АМУ, серія "Техніка" в. 8, с.122-127, 2014
2. Толстикова Е.В. Минимизация избыточности объема передачи данных в сети радиодатчиков / Толстикова Е.В.// Проблеми інформатизації та управління. – 2010. – №1(29). – С.168-171.
3. Лисенко О.І. Алгоритм пошуку доцільного розташування вузлів безпроводових сенсорних мереж / Лисенко О.І., Прищепа Т.О.// Збірник матеріалів Міжнародної науково-технічної конференції «Проблеми телекомунікацій - 17», с.402-405, 2017.
4. Валуйський С.В. Алгоритм пошуку раціонального розміщення ретрансляторів при розгортанні безпровідних сенсорних мереж / Валуйський С.В., Прищепа Т.О., Димид М.Д.// Науковий вісник Академії муніципального управління. Збірник наукових праць. Серія «Техніка». – 2016. – Вип.11. – С.1-9.
5. Liu, B. Mobility Improve Coverage of Sensor Networks / Liu, B., Brass, P., Dousse, O., Nain, P., Towsley, D.// Proceedings of ACM MobiHoc 2005

УДК 621.396.96

АНАЛИЗ ВЛИЯНИЯ КОНФИГУРАЦИИ СЕНСОРНОЙ СЕТИ НА ТОЧНОСТЬ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ ПРИ КОМПЛЕКСНОМ ИСПОЛЬЗОВАНИИ TDOA- И RSS- ИЗМЕРЕНИЙ

Товкач И.О., Жук С.Я.
Национальный технически университет Украины
“Киевский политехнический институт имени Игоря Сикорского”
E-mail: tovkach.igor@gmail.com

Analysis of the influence the sensor network configuration on the accuracy of determining the radio source location with complex use TDOA- and RSS- measurements.

With the help of statistical modeling, the effect of the sensor network configuration and the number of its sensors on the accuracy of determining the location of the radio source with complex use TDOA- and RSS- measurements sensor networks using an isoline family was analyzed. The configurations possessing both directional and non-directional properties are considered.

Для интегрального описания точностных характеристик сенсорной сети, использующей TDOA- и RSS- измерения, применяется семейство изолиний СКО ошибки измерения дальности σ_r источника радиоизлучения (ИРИ), построенных в координатах *x,y* [1,2]. Каждая изолиния, начиная от центра, ограничивает область, где ошибка не превосходит заданного значения $\sigma_r \le \sigma_{r_{доп}}$. По скорости изменения расстояний между изолиниями можно также выявить азимутальные направления, где ошибки по мере удаления от центра растут более медленно или более быстро.

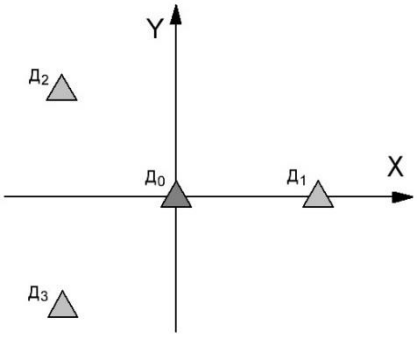


Рис. 1

Графики семейства изолиний для случая СКО ошибки измерения разности расстояний $\sigma_\Delta = 3$м, измерения мощности $\sigma_p = 1.5$ дБ, построены для двух конфигураций сенсорной сети с разным числом датчиков расположенных на окружности 100 м.

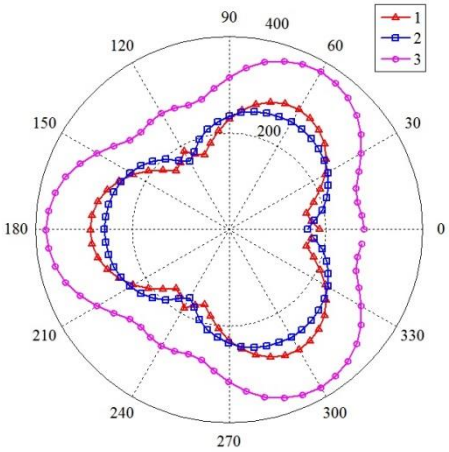


Рис. 2

Первая конфигурация сенсорной сети состоит из четырех датчиков рис. 1. При комплексном использовании TDOA- и RSS-измерений рис. 2 (кривая 3), СКО ошибки определения местоположения, в зависимости от

направления носит неравномерный характер. В направлениях 60°, 180°, 300° оно растет наиболее медленно и на расстоянии 379 м не превышает допустимого значения $\sigma_r \leq 50$ м. На азимутах 0°, 120°, 240° СКО ошибки растет наиболее быстро и на расстоянии 271 м не превышает допустимого значения $\sigma_r \leq 50$ м. Комплексное использование данных позволяет увеличить область, где ошибка не превосходит заданного значения на 45%-62%, по сравнению с их раздельным использованием TDOA-измерения (кривая 1) [3] и RSS-измерения (кривая 2).

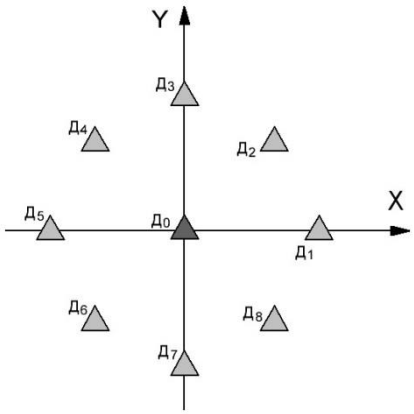


Рис. 3

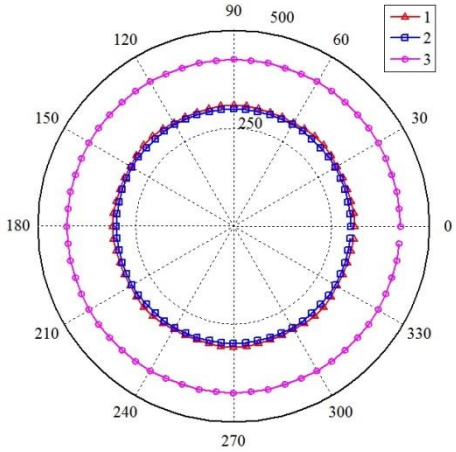


Рис. 4

Вторая конфигурация сенсорной сети состоит из девяти датчиков рис. 3. При комплексном использовании TDOA- и RSS-измерений рис. 4 (кривая 3), СКО ошибки на азимутах 0°-360° растут равномерно и на расстоянии 426 м не превышает допустимого значения $\sigma_r \leq 50$ м. Комплексное использование данных позволяет увеличить область, где ошибка не превосходит заданного значения на 40%, по сравнению с их раздельным использованием TDOA-измерения (кривая 1) и RSS-измерения (кривая 2).

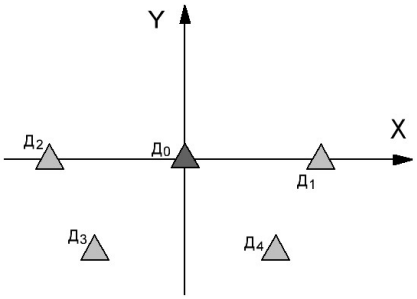


Рис. 5

При увеличении числа датчиков изолинии сохраняют форму концентрических окружностей и при этом существенного прироста в точности определения местоположения ИРИ не происходит. Поэтому, рассмотренная топология сети из девяти датчиков, может быть рекомендована для использования на практике, если направление появления цели неизвестно.

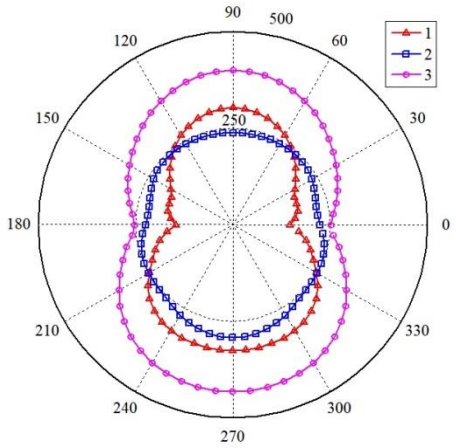


Рис. 6

Была также исследована конфигурация сенсорной сети из пяти датчиков, которая обладает направленными свойствами рис. 5.

При комплексном использовании TDOA- и RSS- измерений рис. 6 (кривая 3), СКО ошибки определения местоположения: при азимуте 90° растет более медленно и на расстоянии 400 м не будет превышать допустимого значения $\sigma_r \leq 50$ м; при азимуте 270° также растет более

медленно и на расстоянии 433 м не превышает допустимого значения $\sigma_r \leq$ 50 м; при азимутах 0°, 180^oрастет более быстро и на расстоянии 252 м не превышает допустимого значения $\sigma_r \leq 50$ м. Комплексное использование данных позволяет увеличить область, где ошибка не превосходит заданного значения на 12%-32%, по сравнению с их раздельным использованием TDOA-измерения (кривая 1) и RSS-измерения (кривая 2).

Рассмотренная конфигурация сенсорной сети из пяти датчиков, позволяет в заданных секторах получить более высоки точностные характеристики при меньшем числе датчиков по сравнению с конфигурацией сети из девяти датчиков, обеспечивающей равномерную зону покрытия.

Выводы. Конфигурация из девяти датчиков, восемь из которых расположены равномерно на окружности, обеспечивает равномерную область покрытия. При дальнейшем увеличении числа датчиков, существенного прироста в точности определения местоположения ИРИ не происходит, и она может быть рекомендована, если направление появления цели неизвестно. Рассмотренная конфигурация сенсорной сети из пяти датчиков, которая обладает направленными свойствами, позволяет в заданных секторах получить более высоки точностные характеристики при меньшем числе датчиков по сравнению с равномерной конфигурацией сети. При этом комплексное использование данных позволяет увеличить область, где ошибка не превосходит заданного значения по сравнению с их раздельным использованием.

Литература

1. I.O. Tovkach, S.Ya. Zhuk (2017). Recurrent Algorithm for TDOA Localization in Sensor Networks, J. Aerosp. Technol. Manag., São José dos Campos, Vol.9, №4, pp.489-494, Oct.-Dec., 2017. http://dx.doi.org/10.5028/jatm.v9i4.727.
2. Симаков В.А. Построение адаптивных систем пассивной радиолокации на принципах разностно-дальномерной координатометрии / В.А. Симаков // Научные ведомости Белгородский государственный университет . — 2005. — №2. — С. 221.
3. Товкач І.О. Анализ влияния конфигурации сенсорной сети на точность определения местоположения источника радиоизлучения на основе TDOA-измерений / І.О.Товкач, С.Я.Жук // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали та системи». Київ, 19 — 25 березня 2018 р.: матеріали конференції — Київ, 2018. — С. 38 — 40.

UDC 621.391.3

BANDPASS MICROWAVE FILTERS ON THE BASIS OF MATERIAL CELLS

Zhivkov A., Zazerin A., Shevtsov K., Krylach O.
National Technical University of Ukraine
“ Igor Sikorsky Kyiv Polytechnic Institute ”
E-mail: zhivkovalex@gmail.com , shewtsov.kostya@gmail.com

ПОЛОСОВЫЕ МИКРОВОЛНОВЫЕ ФИЛЬТРЫ НА БАЗЕ ЯЧЕЕК МЕТАМАТЕРИАЛОВ

В докладе рассмотрены методики расчета полосовых фильтров на базе ячеек метаматериалов. Приведены рекомендации по выбору параметров фильтров для обеспечения их оптимальной избирательности за пределами полосы пропускания.

This article considers methods of calculation metamaterial cell based band-pass filters. The recommendations for the selection of filter parameters to ensure their optimal selectivity beyond the bandwidth.

The most common type of metamaterial cell used in microwave technology is the so-called Split Ring Resonator (SRR). The SRR associated with the microwave transmission line forms a band-stop filter, a embedded in the transmission line gap forms a band-pass filter [1]. Transmission and reflection coefficients of a band-pass filter based on a single SRR cell are given in [2]:

$$\mathbf{T} = К_1/(1 + К_1) - К_2/(1 + К_2); \quad (1)$$

Here $К_1$, $К_2$ – are the complex coupling coefficients of the resonators with the load, defined as:

$$К_1 = K1/[1 + j(Ɛ + a)], \quad К_2 = K2/[1 + j(Ɛ - a)]; \quad (2)$$

where К1, К2 - coupling coefficients of resonators with load, defined as the ratio of the eigen and loaded Q-factors of the first and second resonators, respectively [3]; Ɛ is the generalized frequency deviation of each of the resonators with respect to the central frequency of the passband *fo = (f1 + f2) / 2;* a - a generalized detuning between the frequencies of individual resonators, defined as

$$a = 2*(f1-f2)*\sqrt{(Q1 * Q2)} / (f1 + f2) \quad (3)$$

f1 and f2 are the resonant frequencies of the first and second resonators, Q1 and Q2 are their Q factors.

Since, generally, a metamaterial cell is located in a band-pass filter in a gap of a limited extent (for example, the filter in Fig. 1), we also take into account the final denouement between the input and output of the filter beyond the band-pass filter in the form:

$$\boldsymbol{T} = \mathbf{T} + jD \tag{4}$$

Here, **T** is the transmission coefficient defined by formula (1), and D is the out-of-band decoupling, determined experimentally or calculated for each specific case, depending on the type of transmission line and magnitude of evanescent area.

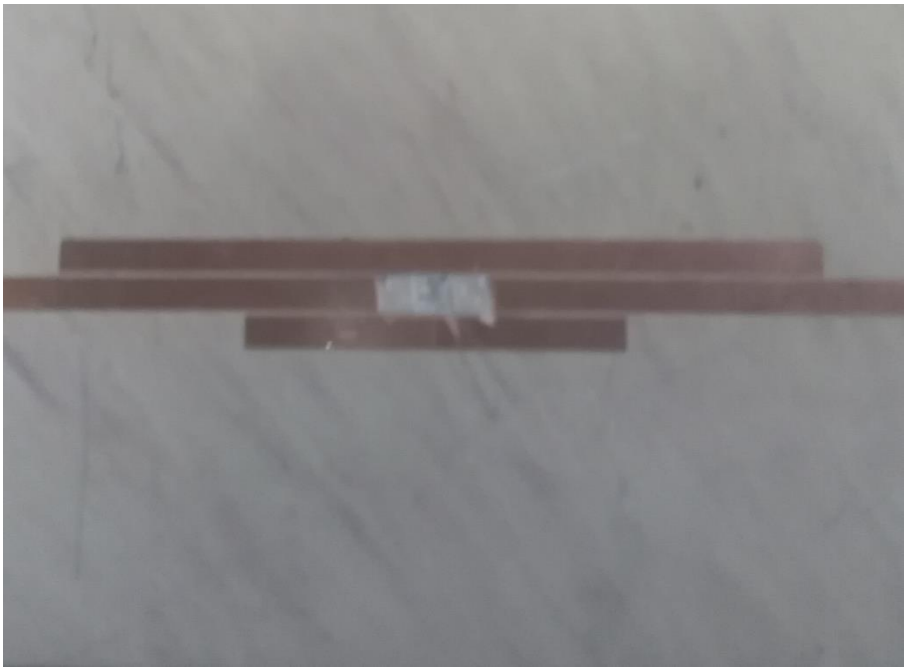
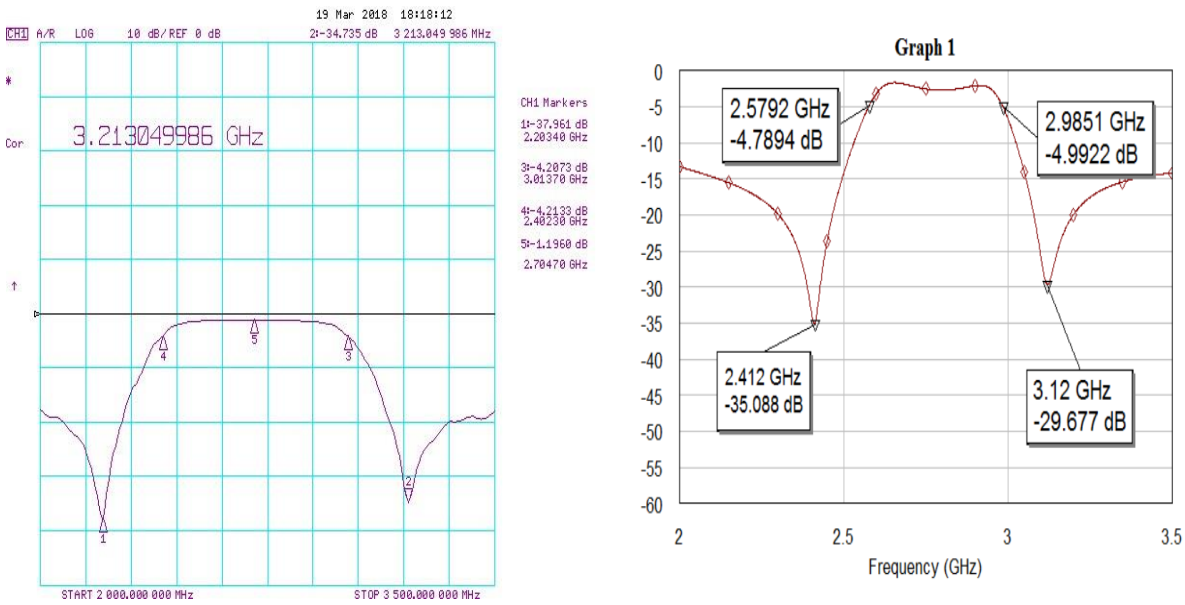


Fig. 1. Band-pass filter with "half-wave" and "wave" resonators connected in parallel

Note that by changing the resonant frequency of one of the resonators (which is equivalent to changing the generalized detuning "a" in formula 2), we are able to control the bandwidth of the filter.

The relations 1-4 given above can be used to construct the characteristics of a band-pass filter based on a metamaterial cell in an analytical form.

Simulation of the band-pass filter in Fig. 1 was made using the Microwave Office program. The simulation results are shown in Fig. 2



a) b)

Fig. 2 a) the experimental characteristic of the band-pass filter in Fig. 1;
b) the characteristic of the filter in Fig. 1, calculated using the Microwave Office program.

A good coincidence of the calculated and measured characteristics of the filter indicates the correctness of the chosen model.

References

1. Ilchenko, M.E., Zhivkov, A.P., Orlov, A.T. (2016). Filters based on resonators with frequency-like modes as metamaterial cells. Naukovi Visti NTUU “KPI” (1), 7— 14.
2. M.E. Ilchenko and A.P. Zhivkov, “Generalized approach to the analysis and design of microwave bandpass mutually detuned resonator filters”, Naukovi Visti NTUU “KPI”, vol. 103, no. 5, pp. 7—14, 2015 (in Russian).
3. D.M. Pozar, Microwave Engineering, 4 edition ,Wiley, Hoboken, NJ, 2011.
4. M.E. Ilchenko et al., “Microwave filter”, USSR Inventor`s Certificate 1518836, June 1, 1989 (in Russian).

УДК 621.396

APPLICATION OF VISIBLE AND NIR REMOTE SENSING DATA FOR DERIVING OF EARTH'S SURFACE THERMAL FIELDS OF HIGH SPATIAL RESOLUTION

Stankevich S.A., Lubskyi M.S.
Scientific Centre for Aerospace Research of the Earth, Ukraine
E-mail: N.Lubsky@nas.gov.ua

Застосування супутникових даних видимого та ближнього інфрачервоного діапазону для картування теплових полів земної поверхні із високою просторовою розрізненностю

Недостатня просторова розрізненність даних космічного знімання у діапазоні 8-14 мкм не дозволяє достатньо детально досліджувати теплові поля територій із високою неоднорідністю поверхонь, наприклад, міського середовища. Дані видимого та ближнього інфрачервоного діапазону, які зазвичай мають значно більшу просторову розрізненність, дозволяють отримати розподіл коефіцієнта теплового випромінювання, що не лише дозволяє розрахувати фізичну температуру земної поверхні засобами дистанційного зондування, а і значно підвищити інформативність отриманого зображення теплового поля.

Sensors that are provide 3-14 μm data have been widely used in the field of Earth remote sensing and allow the creation of products based on the detection of cells of intense thermal radiation (detection of forest fires, study of volcanic activity) or the formation of maps of the thermal field of low spatial resolution for the solution of meteorological problems. However, the possibility of creating of detailed thermal field maps is complicated by constraints associated with significantly lower energy of quantum radiation compared with the visible and near infrared radiance. Therefore, most existing sensor systems have a spatial resolution of 3-14 microns ≈1 km and are unsuitable for studying many of types landscapes like urban areas.

The TIRS sensor installed on the Landsat-8 satellite is used for this purpose [1]. The sensor provides data in two bands (10.3-11.3 μm and 11.5-12.5 μm), has a spatial resolution of 100 m, interpolated to 30 m, which corresponds to the spatial resolution of the second sensor of the visible and infrared data provided by OLI sensor. Landsat-8 continues a series of Landsat satellites, and its data can be combined with Landsat-4, 5, and 7 images, thus, it is possible to create time series from 1982.

The end-product of the long-wavelength infrared radiance data processing is the Earth's surface physical temperature. It takes into account the thermal emissivity of the presented surfaces. The emissivity can be estimated on the basis of the visible and near infrared data processing, which allows obtaining sufficiently detailed data on the thermal characteristics of the presented landscapes and significantly improving the informativity of the resulting surface temperature distribution.

Determination of the Earth's surfaces emissivity distribution using remote sensing data is performed by processing images of the visible and near-infrared range, in particular by establishing of the relationship between emissivity the NDVI index distribution. The source of the visible and near-infrared data can be any satellite sensor that able to provide it. The emissivity is a rather inert surface feature, and for

its determination it is possible to involve data obtained with some time interval in comparison with the data of the long-wavelength range. The determination emissivity and the NDVI index relationship for the surfaces covered with vegetation and bare soil is established separately from other types of surfaces, including artificial ones.

For soils and vegetative cover, this dependence is established on the basis of the projective vegetation cover density for each individual pixel based on the image of the NDVI distribution, which is defined as follows [2]:

$$F = \left(\frac{NDVI - NDVI_0}{NDVI_\infty - NDVI_0} \right)^2 \quad (1)$$

where *NDVI* – the value of the normalized vegetation index in the current pixel; $NDVI_0$ – - maximum value of normalized vegetation index of bare soil; $NDVI_\infty$ – minimum value of the normalized vegetation index of the surface, completely covered with vegetation.

The calculation of the total emissivity is carried out as follows:

$$\varepsilon_\lambda = \varepsilon_{v\lambda} \cdot F + \varepsilon_{s\lambda}(1 - F) + \Delta\varepsilon_\lambda, \quad (2)$$

where ε_λ – surface emissivity in current pixel; $\varepsilon_{v\lambda}$, $\varepsilon_{s\lambda}$ – emissivities for a surface completely covered with vegetation and bare soil or another surface, where there is no vegetation relatively; $\Delta\varepsilon_\lambda$ – an amendment that takes into account the irregularity of radiation due to rough surface (the standard value for a rough surface is 0,005).

This relationship for other types of covers is estimated on the basis of the regressive dependence between artificial surfaces spectra taken from ASTER Spectral Library and NDVI index outside its range which corresponds to the vegetation cover and open soil. On the basis of the obtained spectra a point cloud of dependence of the averaged emissivity of each of the typical spectra from NDVI index is expressed through zonal sensor signals in the red and near infrared bands. The resulting cloud of points is averaged over both axes and the quasi-optimal spline-approximation of the dependence is performed through the obtained averaged point (Fig. 1).

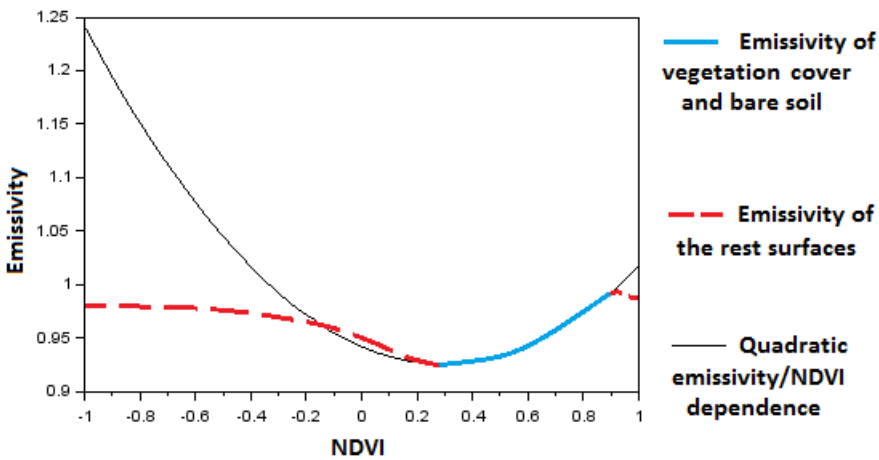
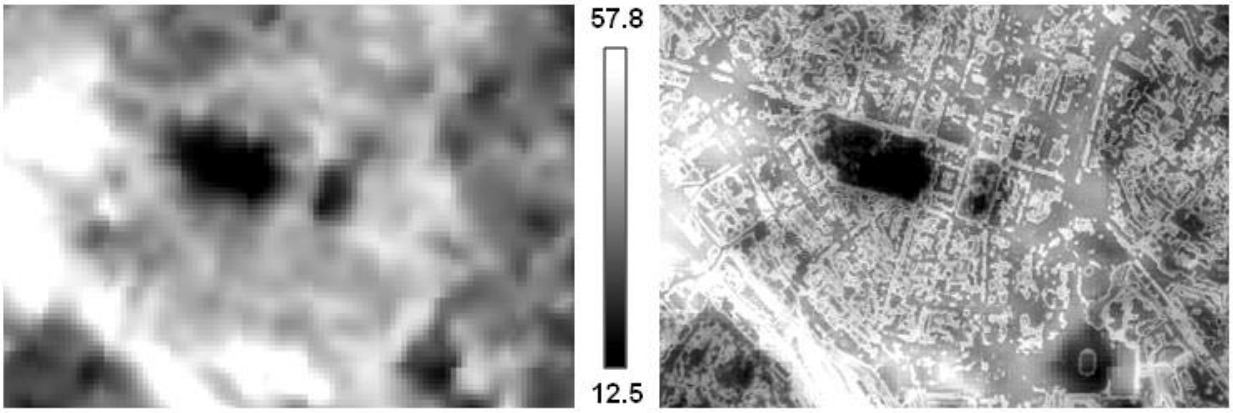


Fig. 1. Distribution of the relationship between Earth's surfaces emissivity and NDVI vegetation index

This method of the Earth's surface temperature distribution obtaining is most effective with the visible and near-infrared data obtained by Sentinel series

satellites of the in combination with the long-wavelength infrared data provided by the Landsat satellites. Although additional image adjustments are required, the Sentinel data has a spatial resolution of 10 m in the visible and near infrared, compared to 30 m for Landsat. Fig. 2 shows a comparison of temperature distribution images based on input data of the TIRS sensor and with use of emissivity distribution based on Sentinel-2 data.



a *b*

Fig.3. The urban landscape temperature destribution: *a*) with generic TIRS sensor data, *b*) with emissivity derived using Sentinel-2 visible and NIR data

It is also possible to achieve further spatial resolution increase using specialized subpixel processing of pairs of emissivity distribution images [3]. Obtaining an image of enhanced spatial resolution from a pair of images of low spatial resolution is achieved by performing a sequence of actions:

- Generation of a noise distribution image common for both input images;
- Merge low-resolution input images into a common resampled image by interlaced scan to a grid of high resolution, replacing two pixels diagonally with pixels of input images, taking into account the subpixel offset and noise matrix;
- Estimation of the inverse operator matrix, due to rest of the pixels restoration;
- Restoration of the image of high spatial resolution;
- Iterative image reconstruction to eliminate irregularities and suppress noise.

References

1. Estoque R.C. Monitoring surface urban heat island formation in a tropical mountain city using Landsat data (1987-2015) / R.C. Estoque, Y. Murayama // ISPRS Journal of Photogrammetry and Remote Sensing, 133, pp. 18-29, 2017.
2. Sobrino J. A., Jiménez-Muñoz J. C., Paolini L. Land surface temperature retrieval from LANDSAT TM 5. / J.A. Sobrino, J.C. Jiménez-Muñoz, L. Paolini // Remote Sensing of Environment, 90, pp.434-440, 2004.
3. Станкевич С.А. Підвищення інформативності зображень теплового знімання на основі субпіксельного зміщення / С.А. Станкевич, С.В. Шкляр, В.М. Подорван, М.С. Лубський // Проблеми телекомунікацій, 2016. 10 міжнародна науково-технічна конференція, с. 40-24, 2016.

УДК 004.77

ОЦЕНКА ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ТРАКТА СВЯЗИ ПРОТОКОЛАМИ RTSP-ВИДЕОВЕЩАНИЯ В ЗАДАЧАХ ПЕРЕДАЧИ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЕЙ РЕАЛЬНОГО ВРЕМЕНИ

Ходнев Т.А., Варфоломеев А.Ю.
Кафедра КЭВА, Факультет Электроники,
КПИ им. Игоря Сикорского, Украина
E-mail: thodnev@gmail.com

Evaluating the efficiency of communication path utilization by RTSP broadcasting protocols in tasks of real-time video sequences transmission

In this paper, a method for estimating the efficiency of communication path usage by network protocols in the form of a number - the payload coefficient is proposed. Using the proposed method, the payload coefficient for the RTSP broadcasting protocols and the communication path based on an IP network with a point-to-point topology and an Ethernet frame was estimated.

Протоколы RTSP-видеовещания (связка RTSP – Real Time Streaming Protocol, RTP – Real-time Transport Protocol, RTCP – Real-time Transport Control Protocol) обладают низкой задержкой, дают возможность гибко управлять параметрами передаваемого видеопотока и широко применяются для организации трактов передачи видеопоследовательностей в реальном времени [1]. Тем не менее, протоколы RTSP и RTP работают на прикладном уровне модели OSI (Open Systems Interconnection), в связи с чем возникает вопрос относительно эффективности использования ими тракта связи [1, 2]. Исходя из того, что сведения о соотношении полезной нагрузки к общему объему передаваемых данных играют важную роль при разработке требований к телекоммуникационным сетям и их проектировании, а также оказывают влияние на их экономико-эксплуатационные параметры, разработка соответствующих способов оценки доли полезной нагрузки в передаваемых данных имеет высокую актуальность.

В работе предложен способ, позволяющий на основе экспериментальных данных оценивать меру эффективности использования тракта связи задействованными в нем протоколами (под эффективностью понимается показатель – коэффициент полезной нагрузки), строить математические модели зависимости коэффициента полезной нагрузки от параметров тракта, определять необходимую пропускную способность тракта при выбранных протоколах, сравнивать конкурирующие протоколы между собой по критерию эффективности использования тракта.

Из теоремы Шеннона [3] следует, что передача данных по каналу связи возможна тогда и только тогда, когда производительность источника

передаваемых данных не превышает пропускной способности канала (1).

$$S_C \geq H[S_S] \ , \tag{1}$$

где S_C – битовая скорость канала связи, бит/с; S_S – битовая скорость потока передаваемых данных, бит/с; *H[•]* – оператор информационной энтропии [3].

Для протоколов, не выполняющих сжатия данных, без учета возможности ошибочной передачи данных (будет учтено далее), неравенство (1) может быть записано в упрощенном виде (2).

$$S_C \geq S_S \ ; \tag{2}$$

Тогда разницу между битовыми скоростями потока передаваемых данных и канала связи можно учесть путем введения коэффициента полезной нагрузки, отражающего эффективность задействования пропускной способности тракта связи используемыми протоколами (3).

$$\overline{S_C} \cdot K_R = \overline{S_S} \ , \tag{3}$$

где $\overline{S_C}$ – средняя битовая скорость канала связи, бит/с; $\overline{S_S}$ – средняя битовая скорость потока передаваемых данных, бит/с; K_R – коэффициент полезной нагрузки ($0 < K_R \leq 1$).

В выражении (3), при необходимости, коэффициент полезной нагрузки K_R позволяет учитывать возможные накладные расходы, связанные с ошибками передачи данных в тракте связи. Более того, для сетей, построенных по многоуровневой модели OSI, K_R может быть подвергнут дальнейшей поуровневой декомпозиции.

Суть декомпозиции K_R состоит в следующем. В процессе передачи потока данных, на каждом последующем низлежащем уровне OSI выполняется дополнение PDU (Protocol Data Unit) предыдущего уровня заголовками, а также инкапсуляция и/или фрагментация данных. В результате, при отсутствии сжимающих преобразований, объем передаваемых данных на каждом последующем уровне OSI возрастает [2]. Таким образом, условие аналогичное (3) выполняется для каждого из уровней модели и результирующий коэффициент полезной нагрузки K_R может быть представлен в виде произведения коэффициентов полезной нагрузки каждого уровня OSI (4).

$$K_R = k_1 \cdot k_2 \cdot \ldots \cdot k_7 = \prod_{i=1}^{7} k_i \ , \tag{4}$$

K_R – результирующий коэффициент полезной нагрузки ($0 < K_R \leq 1$); k_i – коэффициент полезной нагрузки каждого из 7-ми уровней OSI ($0 < k_i \leq 1$).

Таким образом, декомпозиционный подход предоставляет широкие возможности для анализа экспериментальных данных пропускной способности сети, построения моделей, прогнозирования, анализа влияния каждого из уровней модели OSI на итоговую производительность сети и нахождения «узких мест» в производительности.

Предложенный способ использован для экспериментальной оценки эффективности использования протоколами RTSP-видеовещания тракта связи на основе IP-сети с топологией точка-точка и кадром формата Ethernet. Стоит заметить, что сам по себе протокол RTSP реализует управление потоком медиаданных, в то время как за передачу самих данных отвечает протокол RTP, а протокол RTCP осуществляет управление передачей данных в реальном времени [1].

В Linux-окружении была создана пара связных виртуальных Ethernet-интерфейсов, допускающих передачу jumbo-фреймов (с MTU равным 65536). В качестве RTSP-медиасервера использовался VideoLan VLC [4] версии 3.0.1, в качестве медиаплеера – MPlayer [5] версии 1.3.0. Для потокового вещания было отобрано 16 видеороликов длительностью от десяти секунд до одного часа с разной динамичностью картинки и произведено их предварительное кодирование в формат H.264 с заданием среднего битрейта равным 1700 бит/с. В качестве транспортного контейнера потока использовался MPEG-TS. Время кеширования потока медиаплеером задано равным 300 мс.

Было выполнено вещание и воспроизведение выбранных видеороликов с одновременным захватом фреймов виртуального Ethernet-интерфейса утилитой Wireshark [6] с последующим разделением траффика на RTCP-, RTSP- и RTP-составляющие и его дискретизацией с интервалом 1 с. На рис. 1 показаны результирующие графики битовых скоростей для видеоролика длительностью 205 с.

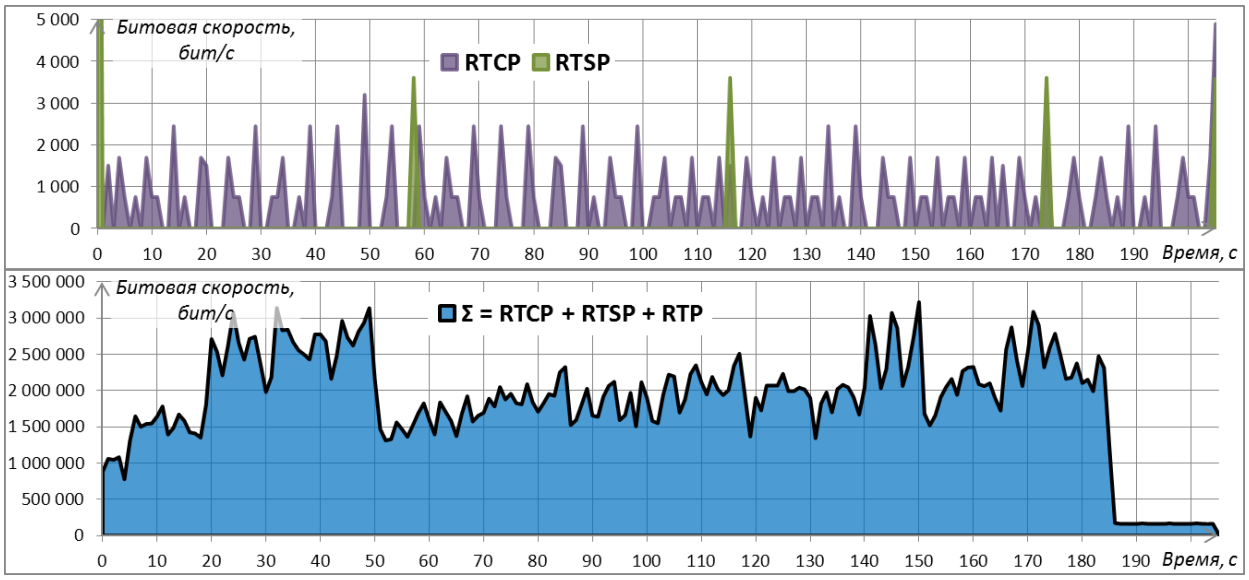


Рисунок 1. Битовые скорости RTSP-видеовещания

В ходе дальнейшего анализа с использованием соотношения (3) были рассчитаны средние значения коэффициента полезной нагрузки для каждого транслируемого видеоролика как отношение средней битовой скорости

суммарного потока RTCP+RTSP+RTP на канальном уровне OSI к заданной средней битовой скорости видеопотока. По результатам эксперимента, коэффициент полезной нагрузки лежит в пределах 0.922 ÷ 0.954. Также была проанализирована динамика изменения битовой скорости тракта. В ходе эксперимента максимальная битовая скорость не превышала 3.42 Мбит/с, со средним значением в 1.78 ÷ 1.84 Мбит/с и его среднеквадратичным отклонением не более 0.49 Мбит/с.

Выводы. В работе предложен способ, позволяющий на основании экспериментальных данных оценить эффективность использования тракта связи сетевыми протоколами в виде коэффициента полезной нагрузки.

Способ применен с целью определения коэффициента полезной нагрузки для протоколов RTSP-видеовещания (RTSP, RTP, RTCP) при передаче видеопоследовательностей реального времени для IP-сети с топологией точка-точка и кадром формата Ethernet.

На основании полученных результатов можно утверждать о сравнительно высокой эффективности задействования тракта связи семейством RTSP-протоколов видеовещания. В то же время, достаточно высокое значение максимальной битовой скорости тракта и отношения среднеквадратичного отклонения к средней битовой скорости свидетельствует о требовании в обеспечении запаса максимальной пропускной способности тракта, превышающей скорость передаваемого медиапотока.

Предложенный способ может быть использован для оценки эффективности используемых сетевых протоколов, построения соответствующих математических моделей, расчета необходимой пропускной способности тракта связи и сравнения конкурирующих протоколов между собой по критерию эффективности использования ими тракта связи.

Литература

1. Video Over IP: IPTV, Internet Video, H.264, P2P, Web RV, and Streaming: a Complete Guide to Understanding the Technology / W. Simpson – 2е изд. – Elsevier/Focal Press, 2008. – 500 с. – ISBN 978-0240810843.
2. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. / Олифер В. Г., Олифер Н. А. 4-е изд. — СПб.: Питер, 2010. — 944 с. ISBN 978-5-49807-389-7.
3. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи / В.А. Варгаузин, И.А. Цикин – СПб.: БХВ-Петербург, 2013 – 352 с. – ISBN 978-5-9775-0878-0.
4. VLC: Official site [Электронный ресурс] // Режим доступа: http://videolan.org/
5. MPlayer – The Movie Player [Электронный ресурс] // Режим доступа: http://mplayerhq.hu/
6. Wireshark [Электронный ресурс] // Режим доступа: http://wireshark.org/

UDC 528.852.6:519.652

MULTISPECTRAL REMOTE SENSING IMAGERY SUPERRESOLUTION: AFTER RESAMPLING

Piestova I.A.
Scientific Centre for Aerospace Research of the Earth, Kyiv, Ukraine
E-mail: pestovai@ukr.net

Вирівнювання просторової розрізненності багатоспектральних дистанційних зображень

У статті наводиться порівняння методів вирівнювання просторової розрізненності різних спектральних каналів багатоспектральних зображень до найкращої. Встановлено принципові недоліки та запропоновано новий підхід, що ґрунтується на аналізі просторових зв'язків опорних спектральних сигнатур.

The superresolution is very important when satellite images or separate bands of different spatial resolution used jointly. A comparison of methods for spatial resolution enhancement or equalizing of different spectral bands up to the best one was carried out.

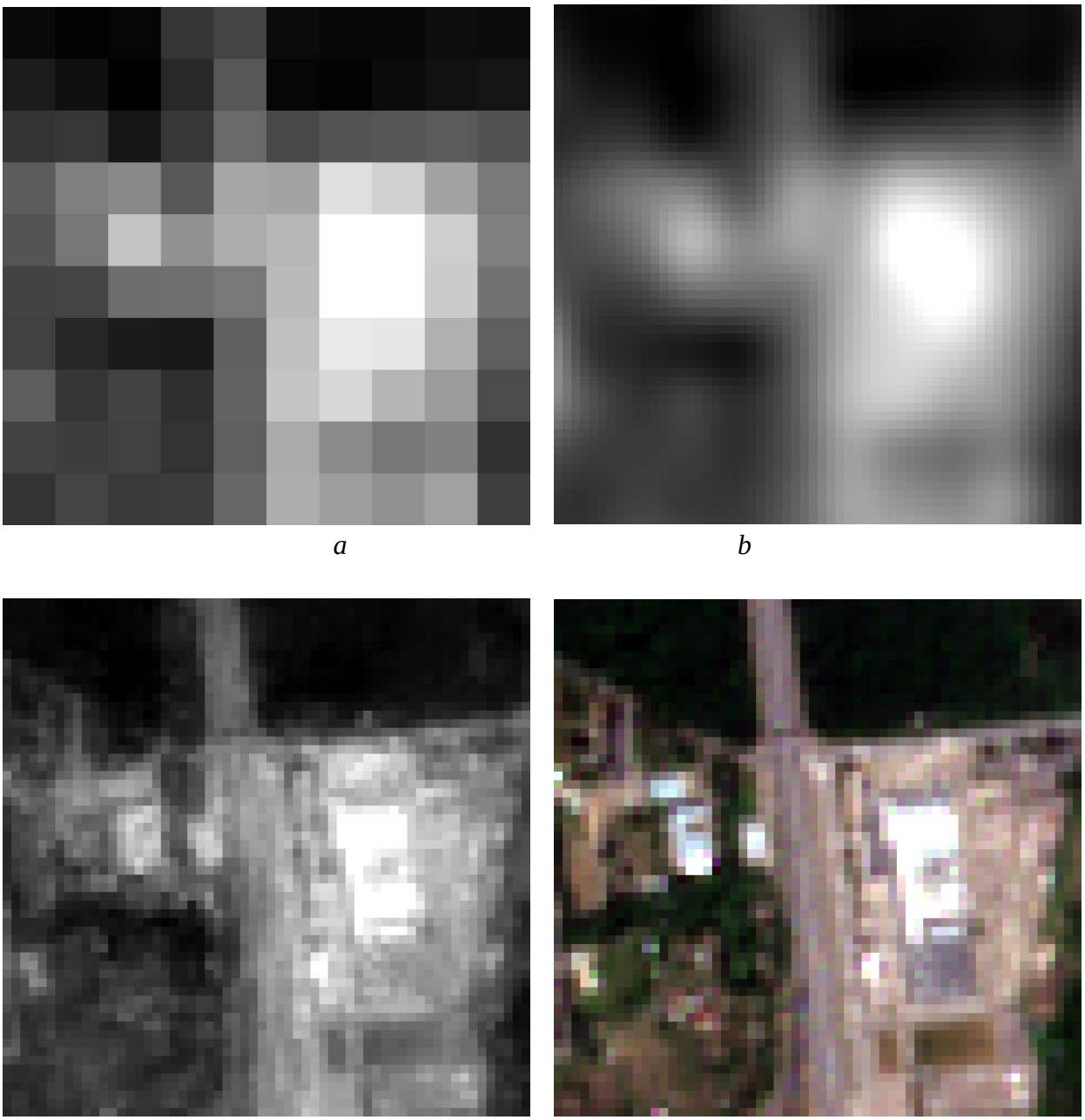
The following three methods were chosen for comparison. The first method consists in simply dividing the pixel by subpixels according to the nearest neighbor rule while preserving the value of original pixel [1]. The second method for calculating the subpixel value engages bicubic interpolation based on a certain number of adjacent pixels of the original image [2]. And the third one is super-resolving multiresolution images method with band-independent geometry of multispectral pixels (Sen2Res) [3]

The results of B1 (443 nm) band processing with a 60 m spatial resolution of the original Sentinel-2 multispectral image by three methods and a subset of the synthesized RGB image with a 10 m spatial resolution are shown in Fig. 1.

The results of B1 (443 nm) band processing with a 60 m spatial resolution of the original Sentinel-2 multispectral image by mentioned three methods as well as a subset of RGB synthesized image with a 10 m spatial resolution are shown in Fig. 1.

Superresolution is intended for two tasks solving. First, the spatial quality of the image should be improved, and secondly, the radiometric consistency of image should be kept up. The nearest neighbor method in comparison with the reference image (Fig. 1*a*) keeps the subpixels' radiometric values within the pixel, but is aliased-prone. Bicubic interpolation method (Fig. 1*b*) slightly smoothing image, but does not preserve radiometry. The average value of subpixels within a pixel is different from the source value of input image. Sen2Res method (Fig. 1*c*) performs

the required tasks quite successfully. The radiometry within the pixel is preserved, and the spatial improvement of the image occurs.



a *b*

c *d*

Fig. 1. The results of B1 (443 nm) band processing with a 10 m spatial resolution: *a* – nearest neighbor, *b* – bicubic, *c* – Sen2Res method, *d* – subset of the RGB synthesized image

Sen2Res method explicitly encodes geometric details from available high-resolution bands and preserves the spectral content of each low-resolution band independently from geometry.

It is proposed to take a method [4] based on the image classification (segmentation) [5] by spectral signatures and the redistribution of values in

subpixels, taking into account both the shape of the spectral signatures and spatial topology relationships for each type of land cover (Fig.2).

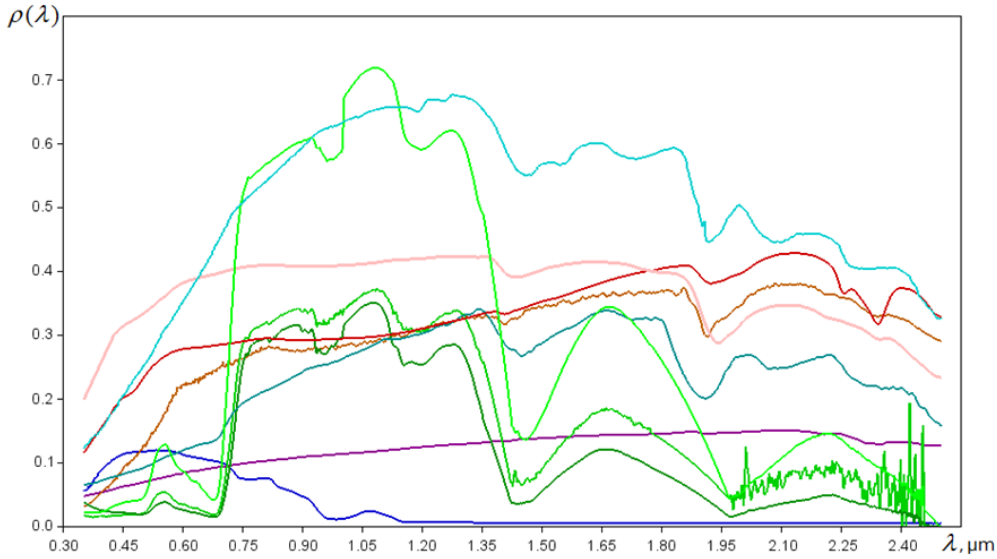


Figure 2. Spectral signatures of basic types of land cover

For each subpixel, similar to the reference spectral signatures, a topological description in *m* bands is calculated as

$$C(X) = \{\text{sign}\,(x_1 - x_2, \varepsilon_1 + \varepsilon_2), \ldots \text{sign}\,(x_{m-1} - x_m, \varepsilon_{m-1} + \varepsilon_m)\}$$
$$C(Y) = \{\text{sign}\,(y_1 - y_2, \sigma_1 + \sigma_2), \ldots \text{sign}\,(y_{m-1} - y_m, \sigma_{m-1} + \sigma_m)\} \quad (1)$$

where x, y – subpixel reflectance values, σ, ε – measurements errors.

The items number in the topological description for each signature depends on the number of bands.

References

1. Rukundo O., Cao H. Nearest Neighbor Value Interpolation // International Journal of Advanced Computer Science and Applications, 2012.– Vol.3.– No.4.– P.25-30.
2. Keys R. Cubic convolution interpolation for digital image processing // IEEE Transactions on Acoustics, Speech, and Signal Processing, 1981.– Vol.29.– No.6.– P.1153-1160.
3. Brodu N. Super-Resolving Multiresolution Images With Band-Independent Geometry of Multispectral Pixels // IEEE Transactions on Geoscience and Remote Sensing, 2017.– Vol.55.– No.8.– P.4610-4617.
4. Piestova I., Stankevich S., Kostolny J. Multispectral imagery superresolution with logical reallocation of spectra // Proceedings of the International Conference on Information and Digital Technologies (IDT 2017). – Žilina: IEEE, 2017.– P.322-326.
5. Stankevich S.A., Piestova I.A., Podorvan V.N. Deep learning concept for hyperspectral imagery classification // Central European Researchers Journal, 2016.– Vol.2.– No.1.– P.30-36.

УДК 621.396

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Степанов М.М., Ткаленко О.М.
Державний університет телекомунікацій, Україна
E-mail: tkalenko-oksana@ukr.net

FEATURES OF A WIRELESS SENSOR NETWORK

Recent advances in the construction of microelectromechanical systems in wireless communications and microprocessor technology led to miniaturized devices that consume little energy, including micro-sensor device is equipped with digital signal processing (DSP) and a wireless transceiver. Meaning sensors in medical technology of the future is simply priceless, they can provide remote monitoring of respiration, body temperature, blood pressure and other physiological characteristics of man. All devices and systems used by people in the personal space of self-tuning will automatically connect and interact with the outside through a gateway to global information environment.

Найновіші технології безпроводового зв’язку та прогрес в області виробництва мікросхем дозволили протягом останніх декількох років перейти до практичної розробки та впровадження нового класу розподілених комунікаційних систем – сенсорних мереж. Останні досягнення технологічного прогресу зробили можливим створення недорогих мініатюрних обчислювачів з надзвичайно малим енергозабезпеченням, які здатні об’єднуватися в мережу та взаємодіяти один з одним за допомогою безпроводових каналів зв’язку.

Сучасні досягнення у побудові мікроелектромеханічних систем в області безпроводового зв’язку та мікропроцесорної техніки призвели до появи мініатюрних пристроїв, які споживають мало енергії, включають мікро-сенсор, який облаштований пристроєм цифрової обробки сигналів (ЦОС) та безпроводовим прийомопередавачем. Такі пристрої можуть бути об’єднані у мережу з декількома тисячами вузлів. Такі мережі широко використовуються у підводній акустиці, польових військових системах спостереження, у пристроях електронної боротьби, в геофізиці, при сейсмічному віддаленому спостереженні, моніторингу оточуючого середовища, в біомедичних системах та ін. Об’єднані у безпроводову сенсорну мережу датчики утворюють розподілену самоорганізовану систему збору, обробки та передавання інформації.

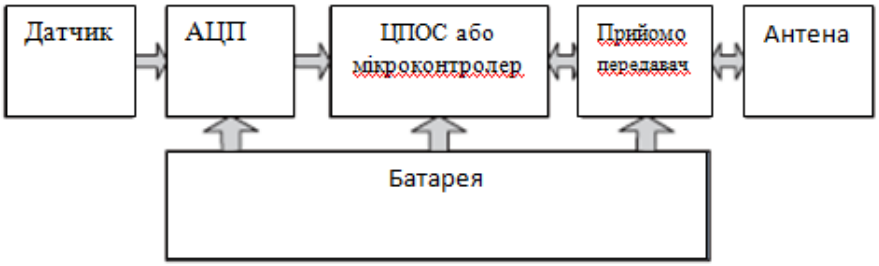


Рис.1 Типова структура БСМ і функціональна схема мота

Основна перевага БСМ – велика кількість вузлів, які покривають контрольовану область із визначеним ступенем рівномірності. Це дозволяє передавати інформацію від одного вузла до іншого, що економить енергію. У більшості випадків БСМ представляє собою багатокоміркову мережу, що має один вузол збирання даних та управління (рис.2).

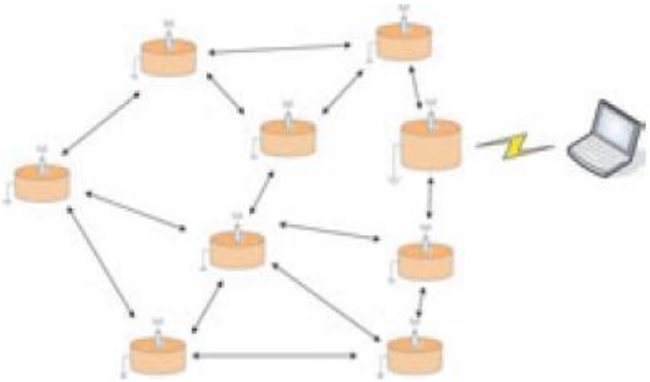


Рис. 2. Багатокоміркова БСМ

Основні відмінні ознаки БСМ: вузли мають малу активність або, іншими словами, малий трафік у мережі; вузли мережі розміщені дуже щільно, і кожний вузол має, як правило, більше, ніж два, доступні по радіоканалу вузли; вузли мають схильність до виходу з ладу, тобто пропадання вузлів внаслідок їх пошкодження або зменшення заряду батареї є штатною подією роботи мережі; топологія мережі підлягає змінам і не завжди може бути визначеною заздалегідь; вузли використовують широкомовну стратегію при передаванні даних і можуть не мати ніякого ідентифікатора або мережної адреси.

Основним стандартом передавання даних у сенсорних мережах є IEEE 802.15.4, який спеціально розроблений для безпроводових мереж з малопотужними прийомопередавачами.

Таблиця 1. Характеристики радіопередавання даних для IEEE 802.15.4

Смуга частот, МГц	**Чи потрібна ліцензія**	**Географічний регіон**	**Швидкість передавання даних, Кбіт/с**	**Кількість каналів**
868,3	Ні	Європа	20	1
902-928	Ні	Америка	40	1-10
2405-2480	Ні	Весь світ	250	11-26

Область застосування технологій БСМ стрімко розширюється. Сенсорні датчики здатні накопичувати інформацію та управляти різними процесами та об’єктами. Вони особливо необхідні для використання в агресивних середовищах та умовах, які є небезпечними для людини. За допомогою сенсорних мереж можуть ефективно вирішуватися задачі контролю навколишнього середовища, визначення сейсмічної небезпеки та спостереження за військовими об’єктами. У промисловості і в побуті їх можна використовувати для моніторингу технологічних процесів та

контролю функціонування систем забезпечення життєдіяльності людини. А значення сенсорів у медичних технологіях майбутнього просто безцінне: вони можуть забезпечувати дистанційне спостереження за диханням, температурою тіла, кров'яним тиском та іншими фізіологічними характеристиками людини. Де б не знаходилися датчики, вони, по мірі необхідності, об'єднаються у безпроводову мережу і будуть готові передавати отриману інформацію.

Таблиця 2. Основні характеристики мотів різних виробників

Параметри	**ML-Node-Z**	**ML-Node-U**	**ZigBit**
Мікроконтролер			
Процесор	Texas Instruments MSP430		ATmega1281
Тактова частота	Від 32,768 кГц до 8 МГц		4 МГц
Оперативна пам'ять	10 Кбайт		8 Кбайт
Flash-пам'ять	48 Кбайт		128 Кбайт
Прийомопередавач			
Тип	IEEE 802.15.4	Cypress WirelessUSBTM LP	IEEE 802.15.4
Діапазон частот	2400-2483,5 МГц		
Швидкість передавання даних	250 Кбіт/с	Від 15,625 до 250 Кбіт/с	250 Кбіт/с
Вихідна потужність	Від -24 до 0 дБм	Від -35 до 4 дБм	Від -28 до 3 дБм
Чуттєвість	-95 дБм	-93 дБм	-101 дБм
Антена	Чіп		1 або 2 чіпи
Зовнішні інтерфейси			
АЦП	12-розрядний, 7 каналів		10-розрядний, 3 канали
Цифрові інтерфейси	I2C/SPI/UART/USB		I2C/SPI/UART/IRQ/JTAG
Інші параметри			
Джерело живлення	Від 0,9 до 6,5 В		Від 1,8 до 3,6 В
Розміри	44x33x10 мм		19x14x3 мм
Температурний діапазон	Від -40 до 85°С	Від 0 до 70°С	Від 0 до 85°С

Наповнення навколишнього середовища гетерогенними сенсорами призведе до формування повноцінної PAN-«мережі персонального простору». Це означає, що всі прилади та системи, що використовуються людьми, у персональному просторі зможуть само- налаштувавшись автоматично зв'язатися та взаємодіяти через шлюз із зовнішнім глобальним інформаційним середовищем.

Література

1. Wang Z.M., Basagni S., Melachrinoudis E., Petrioli C. Exploiting sink mobility for maximizing sensor networks lifetime Big Island Hawaii: 2005. P.287.
2. Hu Fei. Wireless sensor networks: principles and practice / Fei Hu, Xiaojun Cao. – Boca Raton, FL [etc.]: CRC press, cop. 2010. – xxvii, 503 c.
3. Балонин Н.А., Сергеев М.Б. Беспроводные персональные сети на основе ZigBee: Учеб. пособие, СПбГУАП. СПб, 2012.

УДК 621.391

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ

Верес Л.А., Фесьоха Н.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
Військовий Інститут Телекомунікацій та Інформатизації імені Героїв Крут
E-mail: veresleonid@gmail.com, nadya_viti@i.ua

Prospects for the development of virtualization technologies

The paper considers the prospects for the development and environment of the use of virtualization technologies. The architectural decisions used in constructing modern IT infrastructures, problems arising during practical operation and ways of their solution are considered.

Зростаючі потреби бізнесу до кількості і, головне до якості ресурсів вимагають нового, більш системного підходу до побудови ІТ інфраструктури компанії. Віртуалізація серверів і робочих станцій висуває нові вимоги до систем зберігання даних, особливо важливі: швидкість доступу, гнучкість і надійність зберігання даних.

За даними Gartner, в 2012 році майже 58% x86 систем віртуалізовано. У 2015 році їх частка досягла 77%. Темпи віртуалізації не сповільняться. Кількість віртуальних машин, запущених в 2011 році, перевищує кількість віртуальних машин, запущених з 2001 по 2010 рр.

В результаті розвитку технологій, з'являються шести-, восьми-, шістнадцяти- ядерні процесори (і це ще не межа). Зростає пропускна здатність інтерфейсів комп'ютерів, а також ємність і чуйність систем зберігання даних, в результаті такого прогресу перед ІТ-службами виникають одна за одною проблеми:

1. Як уніфікувати безліч серверів і робочих станцій;
2. Як забезпечити сумісність додатків, операційних систем і апаратного забезпечення;
3. Як ізолювати одні сервіси і додатки від інших для зниження числа конфліктів;
4. Як оптимально завантажити нові потужні сервера.

Одним з підходів до вирішення цих проблем, який сьогодні набув широкого резонансу в ІТ-індустрії, є віртуалізація.

Корпорація Microsoft виділяє в своїй стратегії такі рівні перспектив розвитку віртуалізації ІТ, які представлено на рис.1.

Серед безлічі запропонованих рішень по віртуалізації, найбільший розвиток в комерційному застосуванні знайшли:

- віртуалізація представлень;
- віртуалізація операційної системи;
- віртуалізація додатків.

Рис. 1. Рівні перспектив розвитку віртуалізації ІТ

Як показує досвід, технологія віртуалізації представлень є доцільною для додатків, чия архітектура має серйозні обмеження на роботу в мережі, і в свою чергу може вирішувати наступні завдання:

- ізоляція користувача від фізичного комп'ютера шляхом надання на екран зображення і забезпечення засобами введення / виводу (миша, клавіатура, смарт-карти, USB-пристрої, принтери);
- розміщення на одному фізичному комп'ютері декількох робочих місць;
- підвищення безпеки інформації за рахунок обмеження фізичного доступу до серверів і робочих станцій;
- зниження витрат на обслуговування за рахунок ряду факторів: зниження енергопотреб, використання бездискових терміналів, уніфікація устаткування і програмного забезпечення.

Архітектура сучасних серверів x86 передбачає виконання тільки однієї ОС на сервері. Подолати таке структурне обмеження можна за допомогою віртуалізації серверів x86. Ця технологія абстрагує операційну систему та програми від рівня фізичного обладнання, що робить середовище серверів менш складною і більш адаптованою і рентабельною [1]. Завдяки віртуалізації на одному фізичному сервері можна завантажувати декілька операційних систем у вигляді віртуальних машин, у кожної з яких є доступ до обчислювальних ресурсів сервера (рис. 2).

Також не менш популярною є віртуалізація робочих станцій *Virtual Desktop Infrastructure (VDI).*

Віртуалізація робочих станцій дозволяє централізовано зберігати і обслуговувати додатки і дані будь-якої кількості ПК. Доступ до віртуальних робочих станцій здійснюється з клієнтських пристроїв з будь-якої точки земної кулі, де є Інтернет або через звичайну мережу [2].

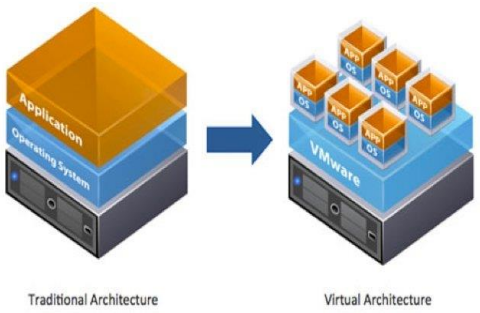


Рис. 2. Віртуалізація рівня серверів

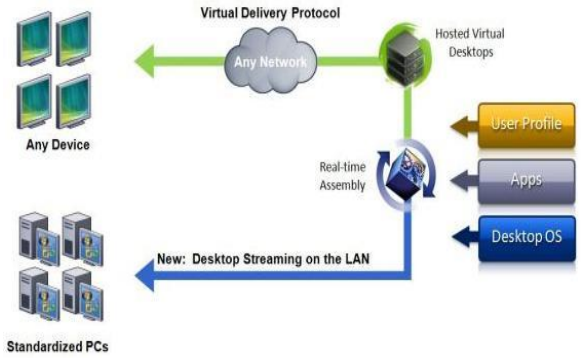


Рис. 3. Віртуалізація робочих станцій

Віртуалізація додатків - процес використання програми, перетвореної з тої що вимагає установки в операційну систему, в ту що цього не вимагає (потрібно тільки вигрузити її у свій десктоп). Для віртуалізації додатків програмне забезпечення віртуалізатора визначає при установці додатку що віртуалізується, які потрібні компоненти ОС та емалює їх, таким чином, створюється необхідне спеціалізоване середовище для конкретно цього віртуалізуємого додатку і, тим самим, забезпечується ізольованість роботи цього додатка.

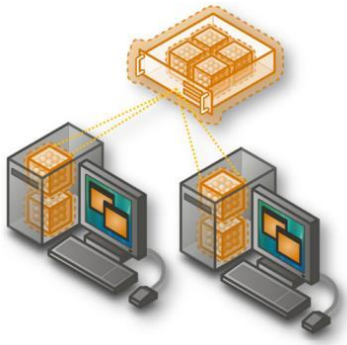


Рис. 4. Віртуалізація додатків

Таким чином, за останнє десятиліття технології віртуалізації зробили значний ривок вперед, завдяки чому стали масово використовуватися при вирішенні різних завдань. Використання різних технологій віртуалізації дасть змогу оперативна розгортати сервера, робочі станції і додатки, забезпечить відмовостійкість і знизить час відновлення після збоїв.

Література

1. Колесов А. Виртуализация операционных систем и приложений // PC Week/RE №10 (616) 25 марта — 31 марта 2008.
2. Самойленко А. Виртуализация: новый подход к построению IT-инфраструктуры // iXBT.com, 2007, http://www.ixbt.com/cm/ virtualization.shtml.

УДК 621.396

ПРОЕКТУВАННЯ СИСТЕМИ МОНІТОРИНГУ НА НЕБЕЗПЕЧНИХ ХІМІЧНИХ ПІДПРИЄМСТВАХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Марціленко С.В., Правило В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: s.martsilenko@gmail.com

Design of a monitoring system at hazardous chemical enterprises using IoT technology

In the given work the system of monitoring of equipment and work process automation is proposed, which is based on the Internet of Things technology (IT) to avoid accidents involving human chemical poisoning and preventing emergencies in hazardous chemical industry enterprises.

Сьогодні хімічна промисловість є однією із найбільших виробничих індустрій у всьому світі. Близько 20млн. людей мають роботу, пов’язану із цією сферою діяльності. При цьому дана сфера діяльності є найбільш небезпечною як для її працівників, так для споживачів і навколишнього середовища в цілому.

Останнім часом велика кількість підприємств у галузі хімічної промисловості все більше розгортають свої власні лабораторії для виведення рецептур із хімічних речовин для виробництва своїх продуктів. Це дозволяє більше контролювати об’єми виробництва у порівнянні з тим, коли вони використовували вже готові рецептури, придбані у підрядників та зменшити собівартість продукції. Але це створює і додаткові проблеми, пов’язані с безпекою.

Ці факти свідчать про те, що існує потреба у автоматизації великої кількості процесів на хімічних підприємствах для зниження рівня або оперативної ліквідації небезпеки.

Хімічні речовини несуть велику небезпеку, що збільшує ризик виникнення вибухів, пожеж або отруєння працівників на таких підприємствах. Тому виникає потреба у створенні системи, яка в відстежувала роботу обладнання, а також всі хімічні процеси у лабораторіях, а в подальшому і керувала ними замість людей.

Також хімічна промисловість виступає у ролі головного каталізатора сучасних прикладних інформаційно-комунікаційних технологій для підприємств.

Наразі вже існують певні технологічні рішення для автоматизованого керування виробничими процесами на хімічно-небезпечних підприємствах.

Наприклад, японська компанія «Kao» для автоматизації процесів,

пов’язаних із виробництвом нітрилу, що набув широкого використання, впровадила вже готове рішення: розподілену систему PlantPAx від компанії Rockwell Automation, що є актуальною для технологічних процесів, побудованих на базі стандарту ISA-S88. Дана система добре зарекомендувала себе на великих підприємствах, але для компаній, що мають набагато менші об’єми виробництва, а через це, і значно менший фінансовий оборот використання PlantPAx може бути не дуже доцільним як з фінансової точки зору, так і збоку функціональних можливостей цієї системи.

Працюючи на обладнанні хімічних підприємств без використання систем моніторингу та керування, працівники самостійно слідкують за параметрами, що забезпечують нормальні умови для роботи цього устаткування (показники температури та вологості, стан загазованості приміщення, тощо). Лаборанти в свою чергу готують приміщення та дотримуються чітких правил техніки безпеки під час роботи із небезпечними речовинами.

Такі правила техніки безпеки існують у кожній організації, однак не всі правила можуть бути чітко виконані через людський фактор. Через це існує потенційна небезпека виникнення фатальних випадків у на хімічних підприємствах.

У роботі запропоновано систему моніторингу основних виробничих процесів, що використовують технологію Інтернету Речей (IoT), для запобігання інцидентам безпеки в хімічних лабораторіях великих і малих компаній. Очікується, що безпеку у лабораторіях та інших приміщеннях і ефективність виробництва на підприємствах хімічної промисловості буде покращено шляхом застосування запропонованої системи на базі технології IoT. Крім того, можна відзначити, що на багатьох підприємствах дана система може покращити і економічну складову виробництва.

Вимоги сервісу. Перед побудовою системи моніторингу обладнання було сформовано основні вимоги для правильної постановки задач:

По-перше, потрібно розділити усі робочі ділянки, надаючи доступ лише тим людям, які працюють на певній ділянці (наприклад, у лабораторії). Це можна зробити за допомогою магнітного ключа або сенсора для зчитування даних (обличчя, відбиток пальця). Це допоможе швидко локалізувати пошук джерела аварії при її виникненні.

По-друге, необхідно на всіх ділянках встановити датчики температури, загазованості, розгерметизації і вологості приміщень. Це дозволить вчасно зупинити обладнання або експеримент у лабораторії при відхиленні цих значень від норми, а також в цілому запобігти будь-якій аварій.

Спроектована система відповідає усім зазначеним вимогам. Крім того, вона має декілька суттєвих переваг у порівнянні з відомими подібними рішеннями: відсутність спеціалізованого програмного забезпечення (всі

пристрої з'єднуються із обладнанням фізично), що робить даний сервіс універсальним; невисока вартість встановлення (в даному випадку близько 400 Євро); відсутність потреби у частому обслуговуванні.

Також даний сервіс доцільно використовувати з економічної точки зору. На підприємстві Rainway завдяки цій системі загальні витрати можна скоротити до 3000 Євро на місяць в середньому (діаграму показано на Рис. 1).

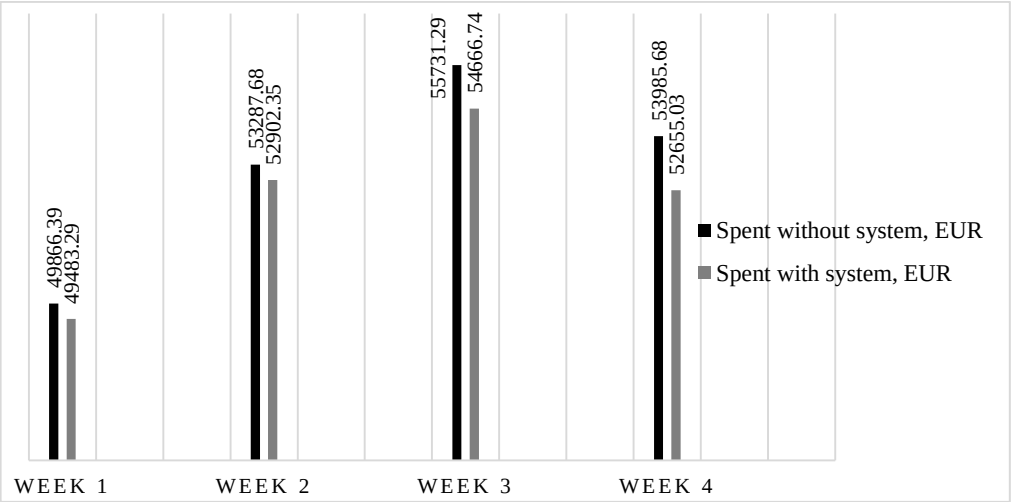


Рис. 1. Діаграма, що демонструє економію при використанні запропонованої системи

Системна архітектура. Було побудовано архітектуру запропонованої системи (Рис.2). Ця архітектура складається з трьох модулі (MSDS Manager, IoT Manager, та Employee Data Manager), бази даних та серверного обладнання.

MSDS менеджер отримує інформацію від менеджера IoT (відповідно до сенсорів) про стан робочої ділянки та склад речовин для лабораторії, яка записується до бази даних та передається на сервер. Також туди передаються дані про співробітника цієї ділянки, отримані від сенсорів відбитків пальців/розпізнавання обличчя.

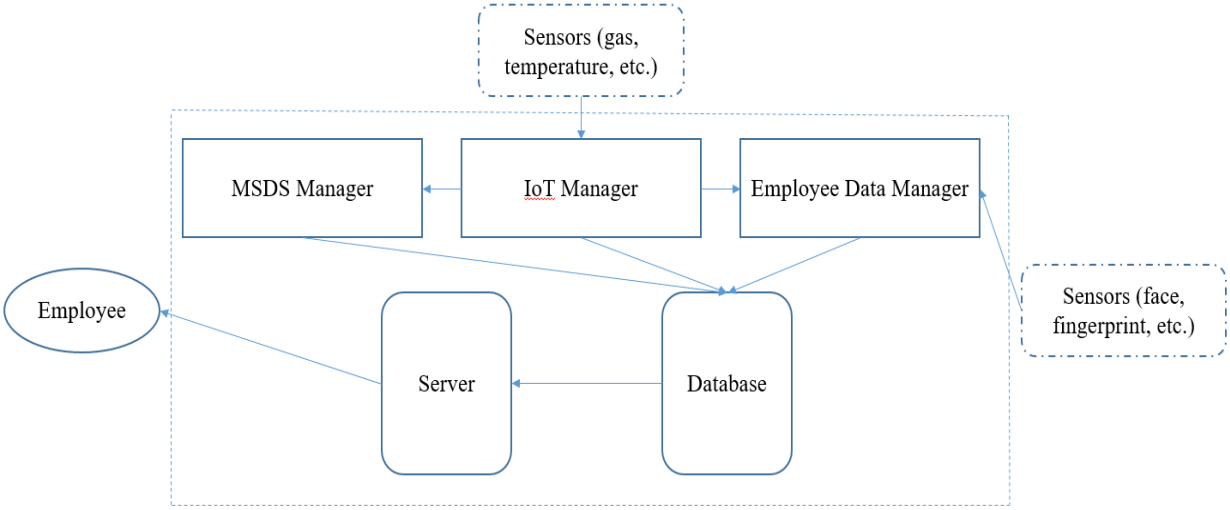


Рис. 2. Архітектура запропонованої системи

MSDS менеджер отримує інформацію від менеджера IoT (відповідно до сенсорів) про стан робочої ділянки та склад речовин для лабораторії, яка записується до бази даних та передається на сервер. Також туди передаються дані про співробітника цієї ділянки, отримані від сенсорів відбитків пальців/розпізнавання обличчя.

За допомогою цих даних працівники можуть розуміти, чи можна використовувати певні речовини для певних дослідів, а також контролювати умови робочого середовища.

Хімічна інформація - це дані, що базуються на MSDS, наданих органами державної охорони навколишнього середовища як відкриті дані. Інформація про MSDS складається з хімічних властивостей, ідентифікації небезпеки, інформації про заходи виявлення випадкового викиду, способу обробки, стабільності, реактивності, токсикологічної інформації тощо.

Менеджер IoT виконує обмін даними з датчиками Arduino та збирає дані, отримані від сенсорів. Дані датчика повинні зберігатися в базі даних і передаватися на сервер для її подальшої обробки.

У цій роботі пропонується система моніторингу та керування, яка використовує датчики IoT. Описано вимоги до обслуговування, архітектури та випадки використання для управління безпекою хімічної лабораторії. Запропонована послуга може поліпшити зручність експериментатора та адміністратора та безпеку хімічної лабораторії, а також контролювати всі виробничі процеси через датчики IOT. У майбутньому буде застосована сервісна архітектура на базі mashup. Оскільки Mashup підтримує сумісність з різними платформами, він може продемонструвати масштабованість та можливість використовувати цю службу.

Література

1. Y. Cohen, R. Waslo, D. Dickson, "Digital Transformation: Are Chemical Enterprises Ready?" Deloitte Journal, p. 4-12, Jan. 2017

2. The chemical industry, [Online]. Available: http://www.essentialchemicalindustry.org/the-chemical-industry/the-chemical-industry.html

3. Quimikao Uses Process Automation and Virtualization Technologies, [Online]. Available: https://www.rockwellautomation.com/global/news/case-studies/detail.page?pagetitle= Chemical-Producer-Quimikao-Uses-Process-Automation-and-Virtualization-Technologies-%7C-Case-Study&content_type = casestudy & docid = 1faf253ca85193cff97f6988876a24e5.

4. ISA-88. Formulation Management Standard, [Online]. Available at: https://appau.org.ua/news/isa-88-standart-upravlenyya-receptptermy-proyzvodstvom/.

5. A. Bradley, PlantPAx Distributed Control System, Rockwell Automation Section Guide, pp. 3-74, Apr. 2016.

УДК 621.391

АТАКА «ЧОРНА ДІРА» В МЕРЕЖАХ MANET

Вовк А.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: anastasiavitaliivna@ukr.net

Black-Hole Attack in Mobile Ad-hoc Network

Were discussed the black hole attack problem in the mobile ad-hoc network. There are various techniques which have been proposed by the researcher for dealing with the black hole attacks and these techniques have been classified into various categories according to their basic operation.

В останні роки активно впроваджуються бездротові децентралізовані мережі з самоорганізацією, що складаються з мобільних пристроїв MANET (Mobile Ad-hoc Network). Кожен пристрій такої мережі може незалежно пересуватися в будь-яких напрямках, і, як наслідок, часто розривати та встановлювати зв'язок з сусідами.

Мережі MANET мають наступні переваги над бездротовими мережами традиційної архітектури:

- можливість передачі даних на великі відстані без збільшення потужності передавача;
- стійкість до змін в інфраструктурі мережі;
- можливість швидкої реконфігурації в умовах несприятливого середовища з завадами;
- простота і висока швидкість розгортання мережі.

Однак мобільність вузлів веде до додаткового підвищення динамічності топології мережі і, отже, до можливості обриву зв'язку через перешкоди або включення/виключення вузла додається ймовірність його переміщення. Окрім цього, існує загроза атак на систему, найбільш відома з них атака «чорна діра».

Black-Hole Attack відома, як атака нападу на систему, що серйозно погіршує продуктивність мережі. У цьому типі атаки у мережі може бути один легітимний вузол або кілька таких вузлів. Коли існує два або більше легітимних вузлів, які співпрацюють один з одним, щоб порушити зв'язок, вони називаються кооперативними атаками «чорної діри». Напад, започаткований справжнім вузлом, називається візантійськими атаками [1]. У звичайному протоколі AODV, коли джерелу потрібно зв'язатися з місцем призначенням, воно передає пакет запитів, якщо не має шляху до місця призначення. Вузол призначення відправляє назад пакет відповіді на отримання запиту маршруту від проміжного вузла. Але атаці «чорна діра», «чорний» вузол на отримання маршрутного запиту пакета посилає у відповідь пакет з неправдивою інформацією, що має мінімальну кількість переходів у напрямку до місця призначення з дуже високим порядковим

номером. Високий номер послідовності вказує на свіжість шляху. При отриманні пакета відповідей з шкідливого вузла, вихідний вузол починає передавати пакети даних з шляху, який містить шкідливий вузол, а потім цей зловмисний вузол починає скидати пакет даних. В мережі маршрут встановлюється на базі двох основних параметрів відповідних пакетів, які є порядковим номером вузла призначення та кількістю переходів. Вузли можуть поводитися по-різному, як представлено в таблиці 1, де 1 означає справжню інформацію, а 0 означає фальшиву інформацію [4].

Таблиця 1. Поведінка вузла при наявності атаки і без неї

Номер призначення	*Кількість переходів*	*«Падіння» пакету*	*Атака*	*Тип атаки*
1	1	Ні	Ні	Відсутня атака
0	0	Так	Так	Black-Hole
0	1	Так	Так	Black-Hole
1	0	Так	Так	Black-Hole
1	1	Так	Так	Gray-Hole

Існують різні методики, які були запропоновані багатьма дослідниками для боротьби з атакою Black-Hole в MANET. Ці методики були класифіковані у десять основних категорій:

- *Криптографічна схема*. Вона включає в себе всі ті рішення, в яких криптографічні технології, такі як симетрична ключова криптографія, цифровий підпис або хешування, використовуються для цілей шифрування, перевірки цілісності для забезпечення захисту мережі від можливих атак.

- *Підслуховуюча схема.* Вона складається з усіх рішень, в яких звичайні мобільні вузли можуть підслухати передачу свого сусіда, щоб перевірити його чесність. Якщо виявиться, що його сусідній вузол виконує деяку несподівану подію, вона буде розглядатися, як шкідливий вузол, а потім інформація пошириться в мережі.

- *Послідовна кількість порогової схеми.* У цій категорії вихідний вузол обчислює порогове значення вартості, використовуючи параметр номера послідовності вузла призначення відповідного пакета і скидає відповідний пакет, якщо він містить номер послідовності, що перевищує порогове значення. Пороговим значенням може бути статичний тип або динамічний тип.

- *Підтвердження на основі схеми.* У цій категорії відправляється пакет вузлу, що має підтвердити про вдалий прийом пакетів.

- *Кластеризована схема.* У цій схемі мережа розділена на кластер, в яких «головний» виявляє атаку чорної діри та повідомляє про це в мережі.

- *Крос-шарова схема співпраці.* У цьому розділі вона охоплює всі ті рішення, в яких більш, ніж два шари співпрацюють один з одним для виявлення шкідливої активність у мережі.

- *Схеми на основі перехресної перевірки.* У цій схемі перехресну перевірку виконує вихідний вузол з іншим вузлом так, щоб природу

проміжного вузла можна виявити. Потрібно використовувати перехресну перевірку без даних таблиці DRI (даних маршрутизації) .

- *Схеми, засновані на довірі.* Він включає в себе рішення, які обчислюють довіру до вузла цінності на основі сусідньої передачі, яка допомагає у виявленні природи вузла, чи злочинець чи нормальний. Якщо довірче значення будь-якого вузла менше, ніж порогове, він вважається шкідливим, інакше - нормальним вузлом.

- *Схеми, основані на IDS.* Ця схема базується на спеціальних вузлах, які називаються IDS вузли, які мають можливість виявити зловмисну діяльність, підслуховуючи її біля передачі і коли виявлено будь-яку аномалію, вона передає повідомлення в мережі - ізолювати її.

- *Інші схеми.* У цій секції є багато рішень, які не підпадають під зазначені вище категорії. Крім цього деякі рішення базуються на механізмі кешування відповідей, повторюється наступний перехід на базі тощо[3].

Як правило, основним не правильним припущенням, яке відноситься до MANET, є те, що кожен вузол є довіреним вузлом. В реальному сценарії існують деякі ненадійні вузли, які виконують атаку «чорна діра», в якій неправильні вузли притягують весь трафік до себе, надаючи неправдиву інформацію про те, що він має мінімальний шлях до пункту призначення з дуже високим порядковим номером призначення та знижує всі пакети даних. Висвітлено різні категорії технік для пом'якшення впливу атаки Black-Hole, які необхідно розглянути під час розробки ефективного протоколу.

Література

1. A. R. Sangi, J. Liu, and L. Zou, “A performance analysis of AODV routing protocol under combined byzantine attacks in MANETs,” International Conference on Computational Intelligence and Software Engineering, pp. 1–5, 2009.
2. Метелёв А.П., Чистяков А.В., Жолобов А.Н. Протоколы муршрутизации в беспроводных самоорганизующихня сетях [Електронний ресурс] / Метельов А.П., Чистяков А.В. та інші. Режим доступу: https://cyberleninka.ru/article/v/protokoly-marshrutizatsii-v-besprovodnyh-samoorganizuyuschihsya-setyah.
3. Shashi Gurung, Siddhartha Chauhan A review of black-hole attack mitigation techniques and its drawbacks in Mobile Ad-hoc Network [Електронний ресурс] / Shashi Gurung, Siddhartha Chauhan Режим доступу: ieeexplore.ieee.org/document/8300186.
4. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative black hole attack in wireless ad hoc net-works,” [Електронний ресурс] / S. Ramaswamy, H. Fu, M. Sreekantaradhya та інші Режим доступу: https://pdfs.semanticscholar.org/ eff7/532e9de97faa4d746b0f37997baf67f68879.pdf.

УДК 621.396

БЕЗДРОТОВИЙ КОНТРОЛЬ ТА МОНІТОРИНГ ЕНЕРГОЄМНОСТІ СПОЖИВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ ZIGBEE

Богданова В.А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:vladabohdanova@gmail.com

Wireless Controlling and Monitoring the Consumption Energy Meter based on ZigBee Technology

This paper introduced a proposed system to development the way of controlling, monitoring, and reading the consumer energy meter by remote wireless ZigBee communication network. The ZigBee is advancing global standard in wireless communications with the low cost, low data rate, and low power consumption.

Традиційний електромеханічний лічильник енергії, який використовується у кожного споживача будинку, може бути змінений. Представлений варіант лічильника обчислює кількість споживаних одиниць завдяки схемі управління, представленою мікроконтролером, який забезпечує годинник реального часу, рідкокристалічний дисплей, що показує споживану енергію та час, а також пам'ять для збереження споживаних даних під час розриву живлення. Це рішення системи контролю, моніторингу та автоматичного читання бездротової енергії дозволяє передавати свої дані за допомогою бездротового зв'язку на базові станції, де здійснюється моніторинг та аналіз даних від споживача енергії для управління енергією. Крім того, система може уникати помилок при зчитуванні вимірювального приладу вручну, а також помилок витоку вимірювань, швидкого, точного, економічного, гнучкого та надійного режиму моніторингу використання електричної енергії.

Електрична енергія має величезний вплив на життя людини. Автоматизація розподілу енергії також є важливою для поліпшення життя людей. Швидке зростання бездротового зв'язку та широке використання мікроконтролерів, призводять до значних покращень у автоматизації багатьох промислових сторін, щоб зменшити ручні зусилля. Ручне зчитування лічильника енергії є неефективним для операційних цілей, що призводить до розсіювання людських зусиль. Автоматизована система контролю, моніторингу та читання вимірювальних приладів буде важливим технічним прогресом, що може призвести до підвищення рівня життя. Також, ця система вирішує кілька питань традиційної системи вимірювання показників, таких як потреба в людських ресурсах, затримка роботи, точність, ефективність. Платіжна система для споживання енергії вручну здійснюється спеціальними працівниками. Дані, зібрані ними,

використовуються для розрахунку білінгу. Ручний процес білінгової системи можна вважати витратою часу і може викликати певні помилки через людський фактор. Таким чином, існуюча білінгова система є досить неефективною та неточною.

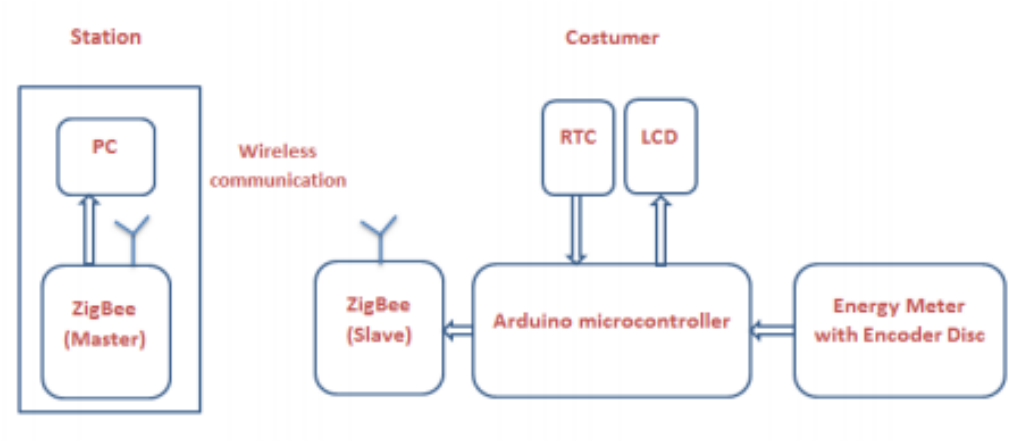


Рис. 1. Пропонована система

ZigBee Device: збирає та зберігає оновлені дані. Потім він передає дані безпосередньому маршрутизатору або концентратору за запитом. Маршрутизатор ZigBee: він передає отримані дані від інших пристроїв ZigBee або передає їх іншим пристроям - ZigBee безпосередньому координатору або маршрутизатору. Концентратор: він має можливість збирати, зберігати та передати вимірювальні дані з інших лічильників. Апаратне забезпечення системи складається з двох частин: 1- Модифікований лічильник енергії, крім того, система включає LCD, щоб відображати результат вимірювань, 2 - частина станції, яка складається з ZigBee для отримання переданих даних з іншого пристрою ZigBee, встановленого на змінену частину. Отримані дані з'являються на РК-дисплеї.

Завдяки швидкому вдосконаленню технології зв'язку, електромеханічний лічильник енергії може використовувати технологію ZigBee для збору споживаних даних від клієнтів. ZigBee - це технологія бездротового зв'язку з двостороннім зв'язком, що має додаткові функції, такі як низьке енергоспоживання на короткій відстані, низька швидкість передачі даних, низьке енергоспоживання, низька складність та низька вартість. Він в основному використовується для обміну даними між малопотужними електронними пристроями на короткий проміжок часу. Мережа ZigBee схожа на телекомунікаційні мережі, такі як GSM або CDMA.

Технічні особливості включають:

1. Надійність: мережа використовує механізм запобігання зіткненню, зберігається спеціальний часовий проміжок до постійної пропускної здатності служби зв'язку, це дозволяє уникнути конфліктів та конкуренції, коли дані передаються. Рівень MAC використовує перевірку переданих

даних, після чого кожен пакет відправлених даних повинен чекати, щоб отримати підтвердження.

2. Безпека: ZigBee пропонує аутентифікацію цілісності даних та перевірку. Використовує алгоритм захисту AES-128.

3. Економія енергії: завдяки дуже короткому циклу роботи, передавання та отримання даних мають низьке енергоспоживання.

4. Короткі затримки: поліпшення затримок зв'язку для чутливих програм. Час затримки зв'язку дуже короткий.

5. Висока ємність мережі: мережа ZigBee може забезпечити розміщення максимально 65536 пристроїв.

Мережевий рівень ZigBee підтримує три структури топології, що представляють топологію зірки, дерева та сітки. Топологія структури мережі, очевидно, є Point to point. У структурі топології зірка є пристрій, який називається координатором ZigBee, який використовується для запуску та відновлення пристроїв мережі, а інші пристрої - для спілкування з координатором ZigBee.

Діапазон зв'язку та покриття зв'язку ZigBee відносно невеликий. Діапазон покриття мережі може бути розширений маршрутизатором ZigBee. Методи зв'язку технології ZigBee представлені трьома моделями, це широкосмугова, одноадресна та багатоадресна передачі. Дані одноадресної передачі можна перенести на конкретний окремий пристрій. Дані передачі можуть бути передані всім пристроям у мережі. Дані багатоадресної передачі можуть бути перенесені на всі пристрої в різні групи, також можна назвати груповою копією. Основними перевагами технології ZigBee є швидкість передачі даних серед багатьох електронних пристроїв на короткий проміжок часу. Типи даних передачі - це періодичні дані (такі як контроль освітлення), повторювані дані з низькою затримкою та періодичні дані (наприклад, дані датчиків).

Переваги цієї системи можна узагальнити шляхом скасування робочої сили людини та зменшення помилки, яка виникає при ручному виставленні рахунків. Також система має економічну перевагу внаслідок того, що вона може зменшити вартість проектування та експлуатації.

Література

1. Noof T. Mahmood and Eyad I. Abbas. Wireless Controlling and Monitoring the Consumption Energy Meter based on ZigBee Technology. International Journal of Current Engineering and Technology. E-ISSN 2277 – 4106, P-ISSN 2347 – 5161.
2. Jinsoo Han, Chang-sic Choi, Wan-ki Park, Ilwoo Lee, Sang-ha Kim. Smart home energy management system including renewable energy based on ZigBee and PLC. IEEE Transactions on Consumer Electronics, 198 – 202,14 July 2014.
3. Citation: Zillner, T. (2016). ZigBee Exploited: The good, the bad and the ugly. Magdeburger Journal zur Sicherheitsforschung, 12, 699–704. Retrieved September 2, 2016.

УДК 621.396

АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В СЕНСОРНИХ МЕРЕЖАХ

Лейко А.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: leven1996@gmail.com

ANALYSIS OF PROTOCOLS OF ROUTES IN SENSOR NETWORKS

The purpose of carried out work is analysis of routing protocols of sensor networks. Characteristics of efficiency of routing protocols are presented in this work and comparing analyze of these protocols was made. The recommendations for their use are given.

Останнім часом БСМ знайшли застосування у широкому колі систем із вимогами та характеристиками, що значно відрізняються. Не дивлячись на наявність сімейства стандартів, багато аспектів роботи та побудови БСМ є не стандартизованими. Використання протоколу, який би ефективно забезпечував роботу БСМ в заданих умовах, при певних параметрах і в залежності від типу вимірюваних величин, є важливою проблемою. Тому ефективність, адекватність одержуваних даних і час життя БСМ безпосередньо залежить від протоколу маршрутизації.

Аналізуючи наступні протоколи можна визначити їх основні параметрами, які впливають на вибір протоколів для конкретних цілей.

В таблиці 1 приведено порівняльну таблицю протоколів маршрутизації сенсорної мережі [1].

Таблиця 1. Порівняльна таблиця протоколів маршрутизації в сенсорній мережі

Протокол маршрутизації	Класифікація	Енергозбереження	Агрегація даних	Масштабованість	По запиту
SPIN	Однорідний/ Ініційована джерелом/ Дата-орієнтований	Обмежено	Так	Обмежено	Так
DD	Однорідний/ Дата- орієнтований/ Ініційована метою	Обмежено	Так	Обмежено	Так
RR	Однорідний	Низька	Так	Висока	Так
LEACH	Ієрархічний /Ініційована метою /Вузло-орієнтований	Висока	Так	Висока	Ні
TEEN & APTEEN	Ієрархічний	Висока	Так	Висока	Ні
PEGASIS	Ієрархічний	Макс.	Ні	Висока	Ні
SOP	Ієрархічний	Низька	Ні	Висока	Ні
GAF	Ієрархічний / За розміщенням	Обмежено	Ні	Висока	Ні
GEAR	За розміщенням	Обмежено	Ні	Обмежено	Ні
SAR	Дата-орієнтований	Висока	Так	Обмежено	Так
SPEED	За розміщенням/ Дата-орієнтований	Низька	Ні	Обмежено	Так

Протокол маршрутизації	Кількість службової інформації	Модель доставки даних	Локалізація	Мобільність	QoS	Кількість службової інформації
SPIN	Низька	Керується подією	Ні	Можлива	Ні	Низька
DD	Низька	Керується вимогою	Так	Обмежена	Ні	Низька
RR	Низька	Керується вимогою	Ні	Дуже обмежена	Ні	Низька
LEACH	Висока	Керується головним вузлом кластера	Так	Фіксований	Ні	Висока
TEEN & APTEEN	Висока	Активний поріг	Ні	Фіксований	Ні	Висока
PEGASIS	Низька	На основі ланцюгів	Так	Фіксований	Ні	Низька
SOP	Висока	Неперервна	Ні	Ні	Ні	Висока
GAF	Змінна	Віртуальна решітка	Ні	Обмежена	Ні	Змінна
GEAR	Змінна	Керується вимогою	Ні	Обмежена	Ні	Змінна
SAR	Висока	Неперервна	Ні	Ні	Так	Висока
SPEED	Низька	Географічна	Так	Ні	Так	Низька

Порівнюючи приведені протоколи не можна зробити висновок, що один із них є найкращим, але очевидно, що кожний протокол маршрутизації буде «сильнішим», а також буде виконувати поставлені задачі правильно і з максимальним забезпеченням якості обслуговування, якщо поставити правильне технічне завдання, а також коректно вибрати протокол маршрутизації. Звичайно, ефективна робота бездротової сенсорної мережі залежить також і від інших чинників, таких як: локалізація вузлів, кількості вузлів, фізичних характеристик вузлів, зовнішньої захисної оболонки і т.д. Але основним чинником є протокол маршрутизації [2].

1. Протоколи сімейства SPIN добре підходять для додатків, де вузли мобільні, так як їм необхідно тільки локальна інформація про сусідів. Недоліком протоколів являється те, що вони не гарантують доставку даних

2. Directed Diffusion використовує обробку/об'єднання даних усередині мережі. Досягає бажаної глобальної поведінки за допомогою локальної взаємодії. Емпірично адаптується до навколишнього оточення.

3. Rumor Routing працює добре тільки коли кількість подій мала. Має зайві витрати на підтримку великої кількості агентів і таблиці подій.

4. LEACH дозволяє проводити обробку даних на cluster-head'і, що може зменшити кількість даних переданих по мережі. Оптимальна кількість кластерів може бути визначено заздалегідь залежно від топології мережі і відношення витрат на обробку/передачу інформації. Перша «смерть» вузла відбувається у вісім разів пізніше, ніж при використанні прямої передачі і статичних кластерних протоколів

5. PEGASIS формує не кластери, а ланцюжки. Дані передаються по ланцюжку і один вузол їх посилає. Краще ніж LEACH за енергетичними показниками. Великі затримки для вузлів на кінцях ланцюжка.

6. TEEN добре підходить для додатків критичних до часу. Має менші енергетичні витрати ніж проактивні протоколи. «М'яка» межа може адаптуватися. «Жорстка» межа може варіюватися в залежності від додатків. Не підходить для періодичного моніторингу.

7. APTEEN: на відміну від TEEN вузол повинен зібрати і передати дані, якщо вони не були відправлені за певний період часу (count time), який встановлюється CH. У порівнянні з алгоритмом LEACH, APTEEN споживають меншу кількість енергії. Має накладні витрати і складність формування багаторівневих кластерів і організації порогових функцій.

8. SOP підходить для додатків де потрібний зв'язок з певним вузлом. Має невеликі витрати на підтримку таблиці маршрутизації. Збереження енергії: використання обмеженого підмножини вузлів. Даний протокол не є протоколом «на вимогу» особливо, що стосується організаційної фази. Існування безлічі розривів підвищує ймовірність реорганізації мережі (витратна операція).

9. GAF - протокол який погано масштабується. Тільки активні вузли посилають інформацію, тому точність інформації не дуже висока.

10. SAR: вибір маршруту залежить від трьох чинників: енергетичні ресурси, QoS на кожен маршрут і рівень пріоритету пакета.

11. SPEED: Кожен вузол зберігає інформацію про своїх сусідів і використовує географічну інформацію для знаходження шляхів [3]. Прагне гарантувати постійну швидкість доставки. Вибирає маршрут на основі затримки відповіді на запит.

Література

1. В. М. Безрук, Восточно-Европейский журнал передовых технологий / В. М. Безрук, А. Н. Зеленин, В. А. Власова, Ю. В. Скорик, Ю. Н. Колтун // Міжнародний наукометричний науковий журнал, 2016.
2. Зеляновський М. Ю. Методи і протоколи обміну даними сенсорних мереж[Текст] / М. Ю. Зеляновський, О. В. Тимченко. – Київ: Зб. наук. пр. ІПМЕ НАН України., № 46, pp. 176-183, 2008.
3. Tian H. SPEED: A stateless protocol for real–time communication in sensor networks [Text] / H. Tian, J. A. Stankovic L. Chenyang, T. Abdelzaher // 23rd International Conference on Distributed Computing Systems, 2003.
1. Villalba L. J. G. Routing Protocol in Wireless Sensor Networks [Text] / L. J. G. Villalba, A. L. S. Orozco, A. T. Cabrera, C. J. B. Abbas // Sensors. – 2009. – Vol. 9. – P. 8399–8421.

УДК 621.396

ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Якорнов Є.А., Цуканов О.Ф.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
E-mail:yakornov@its.kpi.ua

Determine the effectiveness of routing protocols of the wireless sensor network

The method of determination of general index of efficiency of protocols is offered routing of wireless sensory networks (WSN), which does not need bringing in of experts by the account of partial indexes after the different scales of influence on the basis of the use of weigher coefficients of Fishbern.

Задача визначення загального показника ефективності протоколів маршрутизації БСМ відноситься до загальновідомого кола задач оцінки ефективності складних технічних систем [1]. В роботі запропоновано метод визначення загального показника ефективності шляхом векторної оптимізації часткових показників ефективності протоколів маршрутизації за різних умов моделюванні їх роботи. Сутність метода полягає в побудові ряду з вагових коефіцієнтів часткових показників ефективності БСМ a_i за умов:

$$a_1 < a_2 \ldots < a_N, \quad a_{i+1} - a_i = const, \quad \sum_{i=1}^{N} a_i = 1.$$

де a_i − вагові коефіцієнти Фішберна − раціональні дроби, в знаменнику яких стоїть додаток арифметичної прогресії перших членів натурального ряду з кроком 1, а в чисельнику - убутні на 1 значення натурального ряду від N до 1 (наприклад, 3/6 , 2/6, 1/6 в сумі дають одиницю). Тоді сума отриманих чисельників є спільним знаменником дробів Фішберна [2]: Перевага по Фішберну визначається в зменшенні на одиницю чисельника раціональної дробу вагового коефіцієнта відповідного показника ефективності.

Часткові показникі ефективності F_i	a_1	a_2	a_3	a_4
$F_1 \approx F_2 \approx F_3 \approx F_4$	1/4	1/4	1/4	1/4
$F_1 > F_2 \approx F_3 \approx F_4$	2/5	1/5	1/5	1/5
$F_1 \approx F_2 > F_3 \approx F_4$	2/6	2/6	1/6	1/6
$F_1 \approx F_2 \approx F_3 > F_4$	2/7	2/7	2/7	1/7
$F_1 > F_2 > F_3 \approx F_4$	3/7	2/7	1/7	1/7
$F_1 > F_2 \approx F_3 > F_4$	3/8	2/8	2/8	1/8
$F_1 \approx F_2 > F_3 > F_4$	3/9	3/9	2/9	1/9
$F_1 > F_2 > F_3 > F_4$	4/10	3/10	2/10	1/10

При моделюванні сенсорних мереж за допомогою TOSSIM [3] або подібних засобів моделювання спостерігається висока ступень адекватності моделі до реальної поведінки мережі. Дані засоби, фактично, розроблені для випробування програмних чи протокольних рішень без фактичного використання обладнання, що економічно виправдано, особливо при моделюванні великомасштабних мереж.

Метод аналізу полягає у побудові на основі даних моделювання векторів величин для різних протоколів маршрутизації. Такими величинами являються досліджувані параметри, а саме часткові показники ефективності БСМ, зокрема такі, що характеризують: енергоспоживання, пропускну здатність, затримку і т. п. При цьому, вектор часткових показників ефективності є функцією від наступних параметрів БСМ: кількості вузлів в мережі, щільності розміщення вузлів, умов розповсюдження радіохвиль і протоколу маршрутизації.

Спочатку визначаємо часткові показники ефективності БСМ. При цьому вектор часткових показників ефективності $I_n = [x_1, x_2 \ldots x_n]$ замінюється нормованим вектором $I_n* = [x_1*, x_2* \ldots x_n*]$, де $x_i^* = \frac{x_i}{x_{N_i}}$ – нормовані безрозмірні значення величин, x_{N_i}– нормуючі величини, за які можуть бути прийняті будь-які співрозмірні величини. Для зручності приймаються значення із вектора I_n^N, що також є результатом моделювання, але для попередньо обраного протоколу маршрутизації, за нормуючі значення приймаються величини для протоколу Directed diffusion.

Далі нормований вектор множиться на вектор стовпець вагових коефіцієнтів [2] $A = (\alpha_1, \alpha_2 \ldots . \alpha_n)^T$, де α_i – вагові коефіцієнти Фішберна, що визначає важливість конкретного критерія при дослідженні. Знак α_i визначається в залежності від напрямку оптимізації: у випадку необхідності максимізації критерія знак «+» і в разі необхідності мінімізації. Після перемноження векторів I_n* та A отримаємо скалярну безрозмірна величину S, яка характеризує загальний показник ефективності протоколу маршрутизації БСМ:

$$S = I_n^* \times A = [x_1^*, x_2^* \ldots x_n^*] \times [\alpha_1, \alpha_2, .. \alpha_n] = \alpha_1 x_1^* + \alpha_2 x_2^* + \cdots + \alpha_n x_n^* = \sum_{i=1}^{n} \alpha_i x_i^*.$$

В роботі пропонується використовувати множину точок моделювання, одразу для кількох параметрів для кожного окремого протоколу маршрутизації. Таким чином, порівнюючи дані - множини для різних протоколів та шукаючи їх перетини, можна визначити діапазони оптимальних параметрів часткових показників ефективності для застосування конкретного протоколу маршрутизації БСМ.

Для визначеного протоколу маршрутизації БСМ за результатами моделювання будується функція загального показника ефективності протоколу маршрутизації БСМ $S(\gamma_k)$, $k = \overline{1, m}$, де m – кількість вхідних

параметрі, а γ_k – вектор вхідних параметрів: кількість вузлів, щільність вузлів і т. п., крім протоколу маршрутизації. в.

Таким чином, результатом розрахунків методу аналізу є сукупність функцій багатьох змінних:

$$S_j(\gamma_k) = \sum_{i=1}^{n} \alpha_i x_{ij}(\gamma_k),$$

де j – індекс, що відповідає певному протоколу маршрутизації $j = \overline{1,J}$,

J – кількість протоколів маршрутизації що аналізуються;

$x_{ij}(\gamma_k)$ – результат моделювання i – того часткового показника ефективності БСМ (енергоспоживання, затримка, продуктивність і т. п.) для j-го протоколу маршрутизації із J – розглядуваних змінних часткових вхідних параметрів γ_k; $k = \overline{1,K}$, де K – кількість змінних вхідних параметрів.

Імітаційне моделювання з метою визначення загального показника ефективності БСМ здійснювалось для двох основних параметрів БСМ: величина кроку вузлів та кількості вузлів БСМ.

Результати надаються у вигляді тривимірних графіків залежності загального показника ефективності $S_j(\gamma_k)$ j - го протоколу маршрутизації від кроку вузлів s_{vz} та кількості вузлів t_{vz} БСМ:

$$S_j(\gamma_k) = GR(s_{vz}, t_{vz}).$$

Залежності тільки від двох параметрів дозволяють візуально визначити екстремальне значення загального показника ефективності БСМ. Крім того, в порівнянні з відомими методами експертної оцінки запропонований метод не потребує пошуку експертів та дозволяє отримати результат розташований між методами Гаусса-Лапласса та мінімаксним [4]. Таким чином, запропонований метод може бути успішно застосований для аналізу ефективності протоколів маршрутизації БСМ.

Література

1. Антонова А.А. Оценка эффективности протоколов динамической маршрутизации при передачи потокового видео// Автоматизация и управление в технических системах. – 2013. – № 4.2.DOI: 10.12731/2306-1561-2013-4-36.
2. Постников В. М.1 , Спиридонов С. Б. Методы выбора весовых коэффициентов локальных критериев // Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2015. № 06. С. 267–287. DOI:10.7463/0615.0780334.
3. P. Levis, N. Lee, M. Welsh, and D. Culler. TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications, Proceedings of the First ACM Conference on Embedded Networked Sensor Systems (SenSys 2003).
4. “Understanding the protocols underlying dynamic routing”. CNET Networks, Inc. Retrieved p.10-17, 2008.

УДК 621.396

ВИЗНАЧЕННЯ КООРДИНАТ СЕНСОРІВ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Якорнов Є.А., Цуканов О.Ф.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:yakornov@its.kpi.ua

Determination of coordinates of sensors wireless sensor network

The method of determination of coordinates of elements of wireless sensory network is offered by modification of algorithm of MDS of MAR. The estimation of rectangular coordinates and cross-correlation matrix of errors is carried out at local the system of coordinates taking into account the errors of measuring of distances, it allows to promote exactness of determination of coordinates of elements of network.

Можливість вирішення широкого спектру завдань, на підставі використання останніх наукових і технологічних досягнень робить актуальною технологією бездротових сенсорних мереж (БСМ). Однак існує ряд проблем технологічного та експлуатаційного характеру, які вимагають ретельного розгляду, однією з таких яких є визначення місця розташування окремих елементів мережі [1]. Відомі ряд методи та алгоритми визначення координат елементів БСМ, наприклад, метод APS [2] та алгоритм «MDS-MAP» [3].

APS являє собою набір алгоритмів визначення координат (АВК) в БСМ, при цьому кожний об'єкт шукає свої координати самостійно. Алгоритм краще всього працює в однорідних мережах, де відстані між елементами приблизно однакові та дозволяє отримати лише грубі оцінки координат.

Алгоритм «MDS-MAP» є прикладом централізованого АВК. В якості вихідних умов передбачається що кожен об'єкт мережі знає про наявність навколо прилеглих сусідів, а також відстані до них. Частина об'єктів мережі визначає свої координати самостійно, координати інших вершин розраховуються за результатами роботи алгоритму. Для кожної пари об’єктів оцінюється найкоротша відстань один до одного. Коли об’єкти є безпосередніми сусідами один одного, цією оцінкою є безпосередній вимір відстані. Недоліком даного алгоритму є те що визначення координат окремих об’єктів без урахування помилок вимірювань відстаней, що не дозволяє розраховувати помилки визначення координат.

Пропонується метод на основі алгоритму «MDS MAP», який передбачає що кожен об'єкт мережі має інформацію про відстані до сусідніх елементів
r_{ij} $i, j = \overline{1, M}$ та середньоквадратичну помилку (СКП) визначення відстаней, крім того елементи БСМ розташовані нерівномірно.

Сутність методу полягає в тому, що для кожної пари об’єктів оцінюється найкоротша відстань один до одного. При цьому місцева система

координат орієнтована таким чином, що перший елемент знаходиться в началі системи координат (рис.1), а другий на вісі абсцис. Обов'язковою умовою є те, що для визначення прямокутних координат елемента потрібно мати як мінімум два елемента БСМ з відомими координатами.

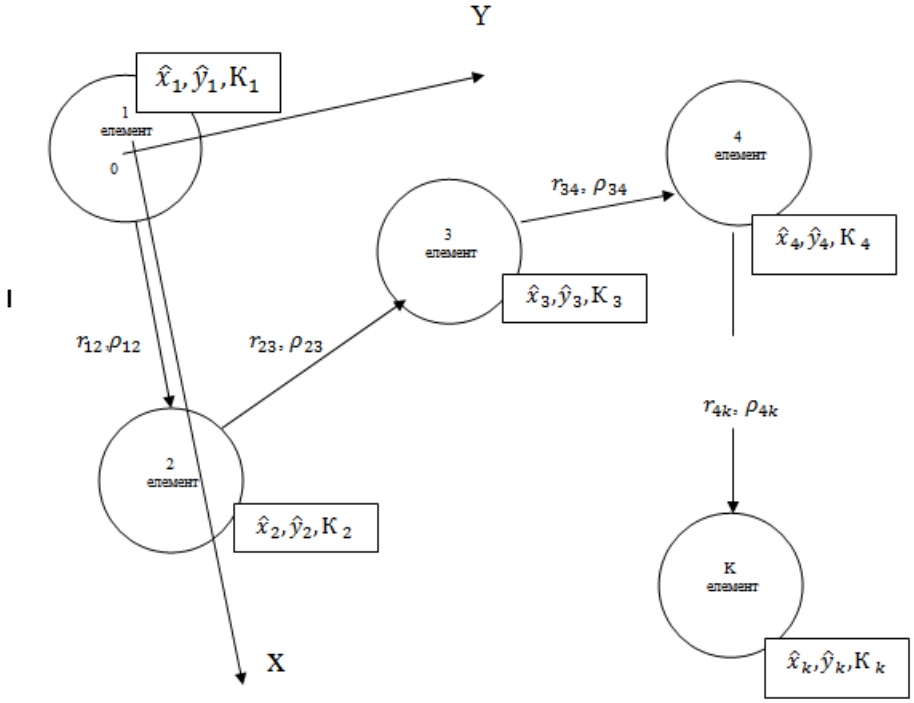


Рис. 1. Місцева система координат

Якщо елементи БСМ є безпосередніми сусідами один одного, цією оцінкою є безпосередній вимір відстані. В результаті будується стричкова матриця відстаней виду:

$$R = \begin{pmatrix} 0 & \widetilde{r_{12}} & 0 \\ \widetilde{r_{21}} & 0 & \widetilde{r_{23}} \\ 0 & \widetilde{r_{32}} & 0 \end{pmatrix}, \qquad (1)$$

де $r_{ij} = 0$, $i,j=\overline{1,M}$,

та матриця СКП визначення відстаней

$$\Sigma = \begin{pmatrix} 0 & \widetilde{\sigma_{12}} & 0 \\ \widetilde{\sigma_{21}} & 0 & \widetilde{\sigma_{23}} \\ 0 & \widetilde{\sigma_{32}} & 0 \end{pmatrix}, \qquad (2)$$

де $\widetilde{\sigma_{ij}} = 0$, $i,j=\overline{1,M}$.

Найкоротший шлях меж елементами БСМ можна розрахувати за допомогою алгоритму Дейкстри [2].

Визначення координат окремих елементів БСМ (x_i, y_i), $i = [1, \dots, M]$ здійснюється шляхом рішення задачі багатомірної мінімізації функціоналу (3) з урахуванням помилок вимірювань (2):

$$\min \sum_{i<j} (\widehat{r_{ij}} - r_{ij})^T \widetilde{\sigma_{ij}}^{-1} (\widehat{r_{ij}} - r_{ij}). \qquad (3)$$

За результатами мінімізації (3) отримаємо декілька значень $\widehat{r_{ij}}$ в залежності від кількості сусідніх елементів $j=\overline{1,m^*}$, де m^* - кількість сусідніх елементів до яких відома відстань r_{ij}.

Тоді координати елементів БСМ (x_i, y_i) можливо визначати: за результатами розрахунку кожного значення $\widehat{r_{ij}}$.

$$(x_i, y_i) = \frac{1}{m^*}\sum_{j=1}^{m^*}\left(x_{ij}, y_{ij}\right) \quad (4)$$

Значення координат елементів БСМ (x_i, y_i) отримується в місцевої системі координат, тому потребує перетворення до центральної системи координат. Кореляційна матриця (КМ) помилок оцінки K_{xy} визначення координат в місцевої координат обчислюється наступним чином:

$$K_{xy} = A^T A\ \sigma_{ij}{}^*,$$

де A - матриця часткових похідних прямокутних координат (x,y) по r_{ij} .

Елементи КМ уточнюються шляхом урахування інформації про кількість сусідніх елементів БСМ:

$$\text{к}_{ij}{}^* = \frac{1}{\sqrt{m^*}}\sum_{j=1}^{m^*}\text{к}_{ij} \quad (5)$$

Запропонований метод дозволяє отримати оцінку координат елементів та КМ помилок на підставі використання одноразово наявних даних по відстані до сусідніх елементів. Кореляційна матриця розраховується на підставі інформації про кількість сусідніх елементів до яких відома відстань. За таких випадках алгоритм дозволяє підвищити точність визначення координат підвищується на $\sqrt{m^*}$ разів (5).

Слід зазначити переваги запропонованого алгоритму:

1) відсутність потрібності маршрутизації мережі на початковому етапі;

2) відсутність необхідності та підтримки зв'язку між об'єктами мережі, які не є безпосередніми сусідніми елементами;

3) алгоритм не потребує обов'язкової наявності базової станції БСМ.

Література

1. Yi Shang .Localization from mereconnectivity, // Wheeler Ruml, Ying Zhang, Markus Fromherz, Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing Maryland, USA, 2003, page. 201-212.
2. Mohinder S "Global Positioning Systems, Inertial Navigation and Itegration" // Grewall, Lawrence R. Weill, Angus R. Andrews, Изд-во "John Wiley & Sons Inc", 2007.
3. Иванов Е.В., Козлов В.Н., Курикша В.А. "Экспериментальное определение координат в сетях стандарта IEEE 802.15.4" // Труды 63-й научной сессии РНТОРЭС им. А.С. Попова, Москва, 2008, 256 с.

УДК 617.753-072.3

МЕТОД РОЗМІЩЕННЯ ПРОМЕНІВ ЗОНДУВАННЯ ПРИ РЕЙТРЕЙСИНГОВІЙ АБЕРОМЕТРІЇ

Ковальський В.І.
Факультет електроніки КПІ ім. Ігоря Сікорського
E-mail: vitaliykovalsky@gmail.com

Method of distribution of the probing rays ray-tracing aberrometry

In this article a method is proposed for the uniform placement of probing beams which are used for ray-tracing aberrometry. In the method, the optimization of the placement of LEDs for a configuration consisting of concentric circles is carried out.

Під час аберометрії оптичної системи ока застосування методу рейтрейсингу є найбільш ефективним при діагностиці в офтальмологічній практиці. Даний метод [1] заснований на зондуванні зіниці ока вузькими лазерними променями, які паралельні зоровій осі ока і здійснюється за допомогою пристрою, схема якого зображена на рисунку 1.

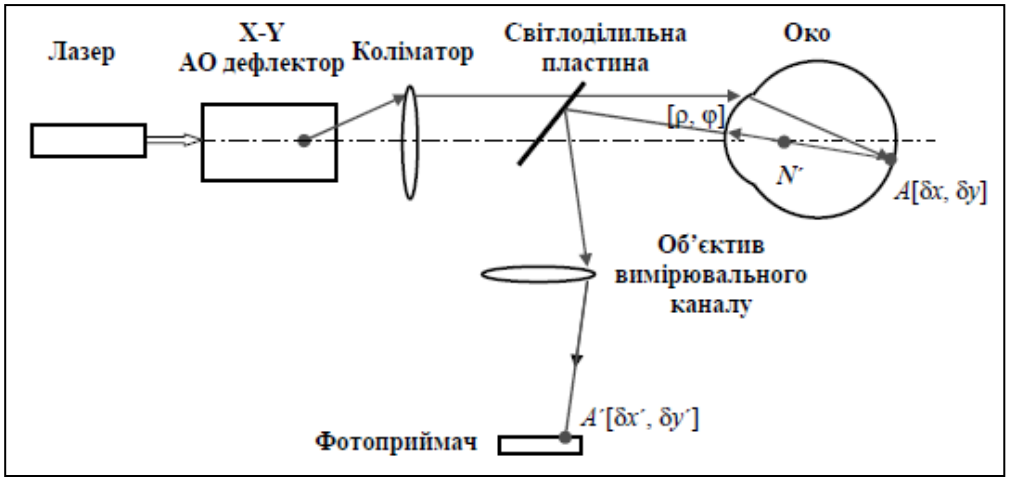
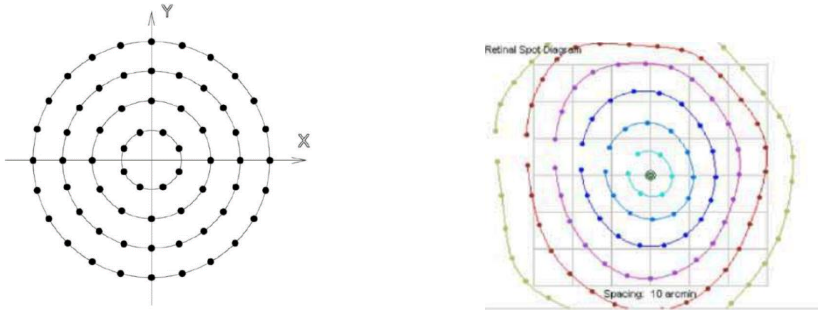


Рис. 1. Спрощена функціональна схема аберометра рейтресингового типу

При цьому процесі відбувається почергове проеціювання променю паралельно вісі ока за допомогою лазера, дефлектора та коліматора, що проходить через світлоділильну пластину.

Зондування променем може відбуватися за схемою, що представлена на рисунку 2, а.



а) б)

Рис. 2. Розподіл зондуючих променів на (а) зіниці та (б) сітківці

Промінь, проходячи через оптичну систему ока, попадає на сітківку та за допомогою оптично спряженої системи, що утворюється світлоділильною пластиною та об'єктивом вимірювального каналу, сприймається фотоприймачем як точка A'[δx', δy'], що відповідає відповідним поперечним абераціям (тобто точці A[δx, δy]). Можливий варіант результуючого розподілу променів на сітківці показано на рисунку 3.

При дослідженнях, що направлені на спрощення та вдосконалення раніше згаданого методу однопроменевої аберометрії ока [2-3], однією із задач є визначення оптимального розміщення заданої кількості зондуючих променів на зіниці ока (див. рис. 2, а). Оптимальність такого розміщення полягає в мінімізації різниці відстаней між променями на кожному із концентричних кіл. Для подальшого формулювання задачі розглянемо конфігурацію, що складається із m концентричних кіл (m > 2) та вміщує в собі N променів, де відстані між променями для кожного концентричного кола виражаються як:

$$l_i \approx \frac{2\pi\frac{R}{m}i}{x_i}, \tag{1}$$

де l_i – відстань між зондуючими променями i-го концентричного кола (i = 1..m); R – максимальний радіус поверхні зіниці, що зондується; m – кількість концентричних кіл, x_i – кількість променів в i-ому концентричному колі.

Відповідно, функція оптимізації являє собою комбінацію всіх можливих квадратів різниць відстаней, що представлені у (1), і її можна записати у наступному вигляді:

$$L = \sum_{i=2}^{m}\left(\frac{2\pi R}{m}\frac{i}{x_i} - \frac{2\pi R}{m}\frac{i-1}{x_{i-1}}\right)^2 \tag{2}$$

При мінімізації даної функції у формулюванні (2) основним є знаходження кількості променів (x_1, x_2, …, x_m) для m концентричних кіл. Проте, для подальшої оптимізації потрібно спростити функцію L. Це можна

здійснити, врахувавши наступні моменти:

- множник 2πR/m можна винести за знак суми рівняння (2), а отже він не впливає на кінцевий результат оптимізації;

- в даній задачі основною є мінімізація різниць відстань, а саме досягнення їхньої рівності. Тому без впливу на кінцевий результат, можна взяти до розгляду не різницю відстаней, а різницю їх обернених величин.

Зі всього вищезгаданого рівняння (2) можна трансформувати в наступне:

$$w = \sum_{i=2}^{m} \left(\frac{x_i}{i} - \frac{x_{i-1}}{i-1}\right)^2 \tag{3}$$

Проте, для подальшої роботи із функцією (3) представимо її у матричному вигляді для задачі квадратичного програмування, а саме:

$$w = \frac{1}{2} X^T H X + f^T X, \tag{4}$$

де, виходячи із аналізу рівняння (3), вектори X та f мають наступний вигляд:

$$X_{m*1} = \begin{bmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_m \end{bmatrix}, \qquad f_{m*1} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{5}$$

Матриця H описується як матриця m*m, де кожен елемент утворюється відповідно до наступної системи рівнянь:

$$h_{ij} = \begin{cases} 2, i = j = 1 \\ {}^{2}/_{m^2}, i = j = m \\ {}^{4}/_{ij}, i = j \\ -{}^{2}/_{ij}, |i - j| = 1 \\ 0, |i - j| > 1 \end{cases} \tag{6}$$

Також для даної задачі накладаються наступні обмеження:

- кількість променів в кожному колі не менше 3 (щоб сформувати хоча б трикутник) і не перевищує загальної кількості променів для зондування N;

- сума всіх зондуючих променів дорівнює N.

- кількість променів в кожному колі є ціле число.

Остаточний вигляд задачі мінімізації можна записати як:

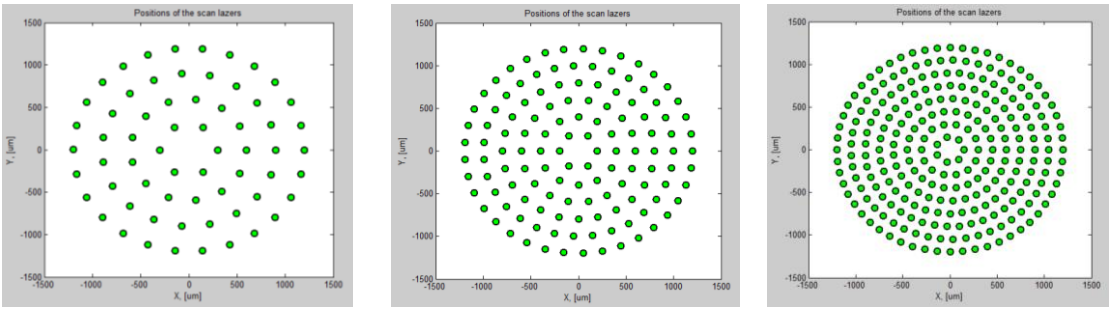
$$w = \sum_{i=2}^{m} \left(\frac{x_i}{i} - \frac{x_{i-1}}{i-1}\right)^2 \to min$$

$$\begin{cases} 3 \le x_i \le N, i = 1..m \\ \sum_{i=1}^{m} x_i = N \\ x_i \in Z, i = 1..m \end{cases} \tag{7}$$

Розв’язок задачі виконано в середовищі Matlab. За основу взято задачу з обмеженнями, що вказані в (7) та форму подачі функції оптимізації за рівняннями (4)-(6). В якості вхідних параметрів при оптимізації вказуються:

- кількість концентричних кіл m;
- кількість зондуючих променів N;
- радіус площі зондування зіниці R в мікрометрах.

Під час розв’язку, виконується попередня оптимізація послабленої задачі, що описана в (7). Для отримання цілочислених значень додатково застосовується алгоритм гілок, що зазвичай використовується для дискретної задачі лінійного програмування. Візуалізація результатів оптимізації для кількох випадків розміщення показана на рисунку 4.



а) б) в)

Рис. 4. Візуалізація розміщення зондуючих променів при:
(а) m = 4, N = 64, R = 1200 мкм;
(б) m = 6, N = 128, R = 1200 мкм;
(в) m = 8, N = 256, R = 1200 мкм

Таким чином представлено метод рівномірного розміщення зондуючих променів. Даний метод полягає в розв’язку задачі мінімізації, що представлена у вигляді задачі квадратичного програмування із застосуванням методу гілок.

Література

1. Молебний В.В., Чиж І.Г., Сокуренко В.М. Однопроменевий метод вимірювання локального розподілу аберацій ока // Вимірювальна та обчислювальна техніка в технологічних процесах. – 1998. – №4. – С. 130-135.
2. Молебний В.В., Яганов П.О., Климов М.В., Ковальський В.І. Вимірювання аберацій методом рейтрейсингу при негомогенності зондуючих променів // Матеріали конференції PREDT-2016. – 2016. – С. 148 – 149.
3. Kovalsky V., Yaganov P. Modification of the Ray-Tracing Aberrometry Method // ELNANO-2017 Proc. – 2017. – P. 384 – 388.

УДК 621.396

ЗАХИЩЕНА БЕЗПРОВОДОВА МЕРЕЖА ДЛЯ МОНІТОРИНГУ ПАРАМЕТРІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА З МОБІЛЬНИМИ СЕНСОРАМИ

Прищепа Т.О., Валуйський С.В., Дакаєв О.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: sandak94@gmail.com

Secured wireless network for environmental parameters monitoring with mobile sensors

One of the main problems in the organization of wireless networks is security. To solve this problem, we suggest using a VPN connection. This ensures not only a very high level of security, but is also a convenient tool for connecting network elements.

В наш час, з кожного роком продуктивність CPU збільшується в кілька разів. Завдяки цьому, існує велика кількість невеликих мікроконтролерів, що мають високу продуктивність (наприклад, Raspberry Pi Zero, Arduino Nano). Це дає унікальну можливість для розподілу обчислювальної потужності між вузлами. Крім того, можна зробити окремий інтелектуальний вузол з широкою функціональністю, власною операційною системою і додатками, що дозволяють будувати великомасштабну розподілену безпроводову мережу датчиків для моніторингу навколишнього середовища. Але як і раніше залишається проблема безпеки і мультисервісної функціональності в таких мережах [1].

У статті запропонована модель, яка використовує концепцію Інтернету речей (Internet of Things, IoT) і являє собою зразок розподіленої безпроводової мережі для екологічного моніторингу міської місцевості (CO, забруднення повітря, вогню, шуму, рівня електромагнітного випромінювання, тощо). Дані, зібрані з фіксованих, а також мобільних датчиків моніторингу (розміщених на автомобілях, автобусах, безпілотних літальних апаратах, тощо) передаються через мережі 3G, Wi-Fi або ZigBee на віддалений сервер для подальшої обробки і візуалізації в режимі реального часу за допомогою веб-додатку. Всі канали використовують VPN з'єднання, що дозволяє створити розподілену і надійно захищену мережу.

Однією з головних проблем в організації безпроводових мереж є безпека. Щоб вирішити цю проблему, ми пропонуємо використовувати VPN з'єднання. Це гарантує не тільки дуже високий рівень безпеки, але є також зручним інструментом для з'єднання елементів мережі. Проста схема захищеної розподіленої мережі показана на рис.1.

Є чотири основних елементи, які в комплексі створюють високоефективну розподілену безпроводову сенсорну мережу. Розглянемо кожен з них.

1. Вузли. Кожен вузол складається з материнської плати, набору датчиків, безпроводового інтерфейсу і джерела живлення. Ми пропонуємо використовувати мікроконтролери як материнські плати, тому що вони

досить продуктивні, щоб використовувати VPN та для запуску деяких програм. Також, вони включають в себе деякі датчики для моніторингу параметрів навколишнього середовища міської зони, таких як CO, забруднення повітря, вогню, шуму, рівню електромагнітного випромінювання. Для безпроводового інтерфейсу, можна використовувати будь-яку доступну мережу (наприклад, GSM, Wi-Fi або ZigBee). У запропонованій моделі, вузли можуть мати власні автономні джерела живлення.

2. Мережевий інтерфейс. Що стосується нашої мережі вони можуть бути різними. Особливо, якщо ми не будемо використовувати власне джерело живлення для вузлів, ми можемо використовувати Wi-Fi, UMTS та інші потужні безпроводові мережі, не думаючи про батареї. Використовуючи нову концепцію «ZigBee-over-IP» можливо доволі просто застосувати VPN у ZigBee мережах.

3. VPN з'єднання. Для того, щоб з'єднати наші вузли і гарантувати високий рівень безпеки, пропонується використовувати VPN з'єднання. Кожен вузол використовує безпроводовий інтерфейс для підключення до сервера VPN. Після встановлення з'єднання, всі дані від вузла до сервера шифруються і передаються по VPN тунелю, інкапсулюються в спеціальних пакетах. Це дуже простий і потужний метод для побудови незалежної розподіленої мережі, тому що після усіх операцій, ми отримуємо чисту мережу, аналогічну локальній мережі з її характеристиками і функціональністю. Ми можемо не тільки отримувати дані від датчиків, але також потокове відео і аудіо дані через цю мережу. Наш VPN сервер використовує протокол GRE через порт UDP для кожного клієнта (вузла) для маршрутизації даних між мережевими елементами.

4. Сервер. Це головна і найпотужніша частина нашої мережі. Ми використовуємо декілька додатків. Перш за все, це сервер VPN, який необхідний для з'єднання наших розподілених вузлів. Другим важливим елементом є сервер бази даних - ми повинні використовувати базу даних високої продуктивності, тому що мережа доволі велика та має величезні потоки даних. Для гарної сумісності, пропонується використовувати веб-додатки, тому HTTP/HTTPS сервер необхідний для нашої системи. Для динамічної генерації веб-сторінок, також потрібний високопродуктивний сервер. Ми можемо використовувати будь-яку популярну серверну мову (наприклад, PHP або Ruby,) для наших динамічних веб-сторінок.

Тепер для розуміння принципу взаємодії розглянемо спрощену структуру мережі, яка показана на рис.2. Всі IP-адреси вузлів в цій схемі є випадковими. Ми маємо просту мережу, аналогічну звичайній локальній мережі. Використання гнучких серверних додатків VPN, дасть змогу розділити нашу мережу на певні частини і встановити маршрутизацію між ними. Наприклад, ми можемо використовувати окрему підмережу для збору даних від датчиків CO, а інша підмережа складатиметься з електромагнітних датчиків або камер і т.п. Однією з переваг VPN є те, що ми робимо нашу мережу розподіленою. Це означає, що ми зможемо використовувати наші

вузли в будь-якому місці, якщо там є безпроводовий зв'язок. Наприклад, ми можемо розташувати деякі вузли в Києві, в той час як інші будуть у Львові чи Харкові. Вони розділені географічно, але логічно – це одна мережа.

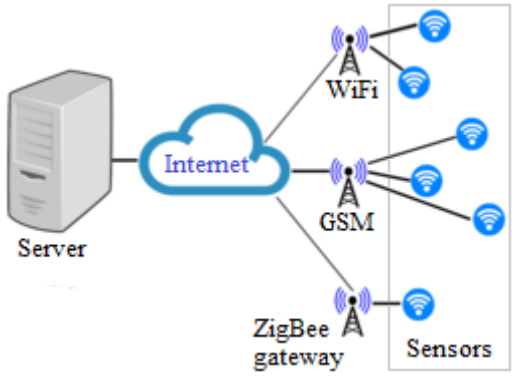


Рис. 1. Приклад архітектури мережі

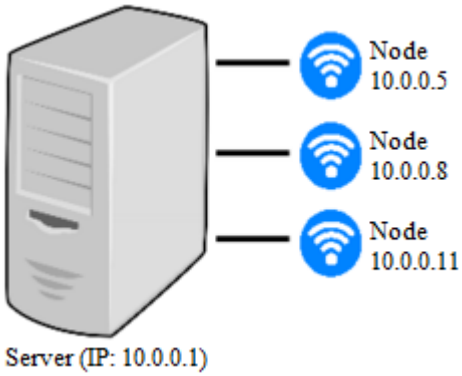


Рис. 2. Спрощена структура мережі

Використання простої мережі є дуже вигідним рішенням для нашої системи. Ми можемо дуже просто використовувати звичайні мережеві додатки, такі як веб-сервер, SSH сервер, потоковий сервер і т.д. Для потокового відео з камери, ми повинні використовувати будь-який потоковий сервер, а потім ми можемо спостерігати відео з простої адреси (наприклад, https://10.0.0.5:8000/stream) з використанням популярних відеовідтворювачів. Для даних планується використовувати відкритий API. Ми можемо використовувати формат JSON для передачі даних. Це дуже популярний формат даних, який простий у використанні з веб-додатків, баз даних та інших програм.

Висновок. Для вирішення проблеми безпеки пропонується модель захищеної безпроводової мережі за допомогою VPN-з'єднання. Також пропонується енергоефективне і компактне рішенням для побудови безпроводового вузла з датчиками, що створений на модулі XBee. Пропонується технологія для розміщення безпеки таких вузлів з використанням повітряного запуску з квадрокоптера. Датчики для моніторингу міського району можуть бути більш складним з використанням зовнішніх процесорів, а також модулів Wi-Fi або 3G. Цілі для розміщення датчиків можуть бути визначені одним з ефективних методів синтезу топології безпроводових сенсорних мереж [2].

Література

1. P. Likhar, R. S. Yadav, and K. Rao M, “Securing IEEE 802.11G WLAN Using OpenVPN and Its Impact Analysis,” International Journal of Network Security & Its Applications (IJNSA), 2011, vol. 3, №6, pp. 97-113.
2. S. Valuiskyi, O. Lysenko, T. Pryshchepa, and S. Chumachenko “The problem of finding a rational topology of wireless sensor networks using UAVs,” 2nd Int. IEEE Conf. PIC S&T, Ukraine, Kharkiv, 13-15 Oct., 2015, vol. 1, pp. 213-215.

УДК 621.396

СИНХРОНИЗАЦИЯ С ИСПОЛЬЗОВАНИЕМ ВРЕМЕННЫХ МЕТОК ЧАСОВ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Брицун А. В., Петрова В.Н.
Институт телекоммуникационных систем КПИ им. Игоря Сикорского
Email: nobodylovesnazi@gmail.com

Timestamp Clock-based Synchronization in Wireless Sensor Networks

Many applications in wireless sensor networks demand synchronizations in a local or global range, but most of existing synchronization protocols consume too much energy of sensor nodes due to periodical synchronization operations. This paper proposes an on demand mechanism, in which a sensor node uses its local clock to generate timestamps for events that it senses, and then the timestamps can be synchronized to a reference time base. By decoupling the synchronization operations from the data communication, the transformation of timestamps can be optimized independently from the delivery of data packets.

Синхронизация времени играет важную роль в беспроводных сенсорных сетях. Единственным рабочим способом большинства этих сетей является обмен пакетами, содержащими временные метки. Если временные метки данных, поступающих с разных узлов датчиков, не основаны на одной и той же ссылке времени, невозможно слияние данных [1]. Для того, чтобы избежать зависимости от достижимости опорного узла, который обеспечивает глобальное время сетей (GNT), каждый узел датчика использует локальные часы для генерации метки времени для событий, которые он мониторит. Каждое событие, обнаруженное узлом, инкапсулируется в два типа пакетов: пакет времени и пакет данных, которые могут быть маршрутизированы независимо и объединены в одно сообщение узле приемника.

Рассмотрим беспроводную сеть, состоящую из узлов, сконфигурированных с помощью генераторов, которые могут обеспечивать локальное время синхронизации. События, собранные на каждом узле, агрегируются и отправляются на узел-приемник для объединения данных или для принятия решения. Предполагается, что диапазон передачи каждого узла ограничен, коммуникация работает в режиме нескольких ходов и единственный способ достижения синхронизации - это обмен пакетами. Местное время синхронизации узла *i* можно приближенно указать как [2]:

$$Ti\,(t) = \beta i * t + Ti(0) \qquad (1)$$

где T_i - временной процесс часов, t - реальное время, β_i - перекос часов узла i по отношению к реальному времени, а $T_i\ (0)$ - начальное время часов узла i. В общем случае $T_i\ (0)$ и β_i будут разными для каждого узла и приблизительно постоянны в течение длительного периода времени [2]. Каждый узел может немедленно запустить операции обнаружения, даже если его часы еще не синхронизированы. Каждое событие, обнаруженное сенсорным узлом, разделяется на два типа пакетов: пакеты времени и пакеты данных с одинаковой идентификацией события (EID) [3]. Пакеты данных направляются непосредственно на приемник. Однако временная метка события генерируется с использованием локальных часов и должна быть преобразована в локальное время узла приемника

или глобального сетевого времени (GNT), если по крайней мере глобальный поставщик времени доступен.

Рассмотрим два сценария. В первом узел датчика сообщает о событии узлу приемника, а глобальный поставщик времени доступен из узла датчика. Временная метка события (EID) преобразуется в GNT, используя процесс преобразования временной метки и переносится на узел приемника. После получения пакета временной метки и пакета данных узел приемника будет соответствовать им с помощью EID и объединить их в одно сообщение о событии (EID, TIMESTAMPgnt, Data) с меткой времени, соответствующей GNT.

Другой сценарий – когда глобальный поставщик времени недоступен от узла датчика, но доступен только с узла приемника. Узел отправит пакет данных в узел приемника и преобразует временную метку события в локальное время узла приемника. Так как последний способен достичь глобального поставщика времени, он может преобразовать временную метку события в GNT. Достаточно преобразовать временные метки в локальное время узла приемника, если GNT не требуется.

Каждый узел преобразует временные метки, встроенные в принятые пакеты, из соседних узлов в локальное время. Хотя преобразование временной метки происходит только между соседними узлами, оно обычно не может быть выполнено в точности из-за непредсказуемости компьютерных часов. Введение эмпирической оценки неизбежно.

A. Временная трансформация. Когда узел j получает сообщение с отметкой времени из узла i, временная метка события будет преобразована в локальное время узла j, используя выражение:

$$Tj\ (t0) = Ti\ (t0) + Di, j\ (t0), \tag{2}$$

где *t0* - недоступное идеальное время, в котором произошло событие, а *Ti (t0)* - метка времени события, соответствующего местному времени узла *i*. Однако конкретные формы функции *Di, j (t)* также недоступны. Мы можем вычислить временную метку локального времени узла таким образом:

$$T_j(t^0) = T_j(t^1) - \frac{\beta_j}{\beta_i} \times (T_i(t^1) - T_i(t^0)). \tag{3}$$

Чтобы получить $T_j(t^0)$, узлу j нужно не только знать $T_i(t^0)$, $T_i(t^1)$) и $T_j(t^1)$, но и вычислить эмпирическую оценку $\frac{\beta_j}{\beta_i}$. Единственный способ получить значения этих переменных - обмен пакетами между узлом *i* и узлом *j*.

B. Процесс синхронизации. Предполагаем, что исходный узел пытается преобразовать метку времени в глобальный провайдер времени. Основные этапы по требованию синхронизации выполняются следующим образом:

1) Исходный узел начинает обнаружение маршрута, передавая пакет запроса (RREQ), чтобы найти маршрут к узлу назначения;

2) Когда глобальный провайдер времени получает RREQ, он отправляет ответный пакет (RREP), который несет информацию о времени, T_{31}, указывающий, когда отправляется RREP;

3) После получения сообщений каждый промежуточный узел будет передавать сообщение RREP, как обычно. Одновременно промежуточный узел должен записывать как информацию T_{31}, так и T_{22} при отправке RREP. Когда исходный узел получает RREP, он также записывает информацию T_{11};

4) Затем исходный узел может преобразовать метку времени в GNT, используя найденный маршрут маршрутизации. Исходный узел начинает посылать пакет временной метки (EID, timestamp1) поставщику времени, где timestamp1 указывает момент, в который собираются события. Чтобы включить промежуточный узел для преобразования временной метки пакет временных меток также содержит информацию T_{22} T_{11} и T_{12};

5) После приема пакета подтверждения при $T_{1,2}$ промежуточное устройство может вычислять смещение тактового сигнала δ и задержку d. Итак, промежуточный узел преобразует Timestamp1 в Timestamp2, соответствующий его местному времени, а затем глобальный поставщик времени преобразует Timestamp2 в Timestamp3, соответствующий его местному времени, то есть, GNT.

$$\delta = \frac{(T_{23} - \mathrm{T}_{12}) - (\mathrm{T}_{11} - \mathrm{T}_{22})}{2} \quad (4) \qquad (4)$$

$$d = \frac{(T_{23} - \mathrm{T}_{12}) + (\mathrm{T}_{11} - \mathrm{T}_{22})}{2} \quad (5) \qquad (5)$$

Предполагая, что задержка обмена сообщениями в обоих направлениях равна, мы можем получить $D_{i,j}(\mathrm{t}) = d$ (для $T_{1,1} < t \leq T_{1,2}$) в уравнении (2). Фактически, из-за больших временных изменений обмена сообщениями расчеты должны повторяться с использованием статистики для получения достаточно точных результатов. Учитывая продолжительность, на которую хранится метка времени в исходном узле, мы можем получить следующие уравнения.

$$\frac{\beta_j}{\beta_i} = \frac{T_{12} - T_{11} + 2d}{T_{12} - T_{11}} \quad (6) \qquad (6)$$

$$Timestamp2 = T_{23} - \frac{\beta_j}{\beta_i}(T_{12} + d - Timestamp1) \quad (7) \qquad (7)$$

$$Timestamp2 = T_{32} - \frac{\beta'_j}{\beta'_i}(T_{24} + d' - Timestamp2) \quad (8) \qquad (8)$$

Где β'_j, β'_i и d' – оцениваемые параметры в двустороннем обмене сообщениями между промежуточным узлом и глобальным провайдером времени.

Литература

1. J. Dong, L. Gu, and C. Zheng, “Research on fault-tolerant strategy of time synchronization for industrial wireless sensor network,” in Proc.ICMTMA Conf, vol. 2, 2011, pp. 1146–1149.
2. M. L. Sichitiu and C. Veerarittiphan, “Simple, accurate time synchronization for wireless sensor networks,” in Proc. IEEE WCNC 2003, vol. 2, 2003, pp. 1266–1273.
3. Z. Zhong, P. Chen, and T. He, “On-demand time synchronization with predictable accuracy” / in INFOCOM, 2011 Proceedings IEEE, 2011, pp. 2480–2488.
4. A. Al-Shaikhi and A. Masoud, “Efficient, single hop time synchronization protocol for randomly-connected wsns,” IEEE Wireless Communications Letters, vol. PP, no. 99, p. 1, 2017.

УДК 621.396

МЕТОДИ ПІДВИЩЕННЯ БЕЗПЕКИ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Афанасьєв Я.Р., Новіков В.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: afanassiev.yaroslav@gmail.com

Methods to Improve Security in Wireless Sensor Network

Currently, wireless sensor networks (BSN) are one of the most promising areas in the development of telecommunications system. The wireless sensor network (BSN) is a technology, which is a self-organizing network of a large number of sensors and devices that are connected to each other via a radio channel. Security and privacy are of great importance in wireless sensor networks, where the unique characteristics of these networks and the purpose of the application they use make them attractive targets for penetration and other attacks.

Безпроводові сенсорні мережі (БСМ) є новим важливим етапом розвитку телекомунікаційних систем. Основу безпроводової сенсорної мережі складають безліч маленьких зчитувальних пристроїв (датчиків), здатних реєструвати зміни різних параметрів навколишнього середовища і транслювати ці параметри іншим подібним пристроям. Сучасні датчики здатні відстежувати тиск, температуру, вологість, склад ґрунту, автомобільний рух, рівні шуму, наявність або відсутність певних об'єктів або речовин та інші. В безпроводових сенсорних мережах спілкуються не тільки один з одним, але і з базовою станцією (БС), через безпровідні канали, що дозволяє їм надавати зібрані дані для віддаленої обробки, візуалізації, аналізу та зберігання. В таких системах виникають проблеми, пов'язані з інформаційною безпекою.

Основні проблеми з якими зустрічаються при використання ефективної схеми безпеки в БСМ пов'язані з розмірами датчиків, обчислювальною потужністю, пам'яттю і типами розв'язуваних завдань, очікуваних від датчиків. Для вирішення основних питань з приводу безпеки в безпроводових сенсорних мережах необхідно застосовувати криптографію та стеганографію. Також доцільно розглянути різні типи загроз і нападів на безпроводові сенсорні мережі.

Безпека була проблемою в обчислювальних системах і мережах протягом декількох десятиліть, під час яких типи атак, і заходи безпеки, і механізми, що протистоять їм, удосконалилися і значно розвинулися, особливо через швидке зростання Інтернету. Мета забезпечення інформаційної безпеки в безпроводових сенсорних мережах можна умовно розділити на основні і другорядні. Основні цілі включають в себе забезпечення конфіденційності, цілісності, аутентифікації і доступності даних. Другорядні цілі забезпечення безпеки включають в себе такі поняття як свіжість даних, самоорганізація, тимчасова синхронізація, захищена локалізація. Розглянемо основні цілі:

1.Конфіденційність даних є фундаментальним завданням безпеки. Дані, зібрані сенсорами, можуть містити конфіденційну інформацію і не повинні бути пропущені до несанкціонованих пристроїв. Також інформація про самі сенсори (наприклад місце розташування, і т.д.), повинні бути захищені, щоб запобігти підслуховуванню і атакам. Ці проблеми вимагають заходів, які забезпечують конфіденційність даних для сенсорних мереж.

2.Цілісність даних в сенсорних мережах визначається здатністю забезпечення захисту даних таким чином, щоб дані не могли змінитись під час транспортування між вузлами сенсорної мережі.

3.Аутентифікація необхідна для підтвердження ідентифікації користувача або пристрою, гарантуючи, що повідомлення прибуло від того, хто стверджує, що його послав.

4.Цілісність даних в сенсорних мережах визначається здатністю забезпечення захисту даних таким способом, щоб дані не могли бути змінені під час транспортування між вузлами сенсорної мережі, наприклад, з метою введення помилкових даних і отже впливу на сенсорні дані.

У всіх типах мережі зв'язку є кілька фундаментальних механізмів безпеки, які можуть бути використані, щоб забезпечити конфіденційність, цілісність і доступність. Щоб захиститися від багатьох можливих атак можна використовувати безліч протоколів захисту та інші захисні механізми. Для цього використовуються криптографічні та стеганографічні методи. Криптографія - процес приховування і захисту інформації, використовуючи кодування і декодування. Підходи криптографії симетричного ключа можуть бути значно ефективнішими з точки зору ресурсів, що робить їх кращим вибором в БСМ. Головний недолік підходу симетричного ключа - проблема ключового розподілу, тобто спільно використовуваний симетричний ключ повинен спочатку бути відомий обом зв'язувальним вузлам, перш ніж вони зможуть надійно обмінюватися даними.

У той час як криптографія спрямована на приховування змісту повідомлення, стеганографія спрямована на приховування існування повідомлення. Вона приховує існування каналу, і, крім того, в тому випадку, якщо ми хочемо відправити секретні дані без інформації про відправника або коли ми хочемо поширювати секретні дані публічно, вона дуже корисна. Однак, безпеку безпроводових сенсорних мереж не має прямого відношення до стеганографії, а для обробки мультимедійних даних (наприклад, аудіо, відео) гостро не вистачає ресурсів, це є відкритою на даний момент проблемою БСС.

Фізичний рівень безпечного доступу до безпроводових сенсорних мереж може бути забезпечений використанням стрибкоподібної перебудови частоти. Динамічне поєднання таких параметрів, як доступні частоти для стрибкоподібної перебудови, час затримки в перебудові і шаблон стрибкоподібної перебудови може бути використано з малою витратою пам'яті, обробкою і енергетичними затратами.

Також для вирішення проблем безпеки розроблені спеціальні протоколи, найбільшу популярність серед яких має технологія ZigBee. В

основі даної технології лежить стандарт IEEE 802.15.4, який описує фізичний рівень і рівень доступу до середовища для безпроводових сенсорних мереж передачі даних. Стандарт IEEE 802.15.4 забезпечує чотири основні моделі безпеки: управління доступом, цілісність повідомлення, конфіденційність повідомлення і захист відтворення. Безпека в IEEE 802.15.4 оброблена рівнем MAC, і програма може вибрати певні вимоги до захисту, встановивши належні параметри. Стандарт розрізняє вісім наборів безпеки (розглянуті в таблиці 1), кожен з різними рівнями захисту для переданих даних.

Назва	**Опис**
Null	Не надає захисту
AES – CTR	Надає тільки шифрування, CTR
AES – CBC – MAC – 128	128-bit MAC
AES – CBC – MAC – 64	64-bit MAC
AES – CBC – MAC – 32	32-bit MAC
AES – CCM – 128	Шифрування і 128-bit MAC
AES – CCM – 64	Шифрування і 64-bit MAC
AES – CCM – 32	Шифрування і 32-bit MAC

Таблиця.1 Набори безпеки які підтримані в IEEE 802.15.4.

Окрім до засобів захисту IEEE 802.15.4 специфікація ZigBee також представляє поняття центру довіри, відповідальність зазвичай прийнята на координатора ZigBee. Центр довіри відповідальний за аутентифікацію пристроїв, що бажають приєднатися до мережі (адміністратор довіри), підтримка і розподіл ключів (адміністратор мережі) і включення безпеки між пристроями (менеджер конфігурації).

Безпроводові мережі застосовуються в багатьох сферах людської діяльності, тому питання безпеки грає важливу роль. Як і будь-яка комп'ютерна мережа, бездротові сенсорні мережі піддаються безлічі загроз і атак, як більшість інших мереж, сенсорні мережі вимагають підтримки конфіденційності, цілісності і аутентифікації для захисту сенсорних вузлів і сенсорних даних. Запропоновані методи підвищення безпеки в БСМ, методи і протоколи захисту мережі можуть забезпечити необхідний рівень безпеки безпроводових сенсорних мереж.

Література

1. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10—15, year 2006.
2. Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM, Page 53—57, year 2004.
3. Pathan A.S.K.; Hyung-Woo Lee; Choong Seon Hong, “Security in wireless sensor networks: issues and challenges” Advanced Communication echnology (ICACT), Page(s):6, year 2006.
4. Zia T.; Zomaya A., “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC) Page(s):40—40, year 2006.

УДК 621.396

РАЗВИТИЕ СПОСОБОВ ПРИМЕНЕНИЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ ДЛЯ КОНТРОЛЯ ТРАНСПОРТНЫХ СРЕДСТВ

Гиенко О.П, Прищепа Т.А.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: oleggienko270797@gmail.com

Development of methods of using wireless sensor networks for vehicle control

Wireless sensor networks (WSN) consist of a large number of nodes of transport sensors. Each node is endowed with a communication interface, which is basically characterized by low power, short transmission distance and minimum data rate. Currently, WSN technology is distributed across a large road area to monitor traffic and the environment. This approach allows multiple intelligent transport systems applications to use primary data gathered to create intelligent solutions based on prior information. Therefore, in this paper we present the MAC protocol, which is suitable for WSN, where its nodes are intended for linear topology.

Интеллектуальные транспортные системы (ИТС) начинают получать много внимания в последнее время от научно-исследовательских институтов, промышленных заводов и организаций стандартизации, поскольку они широко затрагивают жизнь людей. Цель ИТС заключается в предоставлении основных услуг и приложений, которые улучшат безопасность транспорта, а также увеличат доступные ресурсы и время, которые влияют на скорость движения и процент автомобильных аварий. Службы и приложения ИТС зависят от развития передовых технологий и распространения их на интеллектуальных инфраструктурных системах и транспортных системах. Эти передовые технологии состоят из физических технологий восприятия мира, которые способны обеспечить измерения в реальном мире и преобразовать их в цифровой мир, возможности хранения данных для работы с цифровыми измерениями, которые будут сохранять и анализировать эти данные и коммуникационные технологии как проводных, так и беспроводных технологий для обмена собранными данными с транспортными средствами и их инфраструктурой и наоборот [1] [2].

Система, которая контролирует и сообщает о физическом состоянии дорог, таких как коэффициент скользкости, влажность, дорожные работы и т. д.; и оценивает трафик на разных участках дороги, предоставит очень полезную информацию для дальнейшего анализа и принятия решения, которое будет принято или создано системой. Информация, полученная из этой системы, может быть использована службами на основе SMS, которые предупреждают пользователей о перегрузках, светофорах, географических информационных системах, которые предлагают менее перегруженные пути или дороги, которые менее повреждены, системы, которые запускают работы

по обслуживанию и анализу дорог, которые помогают управлять трафиком и планировать расширения дорожной сети, что повысит эффективность циркуляции трафика, минимизирует риски и время для принятия корректирующих действий как на уровне проектирования, так и на уровне управления. Существует несколько проблем при построении такой системы. Такие проблемы возникают в областях

- зондирования,
- обработки сигналов,
- линий связи,
- проектирования протоколов,
- хранения и извлечения информации.

Движение по дороге или состояние дороги можно определить только с помощью некоторых специализированных и специально предназначенных датчиков.

Динамические сценарии дорожного движения меняются, когда многие предыдущие исследования были проведены для характеристики динамического сценария дорожного движения [3], и ответ на перегруженность должен быть быстрым. Следовательно, протокол связи для такой системы должен быть в режиме реального времени для предоставления актуальных и полезных данных.

Системы мониторинга трафика генерируют огромное количество данных, в которых системы по очереди должны обрабатывать эту полезную информацию, особенно те системы, которые нуждаются в исторической информации для правильной оценки текущего состояния трафика. Системы мониторинга трафика обычно пытаются подсчитать, классифицировать или оценить скорость движения транспортных средств на дороге.

Понятно, что условия дорожного движения и система мониторинга трафика должны быть экономически оправданными, поэтому можно применять некоторые настройки к системе, такие как сокращение количества компонентов системы и повторное использование существующей инфраструктуры.

Система должна быть осуществимой и способной избегать необходимости раскапывания дорог или создания дополнительной инфраструктуры в виде прокладки проводов или изготовления надземных сооружений. Целью этой работы является создание системы мониторинга дорожного движения, которая способна лучше оценивать аномалию дороги. Для достижения этой цели мы предлагаем подход к улучшению мониторинга дорожного движения через беспроводные сенсорные сети (используя беспроводные датчики Jennic jn-5148 от NXP(рис.1)) для создания беспроводной сенсорной сети, где несколько датчиков распределены вдоль дороги в форсированной линейной топологии.

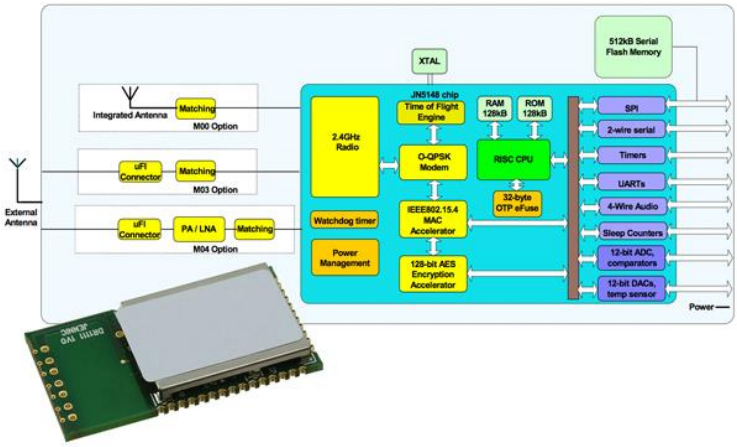


Рис. 1. Беспроводный датчик Jennic jn-5148

В этой работе мы представляем протокол MAC, который подходит для БСМ, где его узлы присваиваются линейной топологии. Исследуемый протокол реализуется путем адаптации уже существующего протокола Jennic MAC. Мы демонстрируем достоверность MAC путем создания полной сквозной системы мониторинга дорожного движения с использованием 4 узлов Jennic, развернутых в помещении, с целью доказать потенциал MAC в ожидании приложений ИТС. Следует отметить, что предлагаемая реализация рассматривает только стационарные узлы WSN.

Реализация предлагаемого протокола просто рассматривает сеть, которая является линейной топологией для беспроводной сенсорной сети (ЛБСМ). Такая сеть состоит из узлов малой мощности, подключенных через беспроводные каналы, расположенные на одной линии. Эти узлы расположены вдоль боковой стороны на участках дороги. Цель этой работы - разработать новый протокол MAC, который будет использовать преимущества линейной топологии и характеристики, чтобы минимизировать потребление энергии, необходимое для обмена собранной информацией среди узлов датчиков.

Литература

1. S. Tarapiah, S. Atalla, and R. AbuHania, “Smart on-board transportation management system using gps/gsm/gprs technologies to reduce traffic violation in developing countries,” International Journal of Digital Information and Wireless Communications (IJDIWC), vol. 3, no. 4, pp. 96–105, 2013.
2. Mao G. Wireless sensor network localization techniques / G. Mao, B. Fidan, B. Anderson // Computer Networks, 51(10), pp. 2529 – 2553, 2007.
3. S. Tarapiah and S. Atalla, “Public transportation management system based on gps/wifi and open street maps,” International Journal of Advanced Computer Science and Applications (IJACSA)., vol. 6, no. 1, pp. 189–194, 2015.
4. B. M. Velichkovsky, S. M. Dornhoefer, M. Kopf, J. Helmert, and M. Joos, “Change detection and occlusion modes in road-traffic scenarios,” Transportation Research Part F: Traffic Psychology and Behaviour, vol. 5, no. 2, pp. 99–109, 2002.
5. S. Coleri, S. Y. Cheung, and P. Varaiya, “Sensor networks for monitoring traffic,” in Allerton conference on communication, control and computing, 2004, pp. 32–40.

УДК 621.396.946

ПІДХІД ДО АНАЛІЗУ СПОЖИВАННЯ ЕНЕРГОРЕСУРСІВ ВУЗЛОМ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Шпанчук О.О., Лисенко О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: oshpantshuk@gmail.com

Consumption of energy resources by a wireless sensor network

The article shows the methodology for calculating the energy consumption of terminal nodes, a router, and also calculates the lifetime of a wireless sensor network. This work will be useful when choosing the hardware to build the WSN.

Однією з головних вимог до бездротових сенсорних мереж (БСМ) є їх автономність, виконати яку можна, зменшивши енергоспоживання кожного вузла. Час життя вузла БСМ обмежений часом життя джерела живлення, і завдання зниження споживання енергії як ніколи стає важливим, а ефективність його рішення безпосередньо впливає на подальший розвиток бездротових сенсорних мереж.

Згідно зі специфікацією IEEE 802.15.4 [1], БСМ включає в себе три типи пристроїв: кінцеві пристрої (КП), маршрутизатори і єдиний координатор, який управляє і збирає всю інформацію з мережі. Відповідно до стандарту [1], роль координатора, в разі його виходу з ладу, повинен взяти на себе будь-який маршрутизатор. Однак таке трапляється вкрай рідко через те, що координатор БСМ, як правило, має стаціонарне джерело живлення і досить часто підключений до шлюзу, наприклад, ZigBee-Ethernet. На практиці свої автономні джерела живлення мають тільки КП і маршрутизатори. Отже, аналіз енергоспоживання необхідно проводити тільки їх.

В структуру вузла бездротової сенсорної мережі входить датчик, що сприймає дані від зовнішнього середовища, мікроконтролер, пам'ять, радіоприймач, автономне джерело живлення. Проаналізувавши енергоспоживання вузла, наведеного на рис. 1 [2], в момент установки адреси і пошуку координатора можна побачити що, основна частина енергії витрачається на прийом, прослуховування і передачу даних, а не на обробку або збереження даних.

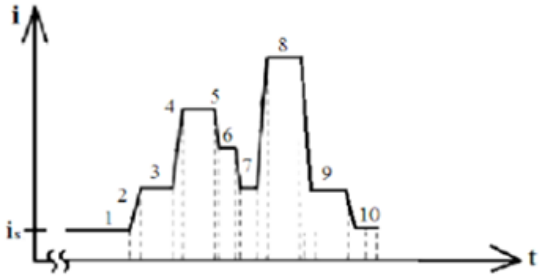


Рис.1. Робота одного енергоцикла для вузла БСМ:

1) режим очікування;
2) ввімкнення прийомника;
3) прийом сигнала активації;
4) вимірювання контролюючих параметрів;
5) обробка результатів вимірювання;
6) включення передавача;
7) прослуховування канала на наявність несучої;
8) передача результатів вимірювань;
9) виключення прийомника;
10) режим очікування.

Всі значення споживання енергії вузлом БСМ будуть залежати від внутрішньої архітектури самого вузла. Як було відзначено вузол БСМ складається з 5 основних компонентів. При цьому мікроконтролер, трансивер і пам'ять

можуть виготовлятися і на одному кристалі, що сприяє як мініатюризації самого вузла БСМ, так і зниження його енергоспоживання.

Енергоспоживання вузла E_e за один цикл, виходячи з проведеного аналізу, можна визначити як суму енергій споживання:

$$E_e = E_{slep}+E_{MCU}+E_{rev}+E_{trans}+E_{ather},, \quad (1)$$

де E_{slep}– енергія під час сну; E_{MCU}– енергія під час роботи мікроконтролера або обчислювального ядра приймача при його відсутності; E_{rev} - енергія під час прийому; E_{trans}– енергія під час передачі; E_{ather}, - енергія в інших режимах (режим пробудження і ін.).

Маршрутизатор БСМ виконує роль «міні координатора» в межах довіреної йому області R. Він може безпосередньо або через проміжні вузли збирати інформацію, а також координувати її передачу. Таким чином, принцип його енергоспоживання такий як і у КП, але більше в результаті більш активної взаємодії з вузлами БСМ.

Енергоспоживання маршрутизатора, за один цикл, можна визначити за формулою (2):

$$E_r = E_e^k + \sum_{m=1}^{m} E_m + \sum_{a=1}^{a} E_a, \quad (2)$$

E_e^k- енергія, споживана маршрутизатором для зв'язку з координатором; E_m - енергія, споживана маршрутизатором для зв'язку з підлеглими йому злами БСМ в кількості m; E_a- - енергія, споживана маршрутизатором для зв'язку з агрегатором мережі.

У виразі (2) величина значення R буде впливати, в основному, на E_m. Чим більше R тим більше E_m буде витрачатися для зв'язку віддаленого вузла з маршрутизатором.

Для визначення середнього енергоспоживання вузлів в мережі необхідно визначити цикли роботи, які присутні в БСМ. Основний цикл роботи наведено на рис. 2.

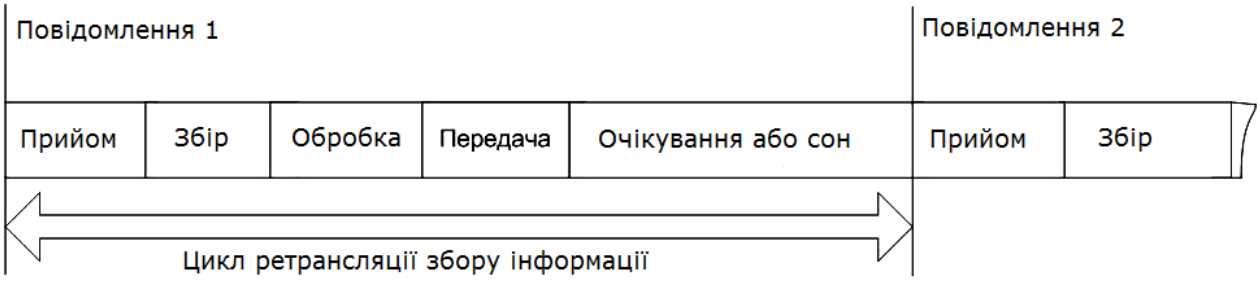


Рис. 2. Основний цикл роботи вузла БСМ при передачі повідомлення або пакета даних

Крім основного циклу роботи вузла БСМ існує ряд інших, але виходячи з імітаційного моделювання [3] і практичних досліджень [2] їх впливом на енергоспоживання всієї мережі можна знехтувати. Для оцінки ефективності алгоритмів збору інформації і використовуваних в БСМ протоколів маршрутизації потрібно знати час життя і енергоспоживання вузла і мережі в цілому. Величина енергоспоживання залежить від безлічі факторів, тому, для того щоб оцінити час життя мережі використовують моделі енергоспоживання [4], здатні реалістично описати споживання енергії мережею.

Енергоспоживання всієї мережі БСМ:

$$E_W = \sum_{k=1}^{k} E_k + \sum_{r=1}^{r} E_r + \sum_{e=1}^{e} E_e, \qquad (3)$$

деE_k - енергія, споживана координаторомk БСМ; E_r - енергія, споживана маршрутизаторами r; E_e - енергія, споживана кінцевим пристроєм e.

Вирази (1) - (3) показують, нащо витрачають енергію джерела живлення, кінцеві пристрої, маршрутизатори і вся БСМ.

Аналізуючи рис.2 видно, що основний цикл роботи вузлів повторюється. Передача 1-го повідомлення, як правило, проходить за один цикл під час циклу активності мережі.

Визначимо енергоспоживання мережі з урахуванням циклів активності і часу їх роботи:

$$E_{all} = \sum_{k=1}^{k} E_k \cdot T_k + a \cdot \left(\sum_{r=1}^{r} E_r \cdot T_r + \sum_{e=1}^{e} E_e \cdot T_e \right), \qquad (4)$$

деa - число циклів активності мережі; T_k - час, витрачений на роботу координатора; T_r - час, витрачений на роботу r-того маршрутизатора під час циклу активності; T_e - час, витрачений на роботу e-того кінцевого вузла під час циклу активності.

Зазвичай час життя мережі визначається часом життя пристрою, який першим вийде з ладу. Розрахуємо час життя мережі, якщо батарея має заряд E_b, то часу життя всієї мережі:

$$t = \frac{E_b}{E_W} T_a = \frac{E_b}{E_{all}}, \qquad (5)$$

деT_a - час циклів активності мережі.

Висновок: За допомогою запропонованого підходу до аналізу енергоспоживання вузлів БСМ можна отримати оцінку пропускної здатності мережі без дорогого натурного моделювання та визначити придатність модулів різних виробників для проектованої мережі.

Література

1. IEEE StandardforInformationTechnology – TelecommunicationsandInformation Exchange BetweenSystems – LocalandMetropolitanAreaNetworks –Specific Requirements – Part 15.4: WirelessMedium Access Control (MAC) andPhysicalLayer (PHY) Specificationsfor Low-Rate WirelessPersonalAreaNetworks (2009). IEEE Std. 802.15.4-2009, 1–39. Available at:http://standards.ieee.org/getieee802/download/802.15.4d-2009.pdf/.
2. MeasuringPowerConsumptionof CC2530 WithZStack [Electronicresource] / TexasInstrumentsApplicationНоте AN079. – Availableat: http://www.ti.com/lit/an/swra292/swra292.pdf/ – 10.06.2014 г.– Titlefronthescreen.
3. Галкин, П. В. Адекватность моделей беспроводныхсенсорныхсетей в средахимитационногомоделирования [Текст] / П. В. Галкин, А. С. Борисенко // Восточно-Европейский журнал передовыхтехнологий. –2013. – Т. 4, № 9 (64). – С. 52–55.
4. Пушкарев, О. Использованиеконечныхспящихузлов в сети ZigBee [Текст] / О. Пушкарев // Электронныекомпоненты. – 2011. – № 5. – С. 91–95

УДК 621.382

КЕРІВНІ ПРИНЦИПИ ТА ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЇ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Туранська О. С., Петрова В.М.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: turanska.o.s@gmail.com

Guiding principles and approaches to information security in Wireless Sensor Networks

Wireless sensor networks (WSN) have many applications in our time. For example in military, rescue works and other areas. WSN have many sensors which can be located in hostile territory. If we want save confidential information, we mustensure information security when it is transmitted over the network. That's why we need to know Guiding principles and approaches to information security.

Питання забезпечення захисту інформації в безпроводових сенсорних мережах(БСМ) є дуже важливим. Це пояснюється тим, що на сьогоднішній день БСМ мають безліч застосувань у військовій, внутрішній безпеці та інших областях.Безпека в таких випадках має важливе значення, оскільки безпроводові сенсорні мережі часто розгортаються на ворожій території і можуть мати важливе стратегічне значення. Атаки на таку мережу можуть призвести до витоку конфіденційної інформації. Крім того, безпроводовий зв'язок, який використовується мережами датчиків, полегшує підслуховування і отримання інформації противником.

Комбінація цих факторів вимагає впровадження заходів безпеки для сенсорних мереж під час проектування, щоб забезпечити надійність роботи та конфіденційність даних у сенсорних середовищах.

Основними керівними принципами захисту інформації в безпроводових сенсорних мережах є:

1. Безпека мережі визначається безпекою всіх шарів.
2. У масово розподіленій мережі, заходи безпеки повинні бути піддані динамічній реконфігурації та децентралізованому управлінню.
3. В даній мережі в будь-який момент часу витрати, пов'язані з заходами безпеки, не повинні перевищувати витрати, які були вирахувані з врахуванням ризиків.
4. Якщо фізична безпека вузлів у мережі не гарантується, заходи безпеки повинні бути стійкими до фізичного втручання з вузлами в області експлуатації.
5. Через різноманітність обмежень у БСМ, при розробці схеми безпеки слід уважно розглянути наступні аспекти: енергоефективність, щільність вузла та надійність, адаптивність, самостійна конфігурація, простота та локальний ідентифікатор.

Впровадження заходів для забезпечення захисту інформації в безпроводових сенсорних мережах ускладнюється особливостями самих мереж, такими як: датчики чутливі до фізичного захоплення, датчики з безпроводовим зв’язком легко підслуховувати, в таку мережу зловмисник може легко внести шкідливе повідомлення, технології захисту від стискання та фізичної витримки неможливі через велику конструктивну складність та споживання енергії, обмеження датчиків роблять безпроводову сенсорну мережу більш сприйнятливими до атаки відмови в обслуговуванні, мала місткість пам’яті унеможливлює втілити централізоване технології набору ключових слівіснує конфлікт між споживанням ресурсів та максимізацією рівня безпеки, при цьому необхідно забезпечували максимально низьку загальну вартість БСМ.

Для досягнення безпеки в БСМ важливо мати можливість виконувати різні криптографічні операції, включаючи шифрування, автентифікацію тощо.Проте рішення щодо вибору відповідного методу криптографії залежить від обчислень та можливостей зв'язку вузлів датчиків. Асиметрична криптографія часто є надто дорогою для багатьох застосувань. Тим не менш, симетрична криптографія не така універсальна, як криптографічні методи публічного ключа, що ускладнює розробку захищених програм. Застосування будь-якої схеми шифрування вимагає передачі додаткових бітів, отже, додаткової обробки, пам'яті та заряду акумулятора, що є дуже важливими ресурсами для довговічності датчиків.Застосування механізмів безпеки, таких як шифрування, також може збільшити затримку, джиттер і втрати пакетів в БСМ.

Захист криптографічної системи залежить, головним чином, від секретності ключа, який в ній використовує. Схеми керування ключами - це механізми, що використовуються для встановлення та розповсюдження в мережі різноманітних криптографічних ключів, таких як окремі клавіші, парні клавіші та групові ключі.Ключове управління - це важливий криптографічний примітив, на якому будуються інші примітиви безпеки. Якщо зловмисник може знайти ключ, вся система зламається.

Ще одним підходом, який використовується для підвищення безпеки при роботі БСМ, є збереження агрегації даних.

Агрегування даних - це процес, в якому проміжні вузли, які називаються «агрегаторами», збирають первинну інформацію з датчиків, обробляють її локально і відправляють тільки результат кінцевому користувачеві.Ця важлива операція істотно зменшує в мережі кількість даних, що передаються, і, таким чином збільшує час життя датчиків. При цьому даний процес може бути уразливим до атак і потребує ефективного захисту даних, що передаються.

Першою лінією захисту даних від загроз та атак є криптографічні

механізми: цілісність і конфіденційність можуть бути досягнуті з використанням криптографічних схем.

Проблемою такого методу є необхідність гарантувати те, що користувач все ще може бути впевнений в точності агрегованих даних, навіть якщо агрегатор і невелике підмножина вузлів датчика знаходяться під контролем противника. У захищених протоколах агрегування даних потрібно порівняння продуктивності з точки зору таких матриць, як безпека, накладні витрати на обробку даних, накладні витрати на зв'язок, споживання енергії і ступінь стиснення даних.

Для вирішення цієї проблеми необхідно розробити нові протоколи агрегації даних, щоб забезпечити більш високу масштабованість і надійність від обману агрегатора і вузла датчика. Забезпечити криптографію всередині внутрішньої обробки даних (захищена обробка даних), безпечні, дуже ефективні і економічні механізми агрегації даних, достовірність і надійність агрегованих даних. Також необхідна безпечна схема агрегації даних в середовищах без великих вузлів.

Внутрішня обробка необроблених даних виконується в безпроводових сенсорних мережах шляхом ділення мережі на невеликі групи і аналізу даних, агрегованих у лідерів групи.

Тому лідер групи повинен аутентифікувати дані, які він отримує від інших вузлів в групі.Для цього потрібно керувати ключовими ключами. Однак додавання або видалення вузлів з групи призводить до більшої кількості проблем.

Отже, потрібні безпечні протоколи для групового управління.

Проблеми безпеки є потенційним каменем спотикання для майбутнього широкого розгортання сенсорних мереж. БСМ все ще знаходяться в процесі розробки, і багато протоколів, розроблені до цього часу для БСМ, не враховують безпеку.З іншого боку, істотні особливості безпроводових сенсорних мереж роблять дуже складною розробку сильних протоколів безпеки при збереженні низьких накладних витрат.

Багато проблем безпеки в БСМ залишаються відкритими, проте розуміння особливостей роботи та керівних принципів забезпечення захисту інформації дозволяє нам знаходити нові підходи до вирішення цієї проблеми.

Література

1. Chris Karlof and David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks, Elsevier Publications, 2003.
2. T.Kavitha and D.Sridharan, “Security Vulnerabilities In Wireless Sensor Networks: A Survey”, Journal of Information Assurance and Security (2010), 2010.
3. Murat Dener, “Security Analysis in Wireless Sensor Networks”, year 2014.
4. Половко А.М., Гуров С. В. Основитеоріїнадійності. – СПб.: БХВ-Петербург 2006. – 560 с.

УДК 621.396.946

МЕТОД СКОРОЧЕННЯ ЧАСОВИХ ЗАТРИМОК СИГНАЛІВ ГЕОСТАЦІОНАРНИХ СИСТЕМ СУПУТНИКОВОГО ЗВ'ЯЗКУ

Явіся В.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya@bigmir.net

A method for reducing the time delays of signals of geostationary satellite communication systems

Satellite communications provides a wide range of telecommunication services in almost anywhere in the world. At the same time, the quality of telephony services depends on the way the satellite system is built. In order to reduce the delay time of the signal in satellite systems using satellites in the geostationary orbit, it is proposed to further utilize the grouping of low-orbital nanosatellites.

Для користувача послугами супутникового зв'язку не має значення спосіб побудови супутникової системи. Головним є спектр послуг, що надаються, та їх якість. На ринку України декількома офіційними дилерами представлені чотири оператори глобального супутникового зв'язку: Inmarsat, Thuraya, Iridium та Globalstar [1].

Всі оператори пропонують два варіанти підключення: ваучери і контрактне обслуговування. В разі надання певного пакету послуг вартість обслуговування у всіх операторів приблизно однакова. Вартість та функціональні можливості обладнання, що знаходиться у користувача, для різних операторів також відрізняється не значним чином [1, 2]. Тому при виборі оператора слід звертати увагу на якість обслуговування, яка певним чином залежить від способу побудови системи супутникового зв'язку.

Низькоорбітальні системи Iridium та Globalstar побудовані таким чином, що супутники постійно обертаються навколо Землі, це спрощує пошук сигналу і гарантує постійний зв'язок в зоні покриття. Системи Inmarsat та Thuraya працюють на геостаціонарних супутниках, які для користувача знаходяться постійно на одному і тому ж місці (приблизно на екваторі). При їх використанні для якісного зв'язку необхідна відкрита видимість в бік екватора [3].

Аналіз принципів побудови глобальних систем супутникового зв'язку дозволяє зробити висновок про те, що системи з апаратами на геостаціонарній орбіті мають ряд переваг [3, 4]:

- можливість обслуговування абонентів мережі без наземних шлюзових станцій;
- висока стабільність рівня сигналу в радіо каналі;
- відсутність ефекту Доплера;

- простота організації зв’язку в глобальному масштабі.

Загальними недоліками є:

- перенасиченість геостаціонарної орбіти на багатьох ділянках;
- неможливість обслуговування приполярних областей;
- високе загасання сигналу;
- значна затримка у проходженні сигналу.

Для користувача послугами супутникового зв’язку з погляду на якість обслуговування найбільш суттєвим є останній недолік, притаманний системам Inmarsat та Thuraya. Він пов'язаний із великою відстанню (36000 кілометрів) від поверхні Землі до супутника. Позбавитись його можливо лише за умови створення коротшого шляху проходження сигналу. Така можливість з’являється за рахунок роумінгу, при умові того, що абонент з двохрежимним терміналом потрапляє до зони обслуговування наземної мобільної мережі GSM. Але така можливість є не завжди.

Пропонується інший спосіб вирішення зазначеного недоліку, який передбачає певного роду модернізацію супутникового угруповання. Мова йде про застосування наноспутників (НС). Такі апарати важать всього кілька кілограмів і можуть виводитися в космос в якості попутного навантаження або відразу пакетами в десятки і навіть сотні одиниць. Доступ абонентів до ресурсів мережі можливий саме через НС. Кластери НС можуть використовуватися в якості ретрансляційної мережі. За умови розташування орбіти НС на висотах до 700 км з’являється потенційна можливість зменшення затримки сигналу за рахунок скорочення протяжності маршруту його проходження.

На рисунку 1 зображений випадок обслуговування абонентів, які знаходяться в зоні обслуговування одного геостаціонарного супутника. Існуючий варіант обслуговування передбачає встановлення з’єднання в декілька основних етапів. На першому етапі ініціатором, наприклад Абонентом 1, надсилається запит на ГС на обслуговування, отримується його підтвердження, після чого передається адресна інформація (ділянка 1.1). По завершенні її аналізу визначається можливість встановлення з’єднання з Абонентом 2 (ділянка 1.2) та за наявності такої відбувається передача трафіку між абонентами по маршруту: Аб.1–1.1–ГС–1.2–Аб.2.

Довжина шляху проходження сигналу без урахування кривизни поверхні Землі, при відстані до ГС близько 36000 км складає порядку $S1$=72000 км, що відповідає часу затримки в проходженні сигналу в одному напрямку: $T_{затр1}=S1/C=0,24$ *(с)*.

При наявності угрупування НС передбачається, що інформація про розташування НС є доступною та постійно оновлюється на ГС. Алгоритм встановлення з’єднання незначно ускладнюється і виглядає наступним чином. Початковий етап (ділянки 1.1, 1.2) практично збігається із попереднім

випадком. Але, після встановлення факту доступності Абонента 2, відбувається аналіз можливості встановлення з'єднання абонентів із певними НС (ділянка 2), а також між зазначеними НС. При значній кількості НС в угрупуванні така можливість високо імовірна.

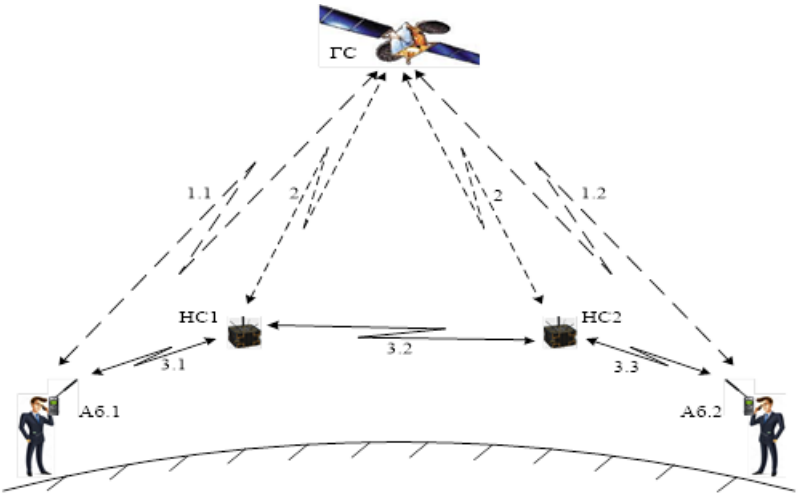


Рис. 1. Етапи встановлення з'єднання та проходження сигналів між абонентами

Тобто, якщо вона є, від ГС надходить сигнал управління як до абонентських терміналів, так і до визначених НС, на встановлення з'єднань між терміналами і НС (ділянки 3.1, 3.3), та між НС (ділянка 3.2). Залежно від відстані між абонентами буде змінюватись кількість ділянок 3.2 в маршруті. На рис. 1 представлений варіант такого з'єднання між абонентами по маршруту: Аб.1–3.1–НС1–3.2–НС2–3.3–Аб.2.

Довжина шляху проходження сигналу між абонентами, які знаходяться на відстані 10000 км один від одного при відстані до НС близько 700 км, складає порядку $S2$=12000 км, що відповідає часу затримки в проходженні сигналу в одному напрямку: $T_{зат2}=S2/C=0,04$ *(с)*.

Слід зазначити, що проведені розрахунки здійснювались без урахування часу обробки сигналів на борту ГС та НС.

Таким чином, застосування угрупування НС у системах з супутниками на геостаціонарній орбіті дозволить значно скоротити час запізнювання сигналу і тим самим підвищити якість обслуговування абонентів.

Література

1. Sattrans, сайт компании. Информация о системах спутниковой связи. /Электронный ресурс/ http://sattrans.ua/index.php?route=common/home.

2. SatcomDV, сайт компании. Информация о системах спутниковой связи. /Электронный ресурс/ http://www.satcomdv.ru/informaciya_o_sistemah_sputnikovoj_sa.

3. Быховский М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие спутниковых телекоммуникационных систем: учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 436 с.

4. Кукк К.И. Спутниковая связь: прошлое, настоящее, будущее. – М.: Горячая линия – Телеком, 2015. – 256 с.

УДК 621.396.946

РЕГІОНАЛЬНА СИСТЕМА СУПУТНИКОВОГО ЗВ'ЯЗКУ

Явіся В.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya@bigmir.net

Regional satellite communication system

The analysis of methods of construction of satellite communication systems, which are presented on the market of telecommunication services of Ukraine, is conducted. In order to satisfy the needs of the population and state structures in satellite communication services, it is proposed to use as one satellite a single geostationary-based satellite.

На сьогоднішній день супутниковий зв'язок – це реальна можливість організації та підключення до всіх існуючих сервісів, від телефонії, високошвидкісного доступу в Інтернет, до побудови корпоративних мереж для передачі даних. Супутниковий зв'язок – оптимальний варіант для створення комунікацій між географічно віддаленими регіонами, а також районами зі слабо розвиненою інфраструктурою.

Затребуваність супутникового зв'язку пояснюється його загальними перевагами, серед яких, зокрема [1]: велика пропускна здатність; можливість обслуговування у важкодоступних районах; можливість побудови мережі без фізично реалізованих комутаційних пристроїв.

Якість послуг, що пропонуються операторами, певною мірою залежить від способу побудови системи супутникового зв'язку.

Взагалі за характером і висотою орбіти розрізняють 4 типи систем супутникового зв'язку:

1. Низькоорбітальні системи (LEO – Low Earth Orbit) – із круговими орбітами висотою 700-2000 км. Супутник, що знаходиться на низькій орбіті, перебуває в зоні прямої видимості з певної точки земної поверхні лише на протязі 8-12 хв. Тому, для забезпечення неперервного зв'язку, необхідна велика кількість супутників. Такі системи мають гарні енергетичні характеристики радіоліній.

2. Середньоорбітальні (MEO – Medium Earth Orbit) – із круговими орбітами 10 000 км. Затримка розповсюдження сигналу складає 130 мс.

3. Високо орбітальні чи геостаціонарні (GEO – Geostationary Earth Orbit) – із круговими екваторіальними орбітами висотою близько 40 000 км. Перевагою таких систем є можливість покриття всієї земної поверхні невеликою кількістю супутників (від трьох). Основний недолік – великий час розповсюдження радіосигналів (затримка радіосигналу).

4. Високо еліптичні (HEO – Highly Elliptical Orbit) – з витягнутими еліптичними орбітами, що мають радіус перигею порядку тисячі кілометрів і радіус апогею порядку одного чи декількох десятків тисяч кілометрів.

На сьогодні в Україні послуги супутникового зв'язку представлені в

основному такими операторами як *Iridium, Inmarsat, Thuraya* та *Globalstar* [2]. За орбітальною ознакою їх умовно можна розділити на дві групи. До першої відноситься супутниковий зв’язок операторів *Inmarsat* та *Thuraya*, який працює на геостаціонарних супутниках. Друга група представлена операторами – *Iridium* та *Globalstar*, які являють собою низькоорбітальні системи.

Компанія *Inmarsat* має і експлуатує мережу супутникового зв'язку, що має парк з одинадцяти супутників (два з яких є резервними) на геостаціонарній орбіті на відстані близько 36000 кілометрів від Землі і включає супутники нового покоління, які являють собою певний еталон для систем супутникового зв’язку з точки зору їх енергетичних можливостей, пропускної спроможності і універсальності. Виведені на орбіту супутники забезпечують глобальне охоплення широкосмуговим зв’язком 98% земної поверхні, за винятком самих крайніх полярних регіонів.

На геостаціонарну орбіту оператором *Thuraya* запущено всього три супутники, один з яких вже відпрацював свій ресурс, однак і надалі перебуває на орбіті, як резервний. Два активних супутника утворюють зону покриття в який існують «білі плями» як у світовому океані, так і на суші: Північна та Південна Америка, більша частина північних територій Росії, а також обидва полюси Землі.

Кожен із супутників *Inmarsat* та *Thuraya*, розташованих на геостаціонарній орбіті, генерує сотні надпотужних сфокусованих променів, які можуть бути оперативно сконфігуровані так, щоб надавати необхідну пропускну здатність мережі в районах підвищеного попиту на послуги шляхом розширення або збільшення кількості променів.

Дзвінок всередині мережі в будь-якій точці зони покриття здійснюється без використання наземних станції. З’єднання абонентських терміналів із наземними мережами оператором *Inmarsat* забезпечується трьома наземними станціями, оператор *Thuraya* використовує одну таку станцію [3, 4].

Термін служби супутників розрахований на 12-15 років [5].

Представником групи низькоорбітальних супутникових систем, якому вдалося забезпечити 100% покриття поверхні Землі, є оператор *Iridium*.

В системі *Iridium* функціонують 77 супутників, 66 з яких є активними і які розміщуються на 6-ти приполярних орбітах. Розроблений для цієї мережі механізм між супутникових зв’язків дозволяє передавати сигнал з одного супутника на інший без ретрансляції цього сигналу на Землю. Таким чином, теоретично *Iridium* може працювати при наявності лише однієї земної станції сполучення, що приймає всі абонентські дзвінки (всього працює 2 такі станції). Супутники *Iridium* знаходяться на висоті 780 км над поверхнею Землі, нижче всіх інших супутників, які використовуються відомими системами мобільного супутникового зв'язку [3, 4].

Супутники *Globalstar* є ретрансляторами з прямою ретрансляцією. В угрупуванні 48 активних та 4 резервних апарати, які знаходяться на висоті 1414 км. Мережа наземних шлюзових станцій забезпечує можливість підключення від 40 супутників до наземних мереж. У зв'язку з відсутністю

міжсупутникового зв'язку, апарати повинні мати вихід до станції з метою надання послуг для всіх користувачів, яких можна розпізнати. Використання мережі наземних шлюзів надає клієнтам локалізовані регіональні телефонні номери для мобільних телефонів супутникового зв'язку. Але якщо немає станцій прийому сигналу в деяких віддалених районах, сервіс не може бути наданий, навіть якщо супутники присутні над ними. Внаслідок цього без покриття залишаються полюси і окремі регіони в Африці та Азії.

Термін служби супутників *Iridium* та *Globalstar* в межах 7-10 років [5].

Сьогодні в Україні існує велика кількість користувачів послугами супутникового зв’язку, в тому числі і відомчих структур. Фактично таки послуги надаються іноземними телекомунікаційними компаніями. Тому певні зміни у міжнародному політичному середовищі гіпотетично можуть привести до відмови в обслуговуванні вітчизняних користувачів. При цьому альтернативним рішенням, що дозволить запобігти зазначеній загрозі, є створення власної регіональної системи супутникового зв’язку.

Аналіз принципів побудови систем супутникового зв’язку дозволяє зробити висновок про те, що системи з апаратами на геостаціонарній орбіті мають ряд переваг перед низькоорбітальними системами, а саме: можливість обслуговування абонентів мережі без наземних шлюзових станцій; високу стабільність рівня сигналу в радіо каналі; відсутність ефекту Доплера; простоту організації зв’язку; більш тривалий термін служби апаратів.

Для забезпечення повного покриття території України достатньо лише одного геостаціонарного супутника, а при використанні низькоорбітальних апаратів, – не менш восьми. Тобто економічно обґрунтованим є створення системи супутникового зв’язку геостаціонарного базування. Звичайно при цьому необхідно пам’ятати і про головні недоліки таких систем: перенасиченість геостаціонарної орбіти на багатьох ділянках; високе загасання сигналу; значна затримка у проходженні сигналу.

Таким чином, для задоволення потреб населення України та відомчих структур держави послугами супутникового зв’язку достатньо розгорнути на геостаціонарній орбіті лише один супутник.

Література

1. Сомов А.М., Корнев С.Ф. Спутниковые системы связи: учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 244 с.
2. Sattrans, сайт компании. Информация о системах спутниковой связи. /Электронный ресурс/ http://sattrans.ua/index.php?route=common/home.
3. SatcomDV, сайт компании. Информация о системах спутниковой связи. /Электронный ресурс/ http://www.satcomdv.ru/informaciya_o_sistemah_sputnikovoj_sa.
4. Быховский М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие спутниковых телекоммуникационных систем: учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 436 с.
5. Кукк К.И. Спутниковая связь: прошлое, настоящее, будущее. – М.: Горячая линия – Телеком, 2015. – 256 с.

УДК 621.396.946

НАНОСУПУТНИКОВІ НАВІГАЦІЙНІ СИСТЕМИ

Явіся В.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya@bigmir.net

Nanosatellite navigation systems

The quality of the operation of satellite navigation systems determines the safety of the movement of surface and aircraft. Disabling or coding the signals of such systems can lead to disastrous consequences. To increase the level of independence from global navigation systems, it is proposed to use the grouping of nanosatellites.

Останнім часом задача визначення місцезнаходження будь яких об’єктів вирішується завдяки супутниковим навігаційним системам. Без їхнього існування неможливо гарантувати безпеку руху надводних та повітряних суден. Значного поширення набувають послуги, які дозволяють відстежувати переміщення вантажів, стежити за транспортними засобами. Навігаційні додатки в мобільних пристроях значно спрощують пошук об’єктів за адресою, дозволяють прокладати оптимальні маршрути до пунктів призначення. Від якості функціонування навігаційних систем напряму залежить не лише безпека, але і якість та комфортність життя сучасної людини.

Забезпечити стабільну роботу навігаційних систем, підвищити їх точність та надійність можливо при реалізації одного з аспектів процесів глобалізації світової економіки, що складається в поетапному створенні до 2025 року світової аеронавігаційної системи відповідно до Глобальної експлуатаційної концепції Міжнародної організації цивільної авіації ICAO (International Civil Aviation Organization). При цьому передбачається, що Росія й США, будучи глобальними гравцями, здійснять інтеграцію своїх аеронавігаційних систем у світову, що припускає перехід до перспективної техніки й технологій концепції CNS/ATM (Communication, Navigation and Surveillance/Air Traffic Management – зв'язок, навігація, спостереження/організація повітряного руху) [1].

Вимоги CNS/ATM орієнтовані на використання на всіх етапах польоту повітряних судів Глобальних навігаційних супутникових систем GNSS (Global Navigation Satellites System) с поступовим усуненням потреби в наземних засобах [2].

Системи аеронавігації GNSS (GPS, ГЛОНАСС й ін.) дозволяють визначати координати об'єктів на великих територіях з високою точністю. Їх можливості значно ширше, ніж у систем на базі наземних засобів. Однак застосування супутникової навігації GNSS, як єдиного засобу одержання аеронавігаційної інформації, несе в собі значні ризики, що може відбитися на безпеці польотів, стабільності перевезень, а також роботі телекомунікаційних

мереж, що базуються на безпілотних літальних апаратах. До основного із цих ризиків можна віднести наступні [3]:

• у силу енергетичної слабості прийнятих навігаційних сигналів абонентські термінали GNSS уразливі для постановників активних радіоперешкод, як навмисних, так і ненавмисних;

• монополізація володінням GNSS (GPS, ГЛОНАСС – військові відомства) не виключає того, що доступна точність навігаційних показників може бути навмисно погіршена, навігаційні сигнали можуть бути закодовані або навіть відключені при зміні міжнародної обстановки;

• внаслідок глобального характеру GNSS локальний вплив на окремі елементи систем (космічні апарати, наземні пункти керування й ін.) здатний унеможливити використання авіації й систем керування повітряним рухом у значній частині земної кулі.

Для нейтралізації можливих негативних наслідків необхідна наявність альтернативних GNSS засобів, які можуть бути використані у якості основних, додаткових або резервних.

При цьому, з урахуванням положень CNS/ATM, вони повинні відповідати наступним основним вимогам [2]:

• володіти аналогічними з GNSS функціональними можливостями по забезпеченню навігації;

• точність визначення місця розташування повинна бути не гірше, ніж у систем, побудованих на базі GNSS;

• бути повністю незалежними від даних GNSS;

• забезпечувати можливість інтеграції з перспективними системами на базі GNSS для поліпшення показників точності, цілісності, безперервності й експлуатаційної готовності в різних територіальних районах.

На 12-й Аеронавігаційній конференції ICAO (Монреаль, Канада) було заявлено про необхідність створення альтернативних стосовно GNSS наземних засобів аеронавігації. Однак у цей час, на ринку системи такого класу поки не представлені.

Значне зниження впливу зазначених негативних факторів досягається шляхом реалізації ряду дій, що включають застосування [3]:

• комплексу спеціально розроблених алгоритмів, що базуються на нових комбінованих способах визначення просторових координат у багатопозиційних системах;

• спеціальних методів синхронізації системи без використання модулів атомного еталону часу й координат GNSS;

• оптимального просторового конфігурування радіомаяків;

• складних сигналів із заданими індивідуальними ознаками;

• сучасної електронної компонентної бази, що забезпечує мінімізацію ваго габаритних характеристик устаткування й високу обчислювальну потужність;

• технології створення бортових багатофункціональних приймачів, сполучених з обладнанням GNSS, що дозволяє звести до мінімуму обсяг

необхідних конструктивних доробок на борту повітряних суден, а в деяких випадках забезпечити їх повну відсутність.

Наземні засоби аеронавігації, будучи альтернативою системам GNSS, все ж таки не зможуть виконувати свої функції в умовах потужних радіоперешкод. Крім того їх ефективне застосування є обмеженим деякою просторовою областю.

Для переважної більшості країн світу реальною загрозою залишається втрата навігаційних сигналів у випадку їхнього відключення або кодування відповідними монополістами GNSS (наприклад GPS, ГЛОНАСС).

Очевидно, що в даній ситуації залишитися незалежним від GNSS можна при розгортанні власної навігаційної системи. Така можливість з'являється, коли мова йде про використання угруповання наносупутників (НС). Завдяки їх відносно невисокій вартості створення й виводу на орбіту, кількість елементів такої системи може бути досить великою, що за умови забезпечення синхронізації випромінюваних сигналів дозволить створити їх достатній енергетичний рівень на вході приймача, навіть в умовах застосування активних навмисних радіоперешкод.

У складній, стосовно наявності перешкод, обстановці, за умови використання спрямованих антен на борту НС, значно збільшити енергетику навігаційних сигналів у заданій області також можливо шляхом рішення завдання забезпечення необхідного керованого просторового положення НС.

У більшості випадків НС не можуть змінювати своє положення в просторі, що пов'язано із ваго-габаритними обмеженнями, які змушують відмовитися від оснащення НС системами стабілізації й орієнтації.

Традиційно для розв'язку завдання орієнтації й стабілізації застосовуються два методи [4]: пасивний і активний. Хоча пасивний метод не вимагає витрат енергії, що запасається на борті супутника, лише активні методи здатні забезпечити зміну орієнтації впродовж коротких інтервалів часу.

Активні методи стабілізації бувають трьох типів: стабілізація за допомогою двигунів-маховиків; стабілізація за допомогою моментного магнітоприводу; система стабілізації з реактивними двигунами.

Основною перевагою систем стабілізації за допомогою двигунів-маховиків і моментного магнітоприводу є те, що вони не вимагають наявності на борті запасів палива.

При використанні двигунів-маховиків система при незначному енергоспоживанні показує досить високу ефективність і швидкодію. Основним недоліком є те, що після закінчення орієнтації необхідно підтримувати швидкість обертання маховиків на заданому значенні. При відсутності достатнього запасу електроенергії (при знаходженні НС у тіні) ресурсу акумуляторів може виявитися недостатньо для забезпечення роботи електродвигунів, що у свою чергу викличе втрату орієнтації [4].

Явною перевагою системи на магнітних виконавчих органах є зручність розташування її елементів у корпусі НС. Крім того, по закінченню орієнтації й стабілізації, система не вимагає додаткових енерговитрат.

Недоліками такої системи є відносно мала величина керуючих моментів, а також те, що без залучення додаткового керуючого пристрою іншого виду моментний магнітопровід не в змозі забезпечити тривісну орієнтацію НС у просторі [4].

Реактивні двигуни мають загальний недолік: обмежений час функціонування у зв'язку з розходом робочого тіла. Сам принцип ежекції маси приводить до необхідності створення її резерву, що підвищує вагу НС при запуску.

Альтернативою реактивним двигунам є використання іонних двигунів, основною гідністю яких уважається економічність. Іони мають швидкість на порядок вище швидкості витікання газів з ракетного двигуна, тому для зміни швидкості НС на задану величину їм потрібно на порядок менше палива.

На даний час розроблені спеціальні надкомпактні іонні двигуни для корекції орбіти НС. Запас палива, або іншими словами реактивна маса, буде зберігатися безпосередньо усередині двигуна в рідкому виді й виходити назовні через мікроскопічний отвір, де її частки іонізуються й прискорюються електричним полем [5]. Виходячи із заявлених в [5] характеристик, можна оцінити ефективність керування НС та зробити висновок, що їх можливості практично збігаються з можливостями системи, що використовує моментний магнітопривід [4].

Системи орієнтації на двигунах-маховиках і магнітних виконавчих органах не дозволяють здійснювати зміну орбіти НС, тому найбільш доцільним буде використання комбінованої системи, що складається з магнітних котушок, які дозволяють вирішувати завдання стабілізації й орієнтації, а також іонних двигунів, які будуть задіяні, в основному, для зміни орбіти НС, що дозволить значно збільшити їхній термін служби.

Таким чином, розгортання власної навігаційної системи, що базується на угрупованні НС із запропонованою комбінованою системою управління, за умови рішення завдань синхронізації випромінюваних сигналів, орієнтації й стабілізації просторового положення НС із необхідною точністю, дозволить підвищити незалежність України в сфері аеронавігації.

Література

1. Doc. 9750-AN/963. Глобальный аэронавигационный план применительно к системам CNS/ATM. – Изд. 2-е. – Монреаль: ICAO, 2002.
2. Системы CNS/ATM: учеб. пособие / Сост. В.А. Казаков. – 2-е изд., перераб. и доп. – Ульяновск: УВАУ ГА, 2008. – 103 с.
3. Кузьминский А.В. Вопросы создания новых систем аэронавигации // Мобильные телекоммуникации – № 2 – М.: «Профи-Пресс», 2014. – С. 10-11.
4. Явися В.С. Способы управления пространственным положением наноспутника // Десята міжнародна науково-технічна конференція «Проблеми телекомунікацій». Матеріали конференції. – К.: НТУУ «КПІ». – 2016. – С. 507-510.
5. Васильков А. Крошечный ионный двигатель будет корректировать орбиты наноспутников /Электронный ресурс/ http://www.computerra.ru/37296/37296/.

УДК 621.396.946

ОПТИМИЗИРОВАННОЕ ОТСЛЕЖИВАНИЕ И ОБНАРУЖЕНИЕ ЦЕЛЕВЫХ УЗЛОВ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Ярмола И.А., Петрова В.Н.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: i.yarmola@gmail.com

Optimized tracking and detection of target nodes in Wireless Sensor Networks

Coverage in a wireless sensor network can be thought of as how well the wireless sensor network is able to monitor a particular field of interest. The proposed system enlightens the approximation of the position of the nodes and that approximated positions are used to guess the location of the nodes. The approximation and the foreseeing of the nodes are done by space Theory and the location of the nodes by using ant colony optimization.

Беспроводная сенсорная сеть (WSN) состоит из пространственно-распределенных автономных датчиков для мониторинга физических или экологических условий и передачи всех собранных данных через сеть на основную базовую станцию. Разработка алгоритмов и прототипов транспортных средств для широкомасштабного наблюдения и разведки с использованием мобильных сенсорных сетей (МСС) в случае, когда датчики являются статическими, где развертывать или активировать узлы; и в случае, когда датчики подвижны, как планировать траекторию мобильных датчиков[1].

Эти два случая в совокупности называют проблемой покрытия в беспроводных сетях датчиков. Покрытие в беспроводной сенсорной сети можно рассматривать то, как беспроводная сенсорная сеть может отслеживать конкретную интересующую область. Предложенная система представляет аппроксимацию положения узлов и эти аппроксимированные позиции используются для угадывания местоположения узлов.

Одним из интересных приложений МССявляется отслеживание целей. Он состоит в том, что он мгновенно оценивает положение движущейся мишени. Это имеет большое значение для наблюдения и безопасности, особенно в военных применениях. Предлагается новая стратегию управления мобильностью датчиков, направленная на улучшение отслеживания одной цели.

Метод состоит из четырех последовательных фаз, которые повторяются на каждом временном шаге следующим образом[2]:

1. Аппроксимируя положение объекта,
2. Предвидеть следующий шаг позиции объекта, используя существующее и предыдущее приближение позиции,
3. Разработка наборов новых расположений, которые должны быть приняты мобильными узлами, чтобы продвигать процесс аппроксимации,

4. Выделение новых местоположений для каждого мобильного устройства с помощью алгоритма оптимизации колони муравьев (ОКМ)

Фаза приближения выполняется с использованием космического анализа [3]. Вся зона мониторинга должна быть покрыта датчиками, чтобы быть надежными для любых других злоумышленников. По этой причине предлагается использовать два типа датчиков: статические и мобильные узлы. В то время как мобильные датчики перемещаются для улучшения качества отслеживания целей, статические узлы распределены равномерно, чтобы обеспечить непрерывный охват сети независимо от движения мобильных устройств.

Расположение Узлов, используя Оптимизацию Колонии муравьев: имея набор положений, которые должны быть приняты датчиками, каждому узлу датчика назначается одна позиция внутри набора при уменьшении пройденного расстояния узлов. Таким образом, проблема определяется как алгоритм оптимизации, который решается с использованием ОКМ. В дальнейшем сначала вводится ОКМ, затем она применяется к задаче репозиционирования.

ОКМ- вероятностный метод решения сложных вычислительных задач. Этот алгоритм был впервые разработан для решения проблемы коммивояжера. Он был применен эффективно впоследствии в различных областях, таких как проблемы квадратичного присваивания [4], маршрутизация транспортного средства [14]. Основная идея ОКМсостоит в том, чтобы имитировать поведение реальных муравьев на пути к поиску кратчайшего пути получения источников пищи. Путь, таким образом, генерируется в соответствии с двумя элементами: химическим веществом, называемым феромоном, и видимостью муравья, который, в свою очередь, определяет путь для поиска цели [5].

Пусть f (x_1, ..., x_n) - функция от n переменных, значения которых взяты из определенного множества S. Оптимизация f состоит в нахождении n-перестановки (x_1, ..., x_n) по всем возможным перестановкам, которая оптимизирует функция f. В таких задачах функция f называется целевой функцией или функцией пригодности, тогда как x_1,. , ., x_n называются переменными решения. Пусть m - кардинал S, то число всех возможных n-перестановок равно m! / (m-n)! с m! являясь факториалом m. Оценка всех решений требует слишком большого вычислительного времени, особенно для проблем большого размера. В таких случаях использование алгоритмов оптимизации, таких как ОКМ, становится решающим для сокращения времени вычисления [6], [7].

Начиная с первоначального решения, ОКМ движется к оптимальным решениям, используя эффективную технику поиска на основе памяти. Генерация решений в основном использует два параметра: видимость и феромон. Эти параметры соответствуют априорной и апостериорной информации о решениях, соответственно. Хотя видимость остается неизменной, феромон модифицируется в процессе оптимизации в соответствии с оценкой решений. Технически алгоритм ОКМрассматривает

фиксированное количество муравьев Км, каждый из которых генерирует одно решение на каждой итерации. Решения, таким образом, кодируются путем назначения каждой переменной решения, один за другим, конкретное значение S.

Задача репозиции состоит в минимизации общего расстояния, пройденного узлами при переходе на новые позиции. Таким образом, функция пригодности равна сумме расстояний, перемещаемых движущимися узлами, тогда как переменными решения являются координаты датчиков. Эти переменные принимают значения в пределах набора позиций. Примером может служить метод репозиции для заданного временного шага t.

Этот метод является оригинальным поскольку в нём происходит отслеживания целей в сетях датчиков с контролируемой мобильностью. Имея движущуюся цель на каждом временном шаге, метод состоит в оценке текущей позиции цели и затем прогнозировании ее следующего положения с использованием модели прогнозирования второго порядка.

Затем выполняется перенос датчиков для оптимизации локализации цели на следующий временной шаг. Таким образом, набор позиций определяется с использованием метода на основе триангуляции.

Затем каждому датчику присваивается одна позиция набора с использованием алгоритма оптимизации колонии муравьев. В то время как фаза перемещения использует метаэвристический подход, этапы оценки и прогнозирования используют интервальный анализ, где целевые позиции представляют собой ящики, включая реальную стоимость.

В предлагаемом подходе используется гибридная сенсорная сеть, состоящая из статических и мобильных узлов, где мобильные узлы используются для оптимизации целевого отслеживания, статические узлы - обеспечивают общий охват сети.

Литература

1. Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions, R. Shorey, ed. John Wiley & Sons, 2006.
2. G. Song, Y. Zhou, F. Ding, and A. Song, “A Mobile Sensor Network System for Monitoring of Unfriendly Environments,” Sensors, vol. 8, pp. 7259-7274, Nov. 2008.
3. S. Aeron, V. Saligrama, and D.A. Castan˜o´n, “Efficient Sensor Management Policies for Distributed Target Tracking in Multihop Sensor Networks,” IEEE Trans. Signal Processing, vol. 56, no. 6, pp. 2562-2574, June 2008.
4. L. Hu and D. Evans, “Localization for Mobile Sensor Networks,” Proc. ACM MobiCom, 2004.
5. Y. Hani, L. Amodeo, F. Yalaoui, and H. Chen, “Ant Colony Optimization for Solving an Industrial Layout Problem,” European J. Operational Research, vol. 183, pp. 633-642, 2007.
6. P. S. Velumani and S. Murugappan”Ant Based Target Tracking and Localization Technique for Wireless Sensor Networks” European Journal of Scientific Research ISSN 1450-216X Vol.70 No.4 (2012), pp. 554-568 © EuroJournals Publishing, Inc. 2012.
7. J. Teng, H. Snoussi, and C. Richard, “Decentralized Variational Filtering for Target Tracking in Binary Sensor Networks,” IEEE Trans. Mobile Computing, vol. 9, no. 10, pp. 1465-1477, Oct. 2010.

УДК 528.831.1

THE SOLUTION OF THE PROBLEM WITH ELEKTROMAGNITNOI COMPATIBILITY RADOCHINA MEANS OF MOBILE COMMUNICATION SYSTEMS IN THE STANDARDS FOR 4G AND 5G

M. N. Stepanov
State University of Telecommunications
T. V. Uvarova
National Defense University of Ukraine, Ivan Chernyakhovsky

Рішення проблеми з електромагнітної сумісності радіоелектронних засобів систем мобільного зв'язку в стандартах 4G та 5G

В статі розглянуто нові тенденції розвитку телекомунікацій та вимоги до нових стандартів мобільного зв’язку. Запропоновано математична модель оцінки стійкості функціонування систем мобільного зв'язку при електромагнітних взаємодіях РЕЗ, що вводяться в систему дозволяє розглядати точки рівноваги системи при взаємодії різних РЕЗ, що дозволяє аналізувати її при конкретному виборі значень керуючих параметрів, наявності ресурсів.

Present in the communications industry due to the transition process in which interval the transition from "industrial age" in the "information age" almost completed.

The increase of the number of devices connected to the Internet over the past 10 years, is 10-100 times. So Cisco predicts 18-fold increase in mobile traffic from 2012 to 2017. Thus the projected growth of data traffic in mobile networks, and constantly growing number of users.

Based on all the above we can conclude that the transition and implementation of standards for 4G and 5G communication is essential to meet the needs of users.

So the fourth generation usually referred promising technology to transmit data at speeds in excess of 100 Mbit / s - moving and 1 Gbit / s - stationary subscribers.

Telecommunications Standards fifth generation connection is not complete, but by Huawei, introduced wireless networking technology that can achieve data rates above 10 Gb / s.

The uniqueness of the new generation is to be used any range of any access technology that is not a fixed radioparametry as in modern wireless networks. Perhaps the concept of roaming disappear, and thus the associated costs subscriber.

Due to the avalanche increase in the number of subscribers in the mobile network and increase traffic transmitted data is a problem in ensuring electromagnetic compatibility of radio electronic devices provider.

To ensure the electromagnetic compatibility of radio electronic devices mobile in their electromagnetic interactions with the introduction of new devices, the mathematical model for evaluating sustainability of the systems.

$$\Phi_i\left(\Psi_i; C_k; t; \frac{d\Psi_j}{dt}; \frac{d^2\Psi_j}{dt^2}; \dots\right) = 0, \quad (1)$$

Thus the model includes elements of the system, control parameters and system parameters (1). As mobile communication system is a dynamic system of the expression (1) can be described across a gradient (2)

$$\Phi_i = \frac{d\Psi_j}{dt} + \frac{\partial V(\Psi_j, C_k)}{\partial \Psi_i}. \quad (2)$$

Fig. 1 submitted Earl functional interactions described by electronic means system (3)

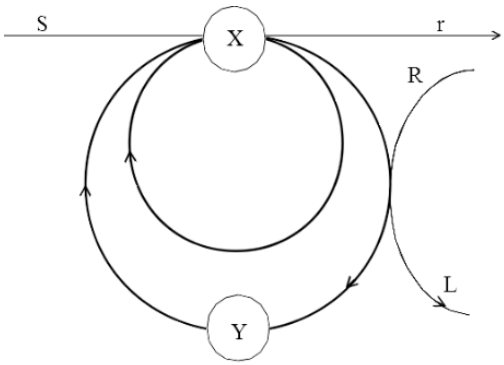


Fig. 1. Count functional interactions SEM

$$\begin{cases} \frac{dX}{dt} = S - (R+1)\cdot X + X^2Y; \\ \frac{dY}{dt} = RX - X^2Y. \end{cases} \quad (3)$$

which included the following functional characteristics of the system evolution:

RX- speed reducing resource through the park RES is introduced into the system;

X^2Y - the resources that came in after failing to resist the system.

The system of equations (3) concluded in the framework bryusselyatornoy model. If align speed (3) to zero, we obtain the equation of equilibrium dynamic systems:

$$\begin{cases} X = S; \\ Y = \frac{R}{S}. \end{cases} \quad (4)$$

In the practical implementation of this model may be deviation values of x and y from the equilibrium state (6). The system thus becomes:

$$\begin{cases} \dot{x} = x(R-i) + y(S^2) + x^2\left(\frac{R}{S}\right) + 2xyS + x^2y; \\ \dot{y} = y(-R) + y(-S^2) - x^2\left(\frac{R}{S}\right) - 2xyS - x^2y. \end{cases} \quad (5)$$

The resulting system should be analyzed from the standpoint of resistance variation parameters. Limited to linear on x and y members get

$$\begin{cases} \dot{x} = a_{11}x + a_{12}y; \\ \dot{y} = a_{21}x + a_{22}y. \end{cases} \quad (6)$$

where.

$$a_{11} = R = i, a_{21} = -R, a_{22} = -S^2$$

After converting the respective (6) takes the form of characteristic equation

$$\lambda^2 = \lambda \cdot (a_{11} + a_{22}) + a_{11}a_{22} - a_{12}a_{21} = 0 \quad (7)$$

where the coefficients which are respectively:

$$a_{11}a_{22} - a_{12}a_{21} = S^2;$$
$$-(a_{11} + a_{22}) = 1 + S^2 - R. \quad (8)$$

Positive and true value of guarantees from the instability caused by zeroing the first factor.

The second factor is zero when. Obviously, if there is a steady focus, while at the - unstable, ie when there is a Hopf bifurcation dynamic that creates the critical limit cycle. Thus, in this case using the parameter R as control leads to a symmetric assembly type disaster or classification Tom to disaster type.

$$R_0 = 1 + S^2R < 1 + S^2R > 1 + S^2R = 1 + S^2\text{A} \pm (2\text{к} + 1)$$

Conclusions. A mathematical model for evaluating sustainability of mobile communication systems with electromagnetic interactions RES entered into the system can be considered the equilibrium point of the system by the interaction of different RECs that can analyze it at the particular choice of values of control parameters, available resources and the related restrictions on quality information transmission. Based on this analysis can predict the development of mobile communication systems, EMC and its timely divert it from disaster. In addition, by analyzing the solutions can not determine the range of possible disturbances that do not cause significant qualitative change in the behavior of the system, ie to determine the range of adaptability.

References

1. Borodich S. V. EMC terrestrial and space Radiocommunication services. The criteria for conditions and payment. − M.: Radio and communication, 1990.
2. Buzov was A. JI. Maximum permissible levels of electromagnetic radiation of radio cellular systems mobile communication / Buzov was A. JI., Kolchugin, Y. I., Chepalova K. V., Paltsev Yu. P., Romanov V. A. // M.: Telecommunications. -1997. - No. 10.
3. Bykhovsky M. A. Analysis of electromagnetic compatibility of the receivers with an account of the phenomena of blocking, intermodulation and cross-distortion / Bykhovsky M. A., Mangalindan D. V. // Proceedings of NIIR. -1990. - No. 4.

УДК 621.396.4

СБОР ИНФОРМАЦИИ МОНИТОРИНГА В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ С БПЛА

Романюк А.В.
Институт телекоммуникационных систем
КПИ им. Игоря Сикорского, Украина
E-mail: anton.romaniuk@gmail.com

Collection of monitoring information in wireless sensor networks with UAV

An analysis of the existing approaches to the organization process of collecting information from the wireless sensors networks using UAV was carried out. The list of tasks and algorithms for the network management systems operation are proposed.

Современные беспроводные сенсорные сети (БСС) могут состоять из большого количества сенсорных узлов. Замена батарей для большого количества узлов может быть непрактичной или не возможной. Сеть может быть предназначена для работы в течение нескольких месяцев или даже лет в труднодоступных районах. В этих условиях актуальным становится применение беспилотных летательных аппаратов (БпЛА) для сбора информации мониторинга [1]. Сенсорные узлы осуществляют мониторинг определенных параметров внешней среды зон своего покрытия, хранят полученные данные и ждут возможности их передачи на центр сбора информации через БпЛА при его появлении в зоне радиосвязности. БпЛА облетают территорию и собирают данные мониторинга от сенсорных узлов

Сенсорные узлы имеют ограниченные ресурсы по энергии батареи, производительности процессора, памяти, мощности передатчика, пропускной способности радиоканала и т.д. Поэтому актуальным является увеличение времени функционирования сети при реализации процесса сбора данных с БпЛА [1 – 2].

Синтез методов сбора информации о БСС зависят от параметров (рис. 1):

- сети (предназначение, размерность, заданное время функционирования, способы развертывания и т.п.);
- сенсорных узлов (количество, тип сенсоров узла, тип трафика, параметры передатчика, энергия батарей, производительность устройств и т. д.);
- БпЛА (тип, время, скорость и высота полета, количество тип оборудования, протоколы информационного обмена и т.д.);
- принятой системы управления сетью (централизованная или децентрализованная), множества заложенных алгоритмов управления, протоколов информационного обмена на различных уровнях OSI и т.д.

Существующие подходы сбора информации с узлов с использованием БпЛА в качестве мобильного шлюза в БСС можно разделить на три группы.

1. Непосредственный сбор БпЛА информации мониторинга с каждого узла. В этом случае БпЛА облетает сенсорное поле по определенному маршруту и собирает данные с каждого узла.

Рис. 1. Сбор информации с БСС при использовании БпЛА

2. Сбор БпЛА информации мониторинга с выделенных узлов-рандеву, хранящих информацию мониторинга узлов выделенного кластера сети. Для обеспечения способа рандеву необходимо синтезировать и реализовать дополнительные алгоритмы управления сетью:

- разбиение сети на кластеры и выбор узлов-рандеву в кластерах (должна быть произведена оптимизация количества и размеров кластеров в зависимости от различных целевых функций) и складывающейся обстановки;
- построение энергоэффективной топологии в каждом кластере;
- организация процесса маршрутизации сбора данных до головы кластера;
- построение, оптимизация и корректировка пути облета БпЛА узлов рандеву.

3. Гибридный. Сеть также разбивается на кластеры. Однако маршрут облета БпЛА строится для посещения узлов-рандеву с корректировкой траектории первоочередного посещения критических узлов (например, с малой энергией батарей или перегруженных).

Требования по периодичности сбора данных мониторинга определяют поведение БпЛА (рис. 1).

Постоянный способ сбора предполагает постоянное покрытие БпЛА сенсорных узлов, сбор и передачу данных на пункт сбора.

Периодический – осуществляется полет БпЛА и сбор данных в определенные моменты времени.

По запросу – развертывание БпЛА осуществляется по мере необходимости.

При организации сбора данных мониторинга системе управления сетью (может быть реализована на пункте сбора информации мониторинга или на БпЛА) важно знать информацию о состоянии БСС. Система управления сетью может принимать различные решения в зависимости от наличия информации (полной, частичной, ее отсутствия) о состоянии сети (координаты размещения сенсоров, остаточная энергия батарей, объемы данных мониторинга и др.).

Целевыми функциями при сборе информации могут быть (рис. 1):

1. Минимизация времени сбора за счет минимизация времени облета БпЛА всех или заданного количества узлов.

2. Уменьшение расхода энергии батарей узлов, которое может быть осуществлено за счет:

- уменьшения расстояния между сенсорным узлом и БпЛА, регулировкой мощности передачи на минимальном уровне;

- оптимизацией количества кластеров и маршрутов передачи между узлами кластера и его головой;

- построением оптимальной энергоэффективной топологии и маршрутов передачи в кластерах;

- оптимизации сбора информации узлами мониторинга в кластере.

3. Балансировка трафика в сети и равномерная загрузка сети, особенно узлов-рандеву.

4. Минимизация служебного трафика.

5. Максимизация пропускной способности сети.

Предложен новый метод сбора информации БСС с использованием БпЛА, ключевыми особенностями которого являются:

1) Решение по маршруту, скорости и высоте перемещения, выбору целевых функций управления и алгоритмов сбора данных по разным уровням OSI – БпЛА принимает отдельно по каждому кластеру (отдельному фрагменту) сети.

2) Решение по кластеризации может приниматься централизованно центром управления сетью при наличии информации о состоянии БСС или распределенно узлами сети при ее отсутствии в центре управления.

3) Метрики кластеризации выбираются с учетом целевой функции управления и могут меняться при обслуживании БпЛА различных кластеров.

4) Система управления сетью постоянно корректирует целевые функции управления в зависимости от ситуации на сети, требований по сбору данных и имеющихся ресурсах.

5) Сочетание централизованного и децентрализованного управления неоднородной сетью (при наличии информации о состоянии сети, решения принимает центр управления сетью, при ее отсутствии – БпЛА и узлы кооперированным способом).

6) Увеличение времени функционирования сети при сборе информации при использовании БпЛА достигается за счет оптимизации: траектории перемещения БпЛА, количества и параметров кластеров обмена, количества узлов-рандеву, расстояния между БпЛА и узлами, применения энергоэффективных алгоритмов физического, канального, сетевого, транспортного и прикладного уровней модели OSI.

Таким образом, проведен анализ существующих подходов к организации процесса сбора информации от БСС с использованием БпЛА, рассмотрен перечень задач, необходимых для ее решения, предложены новый метод и алгоритмы функционирования системы управления сетью.

Литература

1. Yong Zeng, Rui Zhang, Teng Joon Lim. Wireless communications with unmanned aerial vehicles: opportunities and challenges // IEEE Communications Magazine, Volume: 54, Issue 5, May 2016.
2. Cheng Zhan, Yong Zeng, Rui Zhang. Energy-Efficient Data Collection in UAV Enabled Wireless Sensor Network // IEEE Wireless Communications Letters, Volume: PP, Issue: 99, November 2017.

УДК 621.396.99

ВИКОРИСТАННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ ДЛЯ КОНТРОЛЮ ПЕРЕСУВАННЯ ОБ'ЄКТІВ НА КОНТРОЛЬОВАНИХ ТЕРИТОРІЯХ

Турейчук А.М., Лисенко О.І.
Національний університет оборони України
імені Івана Черняховського, Україна
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: a_tureychuk@ukr.net

Using wireless sensor networks to control the motion of objects in a controlled territory

Wireless sensor networks are widely used in applied use.Using sensors with various sensing methods allows you to track air and ground objects.The ability of sensors to track their location and form communication paths makes it easy to create networks in hard-to-reach places.The ability of sensors to operate under any external conditions and to provide objective information through the collection of information by various methods makes it possible to use sensor networks in critical sites that pose a potential threat to human life and cause significant damage to the environment.

Поява безпровідних сенсорних мереж (БСМ) стала причиною створення великої кількості нових прикладних сервісів. Деякі з них виглядають футуристичними, тоді як більшість з них є практично корисними. Наприклад, моніторинг пересуванняоб'єктів на контрольованих територіях.

Існують території, що потребують контролювання доступу до них. Деякі з зазначених територій мають великі площі, наприклад, військові сховищабоєприпасів та озброєння, небезпека яких за останні роки наочно підтверджена рядом катастроф. Необхідно враховувати, що контролюванню підлягають не лише площі самого сховища, а і території навколо. Враховуючи, що дальність пострілу з легкого мінометa складає близько 4 км, а дальність управління літальним апаратом, який можна придбати у вільному продажу, складає близько 7 км, контрольовані території сягають значних значень. Крім того, необхідно розуміти, що контроль повинен здійснюватися цілодобово у будь-яких погодних умовах.

За таких умов доцільно використовувати технічні засоби контролю.

Можливості сенсорних вузлів у БСМ можуть змінюватися в широких діапазонах, тобто, прості вузли датчиків можуть контролювати один фізичний параметр, тоді як в складніших пристроях можуть бути об'єднані різні методи зондування(наприклад, акустичні, оптичні, магнітні). Вони також можуть відрізнятися за можливостями передачі даних, наприклад, за допомогою ультразвуку, інфрачервоних або радіочастотних технологій з

різною швидкістю передачі даних і затримками. Прості датчики можуть тільки збирати і передавати інформацію щодо спостережуваного довкілля, тоді як потужніші пристрої(тобто пристрої з більшими обчислювальними, енергетичними ресурсами) можуть також проводити обробку і агрегацію даних. Такі пристрої часто дозволяють реалізувати додаткові функції у БСМ, наприклад, вони можуть утворювати першочергові шляхи зв'язку, які можуть бути використані іншими сенсорними вузлами з обмеженими ресурсами для з'єднання з базовою станцією. Нарешті, деякі пристрої можуть мати доступ до додаткових допоміжних технологій, наприклад, глобальних систем позиціонування(GPS) для визначення координат вузлів. Проте, додаткові функції часто призводять до надмірних витрат енергії джерел живлення для дешевих і малопотужних сенсорних вузлів[1].

Жоден сенсор не може забезпечити повне покриття всіх цілей на всіх дистанціях. Замість цього необхідно прийняти багаторівневий підхід, тобто одночасне розгортання кількох різних типів повністю взаємопов'язаних сенсорів з метою отримання якомога більшого обсягу інформації.

Поєднання кількох сенсорів в одномувузлу(акустичні, оптико-електронні, інфрачервоні, сейсмічні, магнітні детектори тощо) дозволяє виявляти повітряні і наземні загрози.Систему, що може відстежувати людей і машини через акустичні та сейсмічні сенсори, можна поєднати з оптико-електронною системою, яка буде направлятися на об’єкт, виявлений радаром. У свою чергу, радар можна приєднувати до супутникових засобами зв'язку дальньої дії для передачі даних іншим користувачам.

На рис.1 приведено ілюстрацію фрагменту БСМ,де дві групи сенсорів контролюють різні ділянки території. До вузла входять акустичний, оптико-електронний, сейсмічний та магнітний сенсори.

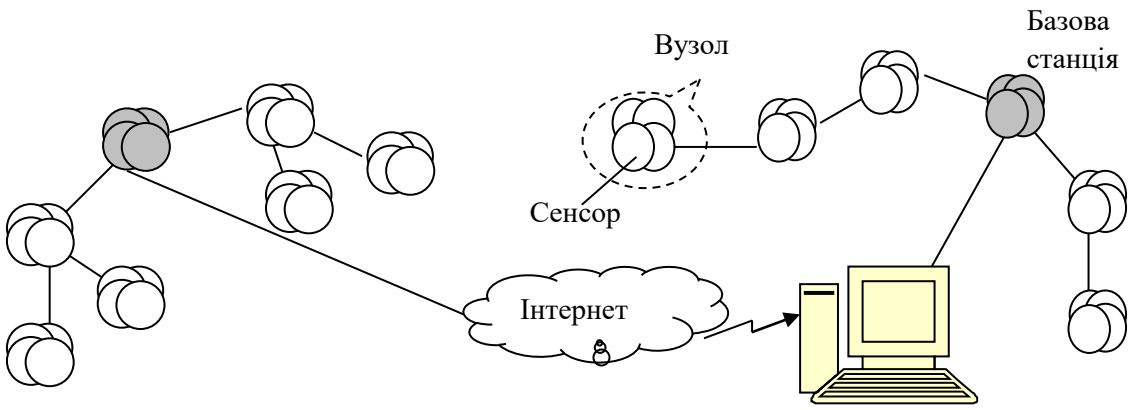


Рис. 1. Фрагмент безпровідної сенсорної мережі. До вузла входять декілька сенсорів із різними методами збору інформації

Для запобігання передчасного виявлення системи контролю та економії енергії живлення можна використовувати пасивні сенсори, які неможливо виявити радіоелектронними засобами. У такому випадку можна розробити алгоритм, коли всі активні сенсори та більшість інших перебувають у вимкнутому стані і вмикаються за сигналом сенсора з низьким споживанням енергії, який постійно перебуває у стані чергування. Після спрацювання зазначеного сенсора відбувається активація всієї мережі з одночасним надсиланням сигналу тривоги на центральний пульт управління.

Наявність GPSпередатчиків та можливість утворювати шляхи зв'язку, які можуть бути використані іншими сенсорними вузлами з обмеженими ресурсами для з'єднання з базовою станцією, дає можливість розгортати БСМ у важкодоступних місцях шляхом встановлення сенсорів з повітря – з вертольоту або з квадрокоптеру. При використанні БСМ для виконання бойових та розвідувальних завдань, наприклад, для контролю пересування противника на імовірних напрямках нападу, сенсори можна оснащати вибуховими елементами, що не дозволять знешкодити сам сенсор, самоліквідують його або вразять противника.

Таким чином, використання БСМ для контролю пересування об'єктів на контрольованих територіях дозволяє забезпечити своєчасне виявлення як повітряних так і наземних об’єктів, при відсутності витрат на створення локальних мереж зв’язку, з забезпеченням скритності самої системи контролю, та можливістю використання сенсорів з різним принципом дії, що підвищує об’єктивність даних та зменшує залежність від зовнішніх умов.

Література

1. Waltenegus Dargie, Christian Poellabauer. Wireless sensorn etworks. Theory andpractice / Wiley Serieson Wireless Communications and Mobile Computing, 2010.
2. Mao G. Wireless sensor network localization techniques / G. Mao, B. Fidan, B. Anderson // Computer Networks, 51(10), pp. 2529 – 2553, 2007.

УДК 621.396

ШИФРУВАННЯ ДАНИХ В СЕНСОРНІЙ МЕРЕЖІ, НА ПРИКЛАДІ ZIGBEE

Зубик С.О., Лисенко О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail zubyk.sergey@gmail.com

Data encryption in the sensor ZigBee-network

The use of wireless data networks in applications such as data collection from energy meters, safety and industrial telemetry require the protection of transmitted information and prevent unauthorized connection of undesirable devices. The article deals with practical issues of data encryption in ZigBee-networks using the example of popular XBee radio modules.

У мережах ZigBee передбачено кілька механізмів криптографічного захисту даних (Security), всі або деякі з яких можуть бути задіяні розробником:

- шифрування AES 128-біт;
- 2 типу ключів шифрування;
- підтримка центру довіри (Trust Center);
- механізми перевірки цілісності повідомлення (Integrity) і перевірки його справжності (Authentication).

Специфікація ZigBee включає три режими безпеки (Security modes) - локальний (residential), стандартний і підвищений. Локальна безпека була вперше введена в стандарті ZigBee 2006. Вона вимагає, щоб ключ шифрування був встановлений на всіх пристроях, що підключаються до мережі. Стандартний режим безпеки додає деякі опціональні можливості, а також вводить шифрування на рівні додатку (APS layer link key). Підвищена безпека передбачає перевірку справжності і деякі інші удосконалення, які в даний час не підтримуються виробниками ZigBee-стеків в достатній мірі.

Модулі XBee ZB, в основному, підтримують стандартний режим безпеки. У той же час, кінцеві пристрої, що підтримують локальний режим безпеки, можуть підключатися і взаємодіяти з вузлами мережі, що працюють зі стандартним режимом безпеки. Далі розглядаються різні аспекти шифрування даних саме для режиму стандартної безпеки.

Безпека в ZigBee використовується як на мережевому рівні, так і на рівні додатку. Передана по ефіру інформація шифрується за допомогою алгоритму AES з довжиною ключа 128 біт. Як ключів шифрування застосовується мережевий ключ (Network Key) і опціональний зв'язковий ключ (Link Key). Ключі шифрування є деякою 128-бітною послідовністю (16 байт), яка вручну завантажується в модуль або формується самостійно. Витягти ключ з модуля неможливо. Тільки ті два ZigBee-вузла, які містять однакові ключі шифрування, можуть взаємодіяти між собою. Роутери та кінцеві пристрої, які працюють в мережі з включеною безпекою, повинні отримати правильні ключі шифрування.

Центр довіри в мережі ZigBee з безпекою авторизує підключаються до

мережі вузли і виконує розсилку ключів шифрування. Зазвичай в якості центру довіри виступає координатор.

Ключ мережі застосовується для шифрування даних користувача (Application Data) і додаткової інформації верхнього рівня (APS Layer). APS Layer - це надбудова над корисними даними, пов'язана з поняттям «профілів» в ZigBee (включає інформацію про профілі, кластери і кінцеві точки). Крім захисту власне корисного навантаження (Payload), безпеку на мережевому рівні забезпечується шифруванням даних, пов'язаних зі службовими мережевим операціями, такими як прокладка маршрутів і команди рівнів APS і ZDO. Мережева безпека не поширюється на MAC-рівень. Якщо в ZigBee-мережі включений режим безпеки, то всі пакети з даними передаються тільки в зашифрованому вигляді за допомогою 128-біт алгоритму AES (див. Рис. 1).

Рис. 1. Шифрування на мережевому рівні

Мережевий заголовок зашифрованого пакета включає 32-біт лічильник фреймів. Кожен вузол в мережі підтримує власний 32-біт лічильник фреймів, який збільшується на 1 при відправці будь-якого пакета. Додатково, кожен вузол відстежує лічильники фреймів всіх сусідніх вузлів. Якщо отримується пакет від сусіднього вузла має номер фрейма менший, ніж був до цього, такий пакет відкидається. Лічильники фреймів використовуються для протистояння та злому захисту шляхом заміщення оригіналу (Replay attacks).

В безпечної ZigBee-мережі пакет дешифрується і шифрується за будь-якої ретрансляції на всьому маршруті проходження. Проміжний вузол дешифрує пакет і перевіряє його цілісність. Якщо пакет призначений не цьому вузлу, то дані знову зашифровуються і аутентифіковані на основі лічильника фреймів і мережевої адреси (входять в мережевий заголовок) проміжного вузла. Додаткові операції в мережі з безпекою збільшують затримки при доставці повідомлень. Крім того, максимальний обсяг корисних даних в пакеті зменшується на 18 байт за рахунок додавання лічильника фреймів, адреси джерела, MIC-коду і деяких інших службових байтів.

Безпека на рівні додатку (APS layer security) дозволяє зашифрувати корисні дані за допомогою ключа шифрування, відомому тільки відправнику і одержувачу пакета. У той час як мережеве шифрування на базі мережевого ключа застосовується до всіх повідомлень всередині мережі, шифрування на рівні додатку є необов'язковим і може використовуватися тільки при надсиланні конкретного пакета. Шифрування на рівні програми не може

застосовуватися до широкомовних розсилок. Шифрування корисних даних і формування коду цілісності повідомлення виробляється на основі 128-біт алгоритму AES (див. Рис. 2).

Рис. 2. Шифрування на рівні додатку

Код цілісності повідомлення (APS Message Integrity Code, aMIC-код) в даному випадку відрізняється від nMIC-коду, одержуваного при шифруванні на рівні мережі (Network Message Integrity Code). Одержувач повідомлення не буде використовувати прийнятий пакет, якщо обчислюється їм хеш-функція над корисними даними дасть результат, відмінний від aMIC-коду в самому пакеті. При шифруванні на рівні програми використовуються два типи ключів - зв'язковий ключ для обміну даними з центром довіри і ключ шифрування даних програми. Проміжні вузли мережі не можуть отримати доступ до цих даних, тому що ключ шифрування даних додатка відомий тільки відправнику і одержувачу. Використання безпеки на рівні додатку зменшує максимальну величину корисних даних на 9 байт. На малюнку 3 наведена діаграма пакета для випадку одночасного використання безпеки на рівні мережі і на рівні додатку.

Рис. 3 . Шифрування на рівні мережі та додатку

Література

1. M. Di Francesco, G. Anastasi, M. Conti, S.K. Das, and V. Neri. “Reliability and Energy-Efficiency in IEEE 802.15.4/ZigBee Sensor Networks: An Adaptive and Cross-Layer Approach,” IEEE Journal on Selected Areas in Communications, 29(8), pp. 1508-24, Sept. 2011.
2. Mao G. Wireless sensor network localization techniques / G. Mao, B. Fidan, B. Anderson // Computer Networks, 51(10), pp. 2529 – 2553, 2007.
3. Chaczko Z. Methods of sensors localization in wireless sensor networks / Z. Chaczko, R. Klempous, J. Nikodem, M. Nikodem // In Engineering of Computer-Based Systems, 2007. ECBS’07. 14th Annual IEEE International Conference and Workshops, pp. 145–152. IEEE, 2007.

УДК 621.396.4

АЛГОРИТМ САМОПОЗИЦІЮВАННЯ ВУЗЛА БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Бондарук О.А., Лисенко О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: alex.bondaruk9@gmail.com

Self-Positioning Algorithm for localization in wireless sensor network

The problem of determining the coordinates of the node of the wireless sensor network for increasing their energy efficiency is considered. It is revealed that the main factor influencing increase of probability of infringement of work of sensory network is the limited power resource of a node. There was explained algorithm of self-positioning of the node of the wireless sensor network.

Безпроводові сенсорні мережі (БСМ) стрімко розвиваються протягом останнього десятиліття. Мережі даного типу мають за мету пов’язати реальний світ, що нас оточує, з комп’ютерними мережами в єдину систему. Ідея безпроводових сенсорних є дуже актуальною і досліджується багатьма науковцями і дослідницькими організаціями зі всього світу. Такий ажіотаж до вивчення даних мереж можна пояснити тим, що існує неймовірний перелік можливостей, які надають нам сенсорні мережі. Завдяки спеціальним сенсорам існує можливість передбачати відмову приладів у аерокосмічних системах. Широкого поширення набуває використання безпроводових сенсорних мереж у будівництві для оптимізації і автоматизації різного роду процесів. Завдяки високій автономності і безвідмовності великої популярності набуло використання таких систем у системах безпеки і у військових цілях.

Постановка задачі. Вибір алгоритму локалізації вузла безпроводової сенсорної мережі безпосередньо впливає на енергоспоживання вузла а отже і на автономність мережі в цілому. Саме тому постає питання вибору методики визначення координат при проектуванні мережі, задля забезпечення максимальної автономності мережі шляхом вибору найоптимальнішого алгоритму за існуючих умов. Мною розглядалася мережа для забезпечення охорони приміщень, що значить що значить, що вузли мережі будуть знаходитись всередині будинку і на невеликій відстані один від одного. За даних умов постає два питання:

- які системи та алгоритми існують для надійної локалізації в приміщеннях?
- чи можемо ми розробити прототип шляхом впровадження такого алгоритму або вдосконалення йогона основі оцінки алгоритмів?

Відповівши на ці запитання до розгляду був обраний алгоритм само позиціонування для вузлів безпроводової сенсорної мережі в приміщеннях.

Алгоритм самостійного позиціонування(АСП). АСП визначає і обчислюєвідносні позиції вузлів у мобільній ad-hoc мережі без використання GPS. Це алгоритм, який не використовує вузли з фіксованими або відомими позиціями. Він передбачаєнаявність методу для оцінки відстані між вузлами і будує відносну систему координат.

В якості першого кроку кожен вузол створює локальну систему координат, яка має центральний вузл.

Даний вузлі визначає локальну систему координат, вибравши вузли p та q такими, що відстаньміж p і q (dpq) відома і більша за нуль, і такі, що вузли i, p та q не лежать на тій же лінії. Система визначається як p, що лежить на осі x, а q має а невід'ємну координату (рис. 1). Реальні напрямки p і q не потрібні, тому щопобудовано відносну систему координат; цю систему доведеться обертати, щоб відповідати місцям фізичного вузла.

Утворюється трикутник і вибравши такі p і qщо при заданих відстанях d_{pq}, d_{iq} та d_{ip} максимальна відстань не дорівнює сумі двох інших. Крім того, вибір p і q повинен максимізувати кількість вузлівдля якихможна обчислити місцезнаходження. Геометричні властивості трикутників використовуються для визначенняпозицій інших вузлів.

На другому кроці напрямки локальних систем координат коригуються, щоб отриматитой самий напрямок для всіх вузлів у мережі. Напрямок місцевої координатисистема може бути скоректований відносно іншої системи шляхом обертання і, можливо, віддзеркалювання системи. Обрана система координат мережі служить як відносна для інших систем. Тоді вузли можуть обчислити свої позиції в по відношенню до обраної системи. Вузол *l*, сусід з k і сусід вузла i. Вузолk знає свою позицію в системі координат вузла *i* і знає положення вузла *l* у йоговласній системі координат. Оскільки координатні системи вузлів k та i мають ті ж напрямки, тоположення вузла *l* в системі координат вузла i просто отримано як сума двох векторівЦе проілюстровано на рис 2.

Проблема виникає після переміщення вузла, оскільки це викликає велику невідповідність між реальними і обчисленими позиціями вузлів, що вимагають від усіх вузлів перераховувати свої позиції. Щоб вирішити цю проблему визначається набір вузлів (відносна група вузлів) яка залишається нерухомою і незамінною(рис 3). Група складається з nсусідніх вузлів, що мають найвищу густину в мережі, де n встановлюється користувачем ($n \in \{2, 3\}$ в

Центр групи є середньою позицією вузлів групи і є центром системи координат мережі. Напрямок мережі координат визначається яксереднє значення напрямків локальних систем координат вузлів групи. Середня швидкість центру групи очікується значно меншою, ніж середня швидкість вузлів. Таким чином, невідповідність позиції, введена рухом, може бути зменшена.

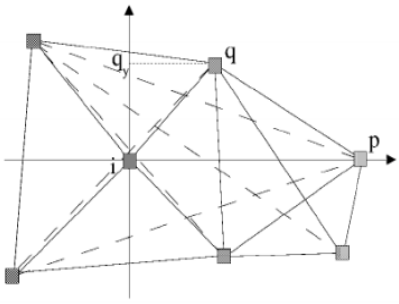


Рис 1.

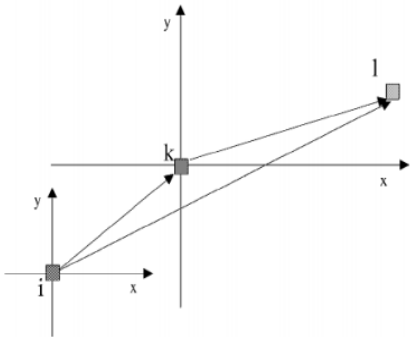


Рис.2.

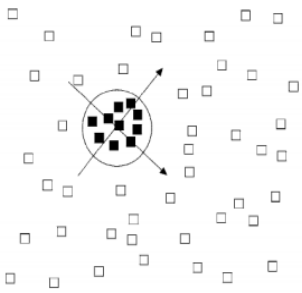


Рис.3.

Було проведено симуляцію з 400 вузлів. Вузли рухались випадковою моделлю руху: вони рухаються за допомогою випадкової швидкості, чекають фіксованого часу, а потім знову рухаються.

Показано, що якщо замість двохопового сусідства використовується більше (трьоххопове) сусідство, то мобільність центру мережі зменшується (тим самим збільшується стабільність). Даний алгоритм спрямований в першу чергу на мережі в яких корисною інформацією являється місцезнаходження вузла.

Висновки. Вибір алгоритму визначення координат вузла в безпроводовій сенсорній мережі є важливим етапом при проектуванні. Саме тому важливо враховувати всі параметри мережі, такі як: корисна інформація, що передається вузлами, місце розгортання мережі, віддаленість вузлів, кількість вузлів і тд. Саме взявши до уваги цю інформацію можливо обрати найоптимальніших алгоритм локалізації для мережі, що проектується.

Література

1. Терентьев, М. Н. Метод функционирования систем мониторинга параметров объектов с изменяемой конфигурацией на базе дискретных беспроводных сенсорных сетей [Текст]: дис. … к. т. н.: 05.13.15 /М. Н. Терентьев. – М., 2010.– 154 с.
2. Иванова, И. А. Определение периметра зоны покрытия беспроводных сенсорных сетей [Текст] /И. А. Иванова // Промышленные АСУ и контроллеры. –2010. – № 10. – С. 25–30.
3. Higuchi, Tatsuro, et al. "Mobile node localization focusing on stop-and-go behavior of indoor pedestrians." MobileComputing, IEEE Transactions on13.7 (2014): 1564-1578.
4. Tomic, Slavisa, et al. "Efficient estimator for distributed RSS-based localization in wireless sensor networks." Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International. IEEE, 2015.
5. Padmapriya, K., and S. Sridhar. "An efficient localization for wireless sensor network using nearest neighbor reference method." Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014.
6. E. Cayirci, H. Tezcan, Y. Dogan, and V. Coskun, “Wireless sensor networks for underwater surveillance systems,” Ad Hoc Netw., vol. 4, no. 4, pp. 431–446, 2006.

УДК 621.396

МАКЕТ СИСТЕМЫ ТРАНСЛЯЦИИ СИГНАЛОВ ЦИФРОВОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ ДЛЯ УЧЕБНОГО ПРОЦЕССА

Авдеенко Г.Л., Трофименко В.В.
Институт телекоммуникационных систем КПИ им. Игоря Сикорского
E-mail: django2006@ukr.net

Digital television system prototype for university education purposes

The design principles of DVB-S and DVB-C digital television radio signals broadcasting system prototype (RP) in 3.6-4.3 GHz band is presented. This prototype is for the purpose of students equation skills improving at such technical areas as microwave antennas and transmission lines, theory of signal generation, amplification, filtering, DVB-C standard, MPEG coding and television transport stream forming. The components of transmitter and receiver structure schemes and basic performance parameters of prototype during laboratory test are shown.

В настоящее время стремительное развитие телекоммуникационной отрасли, и, в частности систем цифрового ТВ (ЦТВ), радиорелейной и спутниковой связи, широкополосного беспроводного радиодоступа, работающих в СВЧ диапазоне, требует повышения уровня теоретической и практической подготовки студентов в ВУЗах. Однако, не смотря на наличие доступной литературы [1-2], посвященной изучению, в первую очередь теоретических аспектов систем ЦТВ, крайне актуальной в настоящее время является задача создания макетов и экспериментальных образцов элементов систем ЦТВ, предназначенных для практических и лабораторных занятий со студентами. Это обусловлено тем, что наличие на телекоммуникационном рынке огромного количества оборудования, предназначенного для практического создания современных систем связи и вещания в первую очередь операторами крупных вещательных сетей, является недоступным для ВУЗов по причине их высокой стоимости. Примером одного из таких макетов для учебного процесса может быть разработка фирмы NXP Semiconductors [3].

В связи с этим, в данном докладе рассматривается один из возможных вариантов построения макета системы трансляции радиосигналов ЦТВ в диапазоне 3,6-4,3 ГГц из относительно недорогих и доступных компонентов. Структурная схема предлагаемого варианта макета системы трансляции радиосигналов ЦТВ стандартов DVB-S и DVB-C по радиолинии СВЧ диапазона показана на рис.1.

Радиосигнал стандарта DVB-S, с несущей частотой 70 МГц, символьной скоростью 27,5 Мсимв/с модуляцией QPSK, скоростью кодирования FEC=3/4 формируется модулятором Radyne Comstream DVB-3030 из многопрограммного транспортного потока, поступающего с выхода профессионального спутникового ресивера IRD-2600. Который в свою очередь настроен на

демодуляцию и декодирование радиосигнала спутникового ТВ стандарта DVB-S с параметрами: частота – 11766 МГц, поляризация излучаемых со спутника радиоволн – горизонтальная, символьная скорость 27,5 Мсимв/с, FEC = 3/4, ширина спектра – 36 МГц, модуляция – QPSK, поступающего с выхода конвертора спутниковой антенны диаметра 0,9м, установленного на крыше учебного корпуса. Далее с помощью преобразователя частоты радиосигнал DVB-S переносится на промежуточную частоту 1475 МГц, а с его выхода он поступает на первый вход широкополосного сумматора мощности.

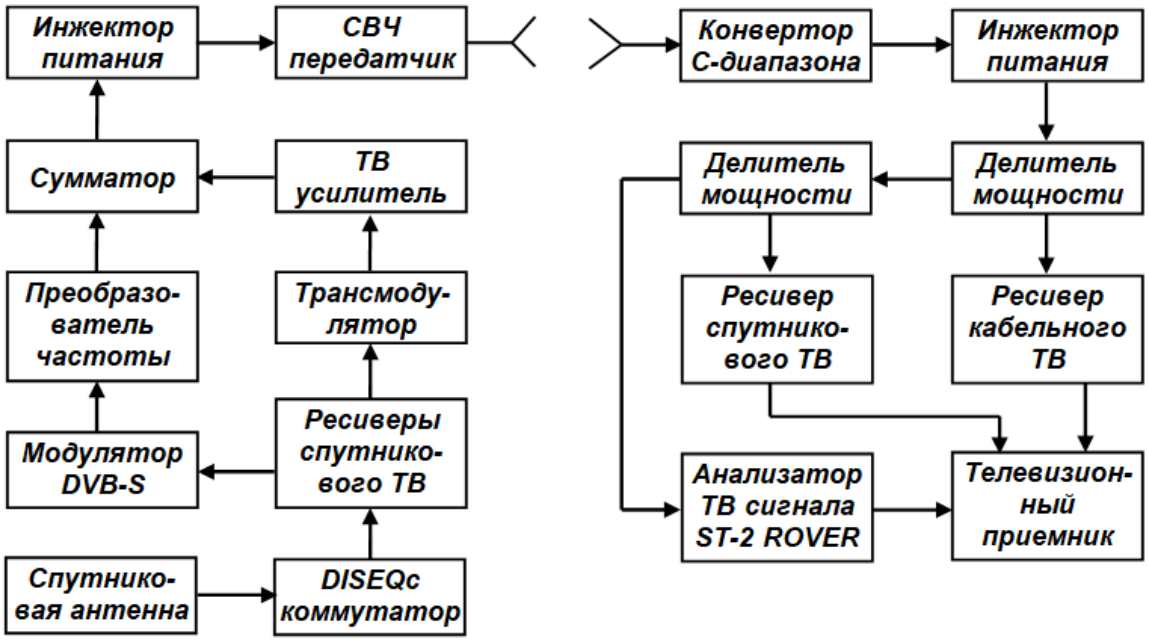


Рис. 1. Структурная схема макета трансляции радиосигналов ЦТВ стандарта DVB-C и DVB-S.

Формирование радиосигнала ЦТВ стандарта DVB-C осуществляется с помощью трансмодулятора WISI OV75 из радиосигнала спутникового ЦТВ стандарта DVB-S с частотой 12073 МГц, горизонтальной поляризацией, символьной скоростью 27,5 Мсимв/с, FEC=3/4. Трансмодулятор программируется как для демодуляции и декодирования радиосигнала ЦТВ стандарта DVB-S до уровня транспортного потока MPEG, так и для модуляции этим потоком несущего колебания из диапазона 47–862 МГц. В результате на выходе трансмодулятора формируется радиосигнал ЦТВ стандарта DVB-C с несущей частотой f_S = 850 МГц, уровнем -30дБм, с модуляцией QAM-64 и шириной спектра до 8 МГц. Далее этот радиосигнал поступает на ТВ усилитель с коэффициентом усиления 20 дБ, а с его выхода – на второй вход широкополосного сумматора. С выхода сумматора сигналы DVB-S и DVB-C поступают в инжектор питания и далее на вход СВЧ передатчика. Передатчик конструктивно выполнен на основе фланцевого конвертора С-диапазона, состыкованного с пирамидальной рупорной антенной размером 26х18 см, имеющей коэффициент усиления около 21 дБ на частоте 4 ГГц. Передатчик состоит из усилителя промежуточной частоты с коэффициентом усиления около

20 дБ, смесителя на полевом транзисторе и транзисторного СВЧ гетеродина на частоту f_{LO} = 5150 МГц, стабилизированного диэлектрическим резонатором.

С выхода смесителя, сигналы DVB-C и DVB-S суммарной $f_{1DVB-C} = f_{LO} + f_S$ = 6000 МГц, $f_{1DVB-S} = f_{LO} + f_S$ = 6625 МГц и разностной составляющих $f_{2DVB-C} = f_{LO} - f_S$ = 4300 МГц, $f_{2DVB-C} = f_{LO} - f_S$ = 3675 МГц и другие продукты преобразования поступают на вход полосового фильтра, на связанных микрополосковых резонаторах с ориентировочной полосой пропускания 3,4 - 4,3 ГГц. Который пропускает на свой выход только радиосигналы с несущими f_{2DVB-C}, f_{2DVB-S} подавляя при этом комбинационные составляющие. С выхода фильтра радиосигнал поступает на трёхкаскадный выходной усилитель мощности на СВЧ полевых транзисторах, собранный по схеме с общим истоком. Выходная мощность передатчика составляет около 1 мВт. Далее, с выхода последнего каскада усилителя радиосигналы DVB-S и DVB-C поступают на вход зонда, связывающего печатную плату передатчика с прямоугольным волноводом, в котором возбуждается электромагнитная волна, излучаемая с помощью рупорной антенны.

В качестве приёмного устройства, расположенного на расстоянии 20 м от передающего, используется обычный конвертор спутникового телевидения С-диапазона, обеспечивающий сквозное усиление около 65 дБ. С выхода конвертора, радиосигналы ЦТВ стандарта DVB-C и DVB-S с уровнем около -10 дБм через инжектор питания конвертора поступают на коаксиальные делители мощности, с одного выхода которого они поступают на вход анализатора сигналов цифрового ТВ ST-2 ROVER а с других – на входы ресиверов цифрового кабельного и спутниковго ТВ, в которых происходит демодуляция и декодирование радиосигналов, в результате чего формируются пакеты ТВ программа, которые и выводятся на телевизионный приёмник через его композитные входы.

Измерения, проводимые с помощью анализатора сигналов ЦТВ ST-2 ROVER и подменю ресивера «Качество» позволяют оценить степень ухудшения основных показателей транслируемых по радиолинии диапазона 3,6 – 4,3 ГГц радиосигналов ЦТВ стандартов DVB-S и DVB-C.

Испытания собранного макета подтвердили возможность трансляции радиосигнала ЦТВ стандарта DVB-C и DVB-S с получением его хороших параметров качества на приёмной стороне (показатель шкалы «Качество» в ресивере составляет 92-100%). Авторы считают, что использование подобных макетов в лабораторном практикуме позволит студентам закрепить теоретические знания по дисциплинам телекоммуникационного профиля.

Литература

1. Смирнов А.В., Пескин А.Е. Цифровое телевидение. От теории к практике. М.: Горячая Линия – Телеком, 2005. 349 с.
2. Карякин В.Л. Цифровое телевидение: учебное пособие для ВУЗов. М.: СОЛОН-пресс, 2013. 418 с.
3. DVB-S Full Line-up: From Satellite LNB through STB to TV Screen (IMS 2013) [Електронний ресурс] – Режим доступу: https://www.youtube.com/watch?v=V7SOH9ahm-0&index=3&list=LLH-NIZKgub8_-ofONEw3rdQ&t=0s – Назва з екрана.

УДК 621.396

ПРИЙМАЧ СИГНАЛІВ СУПУТНИКОВОЇ НАВІГАЦІЇ GPS

Гончаренко О.М., Авдєєнко Г.Л.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: oksanka96goncharenko@ukr.net

GPS satellite navigation signals receivers

The report presents the principles of the construction and operation of global satellite navigation system GPS. For the educational process of ITS the testbed of satellite navigation signals receiver has been constructed and tested with appropriate software. The test results allow getting location information in the form of numerical values, time charts, diagrams.

Приймачі сигналів супутникової навігації застосовуються для визначення місцезнаходження наземних, водних та повітряних об’єктів. Глобальні навігаційні супутникові системи (ГНСС) складаються з космічного сегменту – навігаційних супутників, які розподілені по орбітам рівномірно, щоб у кожний момент часу забезпечувати покриття кожної точки планети, і наземного сегменту (системи управління). У наш час лише дві ГНСС забезпечують повне і безперебійне покриття земної кулі — GPS і GLONASS [1].

Основний принцип використання системи GPS — визначення місцезнаходження об’єкту шляхом вимірювання моментів часу прийому синхронізованого сигналу від навігаційних супутників навігаційною апаратурою споживача (НАС). Для визначення тривимірних координат (довготи, широти та висоти) об’єкта необхідно щоб НАС приймала радіосигнали мінімум 4-х супутників.

Супутниковий сегмент системи GPS включає мінімум 24 штучних супутника Землі (ШСЗ), розміщених рівномірно в шести орбітальних площинах, рознесених по довготі на 60° і нахилених на 55° до екваторіальної площини (рис.1). Кожен супутник рухається по синусоїдальній орбіті і здійснює за добу два оберти навколо Землі. Така конфігурація забезпечує в будь-якій точці земної кулі одночасну видимість від 5 до 11 супутників [2].

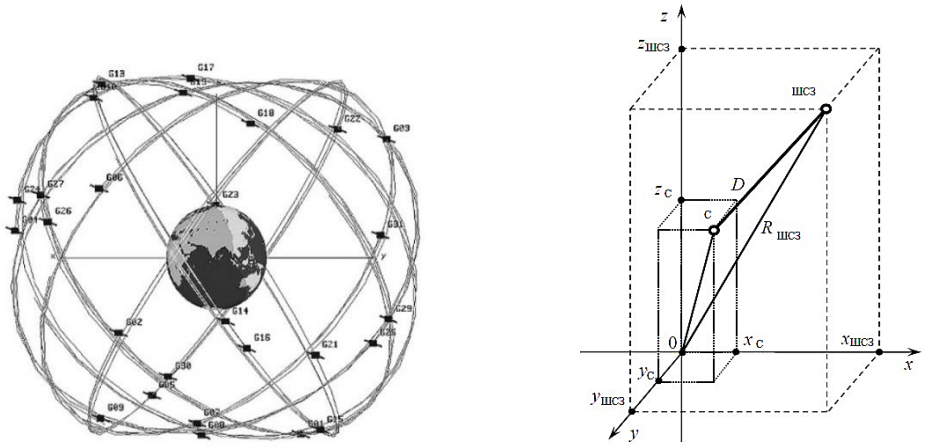


Рис.1 Структура супутникового угрупування GPS

Оскільки для визначення координат об’єкту необхідно мати відомості про місцезнаходження ШСЗ на кожен момент часу, НАС має знати ефемеридну інформацію (сукупність даних навігаційного повідомлення ГНСС). Для знаходження координат споживача (С) у просторі необхідно скласти навігаційні рівняння. Для цього зручно використовувати систему декартових координат (рис.1) з початком в центрі Землі (геоцентричну прямокутну систему координат). Координати навігаційного ШСЗ (НШСЗ) позначимо $x_{ШСЗ}$, $y_{ШСЗ}$, $z_{ШСЗ}$, а координати споживача — x_c, y_c, z_c. Тоді відстань D між ШСЗ і С:

$$D = \sqrt{(x_{ШСЗ} - x_C)^2 + (y_{ШСЗ} - y_C)^2 + (z_{ШСЗ} - z_C)^2} \quad (1)$$

Якщо виконано вимір дальності до трьох супутників D_1, D_2, D_3 і координати всіх трьох НШСЗ відомі, то отримаємо систему з трьох рівнянь виду (1), рішення якої дозволить знайти три невідомі: x_c, y_c, z_c. Однак виміряти справжню дальність між НШСЗ і С можна тільки за умови точного поєднання їх шкал часу, тобто необхідно, щоб супутники випромінювали сигнали синхронно і НАС був точно відомий момент випромінювання сигналів НШСЗ.

Мережа навігаційних супутників координована по руху і випромінюванню сигналів. При наявності розбіжності шкал часу Δt=const з’являється фіксований додаток cΔt в вимірюваних значеннях дальності D і рівняння системи (1) приймає вигляд:

$$D_i + c\Delta t = \sqrt{(x_{ШСЗi} - x_C)^2 + (y_{ШСЗi} - y_C)^2 + (Z_{ШСЗi} - z_C)^2}$$

, (2)

де індекс i — відповідає номеру ШСЗ.

Для розрахунку x_c, y_c, z_c та Δt необхідно провести вимірювання дальності до чотирьох НШСЗ. При цьому отримаємо систему з чотирьох рівнянь виду (2), рішення якої дозволить обчислити координати споживача x_c, y_c, z_c і часову розбіжність шкал Δt.

Вимірювання швидкості руху споживача може здійснюватися, як шляхом обчислення збільшень його координат при послідовних сеансах вимірювання, так і шляхом вимірювання доплерівського зсуву частоти сигналу НШСЗ [3].

Далі розглянемо функціональну схему [4] приймача сигналів ГНСС та створений на його основі прототип НАС для навчального процесу ІТС (рис.2).

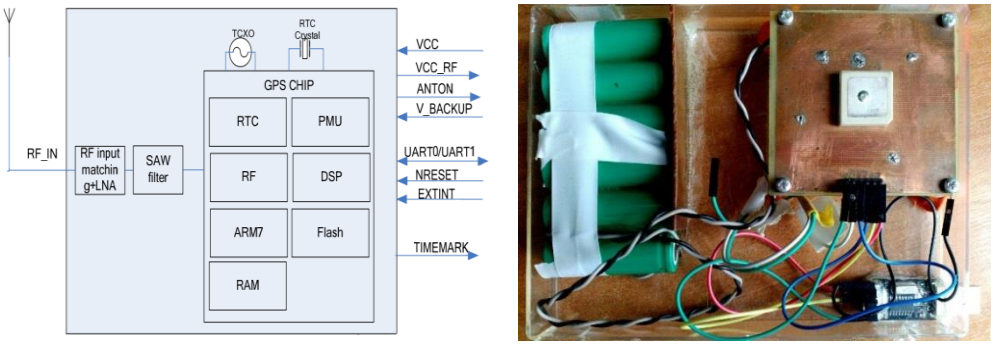


Рис.2 Функціональна схема та прототип GPS-приймача сигналів ГНСС SIM28

На друкованій платі зі склотекстоліту зібрано прототип прийомного пристрою сигналів (НАС) системи супутникової навігації GPS, який складається з пасивної патч-антени 20х20 мм, резервного джерела живлення (акумуляторна батарея 7,2 В, 1500 мА·год), GPS модуля SIMCOM SIM28 на базі чіпсета Mediatek MT3339, стабілізатора напруги 3,3 В. Для його підключення до персонального комп'ютера (ПК) використовується окремий модуль перетворювача інтерфейсів UART-USB.

Параметри приймального пристрою визначаються параметрами модуля приймача супутникової навігації SIM28, а саме: чутливість (у режимі холодного старту) -147 дБм та час визначення місцезнаходження (у режимі холодного старту) 33с. Точність позиціонування визначається функціональними особливостями та характеристиками чіпсета, а також стабільністю джерела напруги.

Готовий прототип може працювати як автономно за допомогою акумуляторів, так і живитись від USB. Для роботи з приймачем використовують спеціальне програмне забезпечення, наприклад Fastrax Workbench 5. Приклад обробки даних у середовищі Fastrax Workbench 5 наведено на рис.3.

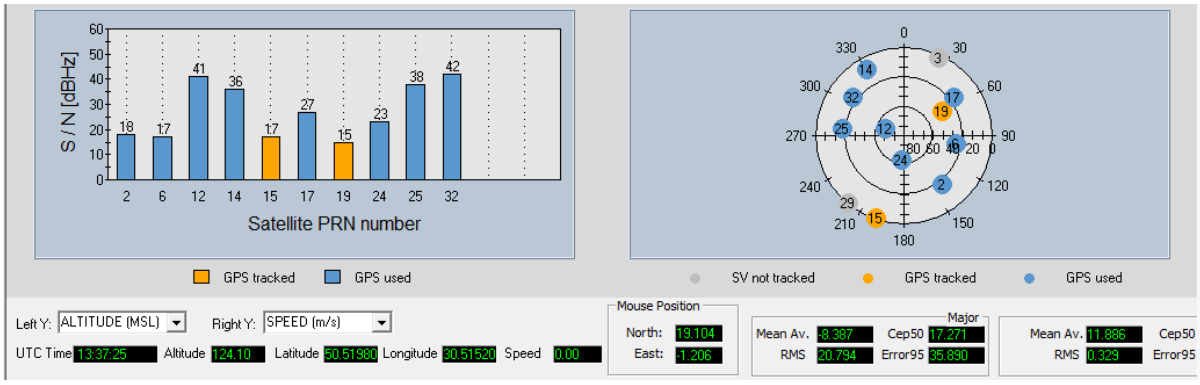


Рис.3. Приклад роботи приймача GPS (дані відображуються в програмі Fastrax Workbench 5)

У тезах доповіді розглянуто принцип побудови та роботи глобальних систем навігації. Створено прототип приймача сигналів ГНСС для учбового процесу ІТС. Його тестування здійснювалось на території кампусу КПІ ім. Ігоря Сікорського. Для цього використовувався ПК, підключений до НАС, зі встановленим на ньому програмним забезпеченням Fastrax. НАС в результаті своєї роботи передає на ПК навігаційні повідомлення в протоколі NMEA, які оброблюються програмою Fastrax, що дозволяє візуально відобразити результати вимірювання місцезнаходження НАС, кількість видимих супутників з їх рівнями сигналів у вигляді числових значень, часових графіків, діаграм.

Література

1. Спутниковая система навигации [Електронний ресурс] − Режим доступу: https://ru.wikipedia.org/wiki/Спутниковая_система_навигации.
2. John G. Grimes GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE PERFORMANCE STANDARD / Washington, DC, 2008, p. 9.
3. Ю.М. Казаринов Радиотехнические системы: Учеб. Для вузов по спец. «Радиотехника» / Ю.П. Гришин, Ю.М. Казаринов. — М.:Высш.шк., 1990.— 496 с.
4. Документація на SIM28 [Електронний ресурс] − Режим доступу: http://www.python-exemplary.com/download/sim28.pdf.

УДК 621.39

НЕОБХІДНІСТЬ ВИКОРИСТАННЯ СТІЛЬНИКОВИХ БАЗОВИХ СТАНЦІЙ НА СОНЯЧНІЙ ЕНЕРГІЇ

Кунєва Н. В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kuneva.nataly@gmail.com

The need to use cellular base stations on solar energy

The theses of the report present the main factors that demonstrate the need to use cellular base stations that operate on renewable energy sources such as solar energy. The advantages and disadvantages of the use of solar power stations are presented

Еволюція мобільних пристроїв, нових додатків і послуг, а також неухильне зростання вимог до пропускної здатності змушують операторів збільшувати продуктивність мереж. Паралельно збільшуються експлуатаційні витрати, потреби в електроживленні і загальну складність мережі. Галузь потребує ефективних концепцій застосування екологічних рішень, і з роками ця потреба стає все більшою.

Маючи більш ніж 6 мільярдів абонентів, індустрія стільникового зв'язку швидко зростає. Щоб підтримати цей ріст в абонентській базі, стільникові оператори розширили своє покриття і пропускну здатність за рахунок розгортання додаткової мережевої інфраструктури. Це, в свою чергу, збільшило споживання енергії стільниковими мережами і їх внесок у викиди парникових газів.

Сьогодні існує понад 3 мільйонів базових станцій у всьому світі. Стільникові мережі в даний час вносять приблизно 3% світового споживання енергії і 2% викидів вуглецю. Крім того, прогнозується, що викиди вуглекислого газу інформаційно-комунікаційних технологій зростуть з 170 метричних тонн в 2014 році до 235 метричних тонн в 2020 році. Базові станції споживають приблизно 60 % загального споживання енергії в стільникових мережах.

Таким чином, одним з найбільш перспективних рішень для зелених стільникових мереж є стільникові базові станції, які працюють на відновлюваних джерелах енергії, таких як сонячна енергія.

Базові станції, які живляться від енергії, зібраної з сонячної радіації, не тільки зменшують вуглецевий слід стільникових мереж, але також можуть

бути реалізовані з більш низькими капітальними витратами в порівнянні з тими, які використовують сітку або звичайні джерела енергії.

Існує другий фактор, що стимулює інтерес до базових станцій з сонячною батареєю. У недавньому минулому основна частина зростання розгортання стільникових базових станцій була в деяких частинах світу, таких як Африка і Азія, де проникнення стільникового зв'язку як і раніше залишається низьким. На жаль, у багатьох з цих регіонів відсутній надійний мережевий зв'язок, тому телекомунікаційні оператори змушені використовувати звичайні джерела, такі як дизель, для живлення базових станцій, що призводить до більш високих експлуатаційних витрат і викидів.

Наприклад, дослідження показують, що з 4 000 000 базових станцій в Індії понад 70% стикаються з відключенням електроенергії понад 8 годин на день. В результаті телекомунікаційна промисловість Індії споживає понад 2 мільярди літрів дизельного палива на рік, витрачаючи близько 1,4 мільярда доларів США і виробляючи більше 5 метричних тонн вуглекислого газу.

Залежно від наявності джерел живлення, базова станція може живитися виключно або частково сонячною енергією. Для сонячних батарей базових станцій використовуються наступні конфігурації:

- Сонячна автономна система: базова станція живиться виключно від сонячної енергії і від батарей.

- Сонячна енергія та дизельне паливо: базова станція живиться від сонячної енергії, але у випадках тривалих поганих погодних періодів дизель-генератори використовуються для задоволення енергетичних потреб базової станції.

- Гібрид: така конфігурація може включати комбінацію панелей, електромережі, дизельних генераторів та інших поновлюваних джерел, такі як енергія вітру для живлення базової станції.

Переваги використання базових станцій на сонячній енергії:

- Сонячна енергія - це відновлювальна енергія, яка є невичерпною.

- Екологічність. Використання джерел відновлюваної енергії передбачає відсутність шкідливих викидів на етапі експлуатації.

- Висока технологічність процесу. У технології отримання сонячної енергії роль людини зведена до мінімуму, та й процес виробництва не можна назвати ризикованим.

- Доступ до сонячної енергії можна отримати в будь-якій точці світу за рідкісним винятком.

- Простота експлуатації. Сонячні станції практично не вимагають технічного обслуговування. Модулі потребують очищення лише декілька разів на рік.

- Економія. Хоча сонячні батареї базових станцій мають високі капіталовкладення, операційні витрати набагато менші, що призводить до економії витрат в довгостроковій перспективі.

Недоліки використання базових станцій на сонячній енергії:

- Висока вартість. Сонячна електростанція - задоволення не з бюджетних, якщо говорити про разове вкладення коштів. Вигоди, безумовно, від такої станції буде куди більше, але, знову ж таки, в довгостроковій перспективі.

- Мінливість. Кількість отриманої енергії безпосередньо залежить від інтенсивності сонячного випромінювання. Саме через це системи без акумуляторів на даний момент не можуть використовуватися в якості основних джерел енергії.

- Дорогі системи зберігання енергії. Для того, щоб використання електроенергії було максимально ефективним, використовуються акумулятори, які зберігають її запаси і завдяки їм система працює більш стабільно.

Зі зростаючим усвідомленням екологічних проблем і прагненням до вирішення зелених інженерних рішень очікується, що сонячні батареї базових станцій будуть відігравати велику роль в майбутньому. Адже сьогодні турбота про екологію телекомунікаційних рішень не модний тренд, а вимога часу.

В роботі було представлено основні фактори, які мотивували їхню зростаючу популярність на ринку разом з поточними можливими рішеннями. У більшості випадків для визначення умов експлуатації мережі може знадобитися дані про прогноз погоди та історичні моделі трафіку. Найбільш широко вивчені проблеми в цьому контексті спрямовані на мінімізацію загального енергоспоживання мережі через різні механізми.

Література

1. H. Bogucka and O. Holland (2013). “Multi-Layer Approach to Future Green Mobile Communications,” IEEE Intelligent Transportation Systems Mag., vol. 5, no. 4, pp. 28–37.
2. M. Marsan (June 2013), “Towards Zero Grid Electricity Networking: Powering BSs with Renewable Energy Sources,” Proc. IEEE Commun. Wksps. (ICC), Budapest, Hungary, pp. 596–601.
3. A. Jhunjhunwala (2012). Powering Cellular Base Stations: A Quantitative Analysis of Energy Options. technical report, Indian Institute of Technology, Madras.

УДК 621.375

ВХОДНОЕ СОПРОТИВЛЕНИЕ ЭЛЕМЕНТАРНОГО ПЬЕЗОЭЛЕКТРИЧЕСКОГО ИЗЛУЧАТЕЛЯ

Карнаух В.Я., Мартынюк Я.В.
Институт телекоммуникационных систем КПИ им. Игоря Сикорского
E-mail: karnauhvy@gmail.com

Input resistance of an elementary piezoelectric radiator

The article “Input resistance of an elementary piezoelectric radiator” presents the research of the input resistance due to the electrodynamic properties of the sample at high frequencies. The corresponding elements of equivalent pattern of the sample substitution are defined on the basis of the research data.

В работе «Входное сопротивление элементарного пьезоэлектрического излучателя» представлено исследование входного сопротивления, обусловленного электродинамическими свойствами образца на высоких частотах. По данным исследований определены соответствующие элементы эквивалентной схемы замещения образца.

Для эффективной работы элементарного пьезоэлектрического излучателя, изображенного на рис.1 в различных электронных устройствах необходимо его согласование режима работы с возбуждающей генераторной или приемной цепью устройства.

Поэтому, в первую очередь для решения поставленной задачи важно знать особенности комплексного входного/выходного сопротивления данного элемента и его поведение в широком частотном диапазоне входных/выходных сигналов.

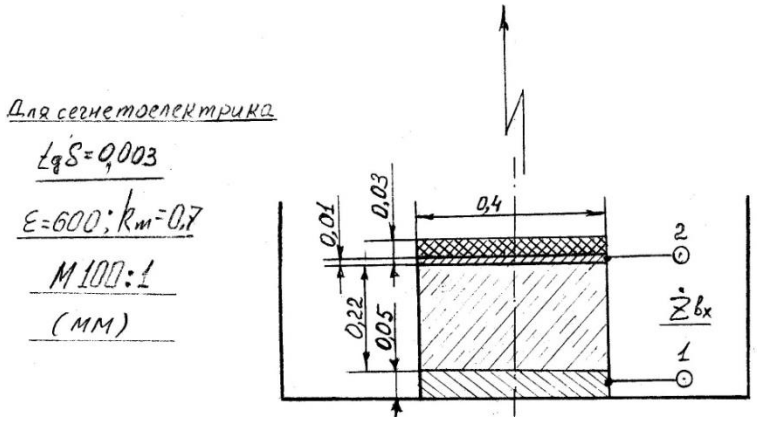


Рис. 1. Конструкция пьезоэлектрического излучателя

При исследовании комплексного входного/выходного сопротивления пьезоэлектрического излучателя будем опираться на работы [1, 2], в которых приведены основные теоретические положения для решения данного класса задач. В работе [1] было представлено упрощенную эквивалентную схему такого элемента (см. рис 2). Представленная схема дает достаточно хорошее,

для практических применений, приближение описания комплексного входного сопротивления.

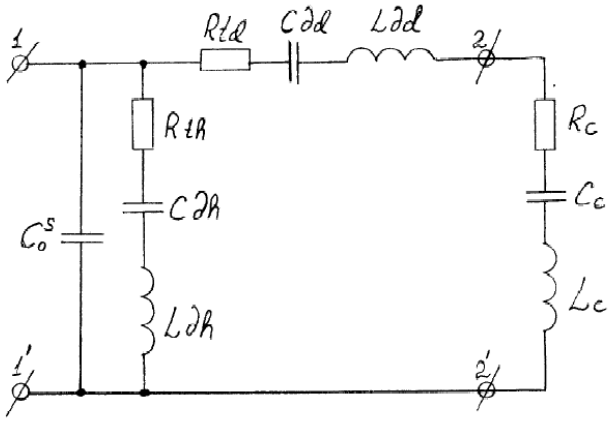


Рис. 2. Эквивалентная схема для входного сопротивления элемента

На представленной (рис. 2) схеме R_{th} , $C_{\partial h}$, $L_{\partial h}$ определяются особенностями колебаний вдоль толщины пьезоэлектрического элемента, а R_{td} , $C_{\partial d}$, $L_{\partial d}$ – определяются особенностями радиальных колебаний в пьезоэлектрическом элементе. В работе [1] – представлены теоретические соотношения для вычисления этих элементов схемы, которые в первую очередь определяют согласование элемента по входу приемного устройства (выводы 1- 1' на рис.2). Данное согласование практически осуществляется на частотах примерно соответствующих механическим резонансам в элементе (единицы мегагерц).

Подача сигналов возбуждения от генератора на образец (выводы 2- 2' на рис.2) может быть выполнена на достаточно высоких частотах (десятки гигагерц).

Данный подход к режимам работы элемента позволяет эффективно развязать его приемные и возбуждающие цепи и не использовать коммутаторы для этих целей, которые вносят дополнительные погрешности в работу устройств.

Поэтому авторами была поставлена задача исследования входного сопротивления представленного пьезоэлектрического излучателя по входу 2-2' на рис.2 с целью последующего его согласования с устройством возбуждения.

Определение выше отмеченного входного сопротивления и связанного с ним расчета значений R_c, C_c, L_c в соответствии с эквивалентной схемой – рис.2 связано с исследованием резонансных электромагнитных явлений в элементе, как электродинамической структуры. Для этого использовано моделирование структуры в соответствии Рис.1 с помощью программы Microwawe Offic (MWO). Результаты моделирования с определением коэффициента отражения электромагнитных волн s_{11} от предложенной структуры представлено на рис 3.

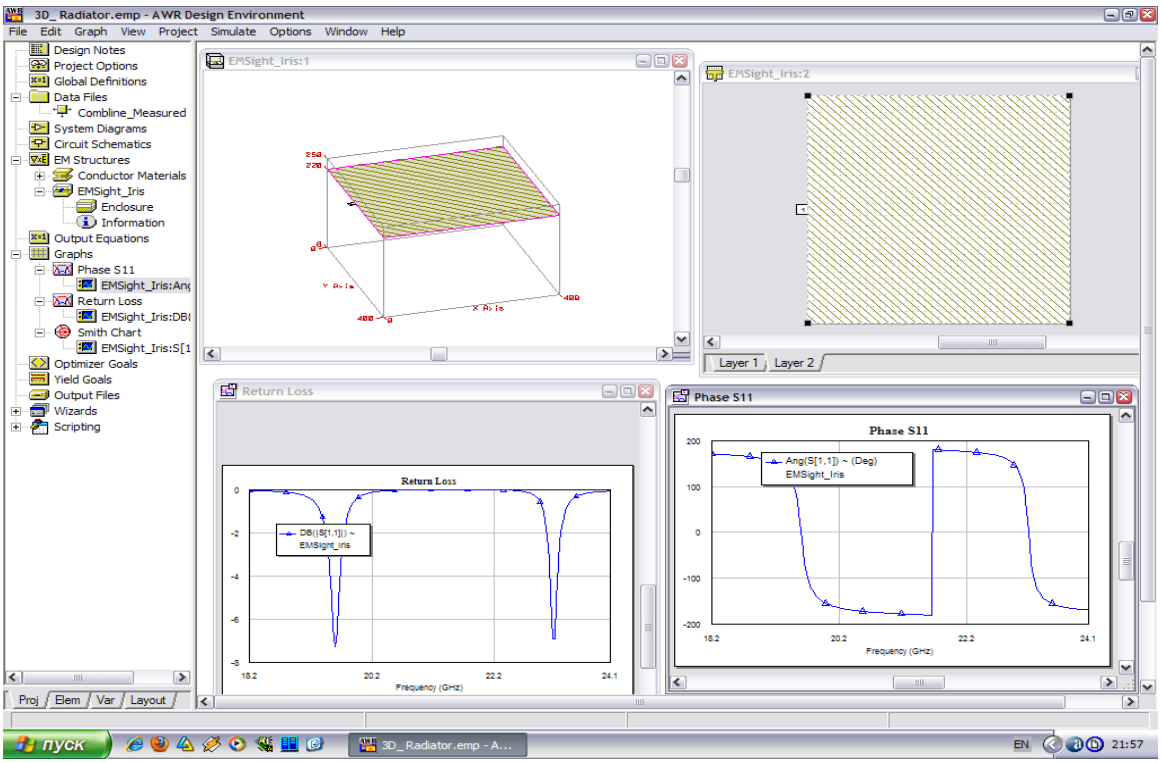


Рис. 3. Результаты моделирования структуры с использованием программы MWO

Из представленных результатов видно, что электродинамическая структура имеет два электромагнитных резонанса:

- радиальный резонанс f_1=19.59 ГГц, $S^{(1)}_{11}$= - 7.23 дБ, Q_1= 392;
- резонанс колебаний вдоль толщины f_2=23.18 ГГц, $S^{(2)}_{11}$= - 6.91 дБ, Q_2= 186;

Из полученных результатов моделирования - используем резонанс колебаний вдоль толщины образца, которые являются основой направленного излучения на рис.1 и определим элементы R_c, C_c, L_c в соответствии с эквивалентной схемой – рис.2:

$$R_c=Z_0(1+ S^{(2)}_{11})/(1- S^{(2)}_{11}) . \qquad (1)$$

В соответствии с (1) - R_c=158.1 Ом, при Z_0=50 Ом (волновое сопротивление порта 1 при моделировании).

Элементы C_c, L_c определяются по полученным из моделирования образца результатам в интерпретации их как для последовательного колебательного контура, который на эквивалентной схеме – рис.2 отражает наличие резонанса вдоль толщины образца:

$$C_c=1/2\pi f_2\rho , \qquad L_c= \rho^2 C_c , \qquad (2)$$

где: $\rho=Q_2 R_c$ – характеристическое сопротивление колебательного контура.

С использованием (2), при подстановке данных моделирования получаем: C_c=0.00023 пФ, L_c=0.199 мкГн.

Литература

1. Я.В. Мартынюк, А.Д. Харламов, Е.И. Кудренко, А.А. Божко, А.А. Верба «О считывании информации в сегнетоэлектрических запоминающих устройствах» - Киев: Техника, 1984, с. 116-128.
2. Т.Д. Шермергор, Н.Н Стрельцова «Пленочные пьезоэлектрики» - М. Радио и связь.

UDC 621.396.946

COUPLING COEFFICIENTS OF DIFFERENT SPHERICAL DIELECTRIC MICRORESONATORS

Trubin A. A.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
E-mail: atrubin@ukrpost.net

КОЕФІЦІЄНТИ ЗВ'ЯЗКУ РІЗНИХ ДІЕЛЕКТРИЧНИХ МІКРОРЕЗОНАТОРІВ СФЕРИЧНОЇ ФОРМИ

Розраховано узагальнені коефіцієнти зв'язку між відмінними за розмірами та діелектричної проникністю діелектричними мікрорезонаторами сферичної форми. Досліджені залежності зв'язку від параметрів резонаторів.

The construction of filters based on the use of different types of microresonators in some cases significantly improves their scattering characteristics. To design such filters it's necessary to be able to calculate the coupling coefficients of different microresonators [1]. The present study examines the mutual coupling coefficients of different Spherical microresonators in the Open space (fig. 1). We obtained general analytical expressions for the coupling coefficients for the excitation of no degenerate oscillations of a magnetic or electric type in resonators, characterized by a given symmetry with respect to the plane AA' (fig. 1, b).

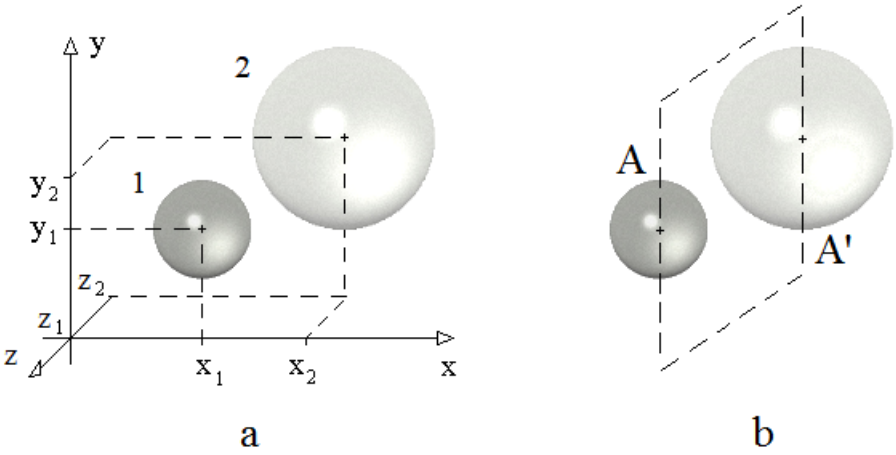


Fig. 1. Different Spherical microresonators in the Open Space (a).
Plane of symmetry AA' for two different microresonators (b)

Using the expressions found, we investigated the dependence of the coupling coefficients of various spherical microresonators on the structure parameters. The obtained analytic expressions of the coupling coefficients become known in the case of identical microresonators [2].

In Fig. 2 shows the dependence of the module of the coupling coefficient multipliers on the dielectric constant of the second microresonator in the case of

two magnetic type oscillations (a); in the case of two oscillations of the electric type (b) and for oscillations of magnetic type in the first microresonator and electric type of oscillations in the second (c). The calculations carried out show different values of the coupling coefficients for microresonators of different sizes.

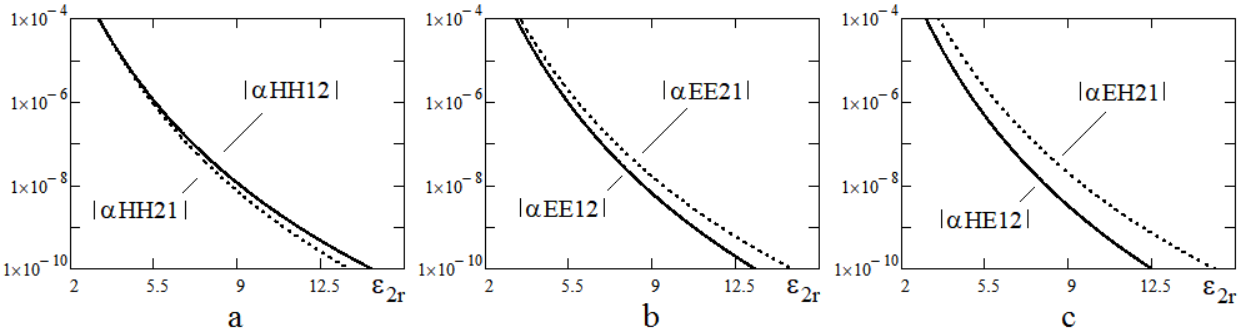


Fig. 2. Dependence of modulus of the Spherical microresonator coupling coefficient multipliers on the relative dielectric permittivity ε_{2r} ($\varepsilon_{1r} = 2,2$; $n_1 = 16$; $n_2 = 21$) for the H_{n_1ml}, H_{n_2ml} (a); E_{n_1ml}, E_{n_2ml} (b); H_{n_1ml}, E_{n_2ml} (c) oscillations

In Fig. 3, 4 show the dependence of the coupling coefficients on the coordinates of the centers of microresonators for oscillations of magnetic types (Fig. 3) and for oscillations of magnetic and electric types (Fig. 4). The real part of the coupling coefficients is represented by solid curves (left axis of ordinates), and imaginary dashed curves (right axis of ordinates). The dependence of κ_{12} is shown in Fig. 3-4, a, b, and the dependence of κ_{21} is shown in Fig. 3-4, c, d.

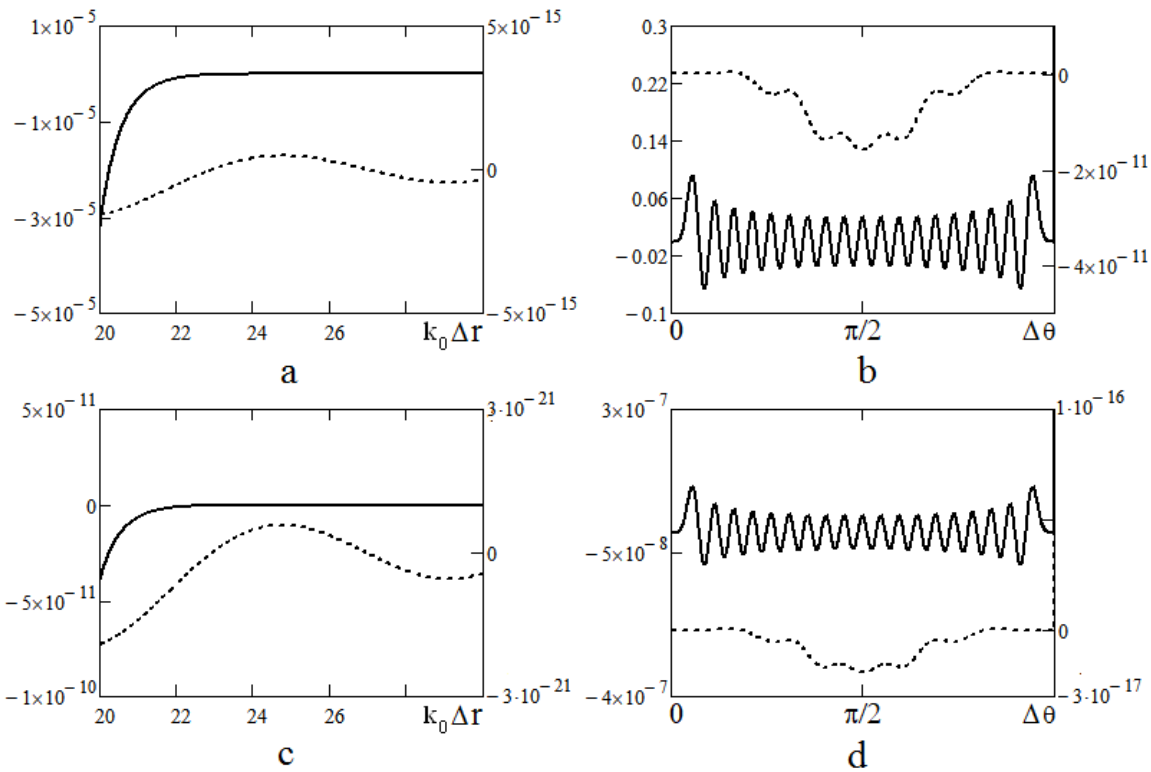


Fig. 3. Coupling coefficients as functions of the microresonator relative coordinates for the $H_{n_1m_1l}$, $H_{n_2m_2l}$ oscillations ($\varepsilon_{1r} = 4$; $\varepsilon_{2r} = 16$; $n_1 = 22$; $n_2 = 20$; $m_1 = 4$; $m_2 = 2$)

Here the $\Delta r = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$ is the relative distance between the centers of the microresonators (Fig. 1, a); k_0 - is the wave number; $\cos\Delta\theta = (z_1 - z_2)/\Delta r$.

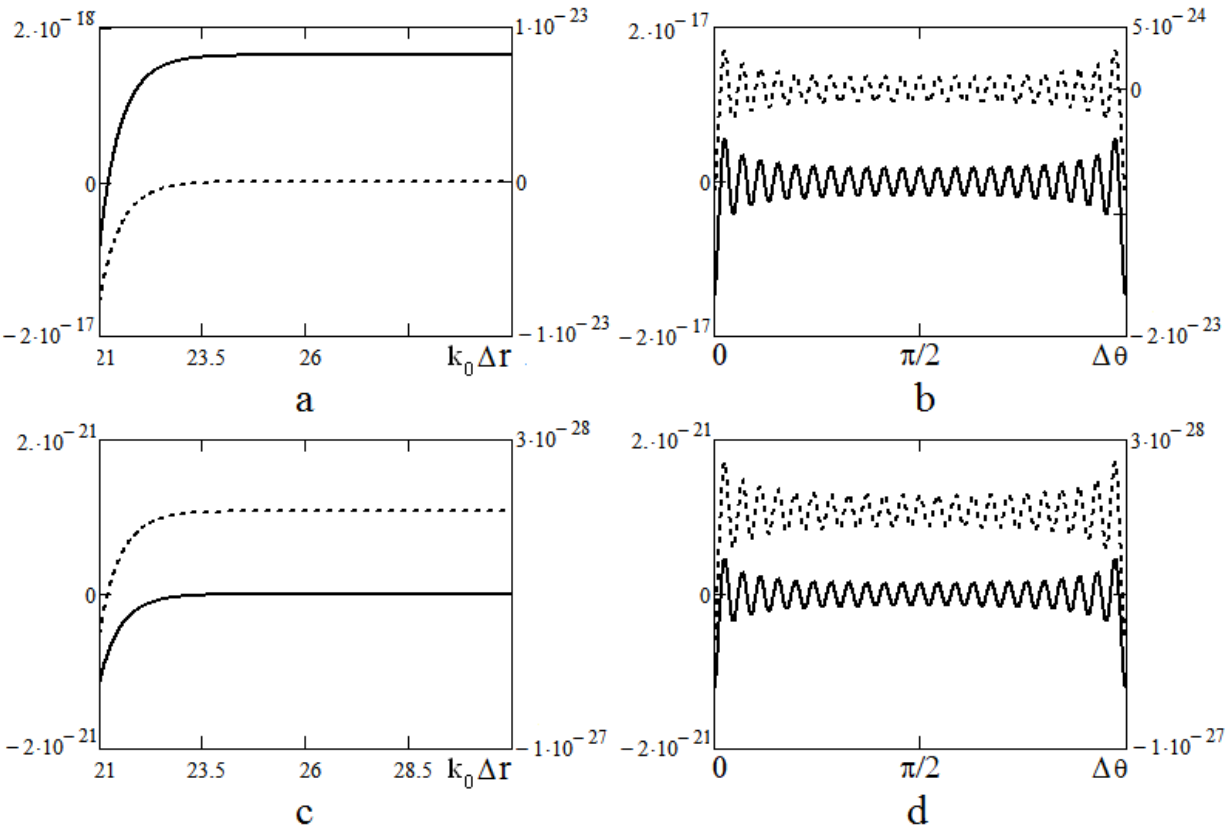


Fig. 4. Coupling coefficients as functions of the microresonator relative coordinates for the $H_{n_1 m_1 l}$, $E_{n_2 m_2 l}$ oscillations ($\varepsilon_{1r} = 4$; $\varepsilon_{2r} = 16$; $n_1 = 22$; $n_2 = 24$; $m_1 = 1$; $m_2 = 1$)

The obtained analytical expressions allow us to calculate the coefficients of mutual coupling of different spherical microresonators for any no degenerate modes.

As can be seen, the coupling coefficients for oscillations of higher types are characterized by a complex dependence on the coordinates of the microresonators and poorly predicted at the level of oscillation modes of resonators.

The use of various microcavities greatly extends the design possibilities of optical filters.

References

1. A.A. Trubin, Modeling of the Optical Filters on Different WGM Disk Microresonators, Information and Telecommunication Sciences, V.8, N1, 2017, pp. 26 - 30.
2. A.A. Trubin, Coupling coefficients of the Spherical Dielectric Microresonators with Whispering gallery modes, Bulletin of NTUU "KPI" ser. Radiotechnique, Radioaparatus Building., 2015. N.62, pp. 49-61.

UDC 621.396.946

BANDPASS FILTERS ON DIFFERENT SPHERICAL DIELECTRIC MICRORESONATORS

Trubin A. A.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
E-mail: atrubin@ukrpost.net

СМУГОВІ ФІЛЬТРИ НА РІЗНИХ ДІЕЛЕКТРИЧНИХ МІКРОРЕЗОНАТОРАХ СФЕРИЧНОЇ ФОРМИ

Досліджуються характеристики розсіювання смугових фільтрів, побудованих на відмінних за розмірами та діелектричної проникністю діелектричних мікрорезонаторів сферичної форми. Знайдені структури мікрорезонаторів та типи коливань, які добре реалізують різні смуги пропускання.

Today, microresonators with whispering gallery oscillations are unique elements of a number of devices in the optical wavelength range [1, 2]. Using of different microresonators in some cases significantly improves filter scattering parameters. In this report, we investigate the scattering characteristics of bandpass filters constructed on the basis of different spherical microresonators with whispering gallery oscillations.

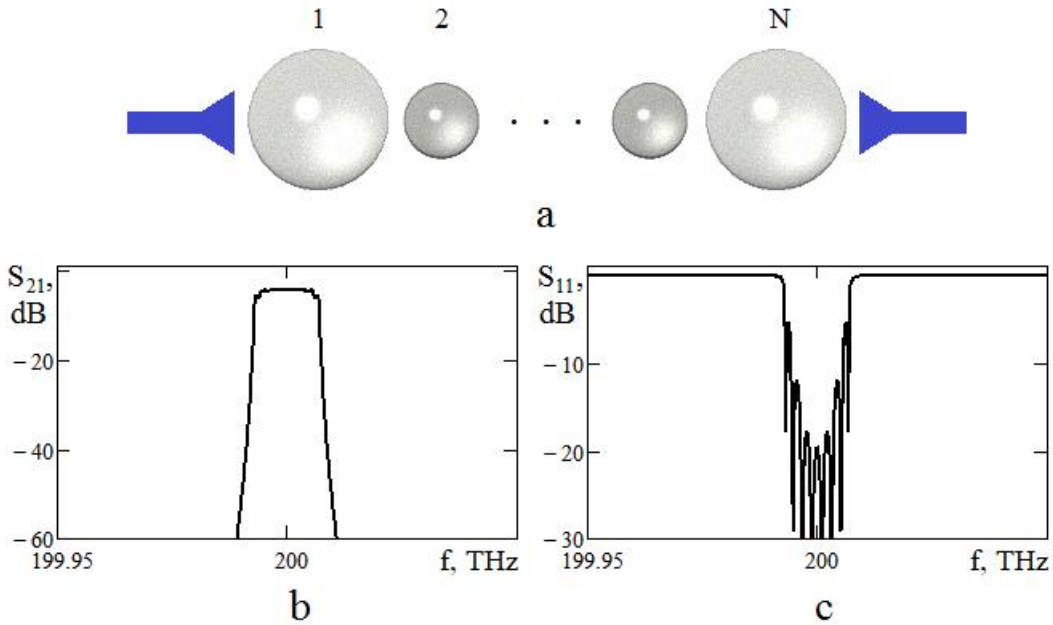


Fig. 1. Bandpass filter on different Spherical microresonators with azimuthally symmetric magnetic modes H_{n01} (a). S-matrix parameters as functions of frequency (b, c) of the filter (a) on 8 ($N = 8$) microresonators: ($\varepsilon_{1r} = 9$; $\varepsilon_{2r} = 16$; $n_1 = 24$; $n_2 = 22$; $m_1 = m_2 = 0$; $l_1 = l_2 = 1$)

Using the relations obtained earlier for the coupling coefficients [3], we constructed the electrodynamic models [4] of the filters shown in Fig. 1, 2, 4, a.

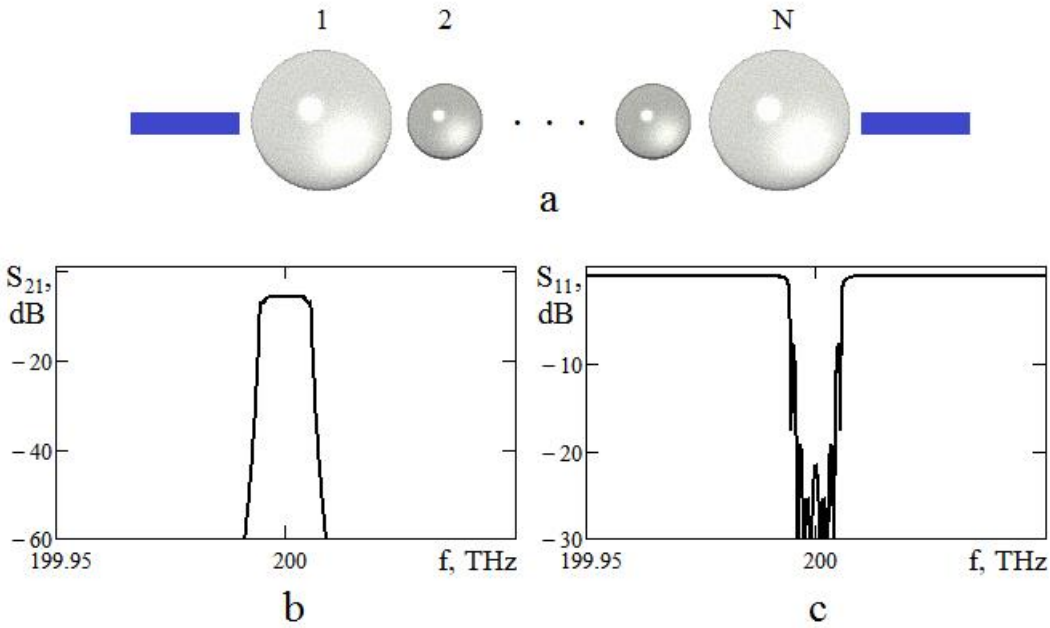


Fig. 2. Bandpass filter on different Spherical microresonators with magnetic modes H_{n11} (a). S-matrix parameters as functions of frequency (b, c) of the filter (a) on 8 ($N = 8$) microresonators: ($\varepsilon_{1r} = 9$; $\varepsilon_{2r} = 16$; $n_1 = 24$; $n_2 = 22$; $m_1 = m_2 = 1$; $l_1 = l_2 = 1$)

The placement of the input and output transmission lines (for example the optical waveguides or tapered fibers) corresponds to the maximum coupling between it and the microcavity for a given type of oscillation. It was assumed that each of these filters contains elements of coupling with the transmission lines that allow exciting non-degenerate types of oscillations in each of the resonators with a given value of the azimuthal number m. It was also assumed that the coupling coefficients k_L of the first and last microresonators with transmission lines are known. The losses

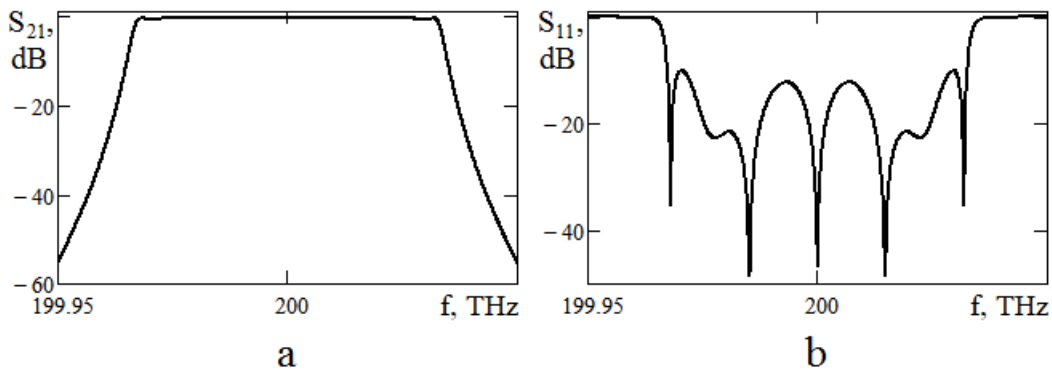


Fig. 3. Frequency responses of S-matrix parameters (a, b) of the bandpass filter on 9 microresonators with electrical E_{n11} modes: ($\varepsilon_{1r} = 9$; $\varepsilon_{2r} = 16$; $n_1 = 24$; $n_2 = 22$; $m_1 = m_2 = 1$; $l_1 = l_2 = 1$)

in the dielectric of each of the resonators were characterized by numbers: $Q_1^D = 1/\mathrm{tg}\delta_1 = 10^6$; $Q_2^D = 1/\mathrm{tg}\delta_2 = 2\cdot 10^6$. It was assumed too, all the resonators were not shielded and their radiation was taken into account in the open space.

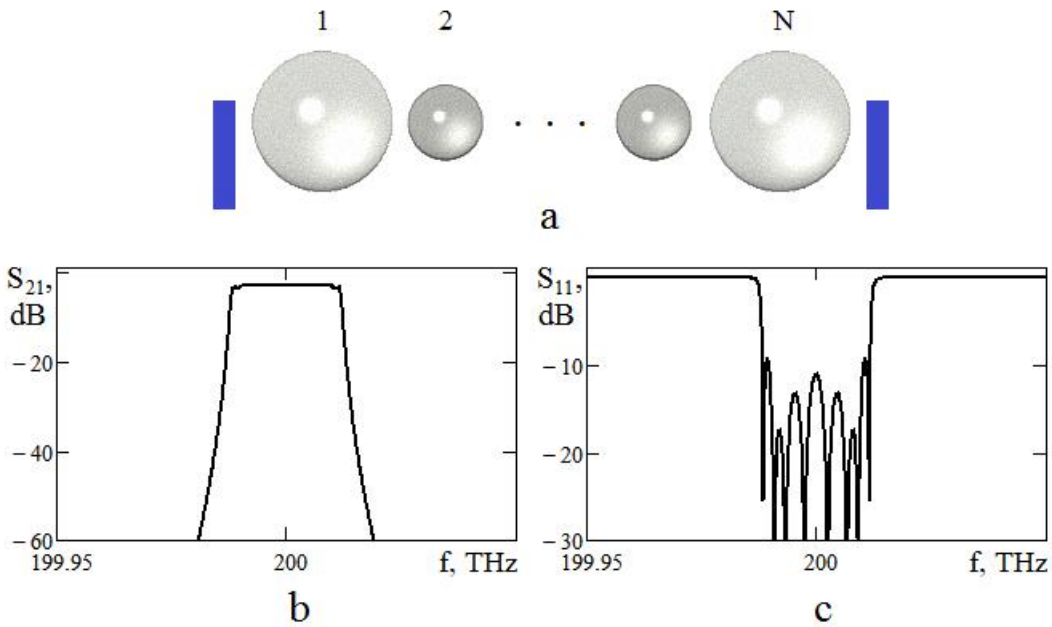


Fig. 4. Bandpass filter on different Spherical microresonators with magnetic H_{mm1} modes (a). S-matrix parameters as functions of frequency (b, c) of the filter (a) on 8 microresonators: ($\varepsilon_{1r} = 9$; $\varepsilon_{2r} = 16$; $m_1 = m_2 = 24$; $l_1 = l_2 = 1$)

The frequency responses of the scattering coefficients of the tuned filters for different types of whispering gallery oscillations are shown in fig. 1-4, b, c.

As can be seen, the use of different types of microcavities in the filters makes it possible to obtain acceptable transmission bands. As noted, such filters have a significant number of advantages over the known ones, for example, they have sparse bands of parasitic oscillations and also provide more opportunities for adjusting the coupling between microcavities and transmission lines.

References

1. G. C. Righini, Y.Dumeige, P. Feron, M. Ferrari, G. Nunzi Conti, D. Ristic and S. Soria, Whispering gallery mode microresonators: Fundamentals and applications. Rivista del Nuovo Cimento, 2011, vol. 34, N. 7, pp. 435 - 488.
2. Y. Li, F. Abolmaali, K. W. Allen, N. I. Limberopoulos, A. Urbas, Y. Rakovich, A. V. Maslov and V. N. Astratov, Whispering gallery mode hybridization in photonic molecules, Laser & Photonics Review, march 2017, pp. 1-11.
3. A.A. Trubin, Coupling coefficients of different Spherical Dielectric Microresonators, 12th International Scientific and Technical Conference “Modern Challenges in Telecommunications” (MCT-2018), Kyiv 2018, pp.
4. A.A. Trubin, Modeling of the Optical Filters on Different WGM Disk Microresonators, Information and Telecommunication Sciences, V.8, N1, 2017, pp. 26 - 30.

УДК 621.396

ТЕХНІЧНА ТВОРЧІСТЬ КОНСТРУКТОРІВ РАДІОТЕХНІЧНОГО КЛУБУ «ПОЛІТЕХНІК» UT7UZA КПІ. МИНУЛЕ І СЬОГОДЕННЯ, 1924 – 2018

Сергієнко М.І., Соколенко Д.О.
Радіотехнічний клуб "Політехнік" UT7UZA КПІ ім. Ігоря Сікорського
E-mail: ux0un@ukr.net, ut7uza@kpi.ua

Technical creativity of constructors from the radio-technical club «Polytechnic» UT7UZA KPI. Past and Present, 2014-2018., 1924-2018

This article outlines the achievements and results of the activity of Polytechnic of the KPI for the period from its foundation in 1925 to the present day. The article shows important role of KPI's radio technical club in technical design, scientific development and patriotic education of it's members. The achievements and results of the development from club members in various fields of radio engineering, energy saving, antennas, transmitting and receiving equipment are presented.

Історія радіотехнічного клубу "Політехнік" Київського політехнічного інституту почалася в далекому 1925 р. Враховуючи величезну зацікавленість студентів КПІ електро- та радіотехнікою відомим вченим-радіотехніком, професором Огієвським Володимиром Васильовичем (в минулому випускником КПІ) було створено радіоаматорський гурток. В тому ж році вийшла в міжнародний ефір клубна аматорська короткохвильова радіостанція. з позивним сигналом – R1KPI. Перший радіозв'язок з радіоаматорами світу провів сам Володимир Васильович Огієвський, який був чудовим радіотелеграфістом!

Активними членами радіо-гуртка і операторами окрім Огієвського В.В., були майбутні всесвітньо відомі вчені-радіотехніки, члени-кореспонденти НАН України Самуїл Тетельбаум (13RB, EU-5AL), Наум Волернер (EU-4CF) і молоді аматори Михайло Шапаренко, Володимир Єфремов, Михайло Бучма та інші.

Після тяжких воєнних років, відроджувався КПІ і разом з ним відроджувався наш рідний клуб з радіостанцією UB5KAG. Це був один із найскладніших і в той же час яскравих етапів у житті нашого клубу - його відродження і становлення. Він увійшов у нашу історію творчими ентузіастами і талановитими радіоконструкторами, які створили потужний творчий колектив, що не лише відновив діяльність клубу, але й приніс йому і визнання та міжнародну славу як в технічному напрямку, так і в спортивних досягненнях.

Далеко за межами клубу були відомі імена Георгія Румянцева (UB5UB), Володимира Черевка (UB5CA), Гарія Апреленка (UB5DX), Юрія Мединця (UB5UG), Сергія Буніна (UB5UN), Вадима Тараненко, Анатолія Чічка (UB5DW), Анатолія Кисельова (UT5BY), Анатолія Жука (UY5AZ), Михайла Шапринського (UT5BW), Георгія Піхура (UB5KAG), Миколи Деревінського (UB5KAG) та багатьох інших. Кожен з них видатна особистість, і у подальшому вони стали відомими вченими, громадськими діячами, керівниками підприємств.

Ми пишаємося випускником КПІ, активним членом клубу, оператором UB5KAG Сергієм Буніним (UB5UN, зараз UR5UN), який пройшов славний шлях від студента, члена радіотехнічного клубу "Політехнік", до доктора технічних наук, професора,

академіка, Лауреата Державних премій, чемпіона Світу, Європи, СРСР з радіоспорту, Почесного радиста СРСР. Протягом багатьох років він очолював кафедру телекомунікацій і телекомунікаційних систем КПІ. Його славне ім'я як радіоаматора відомо в найвіддаленіших куточках планети. Сергій Георгійович зробив величезний внесок у справу розвитку нашого улюбленого Ham-Radio і радіотехнічного клубу КПІ. Його мудрі книги допомогли багатьом знайти справу свого життя.

Один з членів нашого клубу , представник славної плеяди радіоаматорів КПІ тих далеких часів - заслужений майстер спорту, майстер спорту СРСР міжнародного класу, кавалер ордену "Знак Почесті" Георгій Румянцев (UB5UB, в подальшому - UA1DZ). Відомий радіоконструктор, автор численних наукових праць і численних розробок приймально-передавальної техніки і антен, багаторазовий чемпіон світу, Європи, чемпіон СРСР, багатьох міжнародних змагань. До того ж - чемпіон України з велоспорту!

Слід згадати творчі досягнення Юрія Мединця (UB5UG). Він відомий своїми новітніми розробками приймально-передавальної техніки, антен, унікальних пакетних трансиверів для радіоаматорів. Був неодноразовим переможцем і призером багатьох науково-технічних конференцій і виставок. Разом з друзями по клубу - Юрій Рафаілович підготував техніку та забезпечив радіозв'язок першої експедиції на гору Еверест в Непалі і багатьох інших експедицій на Памірі і Кавказі. Тривалий час працював завідувачем спеціалізованої лабораторії НДІ онкології, де 1980-х років, під керівництвом Юрія Рафаїловича було створено медичну технологію радіочастотної помірної гіпертермії та розроблено першу практичну техніку для магнітотермії. За ці наукові досягнення , які були впроваджені в клінічну практику нашої та зарубіжних країн, Ю.Р. Мединець з колегами отримали Державну премію України в галузі науки і техніки.

Ми з особливою гордістю згадуємо вихід у міжнародний ефір знаменитої колективки UK5UDX. Це був надзвичайно пам’ятний етап у житті нашого клубу і творчості радіо-конструкторів КПІ - нове відродження клубу. Керівництво КПІ виділило у новозбудованому корпусі Факультету гірничої електромеханіки та автоматики (зараз IEE) приміщення для радіотехнічного клубу і колективної радіостанції, де він працює і понині, продовжуючи свою славетну історію. Дуже скоро на даху корпусу №22 КПІ з'явилися потужні чудо-антени - наша гордість! Позивний UK5UDX загримів на всіх радіоаматорських діапазонах, і знову став визнаним і авторитетним у всьому світі ! Ми пишаємось своєю саморобною і в той же час – унікальною технікою і антенами, які були одними з найкращих у світі.

Кожного року клуб поповнювався талановитою молоддю, яка багато своїх сил вкладала у відродження і становлення клубу - Сергій Василенко, Юрій Онипко, Олексій Юшин, Микола Першин, Володимир Джулай, та багато інших.

В нашому клубі завжди були умови для творчого розвитку радіоаматорів багатьох поколінь. З гордістю відмічаємо, що все розвивається за рахунок ентузіазму, любові і вірності до нашого улюбленого хобі - Ham-Radio і до нашої Альма Матер - Київського політехнічного інституту! Ми глибоко вдячні нашим вірним друзям з КПІ, які завжди є поруч, а закінчивши КПІ надавали і надають необхідну допомогу рідному клубу. Низький вам уклін, глибока шана і повага, наші дорогі друзі, за Ваші добрі справи, які ви назавжди залишили для майбутніх поколінь радіоаматорів КПІ

Багато добрих справ було зроблено за останні роки в нашому клубі: нові конструкторські розробки в напрямку ефективних технологій радіозв’язку, і їх практичне застосування; проведена офіційна реєстрація радіотехнічного клубу як підрозділу КПІ ім. Ігоря Сікорського з підпорядкуванням його до навчально-наукового напрямку роботи Університету (Проректор Киричков П.О.). В 2017 році, для

підвищення ефективності роботи клубу та його міжнародних зв'язків відкрито офіційний сайт радіотехнічного клубу: ut7uza@kpi.ua Модернізовані старі та побудовані нові, більш ефективні антени, які дозволяють підвищити ефективність зв'язку, встановлено сучасне приймально-передавальне обладнання, впроваджені новітні види модуляції, зроблені ремонти в приміщенні клубу, проведені науково-практичні конференції.

В своїй діяльності ми завжди відчуваємо суттєву допомогу керівництва Університету і інституту енергозбереження та енергоменеджменту, наших випускників. В клубі регулярно проходять науково-практичні конференції, засідання, зустрічі з молоддю, та будуються нові плани на майбутнє.

Клуб відввідували багато радіоаматорів не лише з України, але й з багатьох країн світу – відомі вчені, державні діячі, митці, спортсмени.

Матеріально-технічна база клубу використовується в навчальному і виховному процесі. Тут проводяться показові лекції, практичні роботи, зустрічі з цікавими людьми, конференції, навчально-агітаційні заходи, спрямовані на патріотичне виховання студентів та залучення до вступу в КПІ ім. Ігоря Сікорського випускників навчальних закладів України.

Завжди цікавляться роботою нашого радіотехнічного клубу керівництво нашого Університету. Нам завжди є чим порадувати при особистих зустрічах в нашому клубі Ректора КПІ ім. Ігоря Сікорського, академіка НАН України Михайла Згуровського, проректора і нашого куратора д.т.н., проф. Киричка П.О. Нам надзвичайно приємно, що проректор КПІ ім. Ігоря Сікорського, академік НАН України Михайло Ільченко є також членом клубу і має радіоаматорський позивний UT5UME.

У 2015 році, на честь славного ювілею клубу 90-річчя з дня заснування та виходу в ефір нашої першої колективної радіостанції ми працювали у міжнародному ефірі спеціальним позивним EM90KPI. Були проведені тисячі радіозв'язків з радіоаматорами багатьох країн світу. На честь цієї знаменної події були надруковані спеціальні QSL-картки і спеціальні дипломи які були розіслані усім нашим кореспондентам.

У 2017 році колектив клубу брав участь у багатьох міжнародних змаганнях з технічних видів спорту, тричі ставав чемпіоном України з радіозв'язку, завдяки застосуванню новітніх технологій і техніки , розроблених як членами клубу, так і випускниками КПІ, які отримали глибокі знання та практичні навички в нашому клубі. Наш клуб був ініціатором і організатором ряду науково-практичних конференцій радіоаматорів України, які були проведені на базі КПІ ім. Ігоря Сікорського. Попереду багато планів, і в першу чергу - робота з молоддю, студентами–першокурсниками та виховання в них патріотизму та відданості КПІ ім. Ігоря Сікорського і нашому радіотехнічному клубу.

Література

1. Ільченко М.Ю. Засновник радіотехнічної школи В.В. Огієвський./ М.Ю. Ільченко. – Київ.: Техніка. 2014.– 115 с.
2. Бунин С.Г. Справочник радиолюбителя-коротковолновика / С.Г. Бунин, Л.П. Яйленко // К.: Техника, 1984, – 264 с.
3. Правда В.І. Історичний нарис: Радіотехнічний факультет НТУУ «КПІ» / В. І. Правда // Вісник НТУУ «КПІ». Серія – Радіотехніка. Радіоапаратобудування. – 2006. – No 33
4. Сергиенко Н.И. Профессор КПИ Огиевский В. В [Електронний ресурс]. – Режим доступу: http://uarl.com.ua/bylsluchay/autor/33ogievsky.html
5. Сайт радіотехнічного клубу Політехнік UT7UZA. [Електронний ресурс]. – Режим доступу: http://ut7uza.kpi.ua/about.

UDC 621.391

ANTENNA BASED UWB RECEPTION AND TRANSMISSION

Sergey Bunin
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: sgbunin@ukr.net

ПЕРЕДАЧА И ПРИЕМ UWB СИГНАЛОВ ОСНОВАННЫЕ НА ДЕКОДИРОВАНИИ И КОДИРОВАНИИ АНТЕННАМИ

В работе рассматривается концептуальная возможность декодирования импульсного сверхширокополосного сигнала, кодированного по положению импульсов (Pulse Position Coding) непосредственно приемной антенной приемника и передача закодированного сигнала путем импульсного возбуждения передающей антенны.

The transmission of data using pulsed ultra-wide-pulse signals (IR-UWB) remains an attractive and promising method in connection with many advantages over the transmission of continuous signals based on sinusoidal carriers.

However, ultrashort pulses of practical power (units, tens of watts) carry the small energy equal to the pulse power P_i multiplied by its duration τ_i: $E_i = P_i\ \tau_i$. As a result, the signal-to-noise ratio $E_i\ /\ N_0$, which determines the probability of reception errors, is low. Therefore, data transmission is performed by a series of pulses, the group of which determines the transmitted symbol. This group of pulses T_s is encoded in accordance with a time code (Pulse Position Coding - PPC) orthogonal to codes of other symbols or signals of other transmission systems operating in the same frequency band. An example of such a signal is shown in Fig.1.

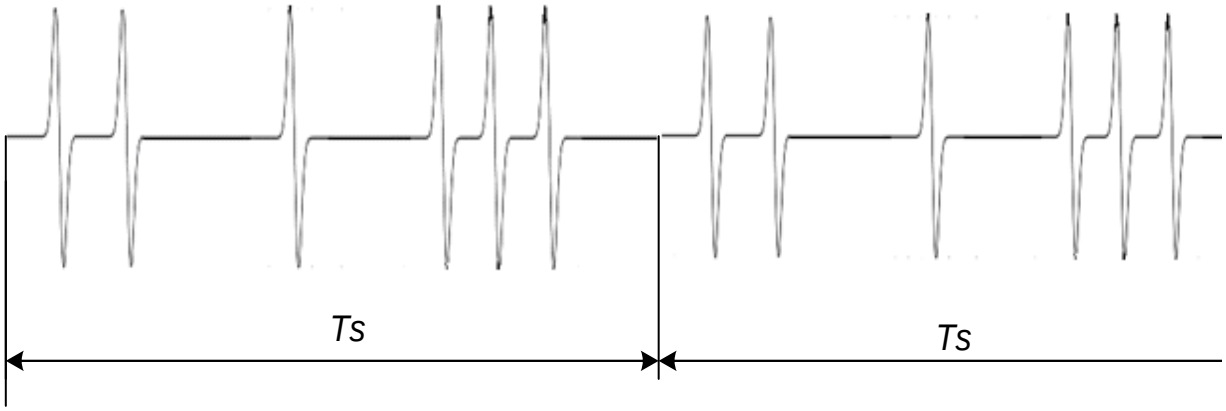


Fig. 1. Pulse Position Coding

To separate the signals at reception it is necessary to apply the correlation method of symbol allocation. The correlator can be an active, selecting symbol by comparing the received signal impulse series with the signal structure (code).

An active correlator requires the synchronization of a sample of the code sequence with the received signal. Ultrashort pulse duration makes it practically impossible to get acceptable accuracy synchronization in receivers.

A passive correlator based on a delay line with taps, also requires high construction accuracy. Such receiver unit can be simplified by applying the "non-energy" receiver circuit [1], in which the received ultrashort pulses are replaced by "standard" pulses of amplitude and duration suitable for processing by digital devices.

UWB RECEIVER WITH CODED PULSE POSITION. The discrete nature of the IR-UWB signal with the encoding of information symbols by the position of the pulses allows them to be received and decoded at the input of the receiver by means of an antenna whose design is consistent with the time structure of the signal.

Figure 2 shows the receiver circuit with such an antenna.

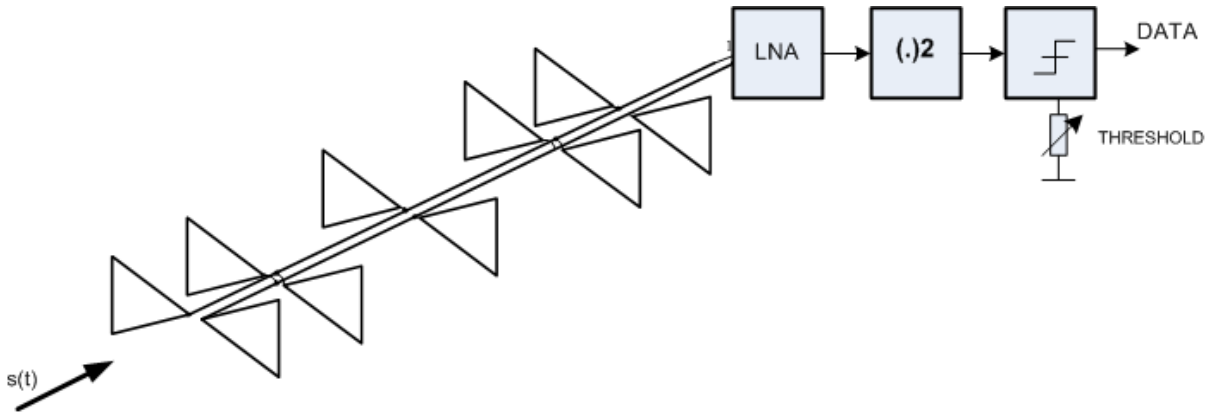


Fig. 2. Pulse Position Coded Receiver

The received signal propagates along the antenna, which is a long feeder line connected to flat ultra-wideband vibrators forming dipoles. The feeder line plays the role of an adder of the correlator: the vibrators are taps-offs of a long line. The position of the dipoles (the distance between them) corresponds to the position of the impulses of the signal in the feeder (taking into account the propagation slowdown in it) when one Pulse Position Coding (PPC) is received. Thus, the antenna is a filter matched to the signal.

With a temporary mismatch, the antenna generates noise at the output of the feeder line, which reflects the separate excitation of the vibrators by the pulses of the signal. When the structure of the signal coincides with the antenna structure, a pulse appears at the output of the feeder line, corresponding to the sum of the

voltages in the vibrators (correlation peak) caused by the coincidence in time of excitation of all or most of the vibrators. In a simplified form - without noise, interference and distortion of the shape of the pulses due to the non-ideality of the characteristics of the antenna elements – signals at the output of the antenna are illustrated in Fig.3.

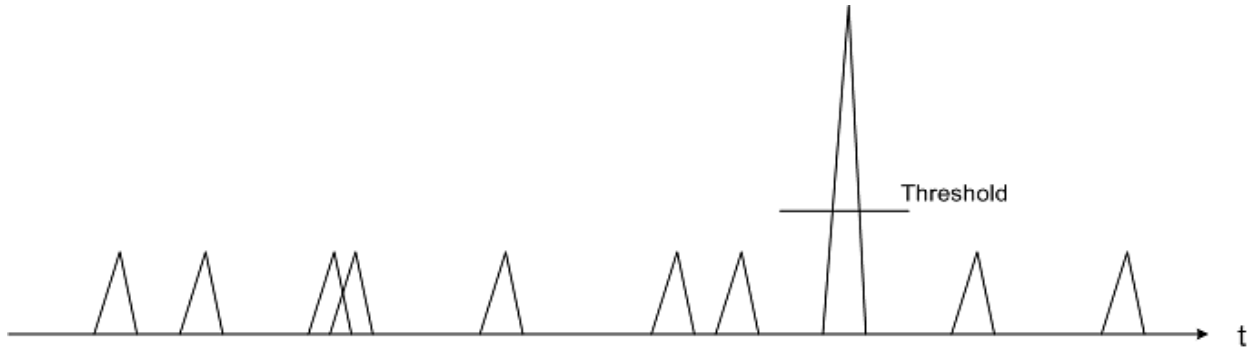


Fig. 3. Signals after Squarer

The signals at the output of the antenna feeder are amplified by a low-noise LNA amplifier, squared to obtain a unipolar voltage, and fed to a threshold device with a pre-set threshold. Exceeding the trigger threshold causes a pulse at the output of the receiver informing you of the reception of a bit of the given antenna code.

The antenna in the horizontal plane has a one way "information" directivity within one-sided lobe of the dipole antenna, i.e. reception of the information with asymmetric code can be conducted only from one side. The energy pattern corresponds to the dipole pattern.

REPEATER. Considering the reciprocity of the antennas for receiving and transmitting, it is possible to transmit the PPC signal by the antenna described above by its pulse excitation. To do this, an ultra-short video pulse is applied to the input of the feeder line. Ultra-wide-band vibrators connected to the feeder in the code sequence will emit radio pulses in the order of propagation of the video pulse along the feeder, i.e. in the form of the PPC code specified by the antenna.

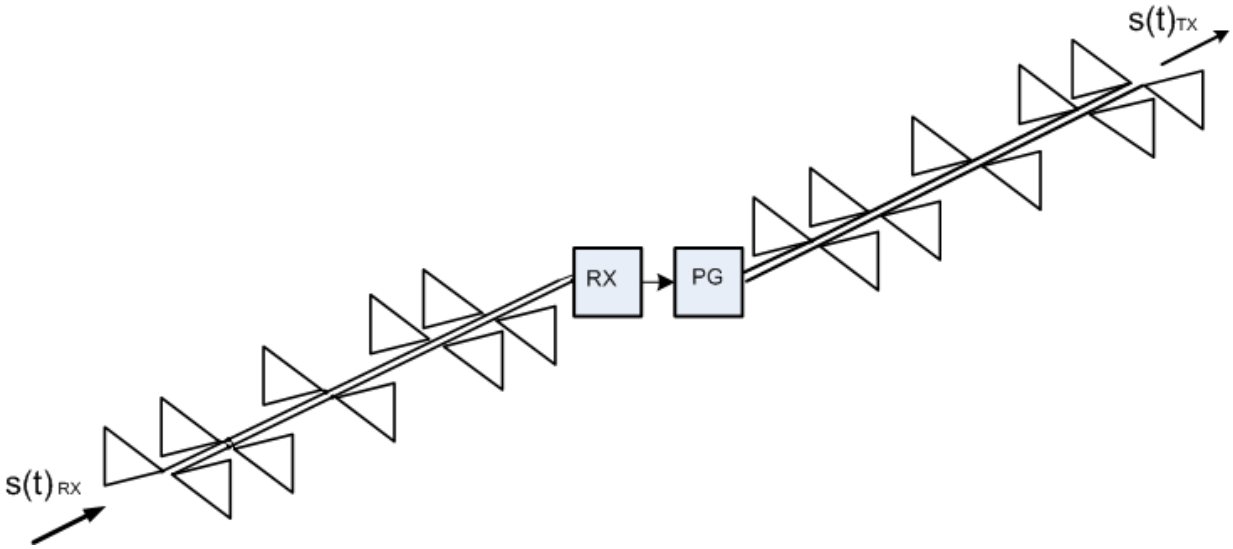


Fig. 4. UWB pulse transcoded repeater

The connection in series of the receiver with decoding antenna and the transmitter with the coding antenna allows the construction of a repeater of encoded or transcoded PPC signals (fig.4). The receiver output (RX) is connected to the input of an ultrashort pulse generator (PG). The reception pulse of the information bit at the output of the receiver triggers the generation of the excitation pulse for the transmitting antenna, which causes radiation corresponding to the code given by this antenna.

The transmitting antenna also has a one-way "information" orientation.

CONCLUSION. The method for receiving, transmitting and retransmitting UWB pulse signals with Pulse Position Coding has been proposed. The discrete nature of UWB signals allows them to be decoded when they are received directly by the receiver antenna, whose design is consistent with the signal.

The transmission of UWB signals with their simultaneous PPC coding can be accomplished by pulsed excitation of a multi-element collinear antenna with a predetermined arrangement of its vibrators. The combination of the receiver and the transmitter allows the repeater to be implemented with or without changing the signal code.

The proposed ideas are conceptual. The paper does not address issues related to signal distortions due to the non-ideality of the characteristics of circuit elements in ultra-wideband signal conversion.

References

1. S. Bunin, Non-Energy IR-UWB Receiver. Telecommunication Sciences, vol.1, No.1, July – December 2010, pp. 7 – 13.
2. S. Bunin. The Self-Organizing Radio Networks and Ultra Wide Band Signals. Telecommunication science, vol.4, No.2, 2014. pp. 3-7.

УДК 621.396.43

TECHNICAL CHARACTER OF TERAHERTZ AND LASER WAVES IN SATELLITE TELECOMMUNICATIONS

Naritnik T.M., Ermakov A.V., Posternak B.S., Onisko O.O.
Institute of Telecommunications of National Technical University of Ukraine Igor Sikorsky KPI, UkraineE-mail:b.posternak@ukr.net

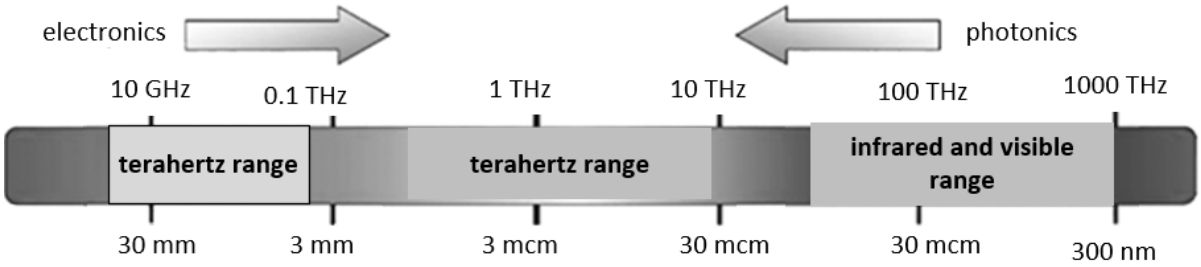
ТЕХНІЧНІ ВЛАСТИВОСТІ ТЕРАГЕРЦОВИХ ТА ЛАЗЕРНИХ ХВИЛЬ В СУПУТНИКОВИХ ТЕЛЕКОМУНІКАЦІЯХ

Терагерцові і лазерні хвилі використовуються для бездротової передачі даних. Порівняні типи хвиль мають великий потенціал для їх використання в телекомунікаціях. В даній роботі проведено аналіз особливостей і властивостей терагерцових і лазерних хвиль, їх потенціалу для використання в супутникових телекомунікаціях.

Terahertz and laser waves are used for wireless data transmission. Comparable types of waves have great potential for their use in telecommunications. In this study an analysis of the features and properties of terahertz and laser waves is carried out. Their potential for use in satellite telecommunications.

Terahertz waves transmit information via radio waves which spectrum of frequencies is located between infrared and ultrahigh-frequency ranges. In this frequency range it was difficult to apply methods, ideas and technical solutions which fully justified themselves in the development of adjacent ranges.

Thus, the terahertz frequency range from 100 GHz to 10 THz (1 THz = 103 GHz) lies at the boundary between electronics and photonics. Below it is determined by the frequency-time constraints (over 100 GHz) of electronic transitions in semiconductor structures, and above – by the maximum wavelength of quantum transitions of laser structures. This wavelength range is on the scale of the electromagnetic waves between the microwave range and the infrared and visible range and partially overlays the high frequency part of the extremely high frequency (HF) band (100 ... 300 GHz) and the low frequency part of the infrared range.



The interaction of terahertz waves with atmospheric gases, fluids, various solid media and materials has its own specificity, which manifests itself in the essential difference in attenuation, permeability, dissipation, reflection and radiation of these waves compared with optical waves.

The line of the optical system of communication between the two points consists of two receiving and transmitting devices located within the line of sight at both ends of the line and directed to each other. In the transmitter, the generator-laser and the modulator of its optical radiation are transmitted by a signal. The modulated laser beam of the optical system is directed toward the receiver. In the receiver, the radiation focuses on the photodetector, where its detection and selection of transmitted information is performed.

The scheme of one version of the receiver-transmitting device of the optical system of communication with the semiconductor laser is given in Fig. 1

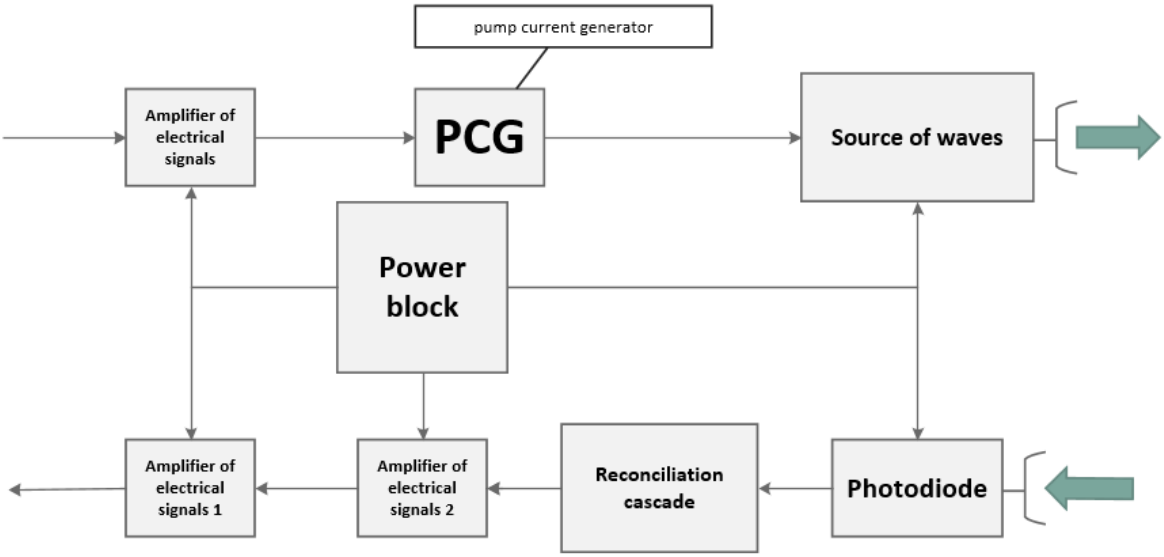


Fig.1 Scheme of the receiver-transmitting device
of the optical communication system

The optical radiation is focused on the antenna. The receiving part contains an antenna, focusing radiation at the reception area of the photodiode.

The atmosphere is a mechanical mixture of gases, steam, liquid droplets and solid particles. In it there is always a variable quantity of dust, smoke, ice crystals. Therefore, the atmosphere is an aerosol, the composition of which constantly changes due to mixing.

Technical characteristics of the atmospheric communication lines are given in Table.1.

Table 1 European Space ACL

Parameter	**Value**
Working wavelengths, microns	0,81—0,87
Average radiated power, mW	50
Information transfer speed, Mbps / channel	1—120
Diameter of antenna of geostationary satellite, cm	35
Diameter of antenna of low-orbit satellite, cm	20
Dynamic aiming/guidance error, microrads	20
Static aiming/guidance error, microrads	0,5
Probability of false reception of a symbol	10^{-6}
Estimated communication distance, km	45000

Thus, the communication on the laser beam via the atmosphere provides today the transfer of large volumes of information with high reliability at distances per kilometer in the earth's atmosphere and in the space in the tens of thousands of kilometers.

The terahertz and laser waves have many differences but can successfully complement each other in one communication system.

References

1. Приемо-передатчик для цифровой радиорелейной системы терагерцового диапазона//Ильченко М.Е., Кузьмин С.Е., Нарытник Т.Н , Радзиховский В.Н// http://www.mitris.com/files/Ilchenko%20in%20Russian.pdf.
2. Обґрунтування частотних діапазонів для високошвидкісних безпроводових телекомунікаційних систем терагерцового діапазону//Г.Л. Авдєєнко, С.Г. Бунін, Т.М. Наритник, А.В. Єрмаков// http:// www.mitris.com/files/171_avdeyenko_terahertz.pdf.
3. http://www.znanius.com/3640.html.

UDC 621.396

PERFORMANCE ANALYSIS OF CARRIER-AGGREGATED MULTI-ANTENNA 4×4 MIMO LTE-A FRONTHAUL

Chernyavsky A. A.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: ruskc2beat@gmail.com

Анализ производительности мульти-антенны 4×4 MIMO с объединением несущих в сети LTE-A FRONTHAUL

В этой статье предлагается и экспериментально оценивается производительность многоантенных систем LTE-Advanced (LTE-A), реализующих мультиплексирование с пространственным разделением MIMO на многоядерном волокне, по сравнению с передачами SISO с одной антенной.

In this paper the performance of multi-antenna LTE-Advanced (LTE-A) systems implementing MIMO space division multiplexing on multicore fiber, compared to single-antenna SISO transmissions is proposed and evaluated experimentally.

As mentioned in [3], wireless data traffic explosion in the last decade has led to higher data rate requirements for wireless cellular networks which are expected to bring Gbps per mobile user by 2020. Mobile broadband network growth is expected to reach 10 billion subscribers by the year 2020, that may result in a compound annual growth rate (CAGR) of 5.4%. The traffic growth connected with this CAGR implies high network densification. To achieve this, new technology is proposed to be integrated in the next-generation networks including cloud radio access networks (C-RAN) and dense heterogeneous networks (HetNets) employing massive multiple-input-multiple-output (M-MIMO) and Carrier Aggregation.

There are two factors driving the capacity increase in LTE-A: First, the use of Carrier Aggregation, where the overall transmission bandwidth is increased by aggregating several signal carriers, each one known as a component carrier (CC). As depicted in Fig. 1, when Carrier Aggregation is used, each CC can serve a different cell, with the same or different coverage. Second, the support of massive MIMO improves the spectral efficiency by using a large number of antennas and accommodating dozens of users in the same radio channel. MIMO is used to increase the overall bitrate through the transmission of two or more different data streams on different antennas. The combined use of Carrier Aggregation and M-MIMO in different degrees defines next-generation 4.5G Pro and 4.9G LTE-A wireless standards. As depicted in Fig. 1, fronthaul antenna systems are usually installed on the top of roofs ensuring line-of-sight communication with mobile terminals. In order to provide M-MIMO connectivity, radio-over-fiber (RoF) transmission has been proposed to provide centralized multi-service delivery.

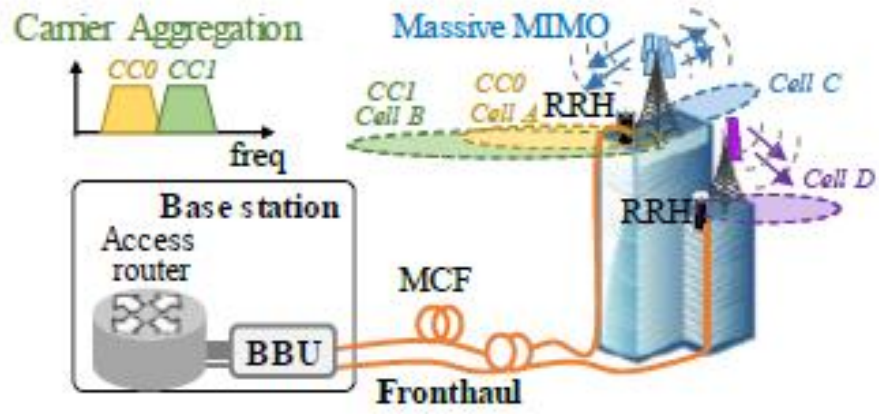


Fig. 1. Fronthaul scenario implementing radio-over-multicore fiber with massive MIMO and Carrier Aggregation

Current LTE-A cellular communication standard implements both aforementioned technologies to provide higher user data rates: multi-antenna MIMO transmission and Carrier Aggregation. Implementing MIMO, the same resources can be used in both frequency and time, separated only through the use of different reference signals (RS) to be received by several antennas. In this work, we configure the LTE-A signal to implement a single-antenna system or spatial multiplexed systems with two or four antennas. In Carrier Aggregation, the most used configuration comprises contiguous component carriers within the same operating frequency band (also called intra-band contiguous carriers). In 3GPP release R10 and R11, the intra-band contiguous aggregation in frequency division duplex (FDD) defines the maximum aggregated bandwidth of 40 MHz with two CCs maximum. Thus, in order to evaluate the most challenging case, in this study the 3GPP FDD LTE-A generator is configured to transmit two aggregated CCs of 20 MHz bandwidth each. The aggregated bandwidth of 40 MHz can be supported with a single transceiver. Each LTE-A 20 MHz CC comprises 100 resource blocks (RB) with 1201 subcarriers for the downlink (DL) and 1200 subcarriers for the uplink (UL). The difference in the number of subcarriers is based on the fact that, for DL signals, the DC subcarrier is not transmitted but counted, while UL signals are symmetric about DC and have no DC subcarrier.

We will analyze the performance of four-antenna LTE-A system implementing 4×4 MIMO spatial multiplexing of four data streams for a single user. We evaluate the performance of LTE-A signal implementing 4×4 MIMO spatial multiplexing and Carrier Aggregation for different frequency bands (fc) and different carrier separation (Δf). Fig. 2(a) shows the EVM of both aggregated carriers for different carrier separation (Δf) maintaining the center frequency at fc=2.655 GHz (center of FDD band 7).

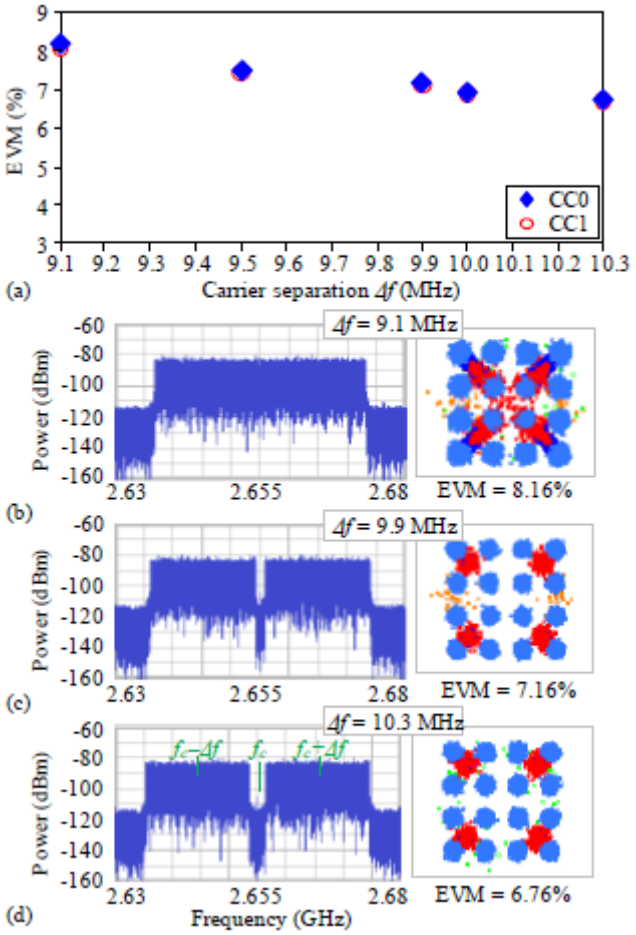


Fig. 2. (a) Measured EVM for two 20 MHz LTE-A 4×4 MIMO CCs vs. carrier separation and measured spectrum (ch1, RBW=1.27 kHz) and constellations for (b) Δf=9.1 MHz, (c) Δf=9.9 MHz, and (d) Δf=10.3 MHz

Comparing the measured spectrum in Fig. 2(b)-(d), for Δf=±9.1 MHz the 20 MHz carriers start overlapping in spectrum which increases the EVM to 8.16% compared with the EVM of 6.76% obtained with Δf=±10.3 MHz.

This paper proposes and evaluates experimentally the performance of multiple-antenna RoF fronthaul over MCF media implementing MIMO and Carrier Aggregation. Different configurations of single- and multiple-antenna systems can be developed assigning one or a group of cores of the MCF to each system. In this work we have evaluated the four-antenna LTE-A system implementing 4×4 MIMO spatial multiplexing.

The experimental evaluation is performed including also Carrier Aggregation with two carriers at the maximum regulated bandwidth.

The experimental results confirm that Carrier Aggregation doesn't affect the signal quality as long as the carriers are not overlapped in spectrum. More carriers could be provided in the same or different frequency bands employing the proposed fiber fronthaul architecture.

References

1. Jun-ichi Kani, "Solutions for future mobile fronthaul and access-network convergence," in Proc. Optical Fiber Communications Conference and Exhibition (OFC), paper W1H.1, March 2016.
2. Kanesan T. et al., "Solution to reduce nonlinearity in LTE RoF system for an efficient DAS topology: A brief review," in Proc. Int. Symp. on Comm. Systems, Networks and Digital Signal Processing (CSNDSP), July 2016.
3. Morant M. Performance Analysis of Carrier-Aggregated Multiantenna 4 × 4 MIMO LTE-A Fronthaul by Spatial Multiplexing on Multicore Fiber / M. Morant, R. Llorente // Journal of Lightwave Technology, Vol.: 36 Issue 2. – Jan.15, 2018. – pp. 594-600.
4. Selim M. et al., "Fronthaul cell outage compensation for 5G networks," IEEE Communications Magazine, vol. 54, no. 8, pp. 169-175, 2016.

UDC 621.396.1

INFLUENCE OF FADINGS ON THE COMMUNICATION CHANNEL AND METHODS OF RESISTING THEM IN THE MULTIPLAYER SYSTEM OF DVB-T2 STANDARD

Solianikova V.Y.

National Technical University of Ukraine " Igor Sikorsky Kyiv Polytechnic Institute"

E-mail: leka-br@mail.ru

ВПЛИВ ЗАВМИРАНЬ НА КАНАЛ ЗВ'ЯЗКУ ТА МЕТОДИ БОРОТЬБИ З НИМИ В МУЛЬТИСЕРВІСНІЙ СИСТЕМІ СТАНДАРТУ DVB-T2

В даній статті описується вплив багатопроминевості на наземній канал телевізійного мовлення. Розглянуто основні методи забезпечення працездатності каналу, а також описано методи боротьби з завмираннями в мультисервісній системі стандарту DVB-T2.

This article describes the multidimensional effects of the terrestrial television broadcast channel. The basic methods of ensuring the efficiency of the channel are considered, as well as methods of fading resisting in the DVB-T2 multiservice system.

The propagation of radio waves is characterized by three partially independent effects, known as loss in proliferation, screening and fading due to multiply propagation. Fading through multidivision is described by the fading of the envelope (independent of the frequency of the amplitude change), the Doppler scattering (time-selective, or temporal, random phase noise), and time scattering. The time scattering leads to the appearance of frequency selective fading [1].

Frequency-selective fading is characteristic for terrestrial television.

The main cause of frequency selective fading is time scattering due to multipath propagation. Phase differences between components of the same frequency propagating in different ways can be practically independent for different frequencies of the spectrum, so that some harmonics as a result of multipath interference can be amplified, while others, on the contrary, can be suppressed.

Frequency-selective fading occurs when the width of the spectrum of the signal exceeds the coherence band of the communication channel - the frequency interval at whose boundaries the fading of the spectral components is characterized by a certain limit value of the correlation coefficient. The level of permissible distortion depends on the processing methods of the signals in the codec and the modem.

In the DVB-T2 multiservice system, there are many tools to improve the system's resistance to interference, such as: cascade coding (BCH and LDPS), modulation (QPSK, QAM-16 ... QAM-256), constellation rotation, four interleaving (bit, cells, time and frequency) and OFDM (Orthogonal Frequency Division Multiplex).

To resist frequency selective fading, the DVB-T2 television standard uses bit interleaving as well as frequency interleaving using OFDM technology.

The bit interleaver alternates the code bits in the low-density parity-check code (LDPC) code word to avoid unwanted interaction between bits that are transmitted in the same cell and structure, is present in the LDPC code [2].

OFDM is a modulation technology using orthogonal carriers, i.e. modulated nominal subcarriers (1K-32K), located in a given band with a fixed frequency step (Fig. 1). The modulation rate of an individual carrier is thus small enough that it allows the use of effective noise-immune encoding and takes measures to prevent intersymbol interference (introduce special guard intervals for each OFDM symbol) [3].

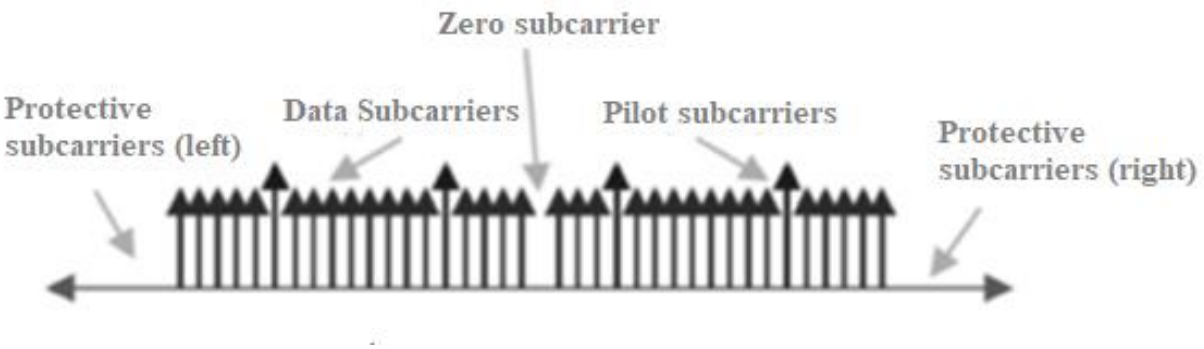


Fig. 1. The sub-carriers of the CRM signal

Generally, OFDM technology today is considered one of the most promising for the construction of broadband digital radio communication systems with multipath channels, providing a fairly high spectral efficiency of these systems.

The frequency interleaver is a pseudo-random block interleaver that operates on OFDM symbols and has several features. First, it mixes cells from different PLPs (Physical Layer Pipe), transmitted in one OFDM symbol. Secondly, this interleaver uses a pseudo-random sequence to output a time interleaver, thereby breaking the structured temporal interleaving. Third, the interleaver alternates between two different permutations, which helps increase the number of OFDM carriers to which each PLP is mapped [2].

Temporal and frequency interleaving is relevant for broadcasting in conditions of complex terrain and urban development, when multipaths and multipath signal propagation, fading zones arise, and so on.

Therefore, the tools used in the multiservice DVB-T2 standard are quite effective in fading resistance, which occurs when reflecting in the conditions of urban development. In the future, these techniques should be used to build duplex communication lines to adapt to the complex and changing operating conditions of telecommunication systems using tools offered by the DVB-T2 standard.

References

1. Беспроводная цифровая связь. – К. Феер, Москва, “Радио и связь”, 2000.
2. Digital Video Broadcasting (DVB); Implementation guidelines for a second generation digital terrestrial television broadcasting system (DVB-T2). – Draft ETSI TS 102 831 V1.2.1 (2012-08).
3. Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2). – Draft ETSI EN 302 755 V1.4.1, February 2015.

УДК 051.7

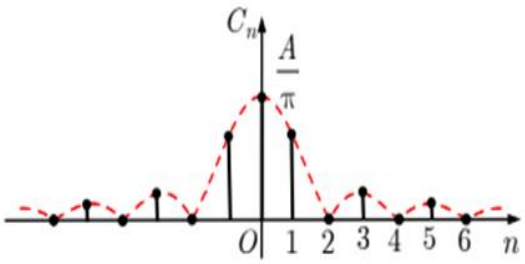
CORRECTNESS OF RESEARSHING SIGNAL SPECTRUMS WITH NONMONOTONIC BASIS FUNCTION

Martynova K.G., Fedorova L.B.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: scorpio.for.teen@gmail.com

КОРЕКТНІСТЬ ДОСЛІДЖЕННЯ СПЕКТРІВ СИГНАЛУ З НЕМОНОТОННОЮ БАЗИСНОЮ ФУНКЦІЄЮ

Дана стаття має на меті наочно показати, як впливає дотримання необхідних умов, викладених в математичних теоремах на правильність отриманих результатів. Конкретно розглядатиметься вплив некоректного переносу інтегральної ознаки Коші на ряди спектрів сигналу на достовірність результатів.

Calculus has its share in various applied tasks. In particular, researching of signal spectrum is essential constituent of studying telecommunications theory: examining series made of spectrums is applied in modern digital signal processing. The most popular are spectrums with basis functions represented as a sine-wave.



For example, let's observe an amplitude spectrum of a signal represented by a periodic sequence of square-wave pulse:

$$C_n = \left|\frac{A}{\pi n}\sin\left(\frac{\pi n}{2}\right)\right|,$$

where A is amplitude.

This article is aimed to illustrate how adhering necessary conditions, which are posed in theorems, have its influence on correctness of obtained results. Therefore, perform examining a series with a summand equal to our original spectrum for convergence applying the integral test.

Integral Test. *Suppose that $f(x)$ is a continuous, positive, and decreasing function on the interval $[k, \infty)$ with $a_n = f(n)$. Then the following hold.*

1. *If* $\int_k^\infty f(x)\,dx$ *is convergent, then so is* $\sum_{n=k}^{\infty} a_n$.
2. *If* $\int_k^\infty f(x)\,dx$ *is divergent, then so is* $\sum_{n=k}^{\infty} a_n$.

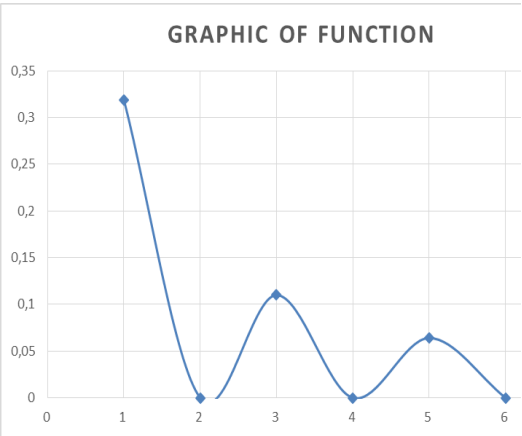
I write series of signal spectrums and examine for convergence:

$\sum_{n=1}^{\infty}\left|\frac{A}{\pi n} sin\frac{\pi n}{2}\right| = |A|\sum_{n=1}^{\infty}\left|\frac{1}{\pi n} sin\frac{\pi n}{2}\right| = |A|\left(\frac{1}{\pi}+0+\frac{1}{3\pi}+0+\frac{1}{5\pi}+\cdots\right) = |A|\sum_{n=0}^{\infty}\frac{1}{(2n+1)\pi}$,

$a_n = \frac{1}{2n+1} \sim \frac{1}{n} = b_n$

$\sum_{n=1}^{\infty} b_n = \sum_{n=1}^{\infty}\frac{1}{n}$ – well-known harmonic series, which diverges, and so do $\sum_{n=0}^{\infty}\frac{1}{(2n+1)\pi}$.

Now, let's build function corresponding our original spectrum $f(x) = \left|\frac{A}{\pi}\right|\frac{\left|\sin\frac{\pi x}{2}\right|}{x}$. Obviously, our function is continuous, positive and decreasing (but not monotonically).



From other side I examine for convergence the integral $\left|\frac{A}{\pi}\right|\int_1^{\infty}\frac{\left|\sin\frac{\pi x}{2}\right|}{x}dx$. In general case integral like $\int_1^{\infty}\left|\frac{sin\, t}{t}\right|dt$ diverges, so we can affirm that so do $\int_1^{\infty}\frac{\left|\sin\frac{\pi x}{2}\right|}{x}dx$.

Conclusion 1: In this example relaxing the monotony condition of examining function in the integral test doesn't lead to incorrect result.

However, resemble relaxing frequently leads to mistakes during calculus. Now let's observe an illustrative case when incorrect transferring Cauchy integral test on random series leads to mistake. Accomplish this I make some alterations in examining spectrum:

$$C_n = \frac{A}{\pi n}(\sin^2(\frac{\pi n}{2}))^n$$

Series $\sum_{n=1}^{\infty}\frac{A}{\pi n}(\sin^2(\frac{\pi n}{2}))^n$ diverges analogically to the first example. Examine the improper integral $\left|\frac{A}{\pi}\right|\int_1^{\infty}\frac{(\sin\frac{\pi x}{2})^{2x}}{x}dx$ for convergence again.

$$\left|\frac{A}{\pi}\right|\int_1^{\infty}\frac{(\sin\frac{\pi x}{2})^{2x}}{x}dx = \left|\frac{A}{\pi}\right|\sum_{n=1}^{\infty}\int_n^{n+2}\frac{(\sin\frac{\pi x}{2})^{2x}}{x}dx \le \left|\frac{A}{\pi}\right|\sum_{n=1}^{\infty}\int_n^{n+2}\frac{(\sin\frac{\pi x}{2})^{2n}}{n}dx$$

Using changing of variables and property of the integral of periodic function and Wallis product get the next expression:

$$\int_{n}^{n+2} \frac{\left(\sin\frac{\pi x}{2}\right)^{2n}}{n} dx = \frac{4}{\pi n}\int_{0}^{\frac{\pi}{2}} (\sin t)^{2n}\, dt = \frac{2(2n-1)!!}{n(2n)!!}$$

Now I have shown that original integral is smaller than original series. $\left|\frac{A}{\pi}\right|$ can be ignored because it is a numeric which I can shrink.

$$\int_{1}^{\infty} \frac{\left(\sin\frac{\pi x}{2}\right)^{2x}}{x} dx \leq \sum_{n=1}^{\infty} \frac{2(2n-1)!!}{n(2n)!!}$$

Suppose $A_n = \frac{(2n-1)!!}{(2n)!!}$ and $B_n = \frac{(2n)!!}{(2n+1)!!}$. A step-by-step comparison shows that each factor in A_n is smaller than the corresponding factor in B_n,, hence $A_n < B_n$. So we have

$$A_n^2 \leq A_n B_n = \frac{1}{2n+1}$$

Returning to our infinite sum and employing the direct-comparison test,

$$\sum_{n=1}^{\infty} \frac{2(2n-1)!!}{n(2n)!!} = \sum_{n=1}^{\infty} \frac{2A_n}{n} \leq \sum_{n=1}^{\infty} \frac{2}{n\sqrt{2n+1}} \leq 2\sum_{n=1}^{\infty} \frac{1}{n^{3/2}}$$

Which is converges hence it is evident that in this case the researching result is incorrect.

Conclusion 2: In this example relaxing the monotony condition of examining function in the integral test leads to incorrect result.

Thus, having observed two illustrative examples of examining series for convergence applying Cauchy integral test it's easy to make sure that following posed in theorems conditions is exceedingly important for calculations, because relaxing even one cannot guarantee absolutely correct result.

References

1. Relaxing the Integral Test: A Challenge for the Advanced Calculus Student. Author(s): Paul Carter and Yitzchak Elchanan Solomon. Source: The College Mathematics Journal, Vol. 48, No. 4 (September 2017), pp. 290-291. Published by: Mathematical Association of America
2. Ряди. Теорія функцій комплексної змінної. Операційне числення. Практикум. (ІІ курс ІІІ семестр) / Уклад.: І. В. Алєксєєва, В. О. Гайдей, О. О. Диховичний, Л. Б. Федорова. — К: НТУУ «КПІ», 2015. — 84 с
3. Примеры и контрпримеры в курсе математического анализа: Учеб. пособие./ Шибинский В.М. – М: Высш. Шк., 2007 – 229 с

UDC 051.7

MODERN WIRELESS INFOCOMMUNICATION TECHNOLOGIES AND INFRASTRUCTURE ANALYSIS FOR IOT IMPLEMENTATIONS IN SCOPE OF SMART HOME AND SMART CITY CONCEPTS

Noskova D., Kvitka A., Osypchuk S.
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: noskova.ds1007@gmail.com, invariant17@gmail.com

АНАЛІЗ ІНФРАСТРУКТУРИ ТА СУЧАСНИХ ТЕХНОЛОГІЙ БЕЗПРОВОДОВОГО ЗВ'ЯЗКУ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ В МЕЖАХ КОНЦЕПЦІЇ «РОЗУМНИЙ БУДИНОК» ТА «РОЗУМНЕ МІСТО»

У статті наводиться аналіз інфраструктури та сучасних технологій безпроводового зв'язку для Інтернету речей в межах концепції «Розумний будинок» та «Розумне місто».

The Internet of Things (IoT) trend has wide scope of applications today [1, 2]. Number of sensors that connected to the network is continuously growing. IoT is a network concept that consists of physical devices that have sensors, as well as hardware and software that allow transmission and data exchange between physical world and Internet.

The infrastructure of any IoT system, regardless of concept, can be characterized by the logical model with levels as presented on Fig. 1, where each level is realized depending on applied problem for which the IoT network is implemented. Some levels may be absent, depending on the task and implementation of the IoT network.

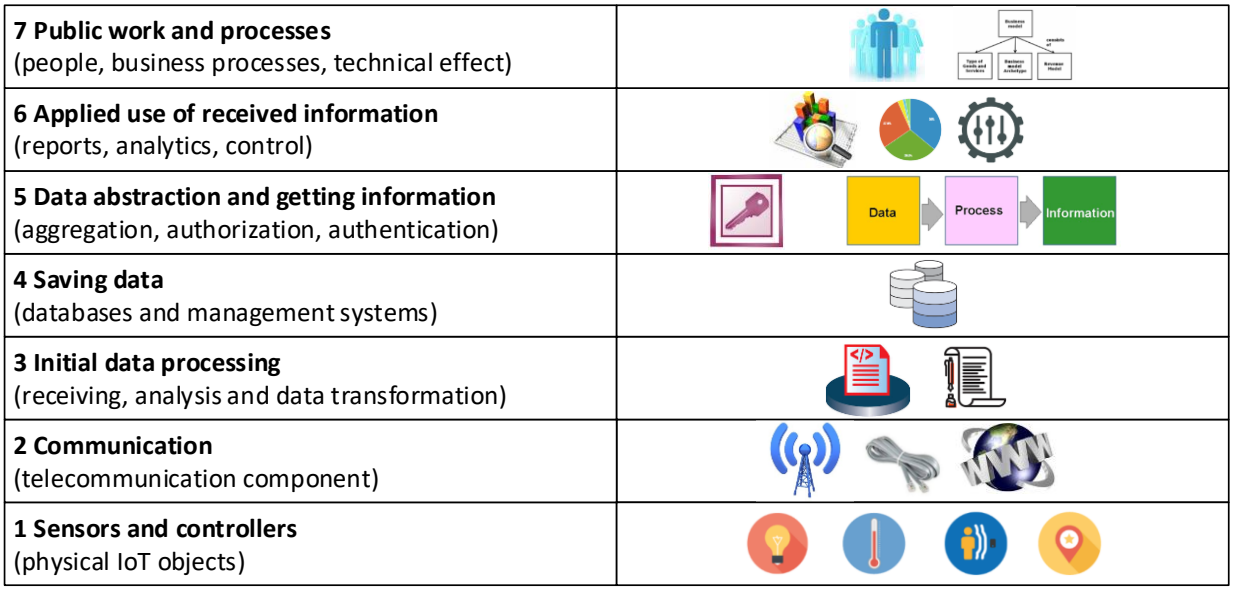


Fig. 1. Logical levels of IoT architecture

Fig. 2 represents a generalized IoT infrastructure for various concepts and applications. Depending on the task, architectural components may be present or absent; at the same time, each architecture component can be realized by different

technologies and approaches. For example, the choice of telecommunication technology for transmitting data from sensors to the data center can be made based on the chosen concept, the number of sensors and location, frequencies of data transmission, the nature of data and its volume, etc.

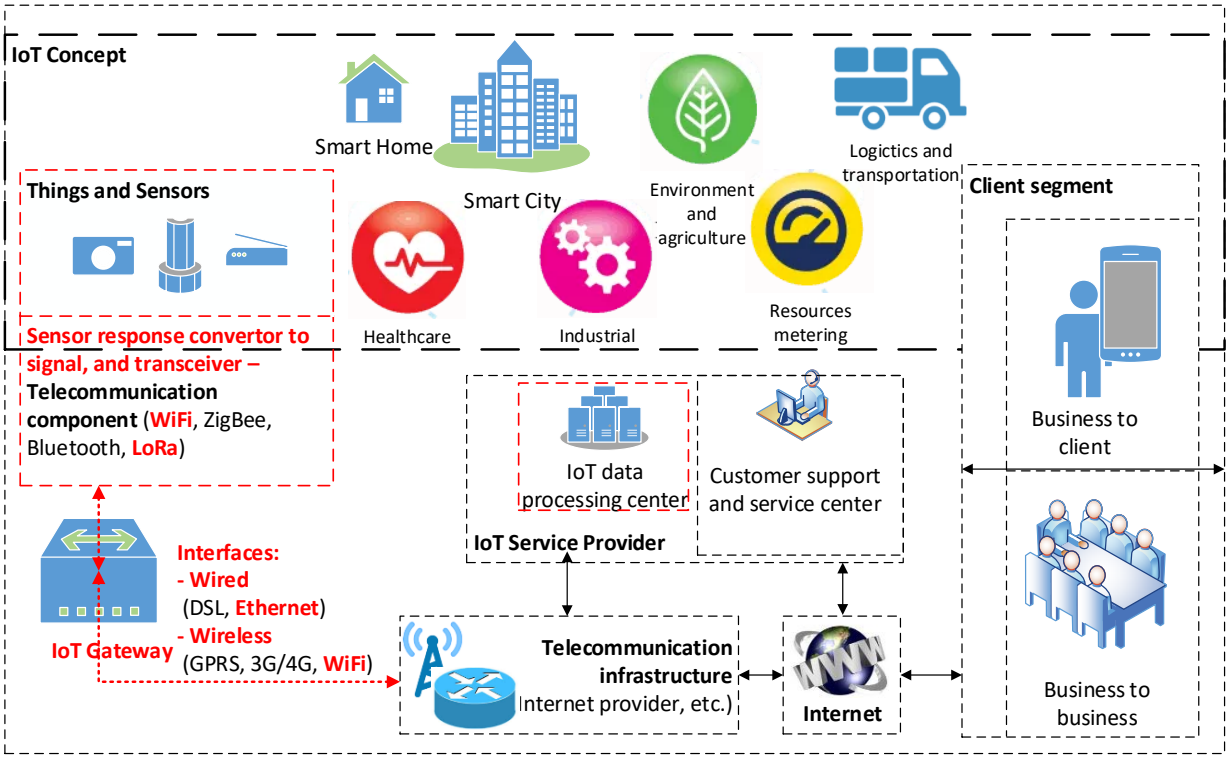


Fig. 2. Generalized IoT infrastructure

Telecommunication component. IoT implementations use wired technologies, but the most often – they use wireless low-power data transmission technologies, which include small-, medium- and long-radius technologies (WPAN, WLAN, LPWAN), for instance [3]:

- LPWAN: LoRaWAN, SIGFOX, Cellular Internet of Things (CioT) – EC-GSM, LTE-M, NB-IoT;
- WLAN: WiFi (IEEE 802.11);
- WPAN: 6LoWPAN, ZigBee, Z-Wave, Bluetooth.

Depending on the IoT concept, a certain telecommunication component implementation is being selected. For example, for implementation the concept “smart home”, the Bluetooth, ZigBee or WiFi can be selected, while for the “smart city” concept it is better to choose technologies like LoRaWAN, SIGFOX, for the possibility to cover areas with a significant radius what WLAN technologies are not able to cover due to known technical reasons.

It’s important to bring attention that the **Infocommunication** term is relevant and valid for telecom technologies used for IoT network and applications, because data from sensors is not only transmitted, but also is being used for analysis, research, processing and obtaining certain information, what brings a certain result and benefits, and promotes the adoption of decisions on control of network objects, adjusting business processes, and so on.

Data transfer protocols. For data transfer in the IoT use cases, the following application-level protocols are used: DDS, MQTT, XMPP, AMQP, JMS, CoAP, REST/HTTP – depending on the features of the solution and the necessary functionality and software compatibility, which is realized for transmitting, receiving and processing data from IoT sensors.

IoT concepts. The most common concepts and applications are "Smart House" (SH), and "Smart City" (SC). There are many other IoT concepts and applications, such as manufacturing, agrarian industry, logistics, environmental monitoring, medicine and many more [4]. **SH** is a system of home devices that connect to the data network and perform certain daily tasks with or without user's involvement: turning on the light, regulating the air conditioning, monitoring the unauthorized invasion, informing about fire or water leakage, etc. **SC** is a city that uses modern technologies to improve the life quality in it. There are five main components of SC: Energy, Water, Buildings, Government, Transportation.

IoT issues. It's possible to highlight couple major problems in IoT. **Compatibility** – compatibility of systems, interfaces and data transfer protocols. There is no single system or regulator that defines common development rules currently, what creates a large number of different solutions and compatibility problems when things are being integrated into a single network [5]. **Security** – the problem of protecting IoT networks from unauthorized third-party interference or information falsification. Thus, there are many developed technical solutions for authentication, authorization, encryption, secure sessions on hardware and software levels in hands of IoT, but still there are cases of unauthorized penetration to IoT systems with consequent brought harm of various sizes. **Readiness for IoT implementation** – readiness for innovations acceptance in the form of IoT, and their implementation in life. SH or SC concepts can be implemented and operate for the benefit purposes only when there is understanding of the specific such a need, the feasibility of such systems, and therefore – it is necessary to have a willingness to make such innovations real and get a positive impact of their work, which is not always takes place.

Saying all above, we can confidently say that IoT have a place in our life, but what kind of IoT will have a place and how quickly in time metrics – that's a reasonable question. IoT opens up many possibilities for us, and it is necessary to wisely use it. At the same time, infocommunication technologies play an essential role in the construction of the IoT, so far as without the infocommunication component there neither Internet not IoT would existing today.

References

1. IoT on Wikipedia https://en.wikipedia.org/wiki/Internet_of_things .
2. Що таке smart city: в світі та в Києві https://hmarochos.kiev.ua/2015/07/22/shho-take-smart-city-v-sviti-ta-v-kiyevi/
3. IoT Communication Technologies Guidebook https://www.postscapes.com/internet-of-things-technologies/
4. IoT solutions in Telecom industry https://www.kaaproject.org/telecom/
5. IoT RELATED STANDARDS http://standards.ieee.org/innovate/iot/stds.html.

УДК 621.391

COGNITIVE ARCHITECTURE OF THE 5G SYSTEM BASED ON THE INTERACTION OF TERRESTRIAL AND SATELLITE COMPONENTS

Drobina O.S.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: oleg.drobina.job@ukr.net

Когнітивна архітектура системи 5G на базі взаємодії наземної та супутникової складових

На сьогоднішній день спостерігається швидке поширення мобільних додатків, стрімке збільшення трафіку бездротової передачі даних та посилення інтеграції бездротового зв'язку у багатьох аспектах повсякденного життя. Це викликає необхідність розгортання мобільних мереж, які можуть підтримувати експоненціально зростаючий трафік бездротової передачі даних. У роботі пропонується гібридна супутниково - наземна мережа, яка забезпечує більш високу швидкість передачі даних та менше енергоспоживання порівняно з сучасними стільниковими архітектурами LTE та LTE-Advanced.

Nowadays, there has been a rapid expansion of mobile applications, a rapid increase in wireless data traffic and increased integration of wireless in many aspects of everyday life. This calls for the deployment of mobile networks that can support exponentially growing wireless data traffic. The hybrid satellite - terrestrial network, which provides higher data rates and lower power consumption compared to the current LTE and LTE - Advanced cellular architecture, is proposed in the work.

The increasing demand for data in mobile communication networks has resulted in the need for developing sufficient and advanced network infrastructures to support higher capacity and data rate. The forecasts in [1] shows that by 2018 the mobile data traffic will be 6.3 times higher than it was in 2013. In addition to this, the global CO2 emissions of the mobile communications sector are expected to rise to 178 Megatons in 2020 [2]. The main concept under investigation in this paper is the separation of the control (C)-plane and the user (U)-plane in the Radio Access Network (RAN). The C-plane provides ubiquitous coverage via the macro cells at low frequency band. On the other hand, the U-plane functionality is provided by the small/data cells at a higher frequency band, such as 3.5, 5, 10 GHz, where new licensed spectrum is expected to be available for future use. The use of such bands for small cells can lead to a significant increase in capacity, since they can offer bandwidth up to 100 MHz [3]. The C-plane and U-plane are not necessarily handled by the same node and are separated. Consequently, this gives the network operators more flexibility, since the C-plane (control/macro cells) manages UEs connectivity and mobility [4].

In this paper, a hybrid satellite terrestrial network architecture is presented, where a satellite is deployed to provide C-plane functionality, while femtocells are deployed to provide U-plane functionality.

The International Telecommunication Union (ITU) defines a “hybrid satellite terrestrial system” as the one that employs satellite and terrestrial components that are interconnected, but operate independently of each other [5]. In systems like this, terrestial and satellite components can use different frequency bands and use separated mannagment systems. An illustration of the proposed Hybrid network is shown in Figure 1.

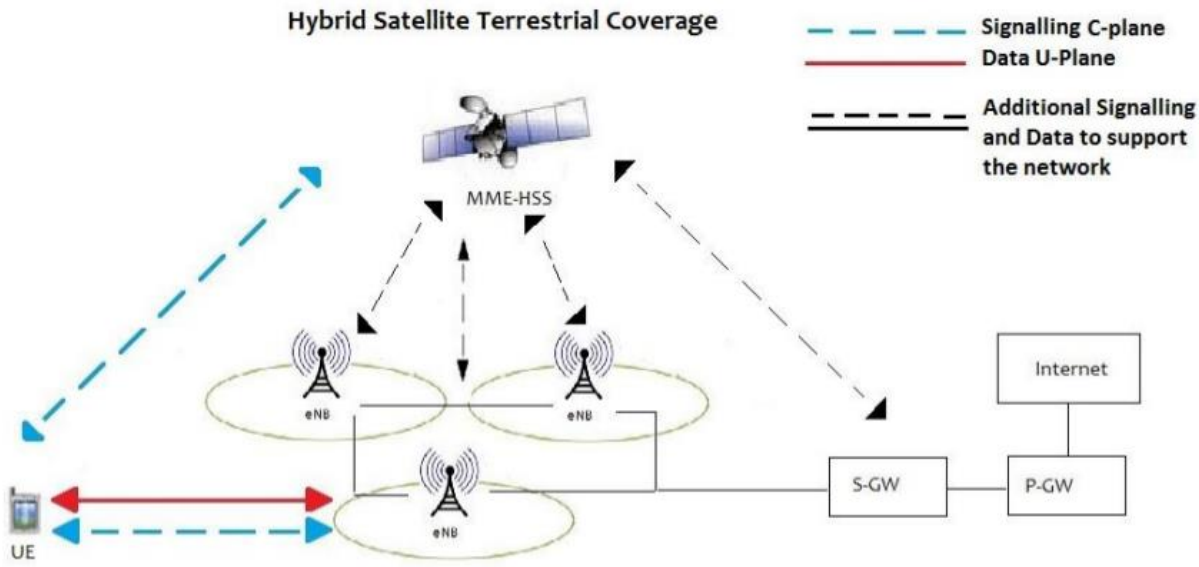


Fig. 1. Hybrid satellite terrestial system architecture

The satellite can provide a coverage of the whole terrestial network and it is also used as a Home Subscribers Server (HSS). It means that satellite caries information about the subscribers. Satellite can also communicate with a backbone network, like Serving Gateway (S-GW) and can be used as a Mobility Managment Entity (MME), in other words it can be responsible for mobility managment of users.

The terrestial part consists of femtocells/eNBs that are connected via fibre optic network. Fibre optic connection can also be used to connect eNBs with a backbone network. This type of connection minimises loses and provides fast data transfer among femtocells. The reason for having two paths for the C-plane communication is that for some User Equipment (UE) activities, signalling from both the U-plane (eNB) and the C-plane (satellite) are required for successful operation. For example, power coordination and handover procedures require accurate measurement, which cannot be provided through the satellite channel due to high latency.

The main advantage of separating the C-plane from the U-plane in cellular networks is the ability to replace part of the resources reserved for the signalling of the U-plane, with actual data. In general, the complete separation of the two planes is not possible, due to the fact that some of the C-plane functionalities have to be in the U-plane to support the reliability of the actual data transmission. But, in general, the main idea is to give the satellite component all the controlling procedures and give data transmission procedures to the terrestial component.

In order to provide the efficiency of the perfomance of this architecture there is goin to be a simulation in Matlab where two main equations are going to be used:(1) that is used to be Friis equation considering Gt =10dB and Gr =1.5dB as the typical antenna gains of the transmitter and receiver respectively, Pr = -80 dBm for the minimum receive power, λ the wavelength, and d the distance of the satellite orbit from the earth user (36,000 km for GEO and 800 km for LEO) and (2) that is used to be Shannon's equation where B = 20 MHz the available bandwidth per cell, No = -174 dBm/Hz the noise spectral density and Io the interference produced by the neighboring active eNBs assuming that the requirement of having and existing line-of-sight (LOS) path between the UE and the satellite is satisfied.

$$P_t = \frac{P_r}{G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2} \quad (1) \qquad C_{per_user} = B\log_2(1+\frac{P_r}{N_0 B + I_0}) \quad (2)$$

The performance requirements for a mobile technology to be considered as 4G or beyond 4G, must comply with the requirements of the International Mobile Telecommunication (IMT) Advanced standard. These requirements suggest that the average spectral efficiency must be greater than 2.2 bits/s/Hz, and also the C-plane latency for the transmission from RRC_IDLE to RRC_CONNECTED state, must be less than 100msec [6].

As a result, the proposed Hybrid Satellite Terrestrial architecture should give encouraging results towards its consideration for possible deployment in future mobile networks. The hybrid architecture, compared with state of the art technologies, should also give the highest capacity per square meter and the lowest power consumption per square meter for wireless transmission purposes. Moreover, the technical specifications of the proposed architecture should comply with the 4G standards.

References

1. W. Rupert, (21 October 2013). Mobile data will grow 6.3 times between 2013 and 2018 and growth will be strongest outside Europe and North America. [Online] Available: http://www.analysysmason.com/AboutUs/News/Insight/Mobile-data-Oct2013/ [Accessed: 18 August 2014].
2. M. Gruber, O. Blume, D. Ferling, D. Zeller, M.A Imran, E.C. Strinati.: EARTH—Energy Aware Radio and Network Technologies. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications , pp. 1-5, Sept. 2009.
3. H. Ishii, Y. Kishiyama, H. Takahashi.: A novel architecture for LTE-B :C-plane/U-plane split and Phantom Cell concept. IEEE Globecom Workshops (GC Wkshps), pp.624-630, Dec. 2012.
4. A. Zakrzewska, D. Lopez-Perez, S. Kucera, H. Claussen.: Dual connectivity in LTE HetNets with split control- and user-plane. IEEE Globecom Workshops, pp.391 396, Dec. 2013.
5. K. Sooyoung, K. Heewook, A. Do Seob.: A Cooperative Transmit Diversity Scheme for Mobile Satellite Broadcasting Systems. Advanced Satellite Mobile Systems, ASMS, pp.72-75, Aug. 2008.
6. ITU Radiocommunication Sector (ITU-R).: ITU global standard for international mobile telecommunications "IMT-Advanced". [Online] Available: http://www.itu.int/ITU-R/index.asp?category=information&rlink=imt-advanced&lang=en.

UDC 004.72:621.39

MAPREDUCE CALCULATING MODEL ON MOBILE DEVICES

Pavlenko V.M.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: ghostor2011@gmail.com

MapReduce обчислювальна модель на мобільних пристроях

Ця стаття пояснює використання найновішої моделі програмування, яка робить велику кількість операцій обчислення паралельно на мобільних пристроях, де програма працює в ізольованому програмну середовищі без особливих потреб і емулює мобільний пристрій таким же потужним, як і ПК.

This article explain the use of the newest programming model that makes big number of operations calculating in parallel on mobile devices, where program runs in sandbox without specific needs and simulate mobile as powerful as PC.

The technology of distributed calculations are gaining popularity about 5 years already. It is caused by the global connection of a large number of computer devices to the Internet, which, in turn, allows the nodes to connect with each other. The idea is based on the statement, that modern electronic machines do not use the whole processor power of their core (RAM, main processor) and spend energy irrationally. The vocation of such technology is the system's loading of various simple tasks during the downtime of the operating system, not blocking application software of root user at the same time. The task is performed as a low-priority background process, taking up to 10% of productivity at parallel work with processes on behalf of the user, and up to 45% when the operating system goes into standby mode.

The nodes, working within one project, receive tasks from the main server, which initially divides the complex task into parts, then sends it to the nodes for execution, and after a set time t_{exec}, begins to collect the processed information by nodes in a single response. The server itself is a unique link in the work of this technology, and needs fine tuning. Unlike it, working units can be different

configuration and even do not know about the existence of each other. This architecture feature allows you to use not only commonly accepted desktops, but also other gadgets, equipped with 32 or 64 bit processors.

Choosing a mobile platform (mobile phones, tablets, smart watches) as nodes of the distributed calculated system has several advantages:

- High performance for simple tasks
- Gadget Mobility
- Simplicity of application settings and creation
- Ability to use a large number of nodes
- Permanent online status due to widespread 3G connection
- Lots of downtime (in standby mode)
- Ability to uniquely identify the node by the gadget parameters (IMEI, GUID, Serial Number, mobile operator card number).

Schematically, the Distributed Calculation System is a network of linked nodes and a server in the Internet, using the popular Http protocol. The system consists of a server, written and working on the Node.js technology, that simplifies the binding of nodes and work with the Internet protocols, and several nodes, connected via WiFi and 3G with various mobile operating systems (iOS and Android). The server, responsible for dividing, mailing and bonding a task, must have a reliable access to the Internet, because it also has to monitor the state of the node and the progress of the calculation. There is also a software snap-in on a mobile client, which carries out the acceptance of the task, sending for processing and formatting the response for further sending to the main node.

After the dispatching of tasks and processing them on the nodes, the gluing to the general answer by the method, reversed to division of a task is performed on the server.

The difference between these processes is that at the gluing stage the completeness and relevance of the data is also checked by the unique identifier of the device. This stage includes an analysis of the node's operation (availability of the online status) and the need to re-send the lost part of the response repeatedly to

another free working node in case of a sudden disconnection of the previous node, engaged in processing this part of the task.

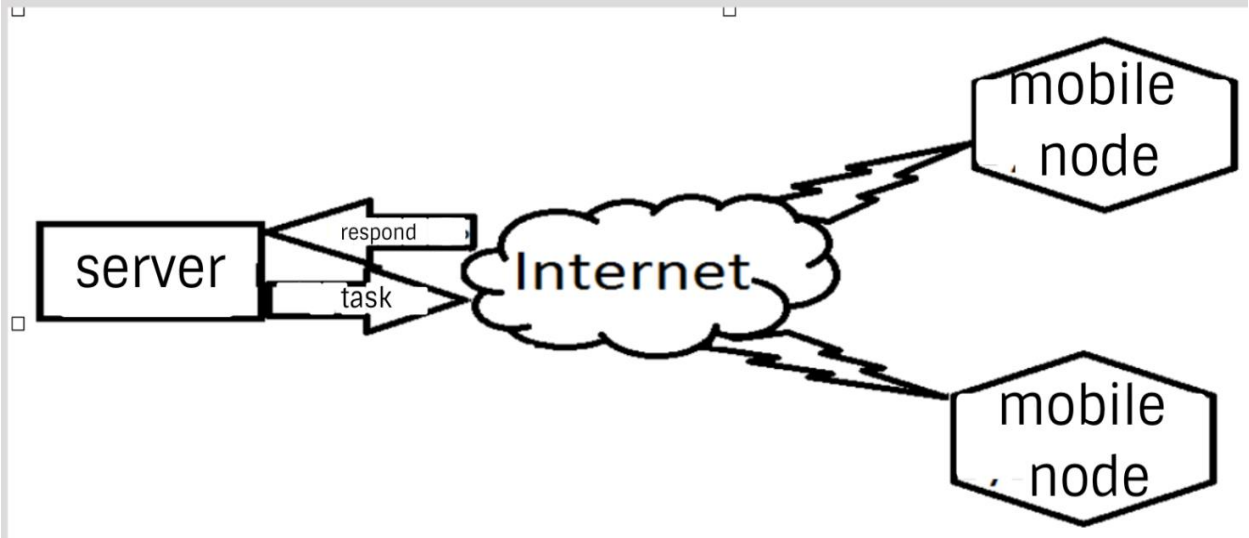


Fig. 1. Distributed Calculating Network Scheme for mobile nodes.

For such a system there has been developed an application on popular mobile platforms - iOS and Android - which can be downloaded from the app store for each operating system, in accordance. It is to perform data receiving, processing, sending and formatting in the form of an answer for easy gluing by the server.

Thus, the use of mobile devices to carry out bulky and long-term calculations as small and medium-sized networks has several advantages over the use of stationary computers, namely: longer downtime of the operating system and standby time, an easy access to the Internet, easiness of platform configuration for tasks execution, centralized distribution system.

References

1. Jeffry Dean and Sanjay Ghemawat (2014). MapReduce: Simplified Data Processing on Large Clusters. Google, Inc.
2. University of California, Barkeley. Source: http://wla.berkeley.edu/~cs61a/fa11/lectures/communication.html.
3. R. G. Gallager, P. A. Humblet, and P. M. Spira (January 1983). "A Distributed Algorithm for Minimum-Weight Spanning Trees".
4. Hamilton, Howard. "Distributed Algorithms". Retrieved 2013-03-03 .

UDC 621.396

LTE TECHNOLOGY FOR SMART GRID COMMUNICATION WITH QOS SUPPORT

Yarosh B.Y.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: gdanyaro@gmail.com

Технология LTE для Smart Grid Communication с поддержкой QoS

В этой статье рассматривается использование технологии LTE для Smart Grid Communication. Рассматриваются приоритеты пользователей в Smart Grid в соответствии с необходимыми для них параметрами QoS.

In this paper, the use of LTE technology for smart grid communication is presented. The priorities of users in the Smart Grid in accordance with the necessary QoS parameters for them are considered.

The Smart Grid (SG) purpose is to meet the needs of modern information grid by utilizing advanced communication technology into the power grid. How to use wireless communication technology to provide better guarantee for smart grid has become the center of the problem in mobile communication research. Proposed by the 3-rd Generation Partnership Project (3GPP), Long Term Evolution (LTE) is one of the most widely accepted technologies in smart grid wireless communication network. It is the long-term evolution of 3G network technology which provides high transmission rate and reduces system transmission delay. In order to make better use of LTE in the smart grid communication environment, some optimization must be implemented.

The LTE system is usually composed of an access network, a core network, an application layer and certain number of UEs. The UE establishes a wireless link with the eNodeB through the Uu interface to obtain an access to the Evolved Packet Core (EPC). In the smart grid communication environment, the application layer mainly refers to the power management station and UEs are considered to be AMI devices, e.g. smart meters and aggregators. These devices, which require LTE system, are very different from traditional LTE users. In the traditional LTE network, UE, with certain mobility, doesn’t have the burst flow and consider the fairness of the system. While in the SG communication environment, UE, e.g. smart meter, is always set in initialized locations, and in most cases its data transmission (including upload and download streams) is strictly periodic. On the other hand, the SG communication environment can be classified as a machine-to-machine (M2M) system. Figure 1 shows the structure of an SG-LTE network.

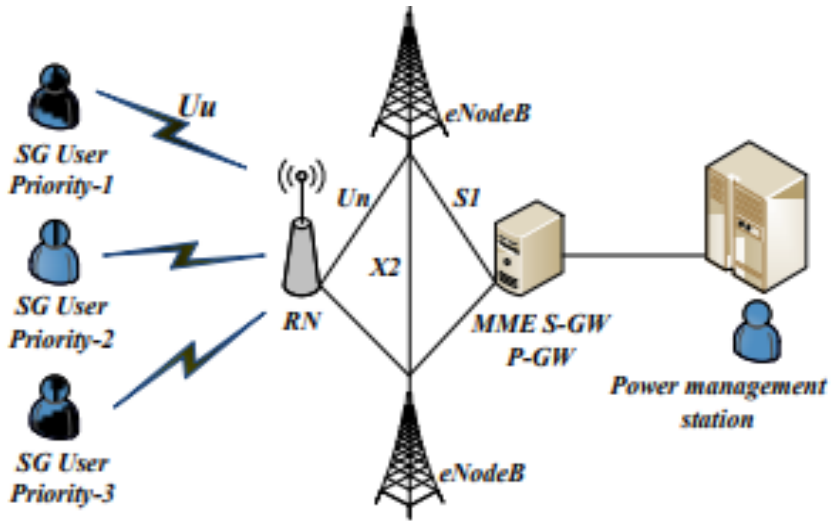


Figure 1: System structure of SG-LTE network

The architecture of scheduler in LTE system is shown in Figure 2. In the downlink LTE cell system, a single cell model is composed of a base station and a plurality of users. eNodeB transmits data through the downlink time-varying channel. In the Media Access Control (MAC) layer, the packets from the upper layer of eNodeB are buffered in the First In First Out (FIFO) queue, and then packets are transmitted to the different users through the resource allocation controller. The scheduler can make full use of channel status information, data buffer queue status, QoS requirements and other information to decide which user will be scheduled. The user measures the Signal to Interference plus Noise Ratio (SINR) of the downlink channel between the eNodeB and user as the basis for the quality of channel state at the next resource allocation. Resource Block (RB) is the scheduling unit in LTE system. Scheduling can be considered as a mapping between users and the resource blocks, as is shown in Figure 3.

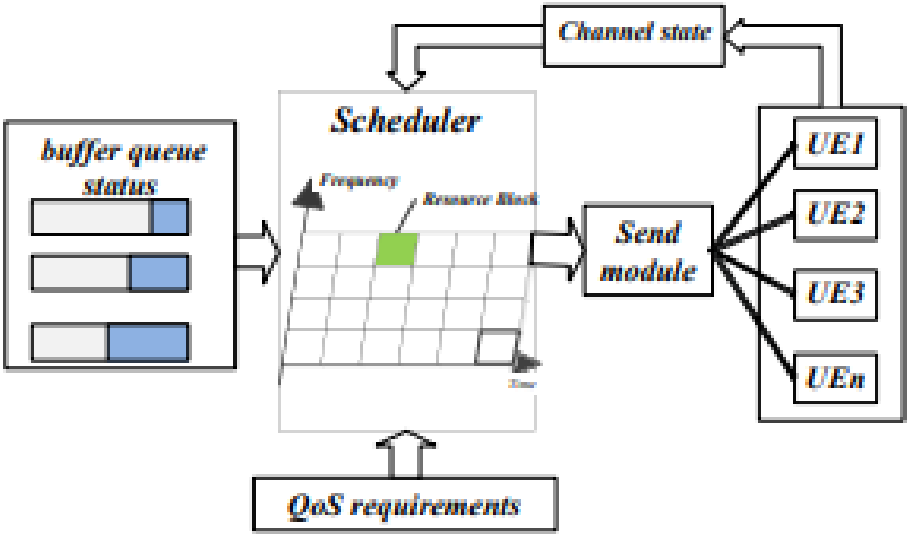


Figure 2: The architecture of scheduling system

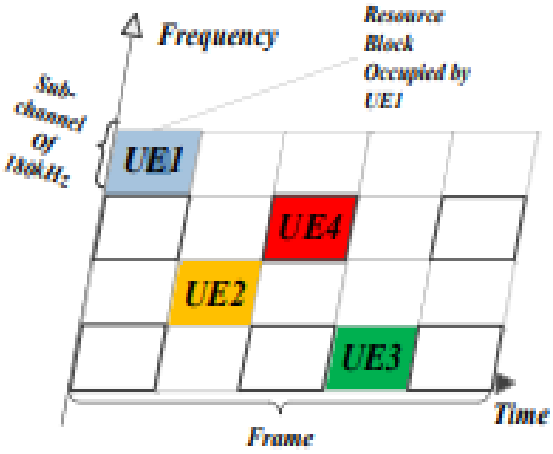


Figure 3: Resource scheduling for UE

In the SG communication environment, the main services of information contain automated smart meter reading, power distribution automation, emergency repair and others. There is a significant difference in the sensitivity of information among different users in SG. According to the user's QoS requirements, we can divide UEs into three priorities:

I) Priority-1: The user needs absolute prioritized transmission and has a high demand for transmission rate and delay, e.g. emergency repair and maintenance.

II) Priority-2: The characteristics of user's QoS requirements are low delay, high reliability, low probability of interruption, e.g. visualization management of mobile asset, distribution automation.

III) Priority-3: Delay requirements are very loose, e.g. automated smart meter reading.

The difference of average throughput, delay, packet loss rate and fairness index among different priority users, that verifies the effect of the proposed scheduler in the given scenario. This improvement is significant in smart grid communication based on LTE network.

References

1. R. Webster, K. Munasinghe and A. Jamalipour, "Optimized resource allocation in LTE networks incorporating delay-sensitive smart grid traffic," 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, NSW, 2016, pp. 423- 428.
2. A. S. Mushtaq, A. Z. Haider, L. Orest and K. Mykhailo, "Improving QoS in MAX C/I scheduling using resource allocation type 1 of LTE," The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv, 2015, pp. 12-14.
3. R. K. Pandey and M. Misra, "Cyber security threats — Smart grid infrastructure," 2016 National Power Systems Conference (NPSC), Bhubaneswar, India, 2016, pp. 1-6.
4. Fakhar Uddin Ahmed, Shikhar Kr. Sarma. "QoS and Admission Controller in IEEE 802.11e WLAN" 2013 4th International Conference on Intelligent Systems, Modelling and Simulation, 2013, page 468.

UDC 004.62

CHALLENGES OF PROCESSING INTERNET OF THINGS DATA

Kurdecha V.V., Trokhymenko D.V.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: theelico@gmail.com

ПРОБЛЕМИ ОБРОБКИ ДАНИХ В МЕРЕЖАХ «ІНТЕРНЕТУ РЕЧЕЙ»

Неоднорідність "речей" робить обсяг, швидкість та мінливість даних Інтернету речей такими, що створює значні труднощі існуючим інформаційним системам. Динамічність та обмежені ресурси створюють деякі проблеми, які слід вирішити для ефективного оброблення даних реального світу. В роботі було досліджено основні проблеми в обробці даних Інтернету речей.

Identifying challenges. The Internet of Things core idea can be summarized in one sentence: ‘A worldwide network of interconnected entities’. In most cases, these entities, ‘things’ have a locatable, addressable, and readable counterpart on the Internet. They can open a communication channel with any other entity, providing and receiving services at any time, any place, and in any way. Many technologies serve as the building blocks of this paradigm, such as wireless sensor networks, cloud services, machine-to-machine interfaces, and so on. Also, this paradigm has a multitude of application domains, such as automotive, healthcare, logistics, environmental monitoring, and many others. And this heterogenous and dynamic nature is what makes developing efficient processing system a challenge. The main difficulties encountered in implementing stable and cost-effective IoT solutions can be divided into several groups: structure of IoT data, determining the proper frequency of sensor readings, accounting for errors and missing readings, security and privacy.

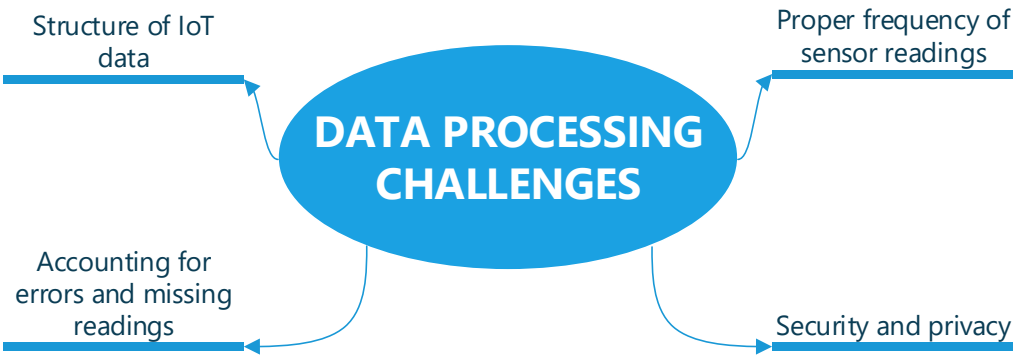


Fig. 1. IoT data processing challenges

Deceptive simplicity of IoT data. Real world data is transient, subject to environment changes and it is mostly time and location dependent. In many currently used data sources it is often necessary to identify what information was

available, how it was formatted. Ironically, this is one area where IoT sensor data can seem deceptively simple compared to these sources. Usually most sensors provide simple-formatted data. The good news is that this makes ingesting raw sensor data fairly straight forward to quickly go from a raw feed to a dataset or table that is ready for further work. Main problem arises after the ingestion of the raw data, due to it being heterogenous, most importantly in fields of how this data should be processed and stored.

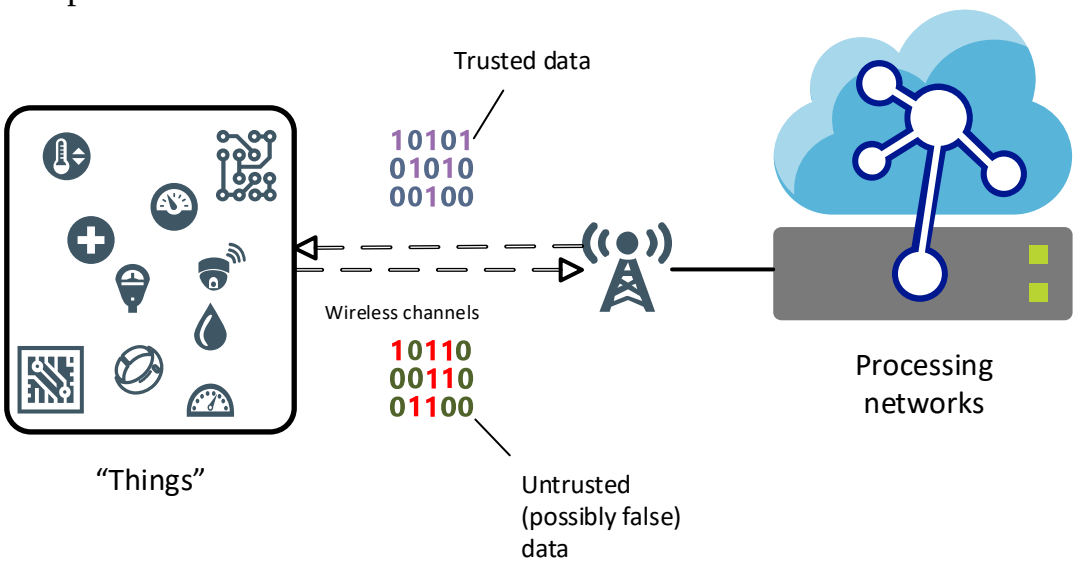


Fig.2 Sample IoT network layout

Determining the proper frequency of sensor readings. With large volumes of data, efficiency of storage and data handling mechanisms become a key challenge, especially considering heterogenous nature and dynamicity of the data sources. Depending on the application, a streamed sensory data could be stored either temporarily or for greater spans of time. So, designing and implementing repositories that enable publishing and accessing the needed data in large distributed and dynamic environments while also providing efficient indexing and discovery mechanism is important issue for IoT. More efficient mechanism on information search and retrieval, indexing, query, and information access will be required to address the issues in this field. However, the solutions for handling, maintaining, and processing the data also need to be scalable and efficient. As a result, due to these limitations it is necessary to determine what data should be gathered and actually has value for the application it is used in. Cloud and fog computing clearly are promising technical approaches that address some of these challenges. It requires the assess each metric to prevent acquiring useless and acquire useful data.

Accounting for errors and missing readings. Inaccuracy and varying qualities in the IoT data are unavoidable. If the next readings are normal, it is easy to correct the error. But, what if a sensor gets moved into an improper position or malfunctions or fails to transmit at all? Detecting and filtering anomalies and false readings from the devices, could be done with quality related attributes of the IoT data, that can help detect errors, and retrieve and process the data according to different quality requirements. But current methods may suffer from over-relying

on assumptions about data. Using correlation can often impose non-existent correlations between sensors that leads to worse estimation as a result. In general, on one hand, the exactness of assumption-based models directly affects the accuracy of prediction results. On the other hand, such assumptions may not hold for various datasets. So, it is necessary to find a new way to learn structures from sensor data that doesn't rely on such knowledge. Also, when data is provided by different resources, such as public sensors, trust arises as another key issue. Trustworthiness of resources, identification of the source providing the data, and an understanding of accuracy and reliability of the data, while semantics can play an important role for defining trust and reliability attributes, trust model development and its feedback and verification mechanisms are major issues that need to be addressed.

Security and privacy. IoT data can often contain our environment, the status of our homes and cities, or our personal health and activities. That's why mechanisms to provide and guarantee the security and privacy of data are crucial issues in IoT. However protecting the Internet of Things is a complex and difficult task. The number of attack vectors available, such as attacks that target communication channels, physical threats, denial of service, identity fabrication, is staggering as global connectivity and accessibility are key points of the IoT. And, the inherent complexity of the IoT, where entities can easily exchange information with each other, further complicates the design and deployment of efficient, inter-operable and scalable security mechanisms. As data is communicated over the Internet and can be shared with different parties and users, it is also important to define appropriate access control mechanisms, e.g., who can use the data, what part of the data they can use, when and where they can use the data. Further development of IoT will also be highly dependent on developing reliable and efficient solutions that can support and maintain security and privacy requirements in resource-constrained environments with various types of devices and communication networks as a part of the IoT design.

Conclusion. To sum everything up, in a near future the creation of a system that will address all of the issues is rather unlikely. Because humanity still needs cheap, fast and reliable data gathering and processing systems. So, for now we have to have tradeoffs, like in choosing sensors and data ingestions method to save either storage space or prolong sensor lifetime. And for determining which tradeoffs should be taken due to nature of IoT data many factors should be taken into consideration considering, but not limited to type, size, location or other.

References

1. Barnaghi, P., Wang, W., Henson, C., & Taylor, K. Semantics for the Internet of Things: early progress and back to the future. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *8*(1), 1-21. (2012)
2. Shao, Yongshuai, and Zhe Chen. "Reconstruction of Missing Big Sensor Data." *arXiv preprint arXiv:1705.01402* (2017).
3. Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." *Computer Networks* 57.10 (2013): 2266-2279.

УДК 621.396.9

THEORETICAL RESEARCH AND PRACTICAL DESIGN OF IOT TESTBED SOLUTION BASED ON ESP8266 SOC AND BLYNK COMPONENTS

Chekunov M., Osypchuk I., Kyrashchuk V., Osypchuk S.
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: osypchuk_ivan@i.ua

Теоретичне дослідження та практична імплементація тестового IoT-рішення на базі плати ESP8266 та сервера Blynk

Робота відображає результати попереднього теоретичного й послідовного практичного проектування експериментального IoT-девайсу, зконструйованого на базі модуля ESP8266, що підтримує стандарт IEEE 801.11, та серверної технології Blynk. Отримані дані дозволяють зробити висновки стосовно можливості використання наявного експериментального макету при роботі як одного IoT-датчика, так і декількох різних датчиків одночасно.

The Internet of Things, also known as IoT, refers to billions of physical devices around the world that are now connected somehow (to the Internet, for example), collecting and sharing data. IoT adds a decent level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate without us, people, being involved, and merging the digital and physical worlds this way [1].

The IoT is more than some kind of convenience for consumers. It offers new sources of data and different business operating models that can boost productivity in a variety of industries: health care, manufacturing, retail, telecommunications, transportation, utilities and others. The proposed IoT architecture used in current work, is presented on Fig. 1.

Internet of Things applications have diverse connectivity requirements in terms of range, data throughput, energy efficiency and device cost. WiFi is often an obvious choice because in-building WiFi coverage is almost ubiquitous, but this is not always the appropriate choice due to high energy consumption and high data rate what is not necessary in most cases of IoT applications. Anyway, WiFi was selected as a wireless technology for IoT testbed as it met the financial and goal purposes [2].

A number of standards based and proprietary last mile connectivity options have evolved to service IoT, and each has advantages and limitations. A reference table of telecom technologies available for IoT connectivity is shown in Table 1. WiFi, or 802.11, is a wireless protocol that was built with the intent of replacing Ethernet using wireless communication over unlicensed bands. Its goal was to provide off-the-shelf, easy to implement, easy to use short-range wireless connectivity with cross-vendor interoperability. WiFi, while being the obvious choice for IoT, has big limitations in both range and energy efficiency [3].

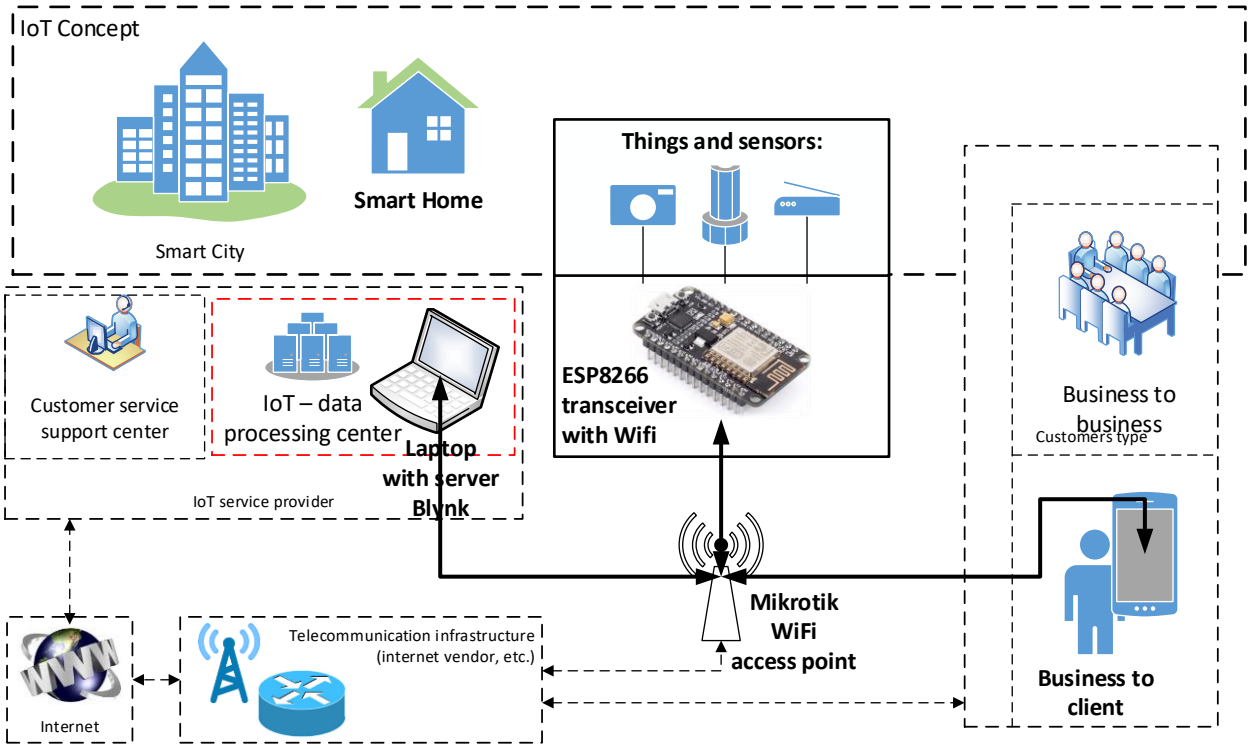


Fig. 1. The proposed and considered IoT architecture used in current work. Bold connections show the implemented part of architecture: WiFi access point, sensors, transceiver, laptop with server application, client terminal with application

Table 1. IoT connectivity technologies

Technology	Network	Standards based or Proprietary	Range	Throughput	Energy requirement	Adoption
LoRa	LWPA	Proprietary (Semtech)	High	Low	Low	Moderate
NWave	LWPA	Proprietary (NWave)	High	Low	Low	High
RPMA	LWPA	Proprietary (OnRamp Total Reach)	High	Low	Low	High
SigFox	LWPA	Proprietary (SigFox)	High	Low	Low	Moderate
LTE-M	3GPP/LTE	Standards based (3GPP)	High	High	Low	Upcoming
NB-IoT	3GPP/LTE	Standards based (3GPP)	High	Moderate	Low	Increasing
NB-LTE	3GPP/LTE	Standards based (3GPP)	High	Moderate	Low	Upcoming
Bluetooth	Bluetooth	Standards based	Moderate	Low	Moderate	Limited Wearables
ZigBee	802.15.4	Standards based (802.15.4)	Low	High	Moderate	Limited PAN & Home
Thread	802.15.4	Standards based (802.15.4)	Low	High	Moderate	Upcoming
Z-wave	Proprietary	Proprietary (Sigma Design)	Low	Low	Moderate	Very Low
WiFi	802.11	Standards based	Moderate	High	High	Very high
HEW	802.11ax	Standards based	Moderate	High	Moderate	Upcoming

As a result, eventually we assembled the test mock-up of the IoT device. It was decided to make it based on the ESP8266 module using the IEEE 802.11 standard. In general, the experimental scheme was created according to the architecture described earlier on Fig. 1, specifically the part highlighted in bold solid line and connections. So we used several sensors: light sensor, temperature and humidity sensor, door opening/closing sensor. All these sensors are able to work simultaneously on the same module [4].

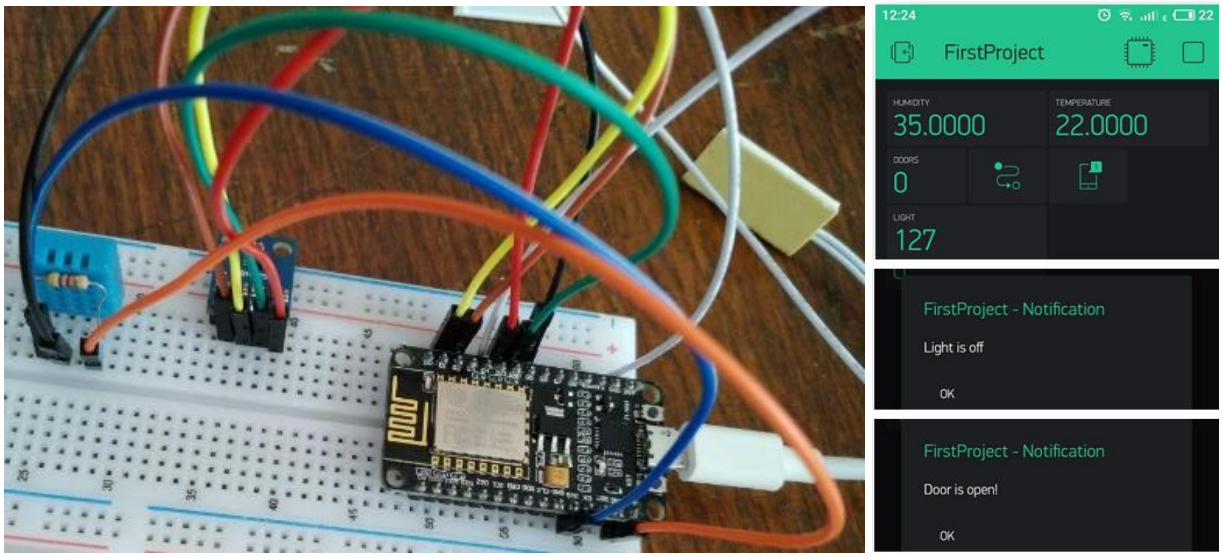


Fig. 2. The developed testbed with sensors based on ESP8266 module using the IEEE 802.11 standard for data transmission, and mobile terminal screen that shows responses and notifications from sensors

The information from the sensors goes to the Blynk server through the Wi-Fi module. Blynk server deployed on the laptop. Then, using the Blynk program, we authenticated the smartphone in the experimental IoT network. So we were able to track all data from sensors in real time directly from the phone, and IoT data stored on the database of Blynk server. The photo of the ESP8266 module working at that moment of the time is shown on Fig. 2.

So, in this work the possible case of IoT solution for smart home concept was designed, configured and implemented; the working testbed is presented. Such solution might be scaled either horizontally or vertically, with other telecommunication technologies used – for specific use cases.

References

1. Chih-Yung Chang, Chin-Hwa Kuo, Jian-Cheng Chen, Tzu-Chia Wang, "Design and Implementation of an IoT Access Point for Smart Home", Applied Science.
2. Daniel Minoli, Kazem Sohraby, Jacob Kouns, "IoT security (IoTSec) considerations requirements and architectures", CCNC 2017 14th IEEE Annual.
3. M. Schwartz, Internet of Things with ESP8266, Packt Publishing Ltd.
4. M.H. Habaebi, N.I.N.B. Azizan, "Harvesting WiFi Received Signal Strength Indicator (RSSI) for Control/Automation System in SOHO Indoor Environment with ESP8266", 2016 International Conference on Computer and Communication Engineering (ICCCE).

UDC 004.72

CLUSTERING METHOD MODIFICATION FOR CONTINUOUS MONITORING IN WIRELESS SENSOR NETWORKS

Kurdecha V.V., Kuzimovych M.M.
National Technical University of Ukraine
*"*Igor *Sikorsky Kyiv Polytechnic Institute"*
E-mail: vt14m@yandex.ua, kuzimovich8@gmail.com

МОДИФІКАЦІЯ МЕТОДУ КЛАСТЕРИЗАЦІЇ ДЛЯ БЕЗПЕРЕРВНОГО МОНІТОРИНГУ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

У статті описується модифікація методу кластеризації сенсорних мереж, що здійснюють постійний нагляд за активними подіями, головна ідея якої полягає у використані поняття прилеглих, суміжних датчиків, взаємно покриваючих зон моніторингу при побудові кластерів для підвищення достовірності отриманої інформації та енергоефективності усієї мережі.

Energy efficiency increasing is the most important issue for wireless sensor networks, which is composed by sensor devices purely limited in power. Solution of this problem were presented in different articles, most of them – by clustering method usage and its modification [1].

But the main aim of monitoring applications built on the grounds of wireless sensor networks is to detect some event and send actual and accurate information to users with minimally possible energy consumption. More often than not the detected event may spread to a larger region or/and may change its location (Figure 1, a-b).

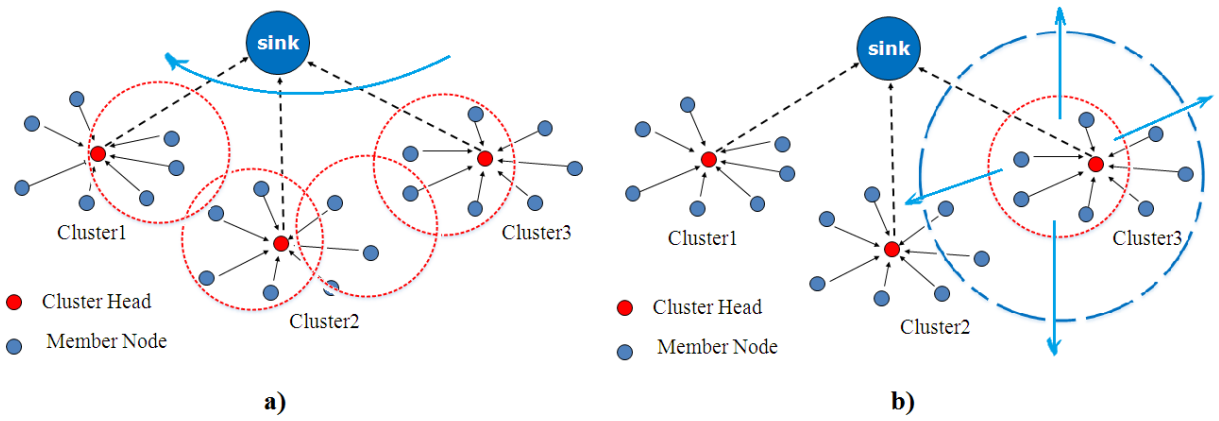


Fig. 1. Event migration (a) and extension (b) example

So it is needed to propose such modification of existed clustering method, which will be focused on continuous monitoring with possibly event fluctuation.

Modification in the form of an energy-efficient 2-logical-coverage overlapping clustering is described in this article. It is designed to adapt to event fluctuation, which ensures that data collected by adjacent sensors in the event area are sent to the same CHs for fusion. Once the event spreads to neighboring regions,

a collaborative CH re-adjustment and cluster migration technique is used to ensure effective cluster formation associated with a 2-logical overlapping clustering.

Both single-hop (LEACH) [2] and multi-hop (hierarchical cluster-based routing algorithm, DEECIC) [3] clusters are formed independent of event developments, which are not suitable for dynamic continuous monitoring applications.

In proposed modification, a novel 2-logical-coverage cluster formation scheme and cluster migration scheme are designed to form and activate proper clusters according to event development. The overlapping cluster formation operation is illustrated in Figure 2. Firstly, non-overlap clusters are formed similar to traditional cluster formation schemes, as in Figure 2 (a). Secondly, each node chooses the next-closest cluster head (CH) to form the 2-logical-coverage overlapping clusters, as in Figure 2 (b).

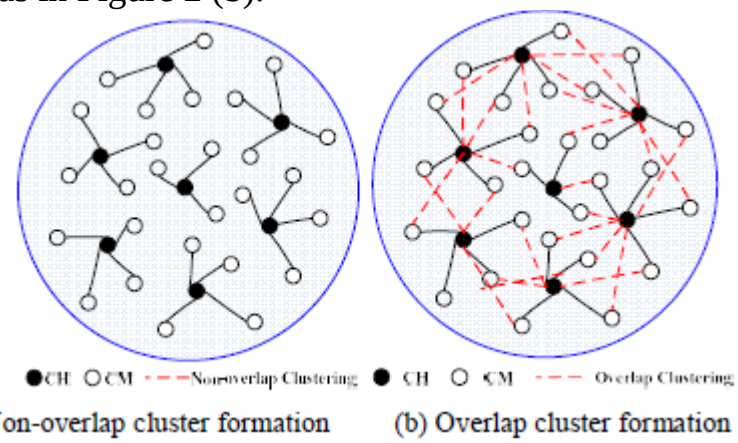


Fig. 2. Cluster formation with 2-logical coverage overlaps

Whole network is divided into 2-logical-coverage subnets - each node belongs to two adjacent clusters simultaneously. The role of boundary nodes includes two aspects: as 1-hop forwarding nodes when the single hop clusters are combined into 2-hop clusters; as alarm nodes to indicate the moving direction of the event.

Cluster migration step with event moving and expanding is provided the next way - for cluster i, suppose the number of boundary nodes in its u_{th} (u = 1, 2, ..., k_0) overlapping area is m^u_i , the reading of the pth sensor at the sampling instant t is $r_p(t)$. Hence, the difference of average reading at the adjacent sampling instant t and (t+1) in the u_{th} overlapping area (denoted as Δr_u（t + 1)) is

$$\Delta r_u(t+1) = \frac{1}{m_i^u}\sum_{p=1}^{m_i^u}(r_p(t+1) - r_p(t)). \tag{1}$$

The difference of average reading at sampling instant t between the u_{th} and v_{th} overlapping areas in cluster i (denoted as $\Delta q_{uv}(t)$) is

$$\Delta q_{uv}(t) = \frac{1}{m_i^u}\sum_{p=1}^{m_i^u} r_p^u(t) - \frac{1}{m_i^v}\sum_{p=1}^{m_i^v} r_p^v(t). \tag{2}$$

The parameter Δr_u indicates whether the detected event will expand. When the reading of a sensor is above lower boundary value r_0, an event is detected in the

network. If Δr_u decreases continuously, the event may disappear sooner. Most of the sensors in these areas will go into the sleep mode while a few of them transmit the sensed data at a low frequency for network connectivity. The parameter Δq_{uv} indicates the motion direction of the event. If Δq_{uv} decreases continuously, it means that the event will move to the adjacent cluster and all sensors of it should go to active monitoring mode.

When the event spreads to a larger area, the adjacent 1-hop clusters are combined into a 2-hop cluster via the boundary nodes. As shown in Figure 3, at the beginning, the event area is covered by the blue chain line cluster. Once the event spreads to a larger area, the three green dotted line clusters will combine with the blue one to form a 2-hop cluster. The nodes can communicate with CH directly or through the nearest boundary nodes. The boundary nodes aggregate the forwarding data and send it to CHs. If the event spreads to an even larger region, more than one 2-hop clusters are combined to ensure all the event development is detected.

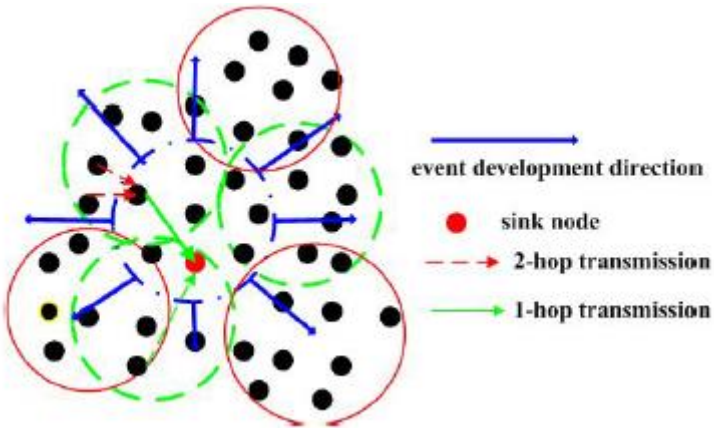


Fig. 3. Cluster migration with event expansion

Conclusion. In this paper, a clustering method modification for dynamic continuous monitoring applications is presented. The modification is that the event-based cluster migration technique is used to activate appropriate clusters for continuous monitoring via the 2-logical-overlapping clustering scheme. As a result, the cluster topology can be switched according to the event development with low energy consumption. It is concluded that the such modification provides clustering protocol to be more suitable for the dynamic continuous monitoring and more energy-efficient in comparison with other existing ones.

References

1. M. M. Afsar, M. Tayarani-N, Clustering in sensor networks: a literature survey. Journal of Network and Computer Applications, 46:198–226, 2014.
2. A. P. Chandrakasan, A. C. Smith, W. B. Heinzelman, An application specific protocol architecture for wireless micro sensor networks, IEEE Transactions on Wireless Communications, 1(4): 660–669, 2004.
3. Z. X. Liu, Q. C. Zhang, L. X., X. P. Guan, A distributed energy-efficient clustering algorithm with improved coverage in Wireless Sensor Networks, Future Generation Computer Systems, 28(5): 780–790, 2012.

UDC 621.391.3

USE OF MACHINE LEARNING TO SOLVE THE PROBLEM OF CUSTOMER CHURN

Baria A.D., Globa L.S.
National Technical University of Ukraine
“ Igor Sikorsky Kyiv Polytechnic Institute”
E-mail: baria.andrii@gmail.com

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ВИРІШЕННЯ ЗАВДАННЯ ВІДТОКУ КЛІЄНТІВ

У статті наводиться приклад застосування машинного навчання для вирішення завдання відтоку клієнтів від операторів мобільного зв'язку. Пропонується використання алгоритму на основі дерева прийняття рішень.

Today, due to competition, mobile communication operators face the problem of churn of customers. Since the cost of retaining a customer is usually less than the cost of attracting a new customer, it becomes advantageous to identify clients prone to care in advance and try to retain them using various methods, for example, by making special offers.

To date, many companies have accumulated a lot of data about their customers, which makes it urgent to apply machine learning methods to solve this problem.

The problem of the churn of customers is solved for the incoming customers, it is necessary to predict the rejection of services and to influence the customer until after he ceases to use the services of the mobile operator.

The solution to the problem of customer churn is to classify clients according to 2 groups: the client is inclined to churn or the client is not inclined to churn. If the client falls into the first group, then it must be influenced by the methods of marketing retention.

This article examines the identification of customers who are potentially inclined to churn.

Forecasting outflow can be viewed as a controlled classification problem in which the user behavior is used to train the binary classifier.

Depending on the recharge, each client can be in one of the following states: (i) new, (ii) active, (iii) inactive or (iv) churn (Figure 1) [1]. The churn of customers is always preceded by an inactive state, and since the aim of the research is to predict the churn, it is suggested to use the inactive state as a reference for forecasting the churn. In particular, we define t = 30 days, without replenishing the balance as the threshold state used to change the state from active to inactive. In

addition, we define q = 30 days without making or receiving calls, if the subscriber does not show activity during the time q, it goes into churn.

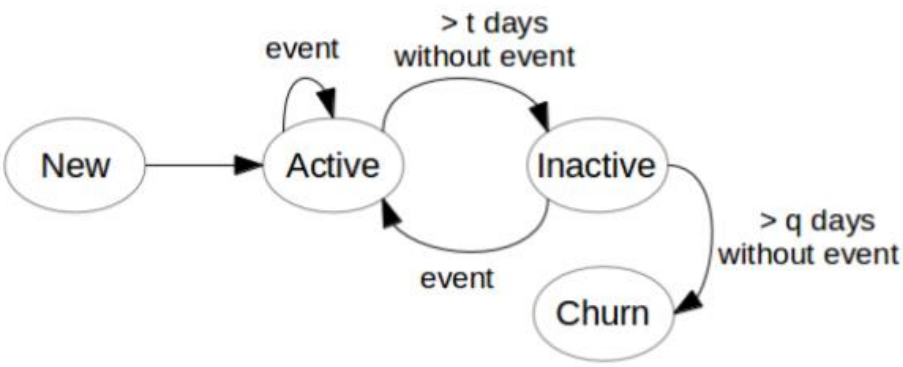


Fig. 1. diagram of possible client states based on recharge events and specific thresholds of t and q

In Figure 2 shows the scheme of the learning and prediction model. To properly train the model, you need expert sampling, which is divided into data for learning the model and data to verify the performance of the model. After that, the model is trained on the first sample and checks its performance on the second, the model is applied to real data, the results of which are used in the subsequent training and improvement of the model.

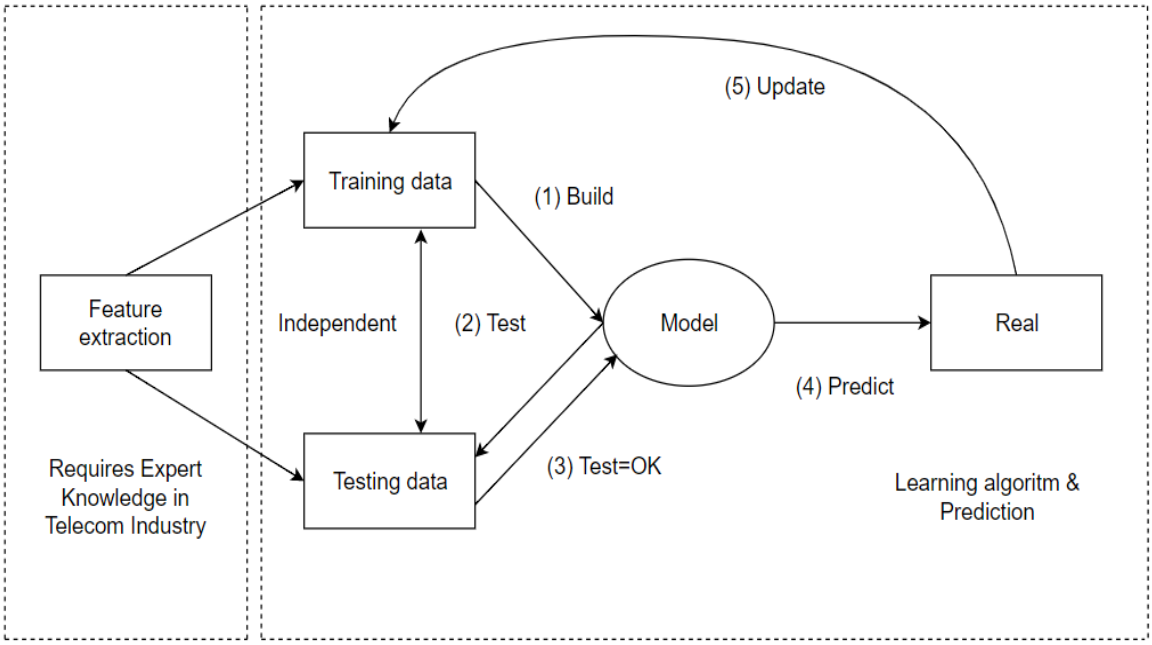


Fig. 2 The scheme of learning and predicting the model of machine learning

To implement the work of the model, an algorithm based on the decision tree can be used. The graphical representation is shown in Figure 3.

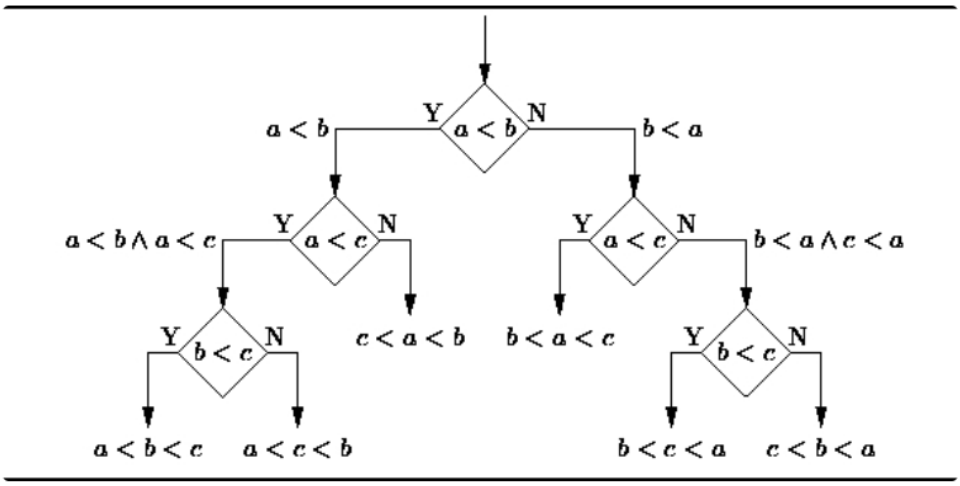


Fig. 3 Graphical representation of the tree structure

Decision trees are a way to represent rules in a hierarchical, consistent structure, where each object has a single node that provides the solution. The decision trees solve the classification problems well, requiring the assignment of objects to one of the previously known classes. The main advantage of the decision tree is that you can observe how the decision was made, unlike other algorithms, which are a "black box".

In this paper, it is proposed to use machine learning to solve the problem of churn of customers using the decision tree algorithm. To make a decision on a possible churn of customers, data are used to replenish the customer's account and make calls, in the future, to improve accuracy, it is possible to use other customer data.

References

1. F. Castanedo & G. Valverde & J. Zaratiegui & A. Vazquez (2016) Using Deep Learning to Predict Customer Churn in a Mobile Telecommunication Network.
2. C. B. Bhattacharya. (1998) When customers are members: customer retention in paid membership contexts. Journal of the Academy of Marketing Science, 26 (1) 31-44.
3. P. Kisioglu & Y. I. Topcu. (2011) Applying Bayesian Belief Network approach to customer churn analysis: A case study on the telecom industry of Turkey. Expert Systems with Applications, 38 (6), 7151-7157.
4. B. Huanh, M.T. Kechadi & B. Buckley. (2013) Customer Churn Prediction in Telecommunications. Expert Systems with Applications, 39, 1414-1425.
5. D. Chakraborty et. al. (2012) Method for Predicting Churners in a Telecommunications Network. US Patent 8194830 B2.
6. B. Eilam, Y. Lubowich & H. Lam. (2013) Method and Apparatus for Predicting Customer Churn.US Patent 8615419 B2.

UDC 004.773.5

THREAD AND DATA SECURITY ANALYSIS IN SIP NETWORK

Pasichnyk O.V.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: alexeypasichnik2.71828@gmail.com

АНАЛІЗ ЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇЇ В МЕРЕЖІ SIP ТЕЛЕФОНІЇ

В роботі досліджуються особливості забезпечення безпеки даних мережі SIP, вектори атак на мережу SIP, такі як: перехоплення реєстрації, перехоплення сесії, підміна сервера, підробка змісту повідомлення, розрив сесії зв’язку, атака типу «Відмова в Обслуговуванні» та «примноження», боти та DDoS атаки; та засоби захисту від подібного роду загроз.

Hackers approach attacks in stages, beginning with probing of the network. Hackers first look for networks with easy access. Once a vulnerability is found, it is recorded for later use. Once a vulnerability has been identified and validated, it is used later for a larger attack. It is a combination of vulnerabilities that allows hackers to reach through many different networks, traverse through all of these networks unnoticed, and launch largescale DoS attacks on unsuspecting networks. [1]

Here are listed some common methods used when attacking a SIP-based network.

Registration hijacking. Since SIP uses clear text, if a hacker can capture these messages, that hacker is able to read subscribers’ sensitive information such as their public and private identities. This information can then be used to gain access into the operator’s network. [1]

Session Hijacking. For maintaining session authorization, the cookie is used. They are generated by a server when the server is first accessed. [2] If these cookies are intercepted and copied, they allow the interceptor full access to the session already in progress. This means the hacker will have access to all of your transactions and account information. [1] This problem can be critical when open Wi-Fi hotspot is used, a cookie can be intercepted through the process of eavesdropping.

To prevent the use of this vulnerability it is possible to check the time and date stamp of an incoming request or response. When a UAS receives a request, it should check the date and time with its own internal clock. If there is a difference in time stamp with internal clock (more than 30 minutes, for example), then it is very likely that the message was intercepted and has been relayed with a changed destination address. [3]

Impersonating a Server. In SIP networks DNS is used to identify the IP address for domains and their applications. [2] In case if DNS records are changed either

both a subscriber and an operator could be redirected to hacker`s server, which in this case will impersonate itself as trusted leading to data leakage.

Tampering with Message Bodies. a hacker may capture an *INVITE* message from a subscriber and change the *FROM* header to reflect his own address. This would provide the hacker access to a network he is not authorized to use and would allow him to initiate sessions with other subscribers while pretending to be someone else [1].

Tearing Down Sessions. Hackers could intercept requests from various subscribers and send a *BYE* message as a response [2]. This would then terminate the session and cause it to be torn down. It is much easier to execute than regular DoS as it requires only one proxy to be hacked however it may cause same result – impossibility to make a call in whole network region.

Denial of Service. DoS attacks can take many different forms and can be launched using many different techniques. The most common is flooding the network with specific traffic types. For example, using a call generator, a hacker can send millions of *INVITE*s into the network attempting to flood the network with call requests [1]. Another form of DoS attack involves application servers [2]. By launching a flood of requests to an application server, the network element is immediately flooded and congested, taking it out of service. This can also happen with the DNS through flooding with DNS queries. When the DNS is attacked, the entire network can be impacted, depending on where the server sits within the DNS hierarchy and whether or not redundancy has been implemented. [3]

Amplification SIP allows registering multiple identities within single user [2]. Utilizing this feature hacker can register a subscriber listing many different user identities for the same subscription. This then provides the registrar with a list of multiple destinations for a request. The hacker then launches requests toward the public identity, which the registrar and proxies then send to multiple destinations based on the registration made by the hacker [1]. Similar result can be accomplished through making registrar to run out of memory. It is done by registering many different identities. The way to prevent this could be different levels of authentication, preventing unauthorized subscribers from accessing the registrar.

Bots and DDoS Attacks. *Bots* are scripts that in different ways are carried to a subscriber’s device then listening opened TCP/UDP sockets and distributing themselves through them. When one hacker successfully launches bots, they create their own little network of bots known as botnets which on demand generate traffic to a single network element resulting in Denial of Service (Distributed DoS)[3]. The main concern is that the botnet in its idle state is hard to track also the user equipment is infected rather than the provider equipment and safety measures are relied on the end user which tends to neglect them.

Good security solution should meet the following requirements:

1. Thread management efficiency
2. Transparency, security measures should not interfere with the end user.

Main aspects of secure SIP network are authentication, authorization, monitoring [3].

Authentication requires the use of passwords and the exchange of credentials. Each time the subscriber registers in the network, the registrar needs to carry out the procedure of initial registration [2].

Authorization requires high performance database containing basic information about the user, including the levels of access to different services. [3]

Monitoring include means that allow operator to have total visibility to every network transaction that takes place. This includes any downloads that the subscriber may have made.

Encryption should be performed, however not all headers are encrypted but only those that do not contain information about the destination and the source of the message because this would lead to the impossibility of the exchange of messages between routers without distribution of encryption keys [3].

Transport Layer Security (TLS) is a good means of providing encryption between networks, while SIP Secure (SIPS) [2] is designed for use within a trusted domain. TLS works at the TCP layer and is best when used between two networks where two network elements do not know each other [4]. To encode voice messages Secure Real-time Transport Protocol should be used [5].

TLS is to be used at proxies, redirect proxies, and registrars when interconnecting with other networks. They should also possess a site certificate for authentication. These proxies also must have the ability to validate certificates from other trusted sites, by storing the certificates from these sites [6].

Another approach to encryption is tunneling a SIP message within another SIP message. The original SIP message is encrypted and then encapsulated within another SIP message for routing. The routing information from the original SIP message is used to populate the routing headers in the outside message, but nothing else is given in the outside message. When the User Agent Server compares the encapsulated message with the outer message, it will identify whether or not there have been any other alterations to the original message [1].

Strict routing. With strict routing, the routing path is recorded as the subscriber registers in the network. The REGISTER message contains the RECORD-ROUTE headers, used to collect the addresses of each of the proxies in the path. These addresses are saved in the order they were added, so that a route list can be established for the subscriber. The route list then becomes part of the subscriber's registration. Stateful proxies in the path then also store the route list for the subscriber so that they know how to route messages (both requests and responses) to the user identity. Even if a hacker attempted a session hijack, for example, the proxies would ignore the routing provided in the message, relying instead on the route list they recorded for the subscriber during the registration [1].

Intrusion detection. Effective monitoring can be accomplished through an intrusion detection system which can operate in real time (or near real time) or historical mode. A real-time system is needed for detecting attacks while they are in progress. However, these systems should also have some capacity of storage to allow for the investigation of network events at a later time. The IDS identifies the source of data (the network, application, or host). It performs analysis on the traffic based on rules (policy) and could also have the ability to establish its own policy

through neural technology. Since IDS systems are passive, they are unable to actively exchange encryption keys and negotiate these keys with other network elements [7].

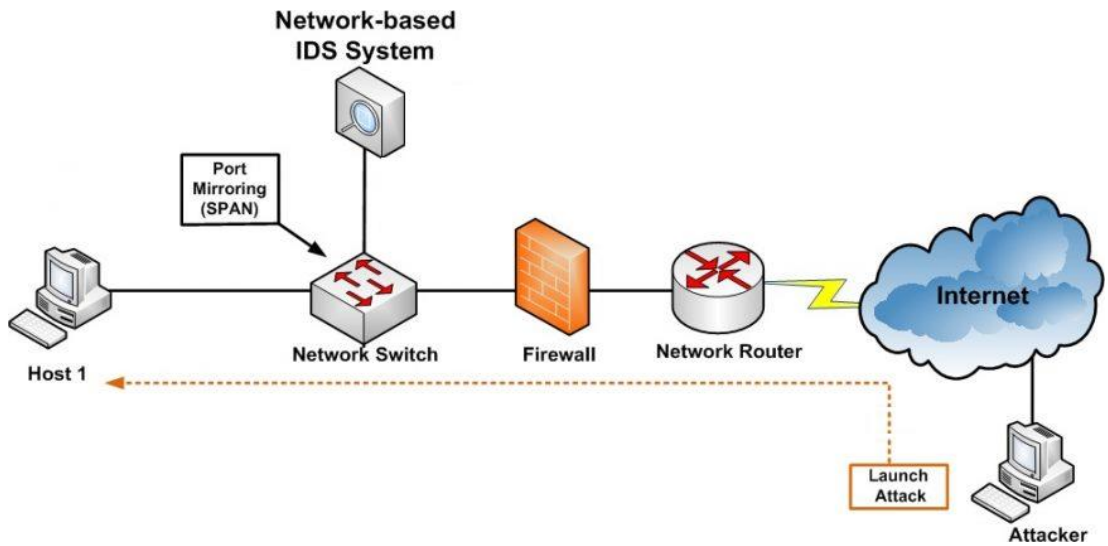


Fig 1. IDS System implementation

Considered attacks are aimed at the SIP signaling and its network equipment. The consequences of an attack could be leaking user's personal data to third parties, a compromising of user actions based on it personal identities and disabling network by overusing its elements with both authorized or unauthorized access. The consequence of such actions is operator money losses, during idle of service and losses of users. From the above it can be concluded that the implementation of network security is the first responsibility for an operator. However, it should be noted that no measures can completely protect the network so the main method to protect data is to create conditions under which the invasion into the network is not economically viable for an attacker.

References

1. McGraw-Hill Communication Series, "Session Initiation Protocol (SIP): Controlling Convergent Networks", 1st Edition, p.133-156
2. J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, T. Haukka "Security Mechanism Agreement for the Session Initiation Protocol (SIP)" RFC 3329, January 2003
3. Porter, Thomas; Andy Zmolek; Jan Kanclirz; Antonio Rosela "Practical VoIP Security. Syngress" 2006.
4. Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1," RFC 4346, April 2006
5. D. McGrew, D. McGrew, M. Naslund, E. Carrara, K. Norrman "The Secure Real-time Transport Protocol" RFC 3711, March 2004
6. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol" RFC 3261, June 2002
7. Amoroso, Edward, "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response," Intrusion.Net Books, Sparta, New Jersey, 1999.

UDC 004.273

FUZZY LOGIC USAGE FOR THE DATA PROCESSING IN THE INTERNET OF THINGS NETWORKS

Kurdecha V.V., Ishchenko I.O., Zakharchuk A.G. Kunieva N.V.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: ivanishchenkoo@gmail.com

ВИКОРИСТАННЯ НЕЧІТКОЇ ЛОГІКИ ДЛЯ ОБРОБКИ ДАНИХ У МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

Перевантажена мережа Інтернету Речей потребує обробки даних для аналізу залежності стану системи від вхідних параметрів. При роботі з великими обсягами даних вже недостатньо простого та статистичного аналізу даних. Метою роботи є визначення найбільш ефективного методу кластеризації для систем, які призначені для визначення якості зв’язку, за рахунок проведення аналізу існуючих методів кластеризації у нечітких системах. В статті розглянуто різні типи кластеризації нечітких систем, які підходять до використання в різних телекомунікаційних систем. У результаті аналізу алгоритм нечітких с-середніх вибрано як найефективнішим за критерієм обчислювальної складності, для кластеризації у мережах визначення якості зв’язку.

An overloaded Internet of Things (IoT) network needs data processing to analyses the state of the system from the input parameters. When working with large volumes of data, there is not enough simple and statistic data analysis. The purpose of the work is to determine the most effective clustering method for systems that are intended to determine the quality of the connection by analyzing existing cauterization methods in fuzzy systems. In the article various types of clustering of fuzzy systems that are suitable for use in various telecommunication systems are considered. As a result of the analysis, the algorithm c-means is selected as the most effective by the criterion of computational composition, for clustering in the networks of determining the quality of communication.

Modern computing and distributed information systems (for example, cloud computing systems, networks based on the dynamic architectures of VANET and MANET, smart-type networks, intelligent controllers and sensors networks, etc.) are complex telecommunication networks that include many different types of network devices, which are integrated into a single information and computing block, work with high network load. These networks are sources of large volumes of data and they support a large number of reconfigurable connections. An overloaded Internet of Things (IoT) network needs data processing to analyses the state of the system from the input parameters.

A huge data sets in the IoT networks

For the implementation of the Internet of Things systems, we need to further develop specialized methods put forward for such systems. Goals that can be used for verification and transmitted in accordance with the rules included in the system. The usual mathematical methods are too complicated for IoT systems, so there is a need for simpler algorithms that can provide the quality of the received technical solutions. In addition, it is important that during the adoption of IoT systems, it is often not possible to use Boolean logic, because sometimes it is not possible to describe the system parameter with two possible states [2].

The usage of cluster analysis algorithms is aimed at dividing the set of data into clusters so that each of them has the closest objects [3]. Fuzzy clustering is one of the most interesting methods for identifying possible groups and testing hypotheses about the data structure. There are a number of clustering techniques. The main methods of fuzzy clustering: fuzzy decision trees, fuzzy Petri nets, fuzzy self-organizing maps [4].

Algorithm of fuzzy self-organization c-means

Purpose: clustering large sets of numeric data.

Advantages: fuzzy when assigning objects to the cluster, allows you to identify objects that are on the border of the cluster.

Disadvantages: computational complexity, specifying the number of clusters at the input of the algorithm, there is uncertainty with objects that are significantly removed from the centers of all clusters.

In the classical algorithm of k-means (c-means), elements are chosen using the ordinary Euclidean distance between the vector x and the center of the cluster c. In this case, the quality of clustering can be significantly improved by using an improved version of the self-organization algorithm, which is called the Gustavsson-Kessel algorithm.

Fuzzy decision trees

Fuzzy decision trees are used in Data Mining to solve classification problems and to solve the regression problem when it is necessary to know the degree of belonging to a particular outcome [5]. They can be used in various fields: in banking for solving the problem of scoring, in medicine for diagnosing various diseases, in the industry for quality control of products and so on.

Unconditional advantage of this approach is the high accuracy of classification achieved by combining the advantages of fuzzy logic and decision trees. The learning process takes place quickly, and the result is simple for interpretation. Since the algorithm is capable of issuing for the new object not only the class, but also the degree of belonging to it, it allows to control the classification threshold.

Fuzzy Petri nets

In the Petri time networks, conditions are represented by a set of positions, and their execution is represented by marking the corresponding position [5]. Auxiliary reduction methods are used, which make it possible to reduce the size of the Petri net while preserving its properties, and the decomposition that divide the source network into subnets. A feature of Petri nets is the possibility of presenting fuzzy processes and the dynamics of their interaction. The disadvantage is that many parameters, indicators and characteristics are not taken into account, without which it is difficult to imagine the real processes of practical implementations.

CONCLUSION. All of the considered algorithms have a common disadvantage of the algorithm complexity and this is very important as the IoT network has a rigid frame of time delays in processing information, obtaining conclusions, etc. Because of this problem, an approach is taken to form the basis of fuzzy knowledge base which allows using previously obtained knowledge about the behavior of the system or process, which allows us to do the analysis of data based on certain rules.

Thus, the analysis of the mathematical methods of data analysis that can be carried out in IoT systems allows us to consider that different data analysis methods allow you to obtain different data, which in turn are close to real ones, which is evidence that all these algorithms can be used in different systems. The algorithm c-means is selected as the most effective by the criterion of computational composition, for clustering in the networks of determining the quality of communication.

References

1. R. Lea, M. Blackstock, Smart cities: An iot-centric approach, in: Proceedings of the 2014 International Workshop on Web Intelligence and Smart Sensing, IWWISS’14, ACM, NewYork, NY, USA, 2014, pp.12–15.
2. M. Nikravesh, Evolution of fuzzy logic: From intelligent systems and computation to human mind, Stud. Fuzziness Soft Comput. 2007, pp. 37–53.3. J. G. Proakis, Digital Communication, 4th ed. Boston, MA: McGraw-Hill, 2000.
3. G. Cueva-Fernandez, J. Pascual Espada, V. Garc´ıa-D´ıaz, R. Gonzalez Crespo, Fuzzy decision method to improve the information exchange in a vehicle sensor tracking system, Appl. Soft Comput. 2015, pp. 708–716.
4. Sugeno M., Yasukawa T. A fuzzy-logic-based approach to qualitative modeling // IEEE Trans. on Fuzzy Systems, 1993, vol. 1, pp. 7–31.
5. Emami M.R., Turksen I.B., Goldenberg A.A. A unified parameterized formulation of reasoning in fuzzy modeling and control // Fuzzy Sets and Systems, 1999, vol. 108, pp. 59–81.

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НДІ ТЕЛЕКОМУНІКАЦІЙ

Десята Міжнародна науково-технічна конференція студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ»

Присвячено Дню науки та Всесвітньому Дню телекомунікацій

16–20 квітня 2018 року

Тези конференції

м. Київ

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ ПРІТС-2016

Співголови конференції:

ІЛЬЧЕНКО М.Ю. – науковий керівник Інституту телекомунікаційних систем, проректор з наукової роботи Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», академік НАНУ, д.т.н., професор;

ЯКОРНОВ Є.А. – заступник директора Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського, к.т.н., професор;

ГАВРИЛЮК В.В. – голова студентської ради Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського.

Члени наглядового комітету:

БУНІН С.Г. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ГЛОБА Л.С. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
КАТОК В.Б. - к.т.н., проф., ПАТ «Укртелеком», Київ;
КРАВЧУК С.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ЛИСЕНКО О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
МАКСИМОВ В.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
МІНОЧКІН Д.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
МОШИНСЬКА А.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
НАРИТНИК Т.М. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ПРАВИЛО В.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
РОМАНОВ О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
СКУЛИШ М.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ТЕРНОВОЙ М.Ю. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ТРУБАРОВ І.В. – к.т.н., доц.., КПІ ім. Ігоря Сікорського, Київ;
ТРУБІН О.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
УРИВСЬКИЙ Л.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ШЕЛКОВНІКОВ Б.М. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ЯВІСЯ В.С. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ.

Члени програмного комітету:

Авдєєнко Г.Л., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Афанасьєва Л.О., асистент каф. ТК, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Валуйський С.В., к.т.н., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Курдеча В.В., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Новіков В.О., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Новогрудська Р.Л., к.т.н., КПІ ім. Ігоря Сікорського, ІТС, Київ;
Прищепа Т.О., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Штогрина О.С., к.т.н., КПІ ім. Ігоря Сікорського, ІТС, Київ.

ОГЛЯД ПЕРСПЕКТИВНИХ ТЕХНОЛОГІЙ ФОРМУВАННЯ СИГНАЛІВ ДЛЯ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ КАНАЛІВ СИСТЕМ СУПУТНИКОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ

Ткаченко Н.К.
Науковий керівник: **Авдєєнко Г.Л.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: nikitargets@gmail.com

Сьогодні найбільш популярними та широко використовуваними супутниковими технологіями є стандарти DVB-S2 та DVB-S2X. Але використання спектру в цих технологіях не є максимальним. Цей факт ставить перед нами завдання створити нові енергоефективні стандарти. І інноваційні шляхи розвитку, запропоновані компанією Novelsat, з більш енергоефективними стандартами (NS3 і NS4).

OVERVIEW OF ADVANCED SIGNAL GENERATION TECHNOLOGIES FOR INCREASING THE CAPACITY OF CHANNELS OF SATELLITE TELEVISION BROADCASTING SYSTEMS

Tkachenko N.K.
Scientific adviser: **Avdeenko G.L.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: nikitargets@gmail.com

Today, the most popular and commonly used satellite technologies are the DVB-S2 and DVB-S2X standards. But the use of the spectrum in these technologies is not the maximum. This fact raises the task of creating new, more energy efficient standards. And innovative new ways of development offered by Novelsat company with its more energy-efficient standards (NS3 and NS4).

СИСТЕМА ВНУТРЕННЕГО ПОЗИЦИОНИРОВАНИЯ, КАК LOCATION- BASED SERVICE

Куклина А.С.
Научный руководитель: **Романов А.И.**
Институт телекоммуникационных систем, КПИ им. Игоря Сикорского, Украина
E-mail: kuklina_as@ukr.net

Сегодня спутниковые системы навигации являются наиболее точным методом определения местоположения, но для решения задачи геоопределения в помещениях рассматривается концепция Системы внутреннего позиционирования, Indoor Positioning System, IPS. Статья основана на описании шагов улучшения определения местоположения мобильного устройства в рамках здания. Проведено сравнение технологий, используемых в IPS.

INDOOR POSITIONING SYSTEM AS LOCATION-BASED SERVICE

Kuklina A.S.
Scientific adviser: **Romanov O.I.**
Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: kuklina_as@ukr.net

Today, satellite navigation systems are the most accurate method of locating, but for the solution of the problem of geo-determination in buildings, the concept of the Indoor Positioning System, IPS, is considered. The article is based on the description of steps to improve the location of a mobile device within a building. Comparison of technologies used in IPS.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ОБРОБКИ ДАНИХ В РОЗПОДІЛЕНОМУ ДАТА ЦЕНТРІ

Прокопець В.А.
Науковий керівник: **Глоба Л.С.**
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vprokopets95@gmail.com

Досліджено можливості використання технології NFV для мережі LTE. Проаналізовано ефективність методу динамічного розподілу ресурсів у віртуалізованій мережі мобільного оператора України з підвищенням енергоефективності обробки даних. Створена імітаційна модель віртуалізованого ядра EPC у середовищі MATLAB.

EXPERIMENTAL RESEARCH OF ENERGY-EFFICIENT DATA PROCESSING IN DISTRIBUTED DATA-CENTER

Prokopets V.A.
Scientific adviser: **Globa L.S.**
Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: vprokopets95@gmail.com

Main capabilities of using NFV technology for LTE network were investigated. Efficiency of energy-efficiency increasing dynamic resource allocation method in virtualized Ukrainian cell operator network was analyzed. Virtualized EPC core MATLAB imitational model was created.

OVERVIEW ON THE MAIN FACTORS, WHICH HAVE IMPACT ON DATA TRANSFER QUALITY IN LTE NETWORKS

Gritsko A.V.
Scientific adviser: **Gatturov V.K.**
Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: allahrytsko@gmail.com

This article defines main reasons of data transfer quality loss in LTE mobile networks and ways to decrease this impact in order to have appropriate quality of service and quality of subscriber’s experience. It analyzes the key factors that affect the quality of data transmission in the LTE network. This influence should be taken into account by the telecom operators during the deployment of the network in order to improve the quality of the services provided, to combat the outflow of subscribers and the corresponding economic effect.

ОГЛЯД ОСНОВНИХ ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА ЯКІСТЬ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ LTE

Грицко А.В.
Науковий керівник: **Гаттуров В.К.**
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: allahrytsko@gmail.com

Ця стаття визначає основні причини втрати якості передачі даних в мобільних мережах LTE та способи зменшення цього впливу, щоб мати належну якість обслуговування та якість досвіду абонента. В ній проаналізовано основні чинники, які впливають на якість передачі даних в мережі LTE. Цей вплив необхідно враховувати операторам зв'язку під час розгортання мережі задля підвищення якості наданих послуг, боротьби з відтоком абонентів і відповідним економічним ефектом.

RESTORING TRANSFER MESSAGES BASED ON NETWORK TRAFFIC ANALYSIS

Bilokha D.K.
Scientific adviser: **Pravilo V.V.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: belohadk97@gmail.com

In this paper, have been described the possibilities of restoring transfer messages based on network traffic analysis. Also, have researched the problems of the transmission protocols, the variety of possibilities saving them and creation of the automation system of providing information of the data.

ВОССТАНОВЛЕНИЕ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Белоха Д.К.
Научный руководитель: **Правило В.В.**
Институт телекоммуникационных систем,
КПИ им. Игоря Сикорского, Украина
E-mail: belohadk97@gmail.com

В работе рассматриваются возможности восстановления передаваемых сообщений основанных на анализе данных собранных в сети. Также были рассмотренны проблемы различных протоколов передачи, различные возможности сохранения данных и возможность построенния автономной системы предоставления информации о данных.

ДИНАМИЧЕСКАЯ МОДЕЛЬ УПРАВЛЕНИЯ ОЧЕРЕДЯМИ ОСНОВАННАЯ НА РАСПРЕДЕЛЕНИИ СЕТЕВОГО РЕСУРСА

Лебеденко Т.Н.
Научный руководитель: **Лемешко А.В.**
Кафедра инфокоммуникационной инженерии
Харьковский национальный университет радиоэлектроники, Украина
E-mail: tetiana.lebedenko@gmail.com

В работе предложена динамическая модель управления очередями основанная на распределении сетевого ресурса. Расчетные решения, полученные в ходе использования предложенной модели, позволили обеспечить согласованное решение таких задач как: распределение потоков пакетов между сформированными на интерфейсе маршрутизатора очередями; агрегирование потоков пакетов в соответствующие очереди на основании соизмеримости классов; распределение пропускной способности интерфейса между отдельными очередями. Новизна модели заключается в учете динамического характера изменения состояния интерфейса маршрутизатора при распределении сетевого ресурса.

DYNAMIC MODEL OF QUEUE MANAGEMENT BASED ON NETWORK RESOURCE ALLOCATION

Lebedenko T.N.
Scientific adviser: **Lemeshko A.V.**
Department of Infocommunication Engineering,
Kharkiv National University of Radio Electronics, Ukraine
E-mail: tetiana.lebedenko@gmail.com

A dynamic model of queue management based on network resource allocation is proposed in the article. Calculation solutions obtained during the use of the proposed model allowed to provide a coordinated solution of such problems as an allocation of packet flows between queues formed on the router interface, aggregation of packet flows to the corresponding queues on the basis of commensurability of classes and bandwidth allocation of the interface between individual queues. The novelty of the model lies in considering the dynamic nature of the change in the state of the interface when distributing the network resource.

ОБМЕЖЕННЯ ДЛЯ ІСНУЮЧИХ РІШЕНЬ СИСТЕМ ПРОМИСЛОВОГО «ІНТЕРНЕТУ РЕЧЕЙ»

Давидюк А.М.
Науковий керівник: **Курдеча В.В.**
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: mr.wokawoka@gmail.com

З розвитком технологій та збільшенням кількості електронних сенсорних приладів, що використовуються на виробництві, постала гостра проблема у виборі ефективного шляху в створенні та адмініструванні відповідних сенсорних мереж. В роботі запропоновано підхід щодо застосування LP-WAN мережі для зменшення витрат та покращення масштабування IoT мереж.

LIMITATION FOR EXISTING INDUSTRIAL INTERNET OF THINGS SOLUTIONS

Davydiuk A.M.
Scientific adviser: **Kurdecha V.V.**
Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: mr.wokawoka@gmail.com

With the development of technology and increasing number of electronic sensors used in manufacturing, the acute problem of choosing an effective way to create and administer appropriate sensor networks has been arose. This paper proposes an approach that uses the LP-WAN networks to reduce costs and improve the scaling of IoT networks.

ДОСЛІДЖЕННЯ БЕЗПЕЧНОГО МЕРЕЖЕВОГО ДОСТУПУ НА БАЗІ ПЛАТФОРМИ CISCO IDENTITY SERVICES ENGINE

Шевченко Д.В.
Науковий керівник**: Созонник Г.Д.**
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: lancha41@gmail.com

Проаналізована практична цінність системи контролю доступу до корпоративної мережі на базі Cisco Identity Services Engine. Досліджено ефективність роботи системи контролю доступу до ресурсів компанії з точки зору IT-процесів.

Overview of Cisco Identity Services Engine

Shevchenko D.V.
Scientific adviser**: Sozonnik G.D.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: lancha41@gmail.com

Analyzed the practical value of the corporate access control system based on Cisco Identity Services Engine. Investigated the effectiveness of the system of access control to the company's resources from the point of view of IT.

АНАЛІЗ ЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ SIP ТЕЛЕФОНІЇ

Пасічник О.В.
Науковий керівник: **Романов О.І.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: alexeypasichnik2.71828@gmail.com

Досліджено особливості забезпечення безпеки даних мережі SIP, вектори атак на мережу SIP, такі як: перехоплення реєстрації, перехоплення сесії, підміна сервера, підробка змісту повідомлення, розрив сесії зв’язку, атака типу «Відмова в Обслуговуванні» та «примноження», боти та DDoS атаки; та засоби захисту від подібного роду загроз.

THREAD AND DATA SECURITY ANALYSIS IN SIP NETWORK

Pasichnyk O.V.
Scientific adviser: **Romanov O.I.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: alexeypasichnik2.71828@gmail.com

Studied data protection methods in SIP, its vulnerabilities and attack vectors, such as registration hijacking, session hijacking, DNS poisoning, impersonating a server, tampering with message bodies, tearing down sessions, denial of service and amplification, bots and DDoS attacks; and security measures which should be followed to protect data.

ПІДВИЩЕННЯ ДАЛЬНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ ПО ВОЛЗ ШЛЯХОМ ЗАСТОСУВАННЯ СОЛІТОНІВ

Полтавська С.Р.
Науковий керівник: **Правило В.В.**
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: sofia.poltavska@gmail.com

На сьогоднішній час актуально виконувати передачу даних за допомогою ВОЛЗ (волоконно-оптична лінія зв'язку), що являє собою систему передачі інформації по оптичних волокнах. Подібна передача даних мережею ВОЛЗ має свої переваги в порівнянні з передачею інформації по мідному кабелю. Так чому і навіщо перетворювати сигнал в оптичний і навпаки?

INCREASING RANGE OF INFORMATION TRANSMISSION OF THE FIBER OPTICAL LINE (FOL) BY THE SOLITON

Poltavska S.R.
Scientific adviser: **Pravilo V.V.**
Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: sofia.poltavska@gmail.com

In this paper, we consider the advantages and disadvantages of using FOL for signal transmission. Exploring the method of using nonlinear effects (solitons) to increase the length of the communication line, while maintaining high spectral efficiency of data transmission. This way, providing better bandwidth performance.

ПЕРСПЕКТИВИ РОЗВИТКУ І ПЕРЕВАГИ ПОБУДОВИ МЕРЕЖ ОПЕРАТОРСЬКОГО КЛАСУ НА ОСНОВІ ТЕХНОЛОГІЇ CARRIER ETHERNET

Бурлака Г.Ю.
Науковий керівник: **Романов О.І.**
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: Oris1111@i.ua

Досліджено особливості побудови мережі операторського класу на основі Carrier Ethernet. Проаналізовано перспективи і переваги цієї технології, а також використання її як засіб підвищення безпеки мережевих сервісів.

PROSPECTS FOR THE DEVELOPMENT AND ADVANTAGES OF BUILDING CARRIER-CLASS NETWORKS BASED ON CARRIER ETHERNET TECHNOLOGY

Burlaka H.Y.
Scientific adviser: Romanov.O.I.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: Oris1111@i.ua

The features of constructing a carrier-class network based on Carrier Ethernet have been investigated. Analyzed the prospects and benefits of this technology and use it as a means of improving the security of network services.

Засідання 2.

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ОСНОВНИХ ПРОТОКОЛІВ ПРИ ПОБУДОВІ СУЧАСНИХ ЗАХИЩЕНИХ VPN МЕРЕЖ

Власенко В.В.
Науковий керівник: **Романов О.І**
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vlasenko199722@gmail.com

Досліджено особливості використання та побудови VPN мереж.Проаналізовано найбільш поширені протоколи, на базі яких будуються сучасні захищені мережі.

INVESTIGATION OF THE FEATURES OF THE MAIN PROTOCOLS IN THE CONSTRUCTION OF MODERN SECURE VPN NETWORKS

Vlasenko V.V
Scientific adviser: Romanov.O.I.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: vlasenko199722@gmail.com

Investigated the features of use and construction of VPN networks. Analyzed the most common protocols based on which modern secure networks are built.

ПОБУДОВА ОПТИЧНИХ ТРАНСПОРТНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ CISCO

Петренко О.В.
Науковий керівник: **Григоренко О.Г.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net

Розглянуто технології та характеристики обладнання, що використовуються при побудові оптичних транспортних мереж. Обладнання з використанням технологій DWDM (Dense Wavelength Division Multiplexing), CWDM (Coarse WDM) та OTH (Optical Transport Hierarchy) дозволяє створювати мережі і розширювати їх пропускну здатність на базі існуючої інфраструктури оптичного кабелю. Проаналізовано приклад побудови вузла реконфігуруємого мультиплексора введення / виведення оптичних каналів на базі обладнання компанії Cisco.

BUILDING OPTICAL TRANSPORT NETWORKS ON THE CISCO EQUIPMENT BASIS

Petrenko O.V.
Scientific adviser: **Grygorenko O.G.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: olenagri@ukr.net

The technology and characteristics of equipment used in the construction of optical transport networks are presented. DWDM (Dual Wavelength Division Multiplexing), CWDM (Coarse WDM) and Optical Transport Hierarchy (DWDM) technology allow you to build networks and expand their bandwidth based on existing fiber optic cable infrastructure. An example of constructing a node of Reconfigurable Add/Drop Multiplexer (ROADM) of optical channels based on Cisco equipment is analyzed.

РЕАЛІЗАЦІЯ МОДЕЛІ МЕРЕЖІ ПЕРЕДАЧІ КОНТЕНТУ

Корнійчук Ю.В.
Науковий керівник**: Валуйський С.В.**
Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: yurchik2404@gmail.com

Досліджено особливості побудови мережі доставки контенту та основні її компоненти (адміністративний інтерфейс управління, реалізований з використанням фреймворка Django і модуль управління узлом мережі, заснований на фреймворке Twisted). Така архітектура мережі дозволяє моделювати всі необхідні для перевірки алгоритмів операції (зміна маршрутів всередині мережі, створення додаткових копій контенту на вузлах) через управління кешом nginx.

IMPLEMENTATION OF THE CONTENT DELIVERY NETWORK MODEL

Korniichuk Y.V.
Scientific adviser: **Валуйський С.В.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: yurchik2404@gmail.com

Investigated the features of building a content delivery network(CDN) and its main components (administrative control interface implemented using the Django framework and the network node management module based on the Twisted framework).This architecture allows modelling all the operations necessary for checking the algorithms (changing routes in the network, creating additional copies of content on the nodes) through the management of the nginx cache.

СЦЕНАРНА МОДЕЛЬ І МОВА ОПИСУ ЗНАНЬ ДЛЯ ОЦІНКИ І ПРОГНОЗУВАННЯ СИТУАЦІЙ

Бикова А.О.
Науковий керівник: **Новогрудська Р.Л.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: bykova.alien@gmail.om

Робота присвячена проблемі оцінки ситуацій і прогнозування її розвитку в додатках, в яких потрібно мати засоби для гнучкої зміни сценаріїв поведінки в залежності від досягнутих станів системи і поточного стану зовнішнього середовища в реальному часі. У роботі пропонується нова мова, яка призначена для опису знань про сценарії, що дозволяє оцінювати поточний стан виконання сценарію, прогноз його розвитку і вибору варіанту продовження в залежно від досягнутих станів і стану зовнішнього середовища.

SCENARIO–BASED KNOWLEDGE MODEL AND LANGUAGE FOR SITUATION ASSESSMENT AND PREDICTION.

Bykova A.O.
Scientific adviser: **Novogrudska R.L.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: bykova.alien@gmail.om

This paper is devoted to the problem of situation assessment and prediction in application where it required to have a flexible means to change the scenario behavior, depending on the progress of the system and the current state of the environment in real time. The paper proposes a new language, which is intended to describe the knowledge of the scenarios to assess the current state of performance scenario, to predict of its development, and to select the option to continue depending on the progress of states and the state of the environment.

ІНТЕРНЕТ РЕЧЕЙ НА ОСНОВІ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ: ПРОБЛЕМИ ТА ВИКЛИКИ

Поліщук І.С.
Науковий керівник: **Курдеча В.В.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: polishchuki73@gmail.com

З розвитком Інтернету речей з'явились велика кількість нових технологій та різних пристроїв, але для правильної та швидкої роботи цих пристроїв потрібно вирішити ряд основних проблем таких як: сумісність, об'єм даних, безпека та конфіденційність і кваліфікованість інженерів. В роботі запропоновані вирішення цих проблем за допомогою Програмно-конфігурованих мереж(SDIoT), а також досліджений протокол OpenFlow для функціонування різноманітних пристроїв в цій системі.

INTERNET OF THINGS BASED ON SOFTWARE DEFINED NETWORKS: ISSUES AND CHALLENGES

Polishchuk I.S.
Scientific adviser: **Kurdecha V.V.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail:polishchuki73@gmail.com

With the development of the Internet, a lot of new technologies and devices have appeared, but for the correct and fast operation of these devices, it is necessary to solve a number of key issues such as compatibility, data volume, security and confidentiality, and the qualifications of engineers. This article proposes solutions to these problems with the help of Software-Configurable Networks (SDIoT), as well as the explored OpenFlow protocol for the operation of various devices in this system.

РОЗРОБКА ЦИКЛУ ЛАБОРАТОРНИХ РОБІТ З ДОСЛІДЖЕННЯ ПАРАМЕТРІВ БЕЗПРОВОДОВИХ ЗАСОБІВ ЗВ'ЯЗКУ CAMBIUM

Максимчук М.Р.
Науковий керівник: **Осипчук С.О.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: maksymchukkolya@ukr.net

Проводиться робота над створенням циклу лабораторних робіт, що передбачають отримання студентами теоретичних знань та практичних навичок налаштування і керування безпроводовими засобами зв'язку Cambium, а саме: базовими станціями ePMP2000 та ePMP1000, абонентською станцією ePMP Force 180, призначених для побудови мереж широкосмугового доступу в діапазоні частот 5 ГГц. Створюваний цикл лабораторних робіт буде включено до існуючих дисциплін, що викладаються на кафедрі.

LABORATORY WORKS CYCLE DEVELOPMENT FOR STUDYING PARAMETERS OF THE CAMBIUM'S WIRELESS COMMUNICATION DEVICES

Maximchuk M.R.
Scientific adviser: **Osypchuk S.O.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: maksymchukkolya@ukr.net

This work is being carried out with the aim to create a cycle of laboratory works what has a goal to ensure students get theoretical knowledge and practical skills in setting up and managing wireless communications built on Cambium's equipment, such as: base stations ePMP2000 and ePMP1000, subscriber station ePMP Force 180, designed to build broadband networks in the 5 GHz frequency range. The created laboratory works cycle will be integrated into the existing disciplines what are being given at the department.

РОЗРОБКА ЦИКЛУ ЛАБОРАТОРНИХ РОБІТ З ДОСЛІДЖЕННЯ ПАРАМЕТРІВ БЕЗПРОВОДОВИХ ЗАСОБІВ ЗВ'ЯЗКУ MIKROTIK

Грищенко О.С.
Науковий керівник: к.т.н. **Осипчук С.О.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: aleksandra_95@ukr.net

Створюється цикл лабораторних робіт для студентів 3-4 курсів з дослідження показників функціонування та налаштування цифрового обладнання для передавання даних виробника MikroTik стандартів IEEE 802.11n/ac. Метою створюваного циклу робіт є отримання практичних навичок студентів у роботі з сучасним телекомунікаційним обладнанням для LAN мереж та дослідженні їх характеристик. Лабораторні роботи передбачають отримання навичок налаштування безпроводових точок доступу та проводових маршрутизаторів, створення базових мережевих структур виду точка-точка, точка-багатоточка, безпроводових ліній з переприйманням. Цикл робіт виконується на основі обладнання Mikrotik Groove A-52HPn, SXT-Lite5, RB951G-2HnD, атенюатора Д3-28 для моделювання каналу із затуханням.

CREATION THE LAB WORKS CYCLE FOR MIKROTIK WIRELESS DEVICES' PARAMETERS LEARNING AND RESEARCH

Ghrishchenko O.S.
Scientific adviser: C.T.S **Osipchuk S.O.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: aleksandra_95@ukr.net

The cycle of laboratory works is being developed for students of 3-4 courses. The purpose of it are indicators research and settings management of digital equipment for data transfer built by manufacturer MikroTik following modern standards IEEE 802.11 n/ac. The objective of laboratory works cycle is obtaining by students the practical skills in working with modern telecommunications equipment for LAN networks and study their characteristics. The laboratory works include the skills gain of setting up wireless access points and wired routers, creating basic network structures like PtP (point-to-point), PtMP (point-to-multipoint) wireless links with re-transmission. The cycle of works is based on devices Mikrotik Groove A-52HPn, SXT-Lite5, RB951G-2HnD; attenuator D3-28 for the channel attenuation simulation.

МЕТОДИ МАСШТ АНАЛІЗ БЕЗСЕРВЕРНИХ ХМАРНИХ ТЕХНОЛОГІЙ І ШЛЯХИ ПОДАЛЬШОГО ЇХ РОЗВИТКУ

Буфін Г.Г.
Науковий керівник: **Міночкін Д.А.**
Інститут телекомунікаційних систем,
КПІ ім. Ігоря Сікорського, Україна
E-mail: blefgufin@gmail.com

Використання хмарних технологій (БСА – Serverless). Аналіз переваг та подальшого розвитку більших екосистем послуг на прикладі AWS (Amazon Web Services) Lambda and Azure Cloud Function.

ANALYSIS OF SERVERLESS CLOUD TECHNOLOGIES AND WAYS OF THEIR FURTHER DEVELOPMENT

Bufin G.G.
Scientific adviser: **Mynochkin D. A.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: blefgufin@gmail.com

Use of cloud technologies (Serverless). An analysis of the benefits and the further development of large ecosystem services on the example of Amazon Web Services AWS (Lambda and Azure Cloud Function).

АБУВАННЯ СИСТЕМ В АРХІТЕКТУРІ «КЛІЄНТ-СЕРВЕР»

Тригубенко Д.О.
Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: ykyllhuk@gmail.com

Термін масштабуємість означає здатність пристрою збільшувати свою ефективність шляхом збільшення кількості функціональних блоків, що виконують однакові задачі. Зазвичай потреба в масштабуванні виникає вже тоді, коли система не здатна обробляти запити з необхідними швидкістю та якістю. Робота будь-якого web-сервера полягає в обробці даних. Відповідь на HTTP-запит призводить до виконання певних операцій над певними даними. Відповідно, ми маємо дві основні сутності – дані (характеризуються об’ємом) та операції (характеризуються складністю).

CLIENT-SERVER APPLICATIONS SCALING METHODS

TrigubenkoD.O.
Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: ykyllhuk@gmail.com

Overall Client-Server application performance depends on the system architecture of the application and the complexity of operations ran on server but almost each system is unable to handle the high load at certain moment, the solution is to scale the system.

АНАЛИЗ ОТТОКА КЛИЕНТОВ В МОБИЛЬНЫХ ТЕЛЕКОММУНИКАЦИЯХ

Корсун Н.А.
Научный руководитель: **Миночкин Д.А.**
Институт телекоммуникационных систем,
КПИ им. Игоря Сикорского, Украина
E-mail: nickorsun@gmail.com

В статье освещается одна из основных задач машинного обучения в телекоммуникациях: анализ оттока клиентов, позволяющий повысить эффективность инвестиций и лояльность клиентов. Проанализирован один из основных методов классификации, основанный на различных моделях и алгоритмах.

CUSTOMER CHURN ANALYSIS IN MOBILE TELECOMS

Korsun N.O.
Scientific adviser: **Minochkin D.A.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: nickorsun@gmail.com

The article highlights the one of main Machine Learning task in Telecom: Customer churn analysis, which allows to increase the efficiency of investments and customers loyalty. Analyzed the most common method of classification customers, based on the different models and algorithms.