МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Т Е З И

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 червня 2022 р.

м. Київ

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE
SCIENTIFIC CYBER SECURITY ASSOCIATION OF UKRAINE

PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

«OPERATIONAL AND SECURITY PROBLEMS OF INFORMATION AND COMMUNICATION SYSTEMS»

June, 7 – 9, 2022
Kyiv, Ukraine

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 червня 2022 р.
м. Київ, Україна

УДК 621.39: 004.9 (082)

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 7 – 9 червня 2022 р., Національний авіаційний університет. – К.: Вид-во НАУ, 2022. – 126 с.

ISBN: 978-611-01-0740-2

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова:

РОМАНЕНКО Є.О. — проректор Національного авіаційного університету з наукової роботи, доктор наук з державного управління, професор, заслужений юрист України;

Члени оргкомітету:

ОДАРЧЕНКО Р.С. — доктор технічних наук, професор, завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету, **головний редактор редколегії**;

ЮДІН О.Ю. — кандидат технічних наук, заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

КОРЧЕНКО О.Г. — доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, лауреат Державної премії України в галузі науки і техніки;

БАХТІЯРОВ Д.І. — кандидат технічних наук, заступник декана Факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету;

Секретар:

ЛАВРИНЕНКО О.Ю. — кандидат технічних наук, старший викладач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету.

ЗМІСТ

УДК 512.624

А.Я. Білецький, А.В. Ковальчук
Національний авіаційний університет, м. Київ

ЕФЕКТИВНИЙ АЛГОРИТМ ФАКТОРИЗАЦІЇ СТЕПЕНІВ СФЕНІЧНИХ ПОЛІНОМІВ

Сфенічними будемо називати поліноми, які можуть бути представлені як добуток трьох *незвідних* над полем $GF(p)$ *поліномів* (НП), зовсім не обов'язково різних. Для запису НП ступеня n використовуємо векторну форму $f_n = \alpha_n\alpha_{n-1}\ldots\alpha_k\ldots\alpha_1\alpha_0$, де α_k – коефіцієнти поліному. Одним з найважливіших питань, пов'язаних з поліномами, є питання щодо *типу* факторизації поліному. Під типом факторизації полінома будемо розуміти кількість k та ступені НП, добуток яких утворює заданий поліном. Основне завдання, що вирішується у даної доповіді, полягає у розробці ефективних алгоритмів розкладання ступеня СП від однієї змінної над полями Галуа довільних характеристик p. До ефективних відноситимемо алгоритми факторизації, що забезпечують мінімум складності обчислень.

Основна частина. Нехай $f_n^{[3]} = f_x \overset{p}{\otimes} f_y \overset{p}{\otimes} f_z$ – сфенічний поліном (СП), в якому x, y та z є апріорі невідомі ступені компонентів поліному. Для визначення невідомих змінних необхідно скласти систему трьох рівнянь, кожне з яких функціонально залежить від цих змінних. У якості першого рівняння обираємо $x + y + z = n$. Друге рівняння отримуємо на основі параметра, названого *періодом циклу* (Cord - cycle order) поліному. Періодом циклу полінома $f_n^{[3]}$ називатимемо число неповторюваних відрахувань, обчислюваних на *лінійно-логарифмічній шкалі* групи, що породжується СП $f_n^{[3]}$ [1]. Вираз для періоду циклу $\mathrm{Cord}(f_n^{[3]})$ поліномів подібно до того, яким визначається порядок цих же поліномів. Зокрема, для СП

$$\mathrm{Cord}(f_n^{[3]}) = C = \mathrm{НОК}(\mathrm{Cord}(f_x), \mathrm{Cord}(f_y), \mathrm{Cord}(f_z)).$$

Введена вище пара рівнянь утворює несумісну систему, яка, на перший погляд, є апріорі нерозв'язною. Але все не так погано, як здається. Проблема стає переборною, якщо залучити на її вирішення як

відношення між параметрами n і C, так і підмножину нетривіальних дільників періоду циклу C полвнома $f_n^{[3]}$.

Справді, якщо, наприклад, виявиться, що $C = n/3$, це означатиме, що три поліноми, які утворюють СП $f_n^{[3]}$, є поліномами ступеня $n/3$. З іншого боку, якщо C дорівнює квадрату натурального числа, рішення системи рівнянь таке: $x = \sqrt{C}$; $z = C$; $y = n - (x + z)$. Повне рішення системи «несумісних рівнянь» відображено у вигляді структурно-логічної схеми, яка відображена на рис. 1.

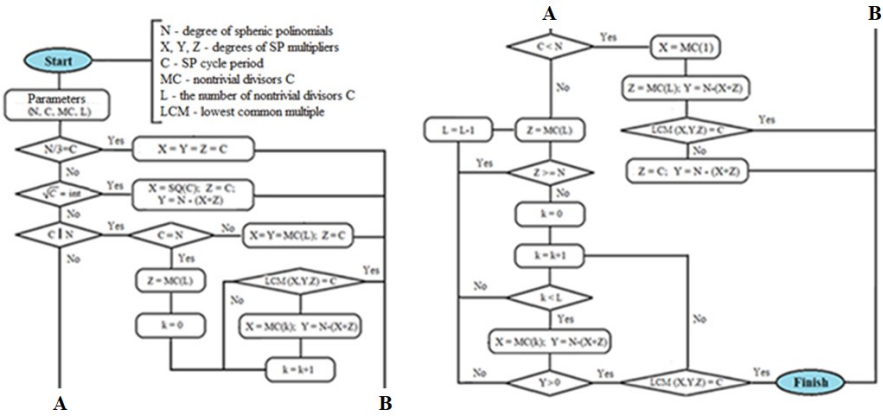

Рис.1. Структурно-логічна схема алгоритму факторизації СП

Висновок. Розглянуто різні варіанти вирішення проблеми факторизації ступенів СП залежно від співвідношення параметрів n і C цих поліномів. Алгоритм факторизації виявився інваріантним до характеристики поля, що породжується співмножниками сфенічного полінома.

Література

[1]. Anatoly Beletsky. Factorization of the Degree of Semisimple Polynomials of one Variable over the Galois Fields of Arbitrary Characteristics. WSEAS Transactions on Mathematics, ISSN / E-ISSN: 1109-2769 / 2224-2880, Vol. 21, 2022, Art. 23, p.p. 160-172. DOI: 10.37394/23206.2022.21.23

УДК 621.396 (043.2)

Л.О. Василенко, Д.І. Бахтіяров, О.Ю. Лавриненко
Національний авіаційний університет, м. Київ

МЕРЕЖА НАДШИРОКОСМУГОВОГО ДОСТУПУ НА БАЗІ ТЕХНОЛОГІЇ UWB

У зв'язку з постійним збільшенням інформаційних потоків та інформатизацією суспільства ця проблема стає все більш актуальною як для радіозв'язку, так і для радіолокації. Актуальність проблеми і визначила швидкий розвиток технологій, які використовують надширокосмугові сигнали.

Моделювання каналу зв'язку UWB-мережі за допомогою програмного середовища MATLAB. MATLAB – пакет прикладних програм для вирішення завдань технічних обчислень та однойменна мова програмування, що використовується у цьому па-кеті. Мова MATLAB є високорівневою мовою програмування, що інтерпретується, що включає засновані на матрицях структури даних, широкий спектр функцій, інтегроване середовище розробки, об'єктноорієнтовані можливості та інтерфейси до програм, написаних іншими мовами програмування. Далі автоматично буде запущено модель передачі сигналу. Дана модель ілюструє часові та частотні форми сигналу для модульованого та немодульованого імпульсних сигналів. Відстань від одного хвоста до іншого на часових діаграмах вважається фактичною тривалістю імпульсів. Передається сигнал із 5 імпульсів «10101».

Для передачі цього сигналу використовується фазо-імпульсна модуляція (ФІМ). При ФІМ амплітуда і тривалість імпульсів не змінюються, змінюється їх позиція, тобто. певні імпульси запізнюються за часом. Маємо послідовність із 5 імпульсів, яка буде немодульованим сигналом. Далі ця послідовність модулюється за допомогою ФІМ, в результаті чого виходить модульований сигнал, у якого 2-ий і 4-ий імпульси запізнюються. Таким чином, імпульси, що відповідають логічній "1", зберігають своє положення, а імпульси, що відповідають логічному "0", запізнюються на 0,2 нс.

На рис. 1 зліва зображені відповідні діаграми, а праворуч також наведені дані діаграми у збільшеному масштабі, з метою наочності запізнення імпульсів, що відповідають логічному «0».

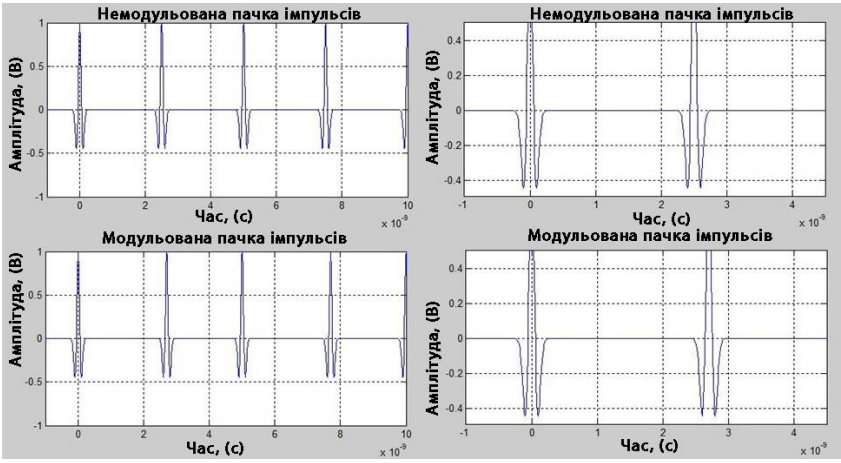

Рис. 1. Часові діаграми сигналів

Для відновлення цього сигналу використовуватиметься кореляційний приймач, так як на його входи надходитиме груповий сигнал. Замість складного АЦП у приймачі використовується простий компаратор (10101). У компараторі обидва сигнали перемножуються і утворюється вихідний сигнал «10101» (рис. 2).

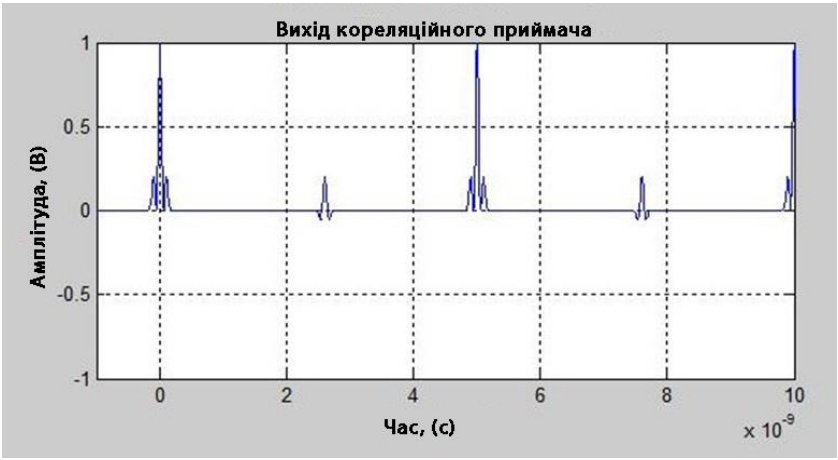

Рис. 2. Часова діаграма прийнятого сигналу

Ця програма додатково представляє спектральні діаграми та графіки залежності рівня сигналу від частоти (див. рис. 3).

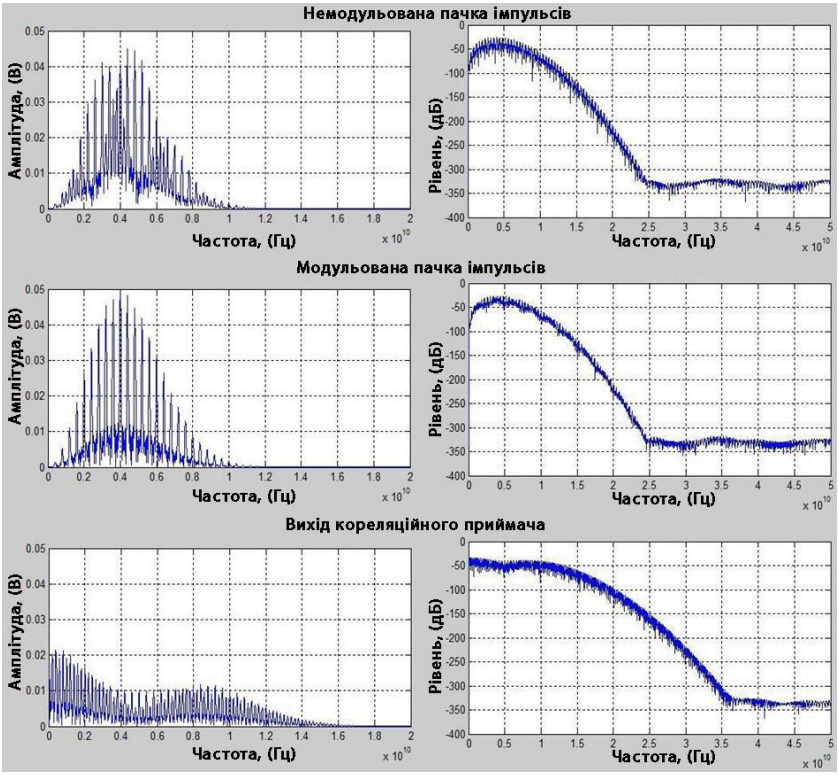

Рис. 3. Спектри та залежності рівня сигналу від частоти

Обґрунтуванням вибору ФІМ є такі факти:

- UWB технологія працює на основі передачі надкоротких імпульсів, що пояснює вибір імпульсного виду модуляції;

- з усіх видів імпульсної модуляції ФІМ має найвищу завадостійкість, що добре поєднується з однойменною гідністю технології UWB.

Висновок. Бездротові технології стали зручним рішенням для мільйонів жителів, які з будь-яких причин не можуть або не хочуть бути "прив'язаними" проводами до стаціонарної точки. У перспективі люди хочуть мати пристрої, що бездротово передають великі обсяги інформації швидко і якісно. Технологія UWB відкриває нові можливості

бездротової передачі сигналів з дуже високою швидкістю передачі. В даний час тенденція на високоякісні мультимедіа дані, такі як відео, стрімко зростає. У свою чергу якісне відео займає великий обсяг, і щоб передавати такі «важкі» дані за допомогою існуючих стандартів бездротового зв'язку доводиться витрачати багато часу, а відтворити в режимі реального часу часом і неможливо. Ця проблема повністю вирішується застосуванням технології UWB. Було проведено розрахунок залежності дальності зв'язку від пропускної спроможності, а також виконано оптимізацію, з метою вибрати оптимальну відстань між приймачем та передавачем для забезпечення зв'язку без затримок та перешкод в умовах екранування сигналу залізобетонною стіною. В результаті чого було знайдено оптимальну відстань, також визначено відстань, на якій обладнання працює з максимальною ефективністю. Крім цього, за допомогою програмного середовища MATLAB була проілюстрована модель каналу зв'язку, що обґрунтовує вибір ФІМ із усіх видів імпульсної модуляції.

Список використаних джерел

1. Z. Yao S. Xiao Z. Jiang L. Yan and B. Wang "On the Design of Ultrawideband Circuit Analog Absorber Based on Quasi-Single-Layer FSS" IEEE Antennas and Wireless Propag. Lett vol. 19 no. 4 pp. 591-595 Apr. 2020.

2. E. O. Johnson "Physical limitations on frequency and power parameters of transistors" RCA Rev pp. 163-177 1965.

3. S. Bajaj O. F. Shoron P. S. Park S. Krishnamoorthy F. Akyol T. H. Hung et al. "Density-dependent electron transport and precise modeling of GaN high electron mobility transistors" Applied Physics Letters vol. 107 no. 15 pp. 153504 2015.

4. Про технологію СШП. Застосування СШП. Інтернет-сторінка компанії UWB Group.

5. Крутов А. Надширокосмуговий зв'язок UWB. Частина 1. Технологія UWB: принципи функціонування, історія розвитку, особливості. Інтернет-сторінка компанії Wirerless Engineering.

6. UWB Technology. Надширокосмугова система зв'язку з високою швидкістю передачі даних. Інтернет-сторінка компанії UltraWide Band.

УДК 004.75

R. Vashchenko, PhD, assoc. prof. I. Ye. Terentieva
National Aviation University, Kyiv

ANALISIS OF MODERN MULTI-SERVICE COMMUNICATION NETWORKS

The current stage of development of world civilization is characterized by the transition from industrial to information society, which assumes the existence of new forms of social and economic activities, which are based on the widespread use of information and telecommunications technologies.

A multiservice network is a single network capable of transmitting voice, video, and data. The main stimulus for the emergence and development of multiservice networks is the desire to reduce the cost of ownership, support complex, rich multimedia applications and expand the functionality of network equipment.

The concept of multiservice contains several aspects related to different aspects of network construction.

First, network load convergence, which determines the transmission of different types of traffic within a single data presentation format. For example, audio and video traffic is currently transmitted mainly through circuit-switched networks, and data is transmitted over packet-switched networks.

Second, the convergence of protocols, which determines the transition from many existing network protocols to a common one (usually IP). While existing networks are designed to manage multiple protocols, such as IP, IPX, AppleTalk, and a single type of data, multiservice networks focus on a single protocol and the different services required to support different types of traffic.

Third, physical convergence, which determines the transfer of different types of traffic within a single network infrastructure. Both multimedia and voice traffic can be transmitted using the same equipment, taking into account different bandwidth, latency and jitter requirements. Resource reservation, priority queuing, and quality of service (QoS) protocols differentiate the services provided for different types of traffic.

Fourth, the convergence of devices, which determines the trend of building a network device architecture capable of supporting a variety of

traffic within a single system. For example, the switch supports Ethernet packet switching, IP routing, and ATM connections. Network devices can process data transmitted according to a common network protocol (eg IP) and have different service requirements (eg bandwidth guarantees, latency, etc.

Fifth, the convergence of applications, which determines the integration of various functions within a single software. For example, a Web browser allows you to combine multimedia data such as audio, video, high-resolution graphics, and more within a single page.

Sixth, the convergence of technologies expresses the desire to create a single common technological base for building communication networks that can meet the requirements of both regional communication networks and local area networks. Such a base already exists: for example, an asynchronous transmission system (ATM) can be used to build both regional and local area networks.

All these aspects determine the various aspects of the problem of building multiservice networks capable of transmitting various types of traffic both in the peripheral part of the network and in its core.

Conclusions

The concept of multiservice covers many aspects of network construction, allowing to achieve the required quality of solving user problems, the functioning of both individual parts and the network as a whole. There may be some milestones in building a multiservice network that allow you to add all the new features you need as your business grows. However, even today it is important to take into account the strategy of multiservice when deciding on the purchase of network equipment.

List of references

1. https://siblec.ru/telekommunikatsii/multiservisnye-seti-svyazi#1
2. https://compress.ru/article.aspx?id=9404#begin

УДК 004.75

I. Voichak I., PhD, assoc. prof. I. Ye. Terentieva
National Aviation University, Kyiv

METHODS OF ARTIFICIAL INTELLIGENCE FOR ANALYSIS AND MANAGEMENT OF CUSTOMER EXPERIENCE OF A TELECOM COMPANY

Nowadays, there are many telecommunications companies that each try to attract the customer's attention. But in order for a company to do this, it needs to refer to some factors, reports. Analyze and monitor the network, eliminate network problems in the regions, increase network speed, add more equipment and more. The quality of the network plays a big role. To improve it, telecom companies use different methods.

Artificial intelligence (AI) is a new technical science that studies and develops theories, methods, techniques, and application systems for simulating and extending human intelligence. AI is divided into two types: strong AI and weak AI. Strong AI – such machines can work independently, think about problems and work out optimal solutions to problems. The weak AI view holds that intelligent machines cannot really reason and solve the problems. These machines only look intelligent, but do not have real intelligence and self-awareness.

In addition to the fact that AI is divided into types, it also has different directions, among them: computer vision, speech processing and natural language processing. The main topics of voice processing research include voice recognition, voice synthesis, voice wake up, voiceprint recognition, and audi-based incident detection. The main topics of NLP (natural language processing) research machine translation, text mining and text analysis. NLP imposes high requirements on technologies but confronts low technology maturity. For computer vision scenarios AI can be used: electronic attendance, smart album and authentication.

If to talk about phases, computing intelligence - capable of storage and computing: machines can compute and transfer information as human beings do. Perceptual intelligence - capable of listening and seeing: machines can listen and see, make judgments, and take simple actions. Cognitive intelligence - capable of understanding and thinking: machines can understand, think and make decisions like human beings.

Consider the peculiarity of the use of artificial intelligence, analysis and management of customer experience in the Ukrainian telecom company - Kyivstar. Kyivstar is a Ukrainian telecom company providing communication and data services based on a wide range of mobile and fixed technologies. The leader among mobile operators in Ukraine in terms of the quality of mobile Internet.

To select the data transfer rate for each subscriber, many factors were evaluated - the amount of search (requested) resources, the quality of the connection, the signal level from the station on the smartphone, and some others. Assessing changing conditions, the mobile stations chose the optimal settings, however, this scheme worked well under light load. But when the load increased several times, for example, during morning or evening rush hours, the network could not provide acceptable service characteristics to all users. Now everything can be changed with the help of artificial intelligence, using a module developed by Siemens - SIMATIC S7-1500 TM NPU module.

Fig.1 SIMATIC S7-1500 module

Thanks to this module the production and analizing characteristics can be improved.

Conclusions

After the study, it was discovered that network monitoring is carried out at the expense of computer systems, but the analysis of the network by humans, so to speed up this process and network quality, you can use artificial intelligence.

List of references

1. https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%B5%D0%B2%D1%81%D1%82%D0%B0%D1%80
2. https://new.siemens.com/ua/ru/products/avtomatizatsiya-promyshlennosti/sistemy-avtomatizatsii/promyshlennyye-sistemy-avtomatizatsii-simatic/io-systems/shtuchnyy-intelekt.html

УДК 004.71 (043.2)

М.В. Волга, Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ NEXANS CABLING SOLUTIONS

Сучасна будівля насичена безліччю кабельних розводок та інформаційних мереж, серед яких: телефонна система, локальна комп'ютерна мережа, мережа кабельного телебачення, системи пожежної та охоронної сигналізації, навіть контроль кліматичних параметрів всередині будівлі. Структурована кабельна система — фізична основа інфраструктури будівлі, що дозволяє звести в єдину систему безліч мережевих інформаційних сервісів різного призначення: локальні обчислювальні та телефонні мережі, системи безпеки, відеоспостереження і т. д. Як правило, ці сервіси розглядаються в рамках певних служб підприємства.

Розподілена Архітектура СКС. Архітектура структурованої кабельної системи з двома рівнями ієрархії, що складається з трьох підсистем: основного першого рівня, другого магістрального і горизонтального рівня підсистеми або одного рівня ієрархії і поперечного зв'язку між ГРП і ERP.

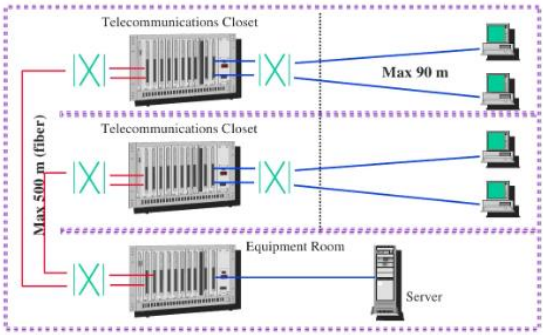

Рис. 1. Розподілена архітектура СКС з 2-ма рівнями ієрархії

Розподілена архітектура є традиційною для структурованої кабельної системи для багатоповерхових будівель і комплексів будівель.

Переваги розподіленої архітектури: забезпечення більшої гнучкості; кабельна система може бути легко розширена; простота установки кабельної системи.

Недоліки розподіленої архітектури СКС: збільшення кількості елементів кабельної системи; більше потрібно площі для телекомунікаційних приміщень; контроль і безпеку важче здійснювати на місці.

Централізована Архітектура СКС. Архітектура структурованої кабельної системи з одного рівня ієрархії без крос-комутації або горизонтальної архітектури підсистеми або СКС не має рівнів ієрархії, що складаються тільки з горизонтальної підсистеми.

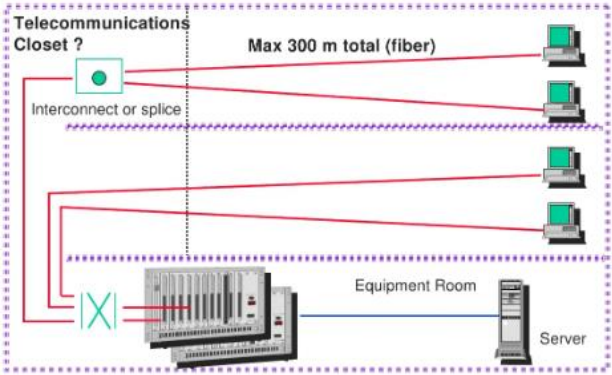

Рис. 2. Централізована архітектура СКС

У централізованій архітектурі, все активне обладнання встановлено і підключено до ГРП, або ERP.

Переваги централізованої архітектури СКС: мінімальна кількість елементів кабельної системи; менші райони повинні бути виділені для телекомунікаційних об'єктів; потрібно менше активних компонентів; не вимагають активного і пасивного обладнання для організації шосе. легше організувати резервну систему активного обладнання в централізованій архітектурі.

Недоліки централізованої архітектури СКС: потрібно більше кабелю; потрібно більше місця в трубопроводі; подальше розширення СКС буде дуже важким; процес установки є складним.

При проєктуванні структурованої кабельної системи в будівлі використовується волоконно-оптичні кабелі LANmark-OF3, ZC, 2HMM50/125, LSZH. Волоконно-оптичний кабель Nexans LANmark-OF ZC призначений для підключення робочих станцій користувачів (рішення Оптика для робочого місця) і може бути використаний для організації невеликих з'єднань

магістральних. Кабелі LANmark - OF ZC LSZH приходять зі стандартними багато-модовими і одномодовими волоконами, які відповідають специфікації OM1, OM2, OM3 і OSI міжнародного стандарту ISO / IEC 11801:2002. Буферизована конструкція кабелю Nexans ZC оптимізована для прямих кінців з вилками різних типів (SC, ST, LC).

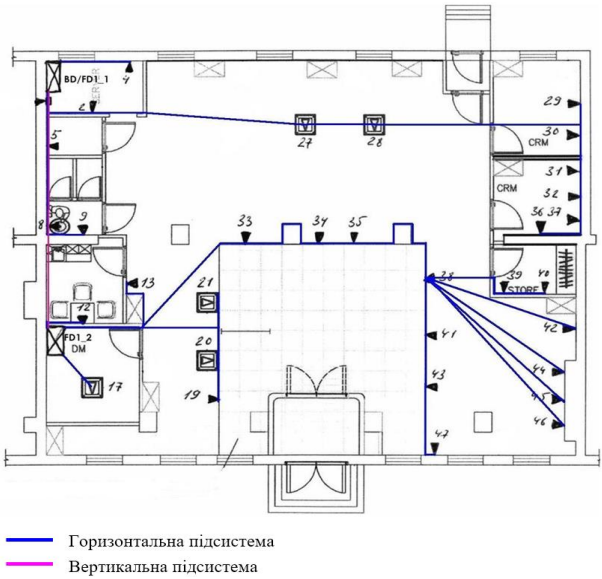

Рис. 3. Схема побудованої СКС

Висновок. Структурована кабельна система є основою обробки даних та телекомунікаційної інфраструктури будь-якого сучасного підприємства від невеликої компанії з кількома співробітниками та закінчуючи Корпорацією, в якій працює кілька десятків тисяч людей. Сучасна СКС організовується в ієрархічному зоряному вигляді і складається зазвичай з декількох підсистем з докладними стандартизованими на міжнародному рівні та параметрами інтерфейсу, взаємодіючи за певними правилами. Інтеграція в єдину систему волоконно-оптичних та електричних кабельних ліній на основі збалансованого кабелю дозволяє забезпечити більшу частину середовища передачі сучасних та перспективних типів мережного обладнання. СКС кабель-них трас, які засновані на серії компонентів забезпечують максимальну дальність зв'язку в 3000 м та інформаційною ємністю 1 Гбіт/с та вище.

УДК 004.71 (043.2)

В.В.Волков. Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

Смарт-розетка на основі мікроконтролера ESP-12F

Смарт-розетка призначена для віддаленого керування підключеним до неї навантаженням за допомогою інтернет з'єднання. Використовується у побутових умовах

Смарт-розетка – це пристрій, який надає можливість віддаленого керування живленням побутових електроприладів (електрочайник, праска, кавоварка, освітлення і ін.). Керування реалізується через мережу WiFi, за допомогою смартфону або через комп'ютер, що дозволяє управляти підключеним приладом з будь-якої точки планети, за умови, що у керуючого пристрою, є доступ до Інтернету. На сьогоднішній день існує досить багато зразків WiFi-розеток, але більшість з них не мають функції відстеження кількості споживаної потужності побутовим приладом, яка дозволяє контролювати і економити витрати електроенергії . В дипломному проекті представлено смарт-розетку з функцією моніторинга кількості споживаної потужності і вимірювання напруги мережі. Побудована вона на основі мікроконтролера ESP-12F. Принцип роботи полягає у наступному: мікроконтролер взаємодіє з користувачем через Інтернет, керує навантаженням за допомогою електромагнітного реле і вимірює напругу та струм вбудованим Аналогово-Цифровим перетворювачем. Пристрій розміщений у компактному білому корпусі, який вмикається напряму в розетку, а навантаження підключається у вбудовану в корпус розетку. Таке рішення не буде сильно виділятися серед інших побутових приладів і не займе багато місця.

Схема електрична структурна показана на рисунку

Схема електрична структурна показана на рисунку 1.1

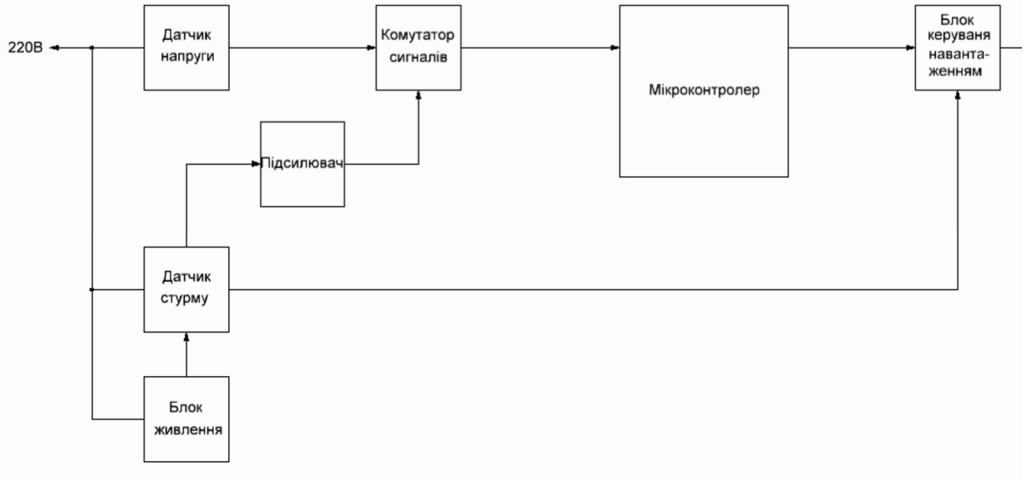

Рисунок 1.1 – Структурна схема пристрою

Пристрій складається з наступних вузлів:
- блок живлення застосовується для подачі стабілізовано напруги 5В на схему;
- датчик напруги та датчик струму використовуються для вимірювання відповідних параметрів і передачі їх до мікроконтролера;
- підсилювач використовується для підсилення сигналу з датчика струму;
- мікроконтролер використовується для обробки інформації з датчиків струму та напруги, керуванням реле та для виконання зв'язку з мережею інтернет;
- блок керування навантаженням використовується для управління навантаженням, яке підключено до пристрою.

Мікросхема ESP-12F

Мікросхема ESP-12F – це модуль побудований на мікроконтролері ESP8266 з інтегрованим Wi-Fi радіо-трактом для зв'язку з мережею Інтернет. Вбудована flash-пам'ять дозволяє зберігати на ній код програми, яку мікроконтролер буде виконувати одразу після подачі живлення. Модуль облаштований захистом від електромагнітних завад – металевим екраном.

Параметри:

- напруга живлення: 3,3 В;

- максимальний споживаний струм: 400 мА;
- діапазон робочих частот: 2400 МГц – 2483,5 МГц:
- потужність випромінювання: +24 дБм;
- об'єм вбудованої flash-пам'яті: 4 МБ;
- діапазон робочих температур: -40°С..+125°С;
- габарити: 16х24х3 мм;
- маса: 6 г;

ВИСНОВКИ

У даному дипломному проекті розроблено смарт-розетку. Призначена для віддаленого керування підключеним навантаженням із функцією відстеження кількості споживаної потужності.

Прилад виготовляється з доступної і недорогої елементної бази. У конструкції пристрою застосовано малогабаритні SMD ЕРЕ, що надає виробу ряд переваг у вигляді високої щільності монтажу, технологічності і як наслідок високої продуктивності праці при виробництві цього пристрою. Виконується на платі з двостороннього фольгованого склотекстоліту. При розрахунку надійності було визначено, що обрана елементна база пристрою, принцип, метод компоновки і побудови конструкції забезпечують вимоги до рівня надійності. Корпус виконаний з пластмаси, має габаритні розміри 128х70х54мм.

При виконанні електричних розрахунків було розраховано транзисторний ключ.

Матеріали і елементна база підібрані так, що собівартість приладу невелика.

При виконанні розрахунку теплових режимів було визначено, що повітря в середині корпусу, нагріта зона, поверхня теплонавантаженого елемента і оточуюче цей елемент середовище знаходяться в межах допустимих значень.

Техніко – економічний аналіз показав, що конструкція має задовільний рівень технологічності.

УДК 004.71 (043.2)

В.В.Гаврись. Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

Антенний аналізатор

В Україні все більше нових домашніх і промислових мереж будується з повним чи частковим використанням безпроводових технологій,

Антена – це пристрій без якого не можливе існування будь-якої передавальної або приймальної апаратури. Вона призначена для приймання та випромінювання електромагнітних хвиль. Зазвичай вона представлена у вигляді штиря визначеної довжини, це проста конструкція, але не ефективна. Більш складні конструкції, наприклад хвильовий канал, мають набагато кращі параметри, але більші габарити та викликають деякі труднощі при їх налаштовуванні. І якщо побутові приймачі не потребують ідеально узгоджених і налаштованих антен, то професійна апаратура , як різного роду трансивери, має бути забезпечена чітко налаштованою антеною(в інакшому випадку, окрім зниження ефективності роботи, може бути виведений з ладу передавальний тракт трансивера).

Для налаштування антен використовують спеціальні пристрої – антенні аналізатори. В залежності від складності та вартості приладу, вони вміють вимірювати ті чи інші параметри.

Схема електрична структурна показана на рисунку

Схема електрична структурна показана на рисунку 1.1

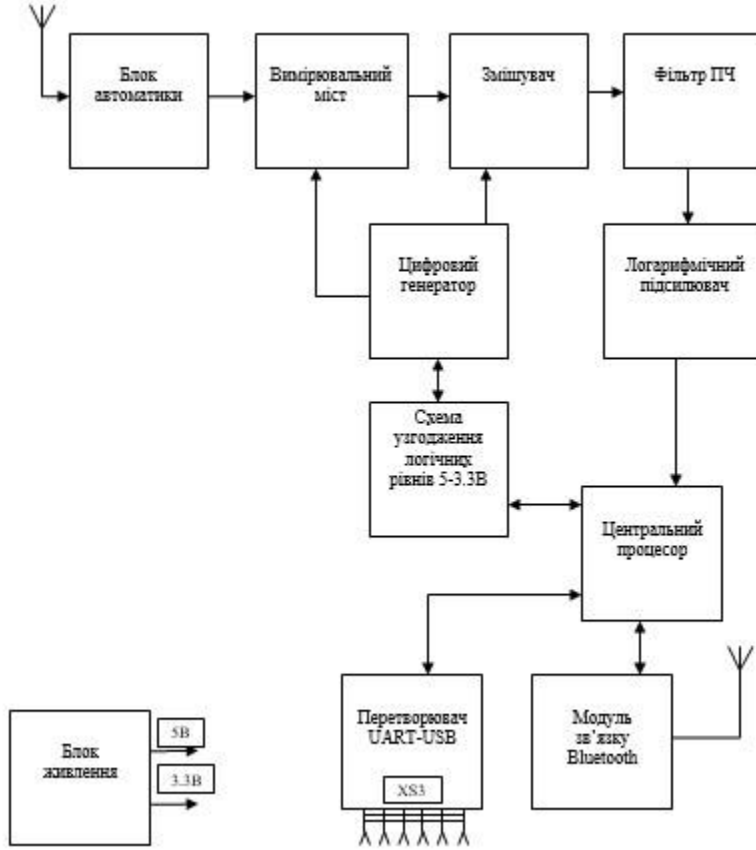

Рисунок 1.1 – Структурна схема пристрою

Пристрій складається з наступних вузлів:

- блок автоматики – реле яке перемикає опір для зміни режиму вимірювання.
- вимірювальний міст – основний компонент схеми, з якого знімається виміряний сигнал.
- змішувач – виконує перенесення спектру сигналу на проміжну частоту.

- цифровий генератор – генерує сигнали для проведення вимірювань та змішувача.
- схема узгодження логічних рівнів – узгоджує логічні рівні 3,3 та 5 В.
- фільтр ПЧ – являє собою п'єзоелектричний фільтр на частоту 455кГц.
- логарифмічний підсилювач – виконує підсилення виміряного сигналу.
- центральний процесор – виконує функції керування усіма каскадами виробу.
- модуль зв'язку – призначений для встановлення зв'язку виробу з пристроєм-клієнтом по радіо протоколу Bluetooth. - перетворювач UART- USB – необхідний для обміну даними пристрою та ПК.
- Блок живлення – забезпечує живлення каскадів схеми від акумулятора 3,7В [4].

Висновки

У даному дипломному проекті розроблено аналізатор антенний. Призначений для вимірювання параметрів антенн при їх налаштуванні та відпрацюванні конструкії.

Прилад виготовляється з доступної і недорогої елементної бази. Виконується на платі з двостороннього склотекстоліту. При розрахунку надійності виявляється, що вибрана елементна база пристрою, принцип, метод компоновки і побудови конструкції забезпечують вимоги до рівня надійності. Корпус виконаний з пластмаси, має габаритні розміри 120х60х30мм.

УДК 004.72:004.77 (043.2)

І.А. Галахін, В.В. Антонов
Національний авіаційний університет, м. Київ

СИСТЕМА АВТОМАТИЗАЦІЇ ОФІСНОЇ БУДІВЛІ

На сьогоднішній день дуже швидкими темпами розвивається наука та техніка. Вченими створюються нові технології та винаходи, доказом цього є поява безпровідної сенсорної мережі. Вона є універсальною, тому що область її застосування є необмеженою, як і територія на якій вона буде розгорнута. Прикладами застосування даної мережі є: офісні будівлі, це дозволить контролювати стан екологічних параметрів навколишнього середовища, завдяки датчикам температури, вологості та інших; безпека будівель та цінних речей, завдяки датчикам руху, присутності, акустичним сповіщувачам розбиття скла та іншим датчикам.

Безпровідна сенсорна мережа – це розподілена, сомоорганізована мережа, що має велику кількість сенсорів та виконуючих пристроїв, що з'єднані між собою радіоканалом. Вузлами даної мережі є так звані моти.

Мот являє собою плату невеликих розмірів, що складається з джерела живлення, прийомо-передатчика, сенсора (датчика), пам'яті. Архітектуру типової безпровідної сенсорної мережі показано на рис.1.

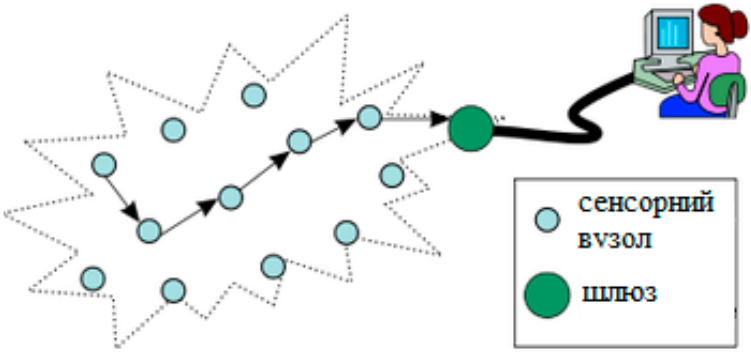

Рис.1. Архітектура безпровідної сенсорної мережі

Що ж до програмного забезпечення та передачі даних, то варто відмітити, що основним стандартом передачі даних в сенсорних ме-

режах є IEE802.15.4, який був спеціально розроблений для безпровідних мереж з малопотужними прийомо-передавачами. Деякі характеристики радіопередачі даних для стандарту IEE802.15.4 наведені в табл.1.

Таблиця 1

Характеристики передачі даних для стандарту IEE802.15.4

Полоса частот, МГц	Чи потрібна ліцензія	Географічний регіон	Швидкість передачі даних, Кбіт/с	Число каналів
868,3	Ні	Європа	20	1
902-928	Ні	Америка	40	1-10
2405-2480	Ні	Весь світ	250	11-26

Для роботи з безпровідними сенсорними мережами найбільшого розповсюдження знайшла операційна система TinyOs, що має відкритий код, тому багато розробників пишуть свою систему управління. Під час виконання роботи було виконано оцінку розробленої мережі, на підставі якої доведено можливість надзвичайно великого заощадження енергії джерел живлення вузлів, що означає значне подовження терміну дії вузлів у ситуаціях неспроможності доставки енергії живлення. Проведено аналіз якості передачі сигналів у мережі. Цей аналіз показує, що розроблена модель мережі з випадковим доступом дозволяє підтримувати якість передачі на обраному рівні ймовірності зітінення.

В ході аналізу було виявлено:

1.Незалежність передачі окремих вузлів та відсутність зв’язку між ними, призводить до значного спрощення обладнання та максимального скорочення протоколів зв’язку.

2.Спрощення та максимальне скорочення протоколів зв’язку призводить до дальшої редукції енергоспоживання для передачі та зменшення руху в радіопросторі, що покращує якість передачі, а також в результаті значно збільшує термін дії окремих вузлів через значне зниження споживання енергії живлення.

3.Можливість під’єднання наступних вузлів та від’єднання інших під час роботи мережі, без необхідності застосування перерв.

УДК 004.5 (043.2)

В.О. Гнатюк
Національний авіаційний університет, м. Київ

СИСТЕМА ОБМІНУ МИТТЄВИМИ ПОВІДОМЛЕННЯМИ ДЛЯ АВТОМАТИЗАЦІЇ НАДАННЯ КОНСУЛЬТАТИВНИХ ПОСЛУГ

На сучасному етапі розвитку суспільство не уявляє своє життя без використання інформаційних технологій, що застосовуються у всіх сферах діяльності людини. Важливою частиною життя сучасної людини є використання систем обміну миттєвими повідомленнями (СОМП), які дозволяють швидко отримувати необхідну інформацію, обмінюватися повідомленнями, файлами, зображеннями, звуковими сигналами, створювати і використовувати групові чати, здійснювати дзвінки, опитування тощо. Серед основних служб для обміну повідомленнями виділяють: Skype, Telegram, Viber, Facebook Messenger, WhatsApp тощо. Найпопулярнішими СОМП в Україні у 2020-2021 роках були Viber, яким користувалися 99 % користувачів смартфонів у віці від 13 до 55 років і Facebook Messenger, Telegram; WhatsApp та Skype поступово втрачають користувачів, ними користуються менше половини користувачів, в той же час популярність Telegram зростає, особливо серед молоді. Відповідно до Telegram являє собою багатоплатформовий клауд-месенджер з функціями VoIP для смартфонів, планшетів та ПК, який дозволяє обмінюватися текстовими, голосовими та відеоповідомленнями, наліпками та фотографіями, файлами багатьох форматів. Також має функції відео- і аудіодзвінків, організації відеконференцій у групах і каналах. Клієнтські програми Telegram доступні для Android, iOS, Windows Phone, Windows, macOS і GNU / Linux. Кількість щомісячних активних користувачів сервісу станом на січень 2021 року становить близько 500 млн. осіб. Окрім обміну повідомленнями в діалогах і групах, в месенджері можна зберігати необмежену кількість файлів, вести канали (мікроблоги), створювати й використовувати ботів. Боти являють собою сторонні програми, які працюють всередині Telegram. Користувачі можуть взаємодіяти з ботами, надсилаючи їм повідомлення, команди та вбудовані запити. Управління ботами здійснюється за допомогою HTTPS-запитів до API ботів

Telegram. Також, Telegram дедалі частіше інтегрується з різноманітними електронними системами, IoT тощо.

Сьогодні заклад вищої освіти (ЗВО), відповідно до Закону України «Про вищу освіту» являє собою окремий вид установи, яка є юридичною особою приватного або публічного права, діє згідно з виданою ліцензією на провадження освітньої діяльності на певних рівнях вищої освіти, проводить наукову, науково-технічну, інноваційну та/або методичну діяльність, забезпечує організацію освітнього процесу і здобуття особами вищої освіти, післядипломної освіти з урахуванням їхніх покликань, інтересів і здібностей. Під час вступу до ЗВО варто керуватися умовами та правилами вступу, проте, зважаючи на велику кількість інформації з якою необхідно ознайомитися вступникам та її складністю, у вступників виникає значна кількість запитань. Зважаючи на це, у структурах ЗВО функціонують консультаційні центри (КЦ), але у пікові періоди, за активної фази вступної кампанії, кількість звернень вступників зростає у сотні, тисячі разів. До прикладу статистика відвідування веб-сайту приймальної комісії ЗВО України за 2021 рік свідчить, що у пікові періоди до 60 000 відвідувань за добу. Подібний приріст звернень спостерігається і при роботі КЦ, як наслідок, працівники КЦ фізично не можуть здійснити обслуговування всіх звернень. З огляду на це, виникає актуальна науково-практична задача автоматизації надання консультативних послуг щодо вступу до університету.

Зважаючи на зростаючу високу популярність Telegram серед молоді, простий та інтуїтивний інтерфейс, забезпечення конфіденційності даних, забезпечення доступу з кількох пристроїв одночасно, відсутності обмежень у розмірі мультимедіа та чатів, наявність відкритого вихідного коду та API для розробників, захищеність від перехоплення та зламу, а також наявність широкого функціоналу метою роботи є автоматизація надання консультативних послуг щодо вступу до університету з використанням сучасних систем обміну миттєвими повідомленнями.

Отже, у роботі формалізована актуальна науково-практична задача автоматизації надання консультативних послуг з використанням сучасних СОМП. Для цього було проаналізовано сучасні СОМП, досліджено роботу ботів, визначено проблемні питання, з якими найчастіше звертаються до консультаційних центрів університету, згодом буде розроблено та експериментально досліджено Telegram-бота.

УДК 004.4 (043.2)

В.О. Гнатюк, М.С. Іванова
Національний авіаційний університет, м. Київ

ІНФОРМАЦІЙНА БЕЗПЕКА У ХМАРНИХ ОБЧИСЛЕННЯХ

Ключові слова: хмарні обчислення, інформаційна безпека

Вступ

Інформаційна безпека (ІБ) у хмарних обчисленнях або хмарна безпека являє собою набір заходів безпеки, призначених для захисту хмарної інфраструктури, додатків і даних. Ці заходи забезпечують автентифікацію користувачів і пристроїв, контроль доступу до даних і ресурсів, а також конфіденційність даних.

Основною метою ІБ у хмарних обчисленнях є захист даних компанії від DDoS-атак, шкідливих програм, хакерів і несанкціонованого доступу або використання користувачами.

Аналіз проблеми

Експерти застерігають від надмірної довіри до високого рівня ІБ у хмарних обчисленнях. Американська асоціація Cloud Security Alliance випустила Cloud Controls Matrix — документ, який є переліком існуючих технологій ІБ, які можуть бути використані в хмарних сервісах. Хоча деякі фахівці вважають, що для управління ІБ при побудові хмари SaaS можуть бути використані стандарти ISO 27001 та ISO 27002. Проте все ж необхідна розробка спеціальних стандартів для хмарних обчислень.

Розв'язання проблеми

Існує три основні типи хмарних середовищ на вибір. Найпопулярніші варіанти на ринку включають публічні хмари, приватні хмари та гібридні хмари. Кожне з цих середовищ має різні проблеми ІБ та переваги, тому важливо знати різницю між ними.

Публічні хмарні служби розміщуються сторонніми постачальниками хмарних послуг. Компанії не потрібно нічого налаштовувати, щоб використовувати хмару. Як правило, клієнти можуть отримати доступ до веб-сервісів провайдера через веб-браузери. Функції безпеки, такі як контроль доступу та автентифікація, мають вирішальне значення для загальнодоступних хмар.

Приватні хмари, як правило, більш безпечні, ніж загальнодоступні хмари, оскільки вони призначені для однієї групи або користувача. Ізольований характер цих хмар допомагає їм залишатися в безпеці від

зовнішніх атак, оскільки вони доступні тільки одній організації. Однак вони все ще стикаються з проблемами ІБ від деяких загроз, таких як соціальна інженерія та порушення. Хмари такого типу можуть важко масштабуватися.

Гібридні хмари поєднують масштабованість публічних хмар з більшим контролем над ресурсами, які пропонують приватні хмари. Ці хмари з'єднують кілька середовищ, таких як приватна хмара і загальнодоступна хмара, які можуть легше масштабуватися на основі попиту.

Нижче наведені критерії для вирішення основних проблем хмарної безпеки видимості та контролю над хмарними даними.

Видимість даних. Повне подання хмарних даних вимагає прямого доступу до хмарного сервісу. Досягають цього за допомогою підключення інтерфейсу прикладного програмування (API) до хмарного сервісу. За допомогою API-з'єднання можна переглянути:

- Які дані зберігаються в хмарі.
- Хто використовує хмарні дані.
- Ролі користувачів з доступом до хмарних даних.
- З ким користувачі хмари діляться даними.
- Де знаходяться хмарні дані.

Контроль над даними. Після отримання видимості хмарних даних, застосовують елементи керування, що включають:

- Класифікація даних — дані класифікують на декількох рівнях, таких як чутливі, регульовані або загальнодоступні. Після класифікації дані можуть бути зупинені від входу або виходу з хмарного сервісу.

- Запобігання втраті даних (DLP) — впровадження хмарного рішення DLP для захисту даних від несанкціонованого доступу та автоматичного відключення доступу та транспортування даних при виявленні підозрілої активності.

- Елементи керування спільною роботою, наприклад, зниження дозволів на доступ до файлів і папок для певних користувачів, можливість редагування або тільки перегляд, видалення дозволів і відкликання спільних посилань.

- Шифрування даних у хмарі може бути використано для запобігання несанкціонованого доступу до даних.

Доступ до хмарних даних і додатків. Як і у випадку з внутрішньою безпекою, контроль доступу є життєво важливим компонентом хмарної безпеки. Типові елементи керування включають:

- Контроль доступу користувачів — впровадження системних і прикладних елементів керування доступом, які забезпечують доступ лише авторизованих користувачів до хмарних даних і додатків.

- Керування доступом до пристрою — блокування доступу, коли неавторизований пристрій намагається отримати доступ до хмарних даних.

- Ідентифікація зловмисної поведінки — виявлення скомпрометованих облікових записів та загроз за допомогою аналітики поведінки користувачів, для запобігання зловмисної фільтрації даних.

- Запобігання потраплянню шкідливих програм у хмарні служби за допомогою таких методів, як сканування файлів, білий список додатків, виявлення шкідливих програм на основі машинного навчання та аналіз мережевого трафіку.

- Привілейований доступ — визначення всіх можливих форм доступу, які привілейовані облікові записи можуть мати до даних і додатків.

Висновки

Інформаційна безпека повинна забезпечуватися на всьому ланцюжку, включаючи постачальника хмарного рішення, споживача та пов'язуючі їх комунікації. Споживач хмарних послуг зобов'язаний вводити до своєї системи відповідну політику безпеки, яка виключає передачу прав доступу до інформації, наданої постачальником, третім особам. Хмари не скасовують необхідність розробки і впровадження політики безпеки у сегменті споживача і використання сервісів безпеки, покликаних гарантувати захист призначених для користувача робочих місць на стороні споживача хмарних послуг.

Список літератури

1. The NIST Definition of Cloud Computing (англ.). [Електронний ресурс]: Режим доступа: http://nvlpubs.nist.gov/nistpubs/Legacy/ SP/nistspecia lpublication800- 145.pdf [2]

2. Документ України щодо обробки інформації в системах хмарних обчислень [Электронный ресурс] - Режим доступа : http://w1.c1.rada.gov.ua/ pls/zweb2/webproc4_1?pf3511=58527

УДК 004.75

O. Lavrynenko
National Aviation University, Kyiv

DATA MINING ALGORITHMS FOR ANALYZING THE CUSTOMER BASE OF A MOBILE OPERATOR

The rapid development of telecommunication technologies in the field of mobile communications is caused by increasing needs of users every time. Nowadays, the technologies cannot please all the needs of users, so next step in the development in the field of telecommunication systems is implementation of Data Mining algorithms. There are known and available a lot of algorithms. During the last 30 years researchers have generated many variants of Data Mining algorithms that are suited to particular areas in the solution landscape. For better customer support service this process involves sifting information gathered from different sources. The patterns have found using Data Mining applications to help to recognize customer trends and be prepared to support them properly. Also it provides one of the best environments for involving business solutions. The smart systems are composed of many individual techniques designed to work to create powerful Data Mining models. Data Mining algorithm is a mathematical expression of aspects of the patterns they find in data. Different algorithms provide perspectives on the complete nature of the pattern. The telecommunications generates and stores a lot of data. It includes calls detail data (which describes calls that traverse the network), the network data (which describes the state of hardware and software components), customer data (which describes customers). For now, in Data Mining you should under-

stand what is Data. Without this the useful applications cannot be developed. So in this section I want to describe the three main types of telecommunication data. As I mentioned before the raw data is not suitable for Data Mining then we should use transformation steps. It is necessary to generate data that can be also described. Also I will show how we can use it for extraction useful information from data sets. Every time when you make a call in the telecommunication network, all information is saved as call detail record. It takes a lot of place (number of call, details record).

Conclusion: Aspects of using of Data Mining in the telecommunication industry is described in the paper. Three main sources of telecommunication data were described, as were common Data Mining applications. The work also highlighted several key issues that affect the ability to mine data and commented on how they impact the Data Mining process. One central issue is that telecommunication data is not in a form or at a level suitable for Data Mining. Other issues that were discussed include the large scale of telecommunication data sets, the need to identify very rare events.

References:

1. C. Baek, T. Doleck, “Educational data mining: a bibliometric analysis of an emerging field,” *IEEE Access*, vol. 10, pp. 31289–31296, 2022, DOI: 10.1109/ACCESS.2022.3160457.

УДК 004.75

O. Lavrynenko
National Aviation University, Kyiv

MODEL OF VOIP SERVICE FOR PRIVATE BUSINESS BASED ON NEXTIVA BUSINESS PHONE SYSTEM

Nowadays, the Internet, various networks based on the IP protocol, as well as IP telephony networks are developing at a rapid pace. The Internet, providing a huge number of services, is truly entering our lives. Today it is almost impossible to imagine the successful operation of any company in the absence of a local network. Large companies organize their networks, which are located in several buildings or even in localities.

1. General information about IP telephony

IP telephony is a technology that uses a packet-switched network to conduct all types of calls and faxes in real-time based on the IP protocol. The most common such network is the Internet. Sometimes you can find such a term - VoIP (Voice Over IP), otherwise known as "voice over IP", which means the transmission of voice information over IP lines. For a long time, circuit-switched networks (ie telephone networks) and packet-switched networks (IP networks) could exist independently of each other.

The following is an example of the principle of operation of an IP phone system based on Nextiva Phone Systems.

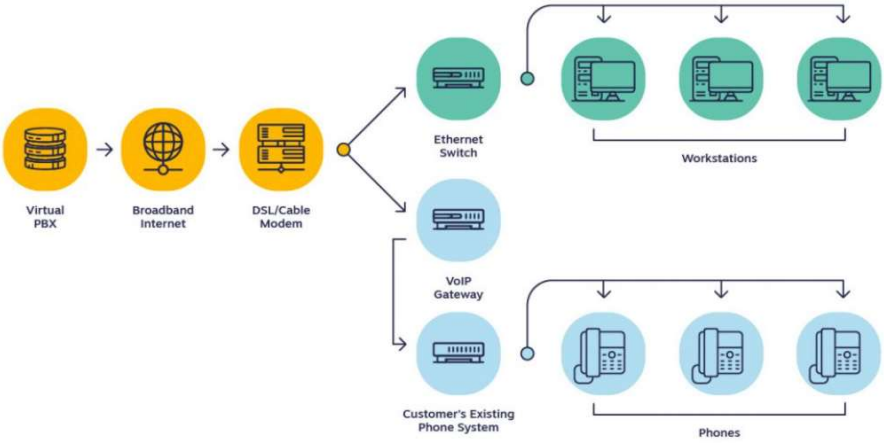

Fig. 1. Example of the Nextiva IP phone system

In the above example, an incoming call first contacts a virtual server hosted by the provider. The VoIP provider converts the call into an audio file and transmits the data to an IP phone. After that, we are connected to the caller by the Internet instead of a cell tower.[1]

2. H.323 IP telephony standard or SIP?

H.323, like SIP, is a relatively old protocol but has been largely superseded by SIP. One of the advantages of SIP is that it's much less complex and resembles HTTP/SMTP protocols. In this respect, H.323 is a binary protocol, making it less technician-friendly in a troubleshooting environment. The major strength of H.323 was its relatively early availability of this standard. H.323 not only defined the basic call model, but also covered the supplementary services needed to address business communication expectations with relevant standards.[2]

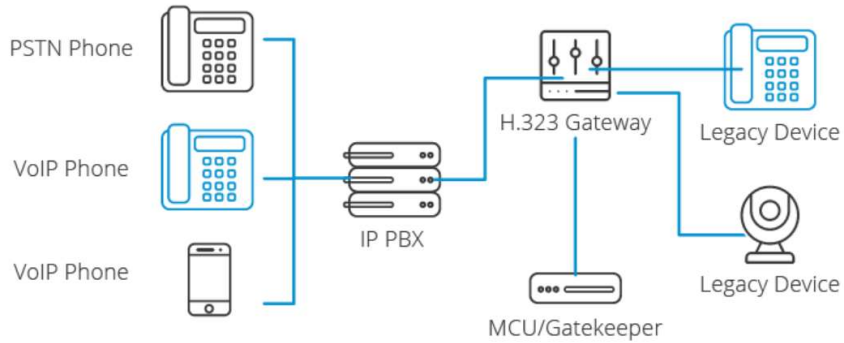

Fig. 2 H.323 and VoIP device interoperability

We can see how H.323 is falling into disuse by looking at endpoint devices (phones in particular). Some years ago, the previous trend of creating devices that could use both protocols was abandoned by many phone manufacturers. The vast majority of devices available on the market today are SIP-only. [2]

3. Ensuring Security in IP Telephony

VoIP technology is the present and future of our telephone communications. But at the same time, we cannot ignore the threats it poses to their security. VoIP has its drawbacks inherent in any IP service, given its complex structure and real-time service requirements. Most of these problems are addressed with secure IP PBXs and phones, deployment of VoIP-optimized firewalls (FWs), security-aware infrastructure upgrades, and

general-purpose security tools. But before resorting to security recommendations, we need to identify existing vulnerabilities and threats.

IP telephony, being a follower of the IP network, inherits from it both advantages and disadvantages of security. IP telephony is considered a unique service of its kind, but it is no better protected than any other IP service, such as e-mail. These services are often the target of attacks, as they have their flaws and vulnerabilities

Conclusion: The analysis showed that the IP telephony service provided on packet-switched networks is currently being actively implemented in corporate networks of the business sector. Saving long-distance voice calls, especially for corporations with large data networks, is an important driver of IP telephony. Transmitting voice traffic on a data network within a business located on a building or campus can also achieve significant cost savings as the operation of modern PBX installations work relatively inefficiently.

There are two very important segments in VoIP: H.323 and SIP. Both protocols are already quite old. H.323 operates at the bit-field level, which, under ideal implementation conditions (not on the Internet), saves network traffic compared to SIP. However, in the current context of the rapid spread of broadband Internet, this advantage no longer looks so significant. SIP is an application layer protocol based on the OSI network model.

References

1. https://www.nextiva.com/blog/ip-phone-systems.html
2. https://www.3cx.com/pbx/h323/

УДК 621.391 (043.2)

О.Ю. Лавриненко
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА TRIPLE PLAY НА БАЗІ ОБЛАДНАННЯ ALCATEL

Сьогодні ринок завойовує технологія мультисервісної мережі Triple Play, надає доступ до всіх видів стандартних та інтерактивних послуг зв'язку: високоякісної телефонії, швидкісного доступу в Інтернет, цифровому телебаченню високої чіткості, відео на запит - по одному інформаційному каналу в квартирі, вдома або в офіс. Телекомунікаційна мережа Triple Play об'єднує всі збудовані комплекси компаній телекомунікацій. Поряд з телепрограмами, можливо слухати і радіопрограми, будуть доступні мережеві комп'ютерні ігри, WEB-чати. Художні і документальні Фільми, можуть зберігатися на мережевих серверах та по Вашому запиту відтворюватися на екрані телевізору.

До думки про необхідність створення реальних комерційних проектів IP– телебачення приходять оператори різного профілю. Сьогодні це можуть бути як «класичні» телекомунікаційні оператори, так і оператори кабельного телебачення. Перші добре знають усе, що пов'язано з класичними мережевими технологія-ми та пакетною передачею даних на базі IP-протоколу, добре розуміють деталі технології Ethernet, однак, як правило, слабо представляють собі елементарні, з точки зору оператора кабельного ТБ, принципи конфігурації цифрових головних телевізійних станцій, склад таблиць сервісної інформації транспортних MPEG-потоків, особливості роботи цифрових супутникових приймальних систем тощо. В свою чергу, оператори кабельного ТБ чудово орієнтуючись у «класичних» цифрових головних станціях, часто відчувають деяку розгубленість, коли йдеться про принципи підбору та конфігурування головної станції IP-TV. Головна станція IP-TV використовує суміжні прикордонні технології як цифрового кабельного телебачення, так і пакетної передачі даних, тому сьогодні не так багато фахівців, які володіють усім одразу.

Розглянемо, як і по яким критеріям вибирати і конфігурувати станцію IP-телебачення. На рис. 1 представлені компоненти IP-TV мережі. Роз-глянемо найважливіші компоненти мережі IP-телебачення.

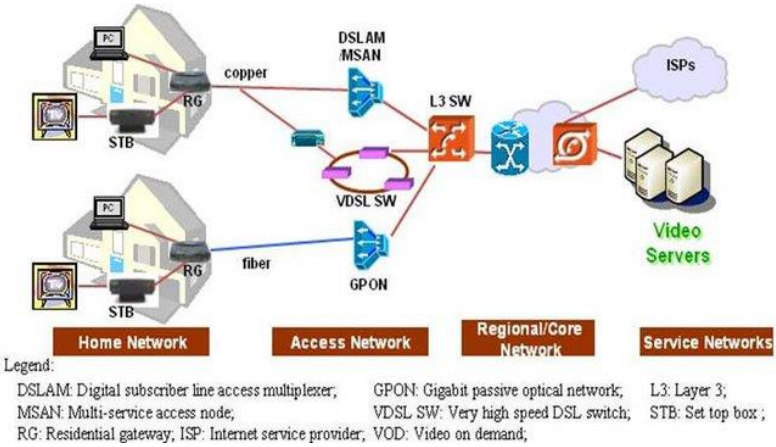

Рис. 1. Головна станція IP-TV в складі транспортної мережі

Alcatel Open Media Suite дозволяє операторам впроваджувати комплексні широкосмугові розважальні послуги і створювати нові джерела доходу. До скла-ду пакету Alcatel Open Media Suite входять такі продукти: 5950 Open Media Platform, 5959 Open Media Content Manager, 5959 Open Media Distribution Manager та відеосервер світового класу 5959 Open Video Server. На базі цих про-дуктів Alcatel пропонує одне з найкращих рішень у галузі. Alcatel Open Media Suite підвищує керованість та гнучкість послуг та дозволяє створювати і достав-ляти конкурентні послуги, налаштовані на потреби конкретного ринку.

Сама велика в галузі база замовників IP-TV і багатий досвід установки рішення допомагають компанії Alcatel полегшувати складні завдання операторського бізнесу.

Alcatel Open Media Suite (OMS) дозволяє операторам створювати і надава-ти практично необмежену кількість каналів мовного ТБ, відео на вимогу (VoD), персональних відеозаписів, електронної програми передач (EPG), перегляду WEB-сторінок та електронної пошти (e-mail) на екрані телевізора і багатьох інших додатків, включаючи ігри, надані сторонніми розробниками або створені з допомогою наданих інструментів розробника (OMS software development kit).

Alcatel OMS працює по ланцюжку від провайдера контенту до кінцевого користувача і включає в себе найкращу в світі платформу middleware, повний на-бір перевірених на практиці прибуткових додатків і систему управління контентом і доставкою послуг, в том числі систему відеосерверів

із необхідним програмним забезпеченням. Широкий набір абонентських функцій дозволяє операторам отримувати усі переваги від широкосмугових мереж доступу і успішно боротися з конкуренцією зі сторони кабельного та супутникового телебачення.

Alcatel OMS розроблений для того, щоб зробити широкосмугові мережі ви-гідними для сервіс-провайдерів, які перетворюються на мультимедійні компанії, що пропонують послуги "три в одному" (triple play), тобто телефонію, інтернет-доступ і розваги мовленнєве телебачення (BTV), відео на вимоги (VoD), персональний відеозапис (PVR), ігри та багато іншого. Alcatel OMS дає можливість широкосмуговим операторам (тобто тим, хто використовує технології DSL, FTTU та ін.) розкривати всі переваги своїх IP-мереж.

Alcatel OMS містить всі компоненти, необхідні для доставки самих різноманітних широкосмугових розважальних послуг та спрощення складних завдань, пов'язаних з управлінням та доставкою контенту: Alcatel 5950 Open Media Platform (Медіа-платформа); Alcatel 5959 Open Media Content Manager (засіб управління контентом); Alcatel 5959 Open Media Distribution Manager; Alcatel 5959 Open Video Server (Система відеосерверів); Irdeto Access PiSys Conditional Access System (CAS - Система умовного доступу); SkyStream Networks iPlex (HeadEnd - Головна приймальна супутникова станція); Thomson IP921 STB (Set Top Box – абонентська ТВ префікс).

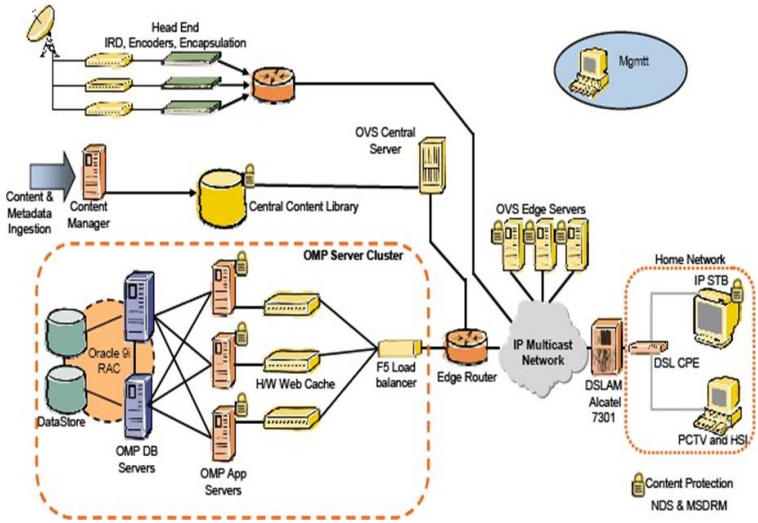

Рис. 2. Відкритий медіа блок Alcatel

Рішення Alcatel передачі відео по IP може бути розгорнуто з використанням великої кількості технологій доступу (xDSL, BPON/GPON FTTP, і Ethernet), по багатьох транспортних мережах передачі даних (ATM, IP, MPLS, Ethernet). Може працювати з будь-якою доступною мережею IP, підтримує QoS і відповідає мінімальним технічним вимогам, поза залежності від технології 2 рівня.

Зокрема, для рішення розробляється архітектура MPLS, яка забезпечує побудову магістральних мереж, що мають практично необмежені можливості масштабування, підвищену швидкість обробки графіки та безпрецедентну гнучкість з точки зору організації додаткових послуг. Крім того, технологія MPLS дозволяє інтегрувати мережі IP та ATM, за рахунок чого постачальники послуг зможуть не тільки зберегти кошти, інвестовані в асинхронне обладнання передачі, але й отримати додаткову вигоду із спільного використання цих протоколів.

Висновок. розглянуті основні питання впровадження мультисервісного доступу Triple Play. Зокрема, передачі відео по IP мережі. Особливу увагу було приділено відео сиг-налу і його характеристикам. В процесі проєктування з'ясувалося, що технологія Triple Play повинна з одного боку, поєднувати у собі гнучкість та можливості швидкого впровадження нових послуг, які потрібні ринку завтра, а з іншої сто-рони, відкривати шляхи переходу до тих видів обслуговування, які здатні забезпечити високі прибутки вже сьогодні. Складність ринкових умов та неоднорідність потреб, диктованих кінцевими користувачами, вимагають пильної уваги до архітектури цього «нового покоління» мереж, щоб все найкраще, що було закладено в мережах «попереднього покоління», не виявилося розгублено в метушні перехідного періоду.

УДК 621.396.96

А.О. Кириченко
Національний авіаційний університет, м. Київ

Аналоговий блок затримки та перетворення сигналів для електрогітари

Поява дилея можна віднести до п'ятдесятих років минулого століття, тоді ефект досягався усуненням зменшених за гучністю копій однієї з доріжок на магнітній стрічці. Потім почалося виробництво стрічкових ехо-машин, у яких магнітна стрічка прокручувалась по колу, її швидкість регулювала час затримки, а ступінь намагнічування – гучність повторів. Цей принцип дії був реалізований у стрічковому дилеї ECHOPLEX EP4. Подібні пристрої мали дуже велику вагу та чималу вартість. Першими, хто замінив магнітну стрічку дискретною аналоговою лінією затримки, були інженери PHILIPS. Але справжній прорив у цій галузі здійснила компанія PANASONIC, яка випустила у продаж чіпи MN3005, MN3007 та MN3205, що дозволили зробити пристрої з ефектом ділів більш доступними та набагато компактнішими.Ефект ділей швидко набув популярності серед музикантів, і виробники почали випускати його у вигляді педалі підлоги і вбудовувати в різні процесори ефектів. В даний час практично всі великі виробники гітарних примочок мають у своїх модельних лінійках гітарні педалі delay. Сучасні ділеї бувають аналогові та цифрові. У цифровому варіанті (digital delay) здійснюється цифрова обробка сигналу (АЦП-пам'ять-ЦАП), а аналоговому (analog delay) – використовуються прилади із зарядовим зв'язком (велика кількість конденсаторів передають один одному заряди під дією синхроімпульсів). Варто зазначити, що цифрові ділі надають більший діапазон часу затримки сигналу. Якщо говорити про розбіжності в звуку, то в аналоговому диле звук буде більш «теплим і розпливчастим», в цифровому - чітким і «холодним». Аналоговий дилей - це тепла і природна луна, що надає вашій музиці ні з чим не порівнянну атмосферу, за яку доводиться розплачуватися кліпінгом і clock noise (високочастотним шумом, що виникає на великих значеннях зворотного зв'язку дилея). Варто згадати про модуляцію в аналогових дилеях, яка нагадує про перші плівкові пристрої та імітує перепади швидкості стрічки, що надають деякий шарм повторам доріжок. Перші цифрові дилеї на основі схем аналого-цифрових та цифро-аналогових

перетворень з'явилися на рубежі 70-х та 80-х. Їхня технологія забезпечувала мінімальну втрату якості сигналу на повторах, тому звук був чітким, читаним, але при цьому досить холодним (порівняно з аналоговими). Найбільш успішною моделлю дилея на основі цієї технології стала BOSS DD-2, що позбавила користувачів від кліпінгу і надавши майже ідеальні повтори. Згодом виробники додали до схем частотні фільтри, імітуючи старі аналогові лінії затримки. Цифрові дилеї, що з'явилися, могли також похвалитися помітно великим часом затримки.

УДК 004.75

O. Lavrynenko
National Aviation University, Kyiv

A MODEL OF TELECOMMUNICATION SYSTEM USING VSAT SATELLITE TECHNOLOGY

Every day, telecommunications networks are becoming more and more in demand and are becoming more and more firmly established in our daily lives. Especially acute is the issue of reducing the cost of technologies and their reliability. VSAT systems have such properties.

1. The concept and definition of the VSAT

A satellite communication station is a complex of equipment for transmitting information over long distances, located in places without a terrestrial network infrastructure.

The exchange of information between satellite stations occurs through an artificial earth satellite (AES) operating as a signal repeater: AES - a communications satellite - receives a signal from one station and, having amplified, transmits to another.

2. The composition of the system

VSAT consists of two main parts - an outdoor antenna post, including an antenna and a transceiver unit (ODU, OutDoor Unit - outdoor unit), and a satellite modem (IDU, InDoor Unit - indoor unit).

The transceiver equipment (ODU) is installed on the irradiator at the focus of the antenna and transmits and receives modulated radio signals via satellite. The ODU includes a semiconductor amplifier (SSPB, BUC), usually of low power, up to 2-3 watts, although it can be more, and a low-noise receiving amplifier-converter (LNB). LNB and BUC are connected to the feed through a polarization selector [en], they receive and transmit a signal in polarizations orthogonal to each other (vertical and horizontal for linear, left and right for circular - depending on the one used by the satellite). The OMT may be included with the ODU or supplied with an antenna. The external unit and the modem are connected by coaxial cables with F or N type connectors. The length of the cable route from the antenna post to the modem is usually up to 20-30 m, when using special types of cables - up to 100 m.

An indoor unit (IDU) is a small desktop unit (satellite modem) that converts information passing between analog communications on the

satellite and local devices such as telephones, computer networks, PCs, TVs, etc. In addition to basic IDU conversion programs may also contain additional features such as security, network acceleration and other features.

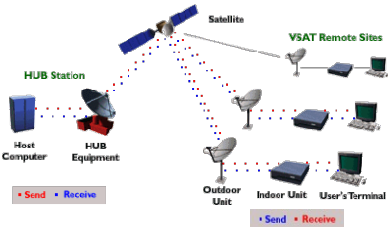

Fig. 1. VSAT network components

3. Advantages and disadvantages

+Compactness. The equipment of the station has small dimensions and weight, is easily transported, quickly and conveniently mounted. The station's VSAT antenna can be mounted on a flat or pitched roof, on a vertical wall, or directly on the ground. If necessary, it can be quickly dismantled and quickly transported to another location. If such a need arises often, it is possible to organize a mobile small earth station, a satellite communication station on a car.

+Ease of obtaining permits. The documents necessary for legal work are obtained simply and are inexpensive. As a rule, operators take care of all the hassle of obtaining permits for the user.

– VSAT installation requires at least 2–3 sq. m on the wall or on the roof, and always on the south or southeast side. If your office is on the first floor of a 5-storey building, and from the south it is blocked from the sun by a 16-storey "Chinese wall", you will have to negotiate a roof lease on that 16-storey building and hang cable "snot" 40–60 m long from there. But if you live on the outskirts of the city or in the countryside, this problem does not exist for you.

– Speed limits. If we ignore the figures written by many operators in their beautiful prospectuses (up to 60 Mbps from the hub, up to 4 Mbps from VSAT), and face the truth, we will see the following: the actual speed of downloading files from the Internet does not exceed 4 Mbps (HN7000 series modems, which Hughes claims is the "most powerful processor in the industry"). The reality is that when using VoIP traffic for transmission, problems begin at 30–40 simultaneously transmitted conversations, and the

point is not in the channel speed, but in the performance of the processor of the satellite modem of the VSAT terminal.

Conclusion: As we saw, VSAT technology has a number of advantages, such as reliability, versatility and autonomy, but also a number of disadvantages, such as price and required conditions for installation. For organizations and enterprises, VSAT will be a good option, but for single users, it is likely to be too expensive and large-scale, but became more accessible every day.

References

1. http://krypton.mnsu.edu/~ga8997yd/whatis_vsat.htm
2. https://www.britannica.com/technology/telecommunication
3. https://www.satixfy.com/dream-sub-100-vsat-getting-closer-reality/

УДК 621.384.3

Ковальчук М.М.
Національний авіаційний університет, м. Київ

«Тепловізійний канал системи моніторингу довкілля»

I. ВСТУП

При високій щільності населення та промислових підприємств у сучасних мегаполісах різко зростає небезпека масового ураження людей при виникаючих надзвичайних ситуаціях та екологічних катастрофах (пожежах, вибухах з виділенням отруйних речовин, забруднення атмосфери транспортом, промисловими підприємствами та ін.).

II. ФОРМУЛЮВАННЯ ПРОБЛЕМИ

Повною мірою це відноситься до Києва, з тією відмінністю, що військові дії та велике зношування промислового обладнання в багато разів збільшує ймовірність виникнення кризових (КС) і надзвичайних ситуацій (НС). У зв'язку з цим різко зростає роль структур, що займаються моніторингом та прогнозуванням КС та НС. У механізмі управління міським господарством особливу роль відіграють системи оперативного попередження про надзвичайні ситуації: пожежі, вибухи, хімічні викиди, екологічні катастрофи тощо.

III. РІШЕННЯ ПРОБЛЕМИ

Автоматична система дистанційного моніторингу «Лідар» призначена для виявлення кризових та надзвичайних ситуацій у місті Київ, одним із показників яких є аварійний аерозольний викид в атмосферне повітря. Стаціонарний пост 1 (СП-1) працює у режимі цілодобового оперативного моніторингу КС. Відповідно до концепції системи, планується встановлення трьох СП із зоною охоплення 10-12 км кожен, що дозволить охопити всю територію Києва. СП-2, другий пост системи АСДМ "Лідар", є еволюційним продовженням СП-1. Сукупність рішень, застосованих у СП-1 і СП-2, послужать основою розробки СП-3 – повністю автоматичного поста. Тепловізійний канал у складі АСДМ «Лідар» призначений для моніторингу в складних метеорологічних умовах, коли звичайні камери не дозволяють вести спостереження. У складі СП-1 тепловізійний канал переконливо довів

свою ефективність, дозволяючи чітко розрізняти шлейфи диму і нагріті тіла від міської забудови.

IV. ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Отже, тепловізійний моніторинг забезпечується вирішенням широкого спектру завдань, які пов'язані з виявленням кризових та надзвичайних ситуацій, управлінням міським господарством, де особливу роль відіграють системи оперативного попередження про пожежі, вибухи, хімічні викиди, екологічні катастрофи тощо. У ході роботи було проведено експерименти, у ході яких виявлено явні переваги та недоліки кожного тепловізора. Зіставивши їх, було обрано тепловізійну камеру «Скат», що задовольняє умовам всіх завдань моніторингу. Висока надійність, тривалий час безперервної роботи, невибагливість до погоди, можливість знімати контрастні теплові зображення вдень і вночі при різних МДВ роблять тепловізор «Скат» незамінним інструментом моніторингу.

Використані джерела

1. Ж. Держсорг. Інфрочервона термографія. Основи, техніка, застосування, 1988 р.
2. Л.З. Криксун. Довідник з основ інфрочервоної техніки, 1978

УДК 004.75

M. Kolchyn, PhD, assoc. prof. O. Gr. Plyushch
National Aviation University, Kyiv

RESEARCH OF TYPICAL ARCHITECTURE OF ONLINE BANKING

Online banking is one of the types of remote banking, by means of which access to accounts and account transactions is provided at any time and from any computer via the Internet. The Internet, as a financial tool, provides banks with excellent opportunities to save on standard transactions related to payment turnover. The cost of the transaction carried out by means of e-business systems is reduced by 80-90%, i.e. the bank does not bear the costs of visual control of submitted documents and communication with the client, and only controls the transaction by means of electronic systems.

1. The concept of Online banking

Internet banking is a type of "home banking" technology remote banking service, which allows the client to receive banking services without visiting the bank office. This technology appeared in the early 80's and has changed significantly since then. There are three main stages in the development of Home banking services:

– Telephone banking - a banking service based on the use of telephones with tone dialing;

– PC-banking, which allows the client with the help of a personal computer and modem to directly connect to the bank's servers and perform banking operations (not via the Internet);

– Electronic banking differs from PC-banking in that extensive Internet capabilities are used to organize interaction with the bank. Is the most promising embodiment of "Home banking" technology.

2. Typical solutions for deploying Online banking

The democratization of financial services has not only affected consumers, but also opened up a wide range of opportunities for entrepreneurs to launch and support online banking without the involvement of IT resources. Banking software companies have played an important role both in improving existing infrastructure and in almost eliminating barriers to entry in a short time and low development costs. Here are some examples of solutions for deploying online banking:

1) User-friendly Design
2) Taking into account the differences of devices
3) Target audience
4) Competition analysis
5) Creating a bank MVP: Definition and Value
6) Types of business models

3. Advantages and disadvantages of Online banking

The advantages of Internet banking for the bank include:

– minimization of operating costs;

– reduction of investments in the development of the branch network;

– expanding the customer base;

– elimination of geographical and temporal barriers to the provision of services.

The disadvantages of Internet banking include:

- the problem of ensuring the security of operations.

- some service functions often require good computer knowledge;

- for Internet banking services, there is also such a thing as a transaction day (transactions are still limited in time).

Conclusion: One can firmly predict the further active development of Internet banking in Ukraine. Its future potential is great, as society is increasingly moving to "online life". Experts say that in the near future through the personal account customers will be able to fully obtain loans by providing all necessary information to the bank online, as well as remotely receive official statements of account. Moreover, one can expect that Internet banking will soon become an integral part of all banking institutions, as customers will expect them to do so.

References

1. Сербина О. Г. Інтернет-банкінг: українська практика та світовий досвід / О. Г. Сербина, О. М. Загузова // Молодий вчений. – 2014. – № 4(07)(1). – С. 122-125.
2. Мошенець О.В. Інноваційні продукти і технології на ринку банківських послуг. Фінансовий ринок України. 2011. № 12. С. 7–8.

УДК 004.725.7 (05.13.06)

В.М. Корчан, аспірант
Національний авіаційний університет, м. Київ
Науковий керівник – Морозова І.В. к.т.н., доцент

АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ ПРИСТРОЇВ І ДОДАТКІВ ІНТЕРНЕТУ РЕЧЕЙ

Вступ

Уразливість мережевої безпеки, що полягає в неможливості аутентифікації пристроїв Інтернету речей, відкриває для зловмисників можливість для виробництва контрафактних фізичних і віртуальних речей. Одним з напрямків забезпечення гарантованої і однозначної ідентифікації пристроїв Інтернету речей (IP) є використання унікального ідентифікатора пристрою IP в МЗЗК в сукупності з параметрами самого пристрою. При цьому треба враховувати, що так званий універсальний ідентифікатор повинен бути сумісний з існуючими методами ідентифікації, такими як IMEI, MAC і ін. Необхідно також відзначити, що кінцевому пристрою інтернету речей з певною фізичною адресою на канальному рівні спочатку призначається відповідний логічний адрес на мережевому рівні, який в подальшому може бути замінений на ідентифікатор на рівні платформи. При цьому дуже важливою властивістю є фіксованість співвідношення ідентифікатора з фізичною адресою Інтернету речей, а також універсальність в застосуванні ідентифікатора в різних галузях.

Основні результати дослідження

Залежно від сфери застосування та вимог користувачів застосовуються різні типи ідентифікаторів. У самій основі Інтернету речей лежить взаємодія між речами і користувачами речей за допомогою допоміжних елементів екосистеми: датчики, виконавчі механізми та бездротовий зв'язок, хмарні платформи та ін. Речі і користувачі повинні бути однозначно ідентифіковані з метою розуміння унікальності того чи іншого об'єкта взаємодії.

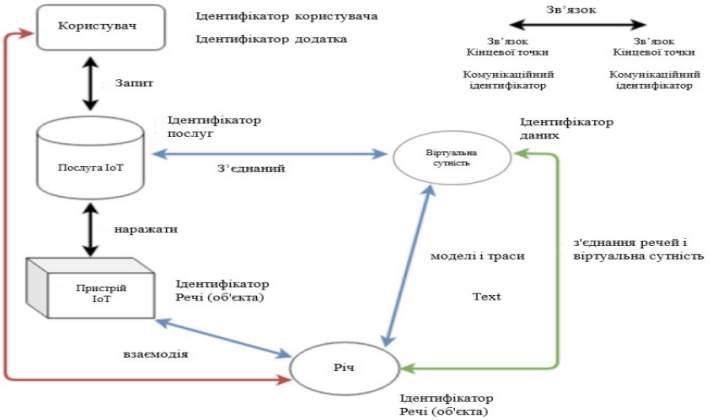

Рис. 1 - Взаємодія різних сутностей з прив'язаними ідентифікаторами в концепції IP

Крім ідентифікації речей, ідентифікації також підлягають Додатки та послуги, користувачі, дані, кінцеве обладнання, протоколи і місця знаходження речей. Ідентифікатор об'єкта визначає цільову сутність Інтернету речей. Це може бути будь-який фізичний об'єкт (обладнання, приміщення, люди) або цифрові дані (файли, набори даних) тобто все, з чим можна взаємодіяти у реальному і віртуальному світі. Крім стандартів ідентифікації певних організацій з розробки стандартів, державними органами визначені ідентифікатори для певних сфер застосування, наприклад, номери соціального страхування та номери автомобілів. Також, компанії можуть мати власні "реалізації" поняття "ідентифікатор", подібно серійним номерам різної продукції.

Висновки

Були проаналізовані системи ідентифікації, їх архітектура, структура ідентифікаторів і приклади їх використання в повсякденному житті. Проведений огляд міжнародної діяльності з досліджень ідентифікації в концепції Інтернету речей показав, що в даний час відсутні прикладні дослідження, присвячені ідентифікації пристроїв і додатків Інтернету речей на базі архітектури цифрових об'єктів. У зв'язку із цим, у дисертаційній роботі особливу увагу необхідно приділити розробці методів і моделей ідентифікації пристроїв і додатків Інтернету речей.

УДК 621.3.089

О.Ю. Лавриненко
Національний авіаційний університет, м. Київ

ЕКВАЛІЗАЦІЯ ГІСТОГРАМИ, ЯК МЕТОД ПОКРАЩЕННЯ ЗОБРЕЖЕННЯ В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

Еквалізація гістограми – це один з найпростіших методів покращення якості зображення. Еквалізацію гістограми проводять в тому випадку, коли в зображенні є багато пікселів зі схожими яскравостями, і мало пікселів з іншими яскравостями.

На гістограмі ми будемо бачити, що на деяких проміжках яскравостей згруповано багато пікселів, в той час як деякі проміжки яскравостей майже не зайняті. При цьому деталі зображення, які зображені цими кольорами, складно розрізнити. Натомість існують такі проміжки яскравості, пікселів з якими взагалі немає на зображенні. Ці вільні проміжки яскравості можна «зайняти» для покращення якості зображення. Для цього роблять еквалізацію гістограм. Якщо маємо піксель початкового зображення з яскравістю k b , яка є k –им рівнем яскравості на гістограмі (k=0…N-1) то яскравість відповідного пікселя результуючого зображення буде розраховуватися:

$$r_k = \sum_{p=0}^{k} H(b_p) = \sum_{p=0}^{k} \frac{N_p}{N}.$$

В результаті еквалізації гістограми яскравості пікселів на ній будуть розподілені рівномірно по всій шкалі яскравостей.

Наведене зображення, яке виглядає дуже темним. Дрібні деталі предметів та людей на ньому розрізнити складно, оскільки вони зображені схожими темними кольорами, які мало відрізняються один від одного. Гістограма цього зображення наведена на рис. 1.1. На ній видно, що багато пікселів знаходяться в лівій частині шкали кольорів, що відповідає темним кольорам. Водночас, права частина шкали майже не зайнята, тобто світлих пікселів на зображенні немає. Цей вільний проміжок гістограми можна використати, щоб перенести туди яскравості деяких пікселів.

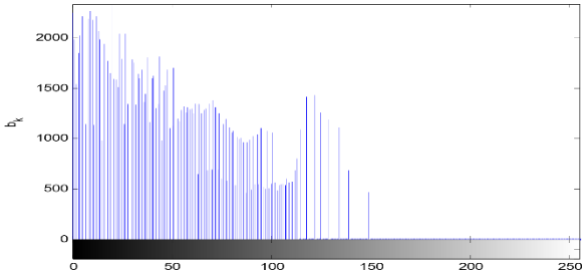

Рисунок 1.1 Гістограма початкового сірошкального зображення

Якщо гістограму цього зображення «розтягнути» на весь доступний діапазон яскравостей, то пікселі, які раніше мали дуже схожі кольори (їх яскравості знаходились близько на шкалі яскравостей), будуть віддалені один від одного на більшу величину яскравості.

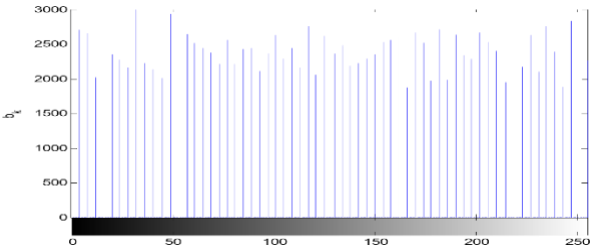

Рисунок 1.2 Гістограма сірошкального зображення після еквалізації

Якщо подивитись на зображення, видно, що діапазон яскравостей пікселів, які присутні на зображенні, розширився: на зображенні тепер є і темні, і світлі пікселі. На гістограмі (рис. 1.2) видно, що з зображенні присутні пікселі всіх яскравостей, і весь діапазон яскравостей тепер зайнятий.

Перевагою еквалізації гістограм є те, що цей метод легко автоматизується і не вимагає задавання ніяких додаткових параметрів для отримання покращеного зображення.

УДК 004.75

A. Lomachevska, PhD, assoc. prof. I. Ye. Terentieva
National Aviation University, Kyiv

ERROR IN TELECOMMUNICATION SYSTEM

A mobile communication system can be defined as a communication system that allows people to communicate without any physical connection, independent of location, time and distance. A modern communications system is needed to support increased data rates, seamless user access to the backbone network, and the integration of multiple services such as video and movie downloads, security tracking, video conferencing, telemedicine, and telerobotics over a wide geographical area.

Table 1.1

Evolution of mobile communication networks from 1G to 5G.

Generation	1G	2G	3G	4G	5G
Band Width	30 KHz	1.25 MHz	5 MHz	20 MHz	100 MHz
Freq. band	824-894 MHz	850-1900 MHz	1.5-2.8 GHz	2-8 GHz	3-300 GHz
Data Rate	Few Kbps	22.8 Kbps	Up to 2 MHz	Up to 20 MHz	1 Gbps/higher
Access	FDMA	CDMA TDMA	WCDMA	OFDM	OFDM MIMO

In practice, the effectiveness of information transmission is limited by the presence of noise in the channel, the physical embodiment of which is random interference in signal transmission. The influence of noise leads to the loss of a portion of the transmitted information. In practice, such losses are compensated, and this requires an additional consumption of sources,

including the transmission time, and, consequently, a decrease in the channel capacity (bit/s).

Errors can be of three types, namely single bit errors, multiple bit errors, and burst errors.

Error tolerance of the information transmission system is the ability to withstand interference created in the external environment, as well as on internal elements of equipment and conductors.

Factors leading to errors:

1. Instability of power supplies of devices;
2. Influence of external factors (operation of electrical installations, atmospheric phenomena)
3. Characteristics of the physical environment
4. Sync errors;
5. Offset of operating points and internal noise of electronic elements of the SPI equipment;
6. Inconsistency of the parameters of the communication channel with the transmitted signals in terms of transmission speed, bandwidth and electrical parameters;

The four main error correction codes are Hamming codes, Binary convolutional code, Reed – Solomon code, Low-density parity check code.

References

1. https://na.eventscloud.com/file_uploads/8cadfdb1f480bd98178c118361792189_war_pap.pdf
2. https://www.tutorialspoint.com/error-detection-and-correction-in-data-link-layer
3. https://www.tutorialspoint.com/error-control-in-data-link-layer
4. http://afu.com.ua/term/interferenciya

УДК 621.392 (043.2)

В.В. Марчук, В.П. Климчук
Національний авіаційний університет, м. Київ

ОЦІНКА МОЖЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LORAWAN В МЕРЕЖІ МЕТЕОЗАБЕЗПЕЧЕННЯ АЕРОПОРТУ

Якість та своєчасність метеорологічного забезпечення авіації – один із основних факторів, які визначають безпеку польотів. Дані, які отримують інструментальними шляхом від метеорологічних датчиків на злітно-посадковій смузі, є основою організації авіаційних перевезень.

Для організації мережі метеозабезпечення пропонується використати перспективну технологію LoRaWAN, яка має комплекс переваг:

- низьке енергоспоживання, можливість автономної роботи кінцевих пристроїв до 10 років від одного акумулятора;

-не значна потужність передавача (25 мВт);

-висока чутливість приймача;

- малий вплив на рівень електромагнітних завад в районі аеропорту;

Виконаємо оцінку практичної приналежності технології LoRaWAN для вказаної задачі.

Щоб використати дану технологію, необхідно провести аналіз необхідної швидкості передачі даних, обсягу метеоінформації, а також необхідної дальності передачі. Відомо, що обсяг метеоінформації, який працює з датчиками на сервері обробки даних незначний. Визначення специфікацій метеодатчиків для аеропортів у будь-якій категорії показує, що швидкість передачі інформації не перевищує значення 10 кбіт/с. Таким чином, з урахуванням запасу на резерві необхідна максимальна пропускна здатність каналу зв'язку досягає величини 20 кбіт/с, при забезпеченні дальності передачі на відстані не більше 5 км.

Залежність радіусу зони покриття мережі LoRaWAN від характеристик сигналу приведена на рисунку.

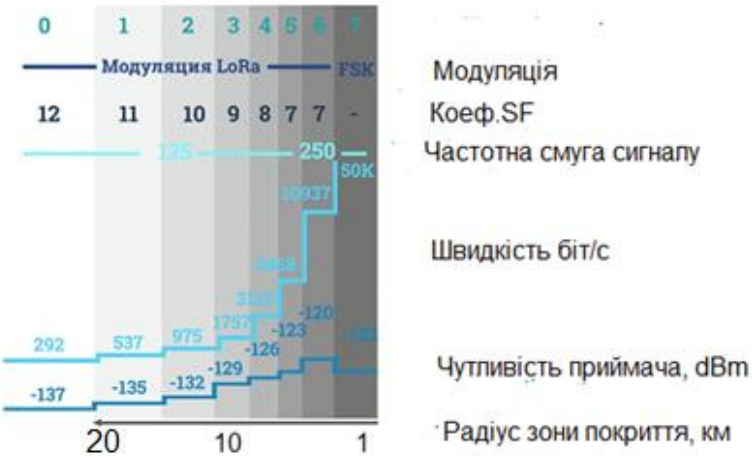

Рис. 1. Залежність радіусу зони покриття мережі LoRaWAN від характеристик сигналу

Проведений аналіз визначає можливість використання технології LoRaWAN для пбудови мережі метеозабезпечення аеропорту.

Список використаних джерел

1. Болелов Э.А. Метеорологічне забезпечення польотів цивільної авіації:

проблеми та шляхи вирішення // Науковий вісник МГТУ ЦА. – 2018. – Т. 21. –

2. LoRaWAN - універсальні логістичні технології. Науковий вісник НТУ КПІ.-2019.-с.24-30.

УДК 621.311 (043.2)

А.О. Мирошниченко, Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА НА БАЗІ ТЕХНОЛОГІЇ POWER LINE COMMUNICATIONS

Мережі доступу реалізують взаємозв'язок клієнтів/абонентів до мереж загального зв'язку. Вони дозволяють великій кількості абонентів користуватися різними телекомунікаційними послугами. Однак витрати на реалізацію, встановлення та обслуговування мереж доступу дуже високі, часто становлять понад 50% інвестицій в мережу. Тому провайдери мереж намагаються реалізувати мережу доступу за якомога нижчою ціною, щоб підвищити свою конкурентоспроможність на дерегульованому телекомунікаційному ринку.

Схема мережі, за принципом якої розроблятиметься мережа в невеликому селищі, зображена на Рис. 1.

В селищі доступ до мережі Інтернет наявний лише в Школі для потреб навчального процесу. У зв’язку з карантинними обмеженнями спричиненими пандемією COVID-19 діти вимушені навчатись дистанційно з дому, що викликало необхідність побудови широкосмугової телекомунікаційної мережі в межах села в найкоротший термін. В якості технології для швидкого розгортання мережі широкосмугового доступу без додаткової прокладки кабелю та залученням значних фінансових витрат була обрана технологія PLC, пропускна спроможність мережі отримана за її допомогою буде повністю задовольняти вимоги дистанційного навчання.

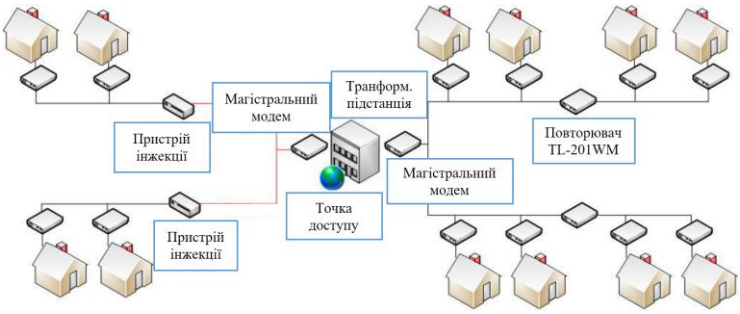

Рис. 1. Схема організації мережі за технологією PLC

Як ми можемо помітити, схема включає і протяжний коаксіальний кабель, і повторювач, і пристрій інжекції. А точка доступу буде розташована на Трансформаторній підстанції.

Побудова мережі PLC з доступом до Інтернету, в своєю чергою, потребує трьох компонентів: адаптер PLC, майстер-пристрій та інтерфейс зі шлюзом (Gateway), DSLAM трансивер. Шлюз підключений до Ethernet (LAN / WAN) і в результаті транспортного середовища для головного пристрою стає Ethernet шлюзом. Настроювання шлюзу контролю програмного забезпечення (у тому числі білінгу та моніторингу) здійснюється постачальником домашньої мережі, що може обробляти трафік PLC та пропонує різні тарифні плани. Таким чином, обладнання PLC – системи операторського класу. Після підключення майстер-пристрій біля входу в будівлю, у всіх сусідів принаймні один вхід буде на загальній шині Ethernet. Щоб підключитися до будинкової мережі, користувачеві не-обхідно отримати MAC-адресу її постачальника, використовуючи існуючі служ-би управління доступом, передбачає, серед іншого, недопущення монополії смуги пропускання, що займається, для доступу в інтернет.

Висновок. В рамках даної роботи було побудовано телекомунікаційну мережу невеликого селища на базі існуючої мережі електропостачання з використанням технології PLC. Низьковольтні мережі живлення, включаючи домашню частину мережі, мають топологію фізичного дерева. Однак на логічному рівні мережу доступу PLC можна вважати мережею шин, що представляє спільне середовище передачі. Оскільки мережі PLC працюють на спільному носії, існує потреба в політиці керування доступом до середовища. Це завдання бере на себе базова станція, яка контролює доступ до середовища по всій або лише частині розглянутої мережі PLC. Базова станція також є точкою, через яку здійснюється можливий доступ до глобальної мережі. Також можуть бути реалізовані додаткові пристрої PLC, такі як повторювачі та/або шлюзи. Низьковольтні мережі були розроблені тільки для розподілу енергії серед домогосподарств, а широкий спектр приладів можна вмикати або вимикати в будь-якому місці і в будь-який час. Така зміна заряду мережі призводить до сильного коливання опору середовища. Ці коливання імпедансу та розриви призводять до багатопроменевої поведінки каналу PLC, що робить його використання для передачі інформації більш делікатним.

УДК 621.398 (043.2)

І.Г. Мясніков, Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

МЕРЕЖА IP-TV НА БАЗІ ТЕХНОЛОГІЇ EPON

Нині в телекомунікаційних мережах застосовуються різні технології передачі. Основою IP – мереж є стек комунікаційних протоколів TCP/IP. IP мережі відкрили можливість надання абонентам однієї з найпопулярніших і найприбутковіших сьогодні послуг – інтерактивних послуг IP телебачення. Рішення базується на прогресивній архітектурі надання послуг за запитом. Технології розвиваються, і вартість обладнання, що встановлюється в абонента, значно зменшилася, з'явилася можливість передачі інформації по широкосмугових мережах передачі даних по протоколу IP. Жодних додаткових витрат користувачеві, який бажає користуватися IP телебаченням, нести не доведеться.

У мережі IP, як у будь-якій іншій мережі, виділяють магістральну мережу, а також мережу доступу. «Кордон» магістральної мережі – це точки підключення локальних мереж до глобальних мереж.

У даній роботі буде розглянуто побудову IP мережі на основі архітектури MPLS (MultiProtocol Label Switching).

У роботі також використовується технологія EPON, завдяки якій між вузлом доступу оператора та абонентським кінцевим пристроєм не потрібно встановлення жодного активного обладнання. Суть технології PON в тому, що між приймальним модулем центрального вузла OLT і всіма абонентськими вузлами ONT створена абсолютно пасивна оптична мережа, що має топологію пасивного дерева. У проміжних вузлах дерева розміщені пасивні оптичні спліттери – невеликі компактні пристрої, які не потребують живлення чи обслуговування. Технологія побудови пасивних оптичних мереж за допомогою Ethernet під назвою GePON або EPON ефективно допомагає вирішити задачу «останньої милі»». Серед переваг цієї технології є суттєва економія оптичних волокон, а це дозволяє витрати значно знизити. Тобто. за допомогою одного єдиного оптичного волокна можливе підклеювання до 64 кінцевих пристроїв, і надання більше 1500 портів Fast Ethernet.

Можливості Ethernet і IP, спільно з технологіями передачі оптоволокном дозволяють побудувати справжні ефективні мультисервісні мережі, а не просто забезпечити широкосмуговий доступ в мережу

Internet. У подібній мережі можна об'єднати і телефонний трафік, і трафік даних та мовлення з усіма супутніми послугами.

Таблиця 1

Фізичні характеристики мережі EPON

	1000BASE-PX10-U	1000BASE-PX10-D	1000BASE-PX20-U	1000BASE-PX20-D
Тип волокна	Одномодове волокно A-DF(ZN)2Y3X4E9/125 0.38F3.5+0.22H3.5			
Число волокон	1			
Довжина хвилі	1310 нм	1490 нм	1310 нм	1490 нм
Напрямок передачі	Висхідний потік	Низхідний потік	Висхідний потік	Низхідний потік
Максимальна відстань	10 км		20 км	
Максимальне згасання	20 дБ	19,5 дБ	26 дБ	24,5 дБ
Мінімальне згасання	5 дБ		10 дБ	

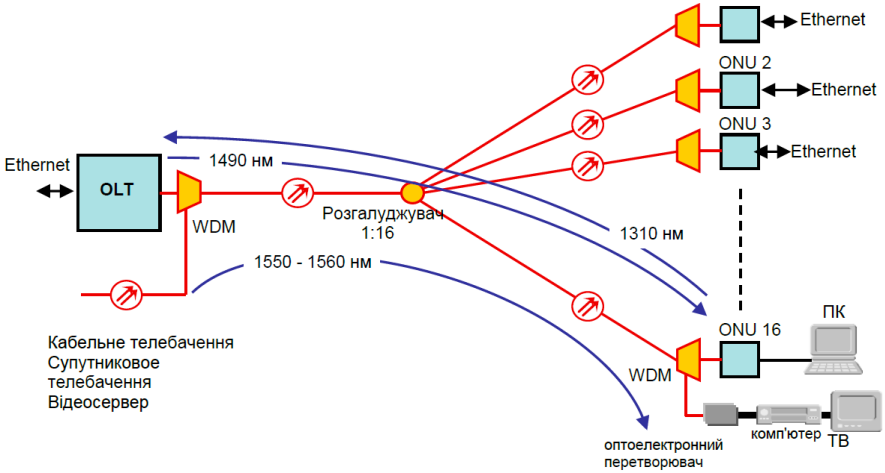

Рис. 1. Мережа EPON, що надає послуги аналогового (AM - VSB) або цифрового (DVB-C) телебачення

Для управління трафіком мережі в EPON потрібен додатковий протокол канального рівня (2 рівень в моделі OSI), саме тому використовується протокол Multipoint MAC Control (MPMC). Цей протокол для управління трафіком використовує три види повідомлень довжиною по 64 байта: GATE (строб), REPORT (повідомлення), REGISTER (реєстрація). Пакет Gate передається від обладнання OLT до ONU, переносячи інформацію про початок і про тривалість часового інтервалу, який зарезервований для посилаються обладнанням ONU пакетів. У повідомленні GATE вказана інформація, що отримується в повідомленні REPORT, яке посилає обладнанням ONU. Повідомлення REPORT містить інформацію про загальну кількість байт даних, що містяться в буфері ONU, обладнання Olt попереджається про те, що ONU підключилося до мережі. OLT також може використовувати протокол MPMC для обчислення часу поширення, а так само відстані до кожного ONU мережі. Дані про час поширення необхідні для виділення необхідних часових інтервалів обладнанню ONU.

Відповідно до стандарту IEEE 802.3 ah, EPON призначений виключно для цифрового зв'язку, а точніше для передачі кадрів Ethernet. але, так як мережі EPON є повністю оптичними, можливе фізичне використання для інших додатків, наприклад для передачі аналогового телебачення. Для цих цілей використовується діапазон довжин хвиль 1550 - 1560 нм (рис. 1).

Висновок. В даній роботі були розглянуті технології EPON і MPLS, ґрунтуючись на яких було вироблено проєктування IP мережі, призначеної для надання послуг IPTV в місті Жовті Води Дніпропетровської області. В роботі був проведений вибір обладнання, що дозволяє надати найбільш ефективним способом послугу IP телебачення. Обґрунтування вибору обладнання проводилося з урахуванням: технічних характеристик, можливості застосування, вартісних характеристик.

УДК 621.396.2, 621.396.6 (043.2)

Д.О. Навроцький
Національний авіаційний університет, м. Київ

ПІДКЛЮЧЕННЯ SWO ДО ПРОГРАММАТОРА ST-LINK V2

Основний недолік клону ST-Link v.2 це відсутності розпаяних контактів SWO (Serial Wire Output) та VCP (Virtual COM port) і, як наслідок, неможливість використовувати SWD (Serial wire debug).

Переробимо ST-Link v.2 щоб скористатись можливостями ITM (Instrumentation Trace Macrocell) в STM32CubeIDE, а саме, це дозволить використати команду *printf* та відслідковувати значення змінних не через UART, а по SWO.

Підріжемо ніжку живлення +5В і замість неї використаємо SWO припаявши послідовно опір 22 Ом (див.рис.1) [1].

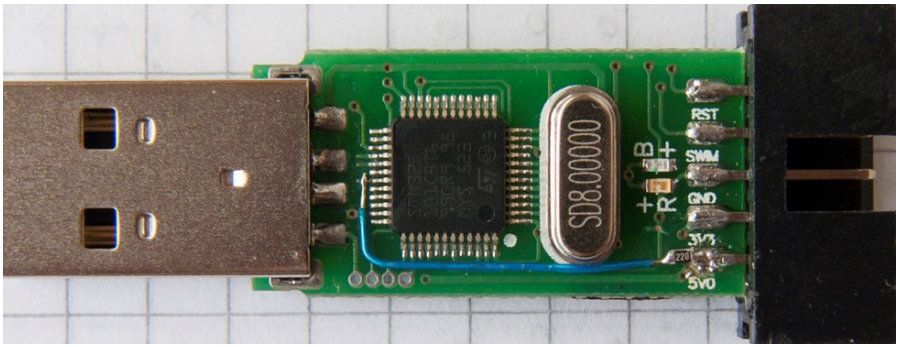

Рисунок 1 – ST-Link v2 в якому SWO замість відрізаного контакту +5В

Рекомендується [2] крім 22 Ом ще зробити підтяжку 10 кОм до живлення, але, перевірили, працює і без підтяжки.

Перевірку робили з використанням STM32CubeIDE та плати STM32F401CCU6 [3]. Оскільки SWO вже припаяний до ST-Link v.2, то для Debug обираємо не Serial Wire, а Trace Asynchronous Sw [4].

Тепер можна передавати дані не через UART у консоль, а використовувати команду *printf* (див.рис.2), для цього потрібно добавити дещо у код (див. стр.76 документу AN4989 [5]).

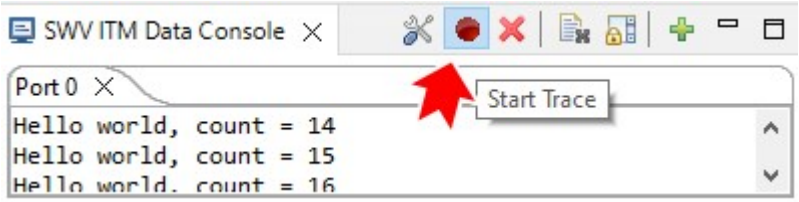

Рисунок 2 – Відслідковування даних з порту (те, що передається командою *printf*), які надходять по SWO

Якщо цікавить не тільки вивід даних через *printf*, а ще і ввід даних через *scanf*, то STM32CubeIDE, це не підтримує [6] і потрібно використати Keil або IAR.

Висновки.

1. Можна використовувати SWO в клоні ST-Link v.2, не змінюючи його прошивки на v.2.1.

2. Можна виводити дані командою *printf* у ITM консоль в IDE (STM32CubeIDE, Keil, IAR) замість використання UART і виводу в звичайну консоль (термінал).

.

Список літератури:

1. *“Adding Trace support to ST-Link clones” [електронний ресурс]. – Режим доступу: https://lujji.github.io/blog/stlink-clone-trace/*

2. *“Getting Started with Instrumentation Trace Macrocell in STM32CubeIDE ” [електронний ресурс]. – Режим доступу: https://medium.com/@g.bharathraj19/getting-started-with-instrumentation-trace-macrocell-in-stm32cubeide-4af179eb0034*

3. *“Плата STM32F401CCU6”[електронний ресурс]. – Режим доступу: https://www.mini-tech.com.ua/stm32f401-board*

4. *“STM32 Debugging With ST-Link v2 SWD | Serial Wire Viewer” [електронний ресурс]. – Режим доступу: https://deepbluembedded.com/stm32-debugging-with-st-link-v2-swd-serial-wire-viewer/*

5. *AN4989 “STM32 microcontroller debug toolbox” [електронний ресурс]. – Режим доступу: https://www.st.com/resource/en/application_note/dm00354244-stm32-microcontroller-debug-toolbox-stmicroelectronics.pdf*

6. *“Serial Wire Viewer (SWD + SWO)” [електронний ресурс]. – Режим доступу: https://www.codeinsideout.com/blog/stm32/swv/*

УДК 004.056.5

В.С. Наконечний, В.Г. Сайко, А.П. Лінецький
Київський національний університет імені Тараса Шевченка, м. Київ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ АВТОРИЗАЦІЇ ЗА РАХУНОК ВИКОРИСТАННЯ ВЕБ-ТОКЕНУ JSON

Вступ

Відомо, що для забезпечення безпеки ІС використовуються різні механізми. При цьому найбільшу загрозу представляють атаки, спрямовані на порушення протоколів автентифікації та авторизації. В сучасних ІС перевага надається методам автентифікації за допомогою веб-токенів JSON [1-5]. Проте і в таких методах авторизації є недоліки. Тому покращення методів автентифікації та авторизації за допомогою веб-токенів JSON є актуальним завданням.

Структура JWT

JSON Web Token – це JSON об'єкт, визначений у відкритому стандарті RFC 7519 [5]. Коли користувач входить до системи, кожен наступний HTTP-запит включає JWT, який дає йому доступ до захищених служб та ресурсів веб-застосунків. JWT токен розділений на три частини: Header – заголовок; Payload – корисні дані; Signature – підпис. Заголовок (Header) містить у собі інформацію про те, як повинен обчислюватися JWT підпис. Заголовок передається у вигляді JSON об'єкта. Корисні дані (PayLoad) – зберігаються всередині токена JWT, їх ще називають JWT claims (заявки). Алгоритм кодує заголовок та корисні дані, з'єднує закодовані дані через точку і далі отриманий рядок хешується алгоритмом, заданим у хедері на основі секретного ключа [2-5]. Сенс використання JWT – це перевірка того, що надіслані дані були з авторизованого джерела і, що дані були закодовані та підписані. Користувач, який хоче авторизуватися, переходить на сервер автентифікації, де перевіряються його облікові дані та створюється JWT. У JWT сервер автентифікації включає такі дані, як ім'я користувача, емітент токена, тему токена, дату випуску, а також дату закінчення терміну дії токена. Далі сервер автентифікації створює заголовок, що сповіщує, який тип токена і який алгоритм підпису та розміщує це значення в заголовок токена. Потім створюється підпис JWT, що має вбудовані функції безпеки, завдяки яким він забезпечує автентифікацію відправника та захист цілісності. Для мінімізації ймовірності атак при використанні JWT потрібно дотримуватись наступних рекомендацій:

1. Токени бажано використовувати з коротким терміном дії. Вони мають бути дійсними лише кілька хвилин, щоб клієнт міг розпочати роботу.

2. Токен бажано використовувати лише один раз. Сервер програм видає новий токен для кожного завантаження.

3. Не рекомендується використовувати JWT для постійних, довготривалих даних.

4. Рекомендується використовувати під час передачі токенів захищене з'єднання та не передавати в токенах чутливі дані користувача, обмежившись знеособленими ідентифікаторами.

5. Використовувати ключові фрази великої довжини, що складаються з великих і малих літер латинського алфавіту, цифр і спецсимволів, та зберігати їх у суворій конфіденційності. Забезпечити періодичну зміну ключової фрази.

Авторизація з використанням веб-токену JSON з додатковим сервісом управління доступом за допомогою Redis

Запропонований метод із вбудованим сховищем та підтримкою перевірки дублювання токенів працює наступним чином.

Користувач вводить дані для автентифікації до клієнтської частини, переходить на сервер автентифікації, де перевіряється облікові дані користувача та створюється JWT. Далі токен зберігається в базі даних Redis та повертається до клієнта, де зберігається в локальному сховищі. Коли користувач входить до системи, кожен наступний HTTP-запит включає JWT, який дає йому доступ до захищених служб та ресурсів веб-застосунків. Сервер автентифікації перевіряє облікові дані користувача, здійснює декодування та перевірку на наявність JWT в базі даних Redis. Якщо токен є, то він його видаляє й створює новий токен.

Висновок

Запропонований метод авторизації з використанням веб-токена JSON та базою даних Redis дозволяє уникнути використання вкраденого зловмисниками токена. Результати цього дослідження можуть бути використані при впровадженні систем авторизації в різні ІС та для механізму надання прав доступу конкретним користувачам або групі користувачів з метою підвищення ефективності захисту інформації.

Література

[1] Jones M. B. et al. JSON Web Token (JWT) profile for OAuth 2.0 client authentication and authorization Grants. – 2016.

[2] RFC 7515. JSON Web Signature (JWS). [Електронний ресурс] – https://datatracker.ietf.org/doc/html/rfc7515

[3] RFC 7516. JSON Web Encryption (JWE). [Електронний ресурс] – https://tools.ietf.org/html/rfc7516

[4] RFC 7518. JSON Web Algorithms (JWA). [Електронний ресурс] – https://datatracker.ietf.org/doc/html/rfc7518

[5] RFC 7519. JSON Web Token (JWT). [Електронний ресурс] – https://tools.ietf.org/html/rfc7519

[6] RFC 8725. JSON Web Token Best Current Practices. [Електронний ресурс] – https://datatracker.ietf.org/doc/html/rfc8725

УДК 05.13.21 (043.2)

В.Р. Обремський
Національний авіаційний університет, м. Київ

МЕТОДОЛОГІЯ ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Сьогодні інформація вважається стратегічним національним ресурсом – одним з основних багатств країни. Під впливом інформатизації всі сфери життя суспільства набувають нових якостей: гнучкості, динамічності тощо. Однак водночас зростає й потенційна вразливість суспільних процесів від інформаційного впливу.

Широке використання в процесі інформатизації суспільства сучасних технологій автоматизованої обробки інформації та управління технологічними процесами створило не тільки об'єктивні передумови підвищення ефективності всіх видів діяльності особи, суспільства та держави, але і ряд проблем захисту інформації.

Під захистом інформації розуміється комплекс заходів, які здійснюються власником інформації щодо виокремлення своїх прав на володіння й розпорядження інформацією, створення умов, які обмежують її поширення, виключають чи суттєво ускладнюють несанкціонований, незаконний доступ до таємної інформації та її носіїв.

Проектування систем захисту інформації – це комплексна проблема, в якій в складному взаємозв'язку перемежовуються задачі моделювання, аналізу, синтезу, оцінки, відбору альтернатив і прийняття рішень на створення складних технічних і програмних систем захисту і організаційних заходів по забезпеченню безпеки інформації на об'єкті.

Проектування по етапам робіт можна поділити на наступні роботи:

1. Ескізне проектування;
2. Технічне проектування;
3. Робоче проектування (розробка експлуатаційної документації);

На етапі ескізного проектування здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Зміст та стиль документації повинні

бути достатніми для повного опису проектних рішень рівня ескізного проекту.

Основна увага при технічному проектуванні СЗІ приділяється аналізу функціонування системних, технічних, програмних об'єктів СЗІ з метою визначити вплив різних факторів на правильність, функціональність і економічну ефективність їх роботи.

На етапі робочого проектування здійснюється розроблення, оформлення та затвердження робочої та експлуатаційної документації СЗІ та, у разі необхідності, її окремих складових частин.

При використанні методології системного підходу до процесу проектування багато проблем в цій області можуть бути вирішені. Головним при цьому є положення в тому, що специфіка складних технічних, програмних об'єктів СЗІ і процесів не вичерпуються особливостями складових їх функціональних елементів; вона заключається в характері зв'язків і відношень між ними. Розширення вихідної бази уявлень шляхом застосування понять, таких як «структура», «функція», «зв'язок», «відношення», забезпечує системному підходу в технічному проектуванні СЗІ переваги перед традиційним методами і дозволяє створювати більш адекватні діям середовища моделі складних технічних, програмних об'єктів СЗІ.

Виходячи з основних положень системного підходу послідовність рішення багатоваріантних проектних задач можна представити у вигляді загальносистемної схеми технічного проектування СЗІ, яка уявляє собою загальну методологію технічного проектування СЗІ.

Проектно-конструкторський процес, яким є етап технічого проектування СЗІ, носить ітераційний характер, причому результат одного етапу є постановкою задачі для іншого. Слід також пам'ятати, що кожен етап, в свою чергу, реалізується в вигляді визначеної послідовності проектних процедур і операцій.

Постановка загальної задачі створення нових технічних, програмних об'єктів СЗІ, їх концептуальне проектування є, в основному, творчими етапами і в цієї якості важко піддаються формалізації, хоча є великий шлях для досліджень в напряму автоматизації методик аналізу варіантів рішень і прийняття рішень на різних стадіях проектування. Для чого необхідно визначити критерії і показники.

УДК 004.4’2 (043.2)

М.С. Одарченко, М.Ю. Заліський, Р.С. Одарченко
Національний авіаційний університет, м. Київ

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ SMS У МЕРЕЖАХ П’ЯТОГО ПОКОЛІННЯ

Інтернет речей (IoT) в даний момент дуже швидко розвивається, збільшуючи кількість об’єднаних пристроїв, згідно з деякими прогнозами [1], з 2.1 мільярда пристроїв до більш ніж 5 мільярдів пристроїв до 2027 року. І серед багатьох факторів, які пришвидшують цей ріст, одним з головних є розвиток мереж п’ятого покоління (5G) [2].

Згідно останніх даних, 5G мережі зможуть забезпечити майже вдесятеро більшу швидкість, ніж мережі LTE. Це збільшення швидкості дозволить IoT пристроям ділитися інформацією ще швидше. Окрім збільшення швидкості, мережі 5G матимуть покращену надійність.

Розвиток мобільних мереж надає користувачам широкий вибір каналів зв’язку та передачі даних, але SMS (Short Message Service) все ще залишається одним з каналів який найширше використовується і його важливість продовжує зростати. SMS є єдиним каналом, який забезпечує покриття у майже 5 мільярдів користувачів мобільних пристроїв, а також зростаючою кількістю IoT пристроїв.

Безперебійна підтримка та доступ до Person-to-Person (P2P) SMS залишається обов’язковим сервісом при переході користувачів у мережі 5G [3]. Окрім цього, використання Application-to-Person (A2P) CMC Ентерпрайз компаніями продовжує зростати.

CMC в мережах 5G може доставлятися як за допомогою IP підключення через IP-SM Gateway, так і без IMS інфраструктури, через SMSF (SMS over NAS) [4] у більш спрощеному варіанті. І хоч обидва варіанти є необхідністю у 5G, SMSF є особливо важливим для використання у IoT та M2M (Machine to machine) середовищах.

Основною технологією в IoT, яка використовує SMS є SIM OTA (Over-The-Air) [5]. OTA дозволяє оператору зв’язуватись, закачувати додатки, а також управляти SIM-картою не маючи до неї фізичного доступу. OTA надає можливість змінювати конфігурацію SIM-карти, а також активувати додаткові сервіси віддалено. Сервери оператора генерують запит через OTA-шлюз, який перетворює його на SMS і відправляє пристрою/пристроям через SMSF.

SMS також може використовуватись в разі коли IoT пристрої мають обмежену автономність та не можуть постійно перебувати в режимі активної передачі даних. Це можуть бути такі пристрої, як датчики температури, електричні, газові та інші типи лічильників. Дані з цих пристроїв можуть передаватись з певною періодичністю використовуючи SMS. Для пристроїв, які передають дані через IP мережі, SMS може використовуватись задля активації пристрою та початку передачі даних.

Хоч SMS технологія була представлена світові майже 30 років тому, як ми бачимо використання SMS як каналу зв'язку зі зростаючою кількістю абонентів у світі, а також збільшення кількості IoT пристроїв, залишають цей сервіс дуже важливим і в мережах нового покоління. Універсальний доступ, простота та надійність залишають SMS одним з улюблених сервісів для взаємодії між цифровими компаніями і їх клієнтами. Таким чином, технологія SMS залишається актуальною та має широкі перспективи використання в мережах нового покоління.

[1] *Ericsson: IOT Connections Outlook. URL: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook/ (дата звернення: 30.05.2022).*
[2] *ETSI: What is 5G. URL: https://www.etsi.org/technologies/5G (дата звернення: 30.05.2022).*
[3] *The 5G Messaging Service. URL: https://www.gsma.com/futurenetworks/wp-content/uploads/2020/04/5G-Messaging-White-Paper-EN.pdf (дата звернення: 30.05.2022).*
[4] *GSMA: SMS Evolution Version 2.0. URL: https://www.gsma.com/newsroom/wp-content/uploads//NG.111-v2.0.pdf (дата звернення: 30.05.2022).*
[5] *Over-The-Air (OTA) technology. URL:ftp://www.3gpp.org/tsg_sa/WG3_Security/TSGS3_30_Povoa/Docs/PDF/S3-030534.pdf (дата звернення: 30.05.2022)*

УДК 662.74.002 (043.2)

Є.О. Олійник, В.В. Антонов
Національний авіаційний університет, м. Київ

ОПТИЧНА МЕРЕЖА ПІДПРИЄМСТВА З АРХІТЕКТУРОЮ DEEP FIBER

Останнім часом постачальники послуг на ринку доступу дедалі частіше говорять про перехід своїх підприємств до архітектури Fiber Deep (FD). Хоча тенденція до прокладання оптоволокна у кабельній системі і скорочення каскадів RF-підсилювачів не є новою, сьогоднішні обговорення здаються провісниками набагато більш значних змін у розподільчих мережах. Зміни стосуються не тільки фі-зичного обладнання, а й змін як в управлінні, так і в повсякденній роботі доступу. Але що таке Fiber Deep та які зміни вона має на увазі?

Щоб оцінити значення Fiber Deep, корисно зрозуміти кілька речей. По-перше, нам потрібно описати фізичні зміни у системі доступу та їх вплив як на оператора, так і на його клієнтів. Потім нам потрібно визначити ті операційні зміни, які призводять до очікуваних покращень кабельної системи, обслуговування та усунення несправностей у майбутньому. Нарешті, нам потрібно зверну-ти увагу на екосистему послуг та доставки додатків, яка допомагає постачальнику послуг орієнтуватися у варіантах, щоб отримати вигоду з переваг Fiber Deep та краще кількісно оцінити окупність інвестицій.

Сьогодні в нових сценаріях оператори стали частіше прокладати оптоволокно до будинку або MDU (Fiber to the Premise - FTTP), оскільки з точки зору виробника це сприймається як кінцевий результат. У зв'язку з постійним зростанням швидкості широкосмугового доступу, оператори тепер починають розглядати можливість переходу HFC на FTTP також і для існуючих сценаріїв.

Для цього необхідно детально розглянути приклад кількох фактичних конструкцій вузлів та досліджувати вплив на вартість різних модернізацій підприємства; від простого поділу вузлів до вирішення звичайних вимог, аж до FTTP. Також необхідно висвітлюювати деякі новітні інноваційні концепції архітектури розподіленого вузла, яка економічно ефективно дає можливість розробки Fibre Deep (FD), таких як Fiber to the Last Active (FTTLA) або Fiber to the Curb (FTTC).

Необхідно починати з комплексного аналізу пропускної здатності мережі, який показує, які потужності можуть знадобитися і в який час

протягом найближчих десятиліть. Це дозволяє розробити стратегію міграції HFC на FTTx протягом 10+ років. Аналіз чистої поточної вартості показує, що цей багатоетапний підхід є більш економічно ефективним, ніж занурення в FTTP. Це також покаже, що для багатьох або більшості передплатників на сьогоднішній HFC FTTP може не обов'язково бути кінцевою точкою, швидше FTTLA або FTTC може бути достатньо.

Інтернет розвивається з шаленою швидкістю з моменту свого заснування. І разом із цим ми спостерігаємо відповідне зростання пропускної здатності виділеної мережі.

На рисунку 1 показано зростання різних рівнів обслуговування протягом наступних двох десятиліть. У той час як 1% абонентів у найвищому рівні «білбордів» досягли б 10 Гбіт/с приблизно в 2024 році, 14% підключень на рівні продуктивності не досягають цієї позначки до ~2032 року. Зауважте, що 85% абонентів флагманського базового та економічного рівня залишаються нижче цієї позначки протягом кількох десятиліть.

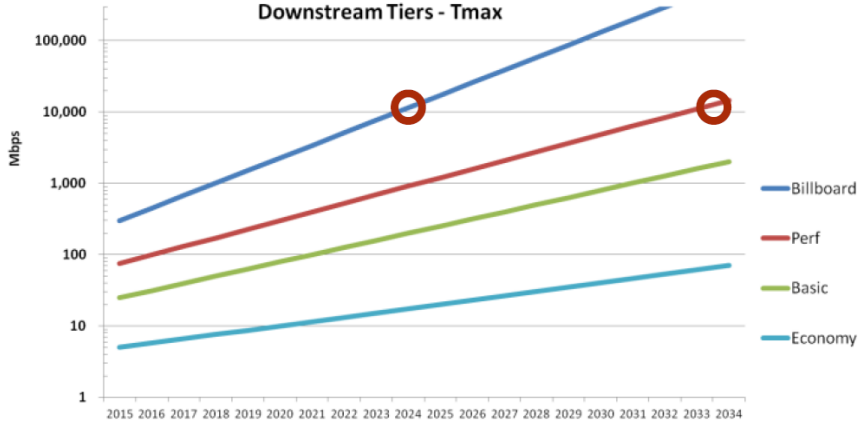

Рис. 1. Зростання низхідного потоку з кількома рівнями обслуговування

Дані були введені в модель пропускної здатності мережі ARRIS, щоб ближче розглянути зростання мережевого трафіку.

Важливо зазначити, що 99% абонентів все ще комфортно використовують сучасну технологію DOCSIS на HFC через десять років.

Деякі результати моделі пропускної здатності мережі ARRIS показані на рисунку 2. Вона дає уявлення про Tmax і SG Tavg поведінку. Пропускна здатність, необхідна для верхнього рівня «білбордів», домінує в порівнянні з SG Tavg.

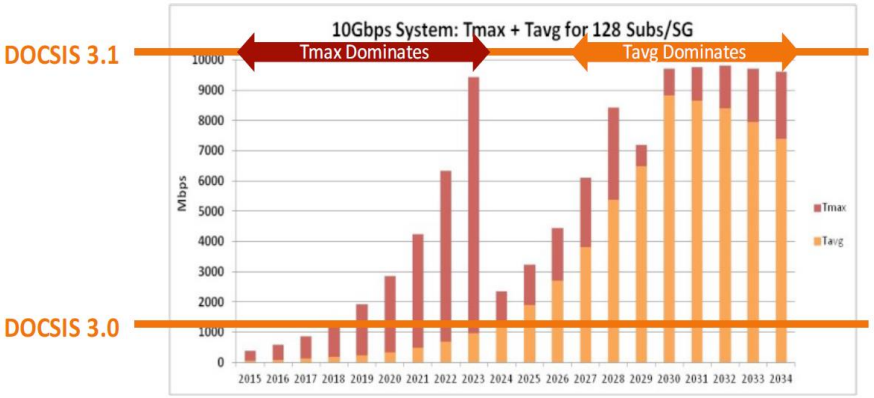

Рис. 2. Результати моделі пропускної здатності мережі

Це приводить нас до стратегії вибіркової міграції передплатників, яку потрібно буде розпочати протягом наступних 5-8 років. Переміщення верхнього рівня «білбордів» до мережі доступу Fiber Deep, яка відокремлена від загальної побудови з HFC, значно зменшує необхідну потужність DOCSIS. Це зменшення можна побачити в 2024 році на рисунку 2, після того як верхній рівень «біл-бордів» буде вилучено з мережі HFC. Рівень продуктивності потім переміщується в 2029 році, для меншого зниження.

Зверніть увагу, що мережа доступу Fiber Deep може бути одним із кількох варіантів FTTx, включаючи: FTTP, Fiber to the Curb (FTTC), Fiber to the Tap (FTTT), Fiber to the Last Active (FTTLA) або Node+0 HFC. Ці варіанти детально розглянуто далі.

Зрештою, коли верхні рівні переведені на FTTx, SG Tavg нарешті наздоганяє, і операторам доведеться знову розглянути можливість зменшення розмірів SG. Модель у цьому прикладі передбачає, що це буде приблизно через 10-15 років.

Інше спостереження з цього аналізу полягає в тому, що D3.1 є ключовою технологією для продовження терміну служби HFC на десятиліття вперед, особливо для переважної більшості (наприклад, 65-

95%), які знаходяться у флагманському базовому та економічному рівнях. Будь-який перехід до FTTx може за-йняти десятиліття, тому D3.1 успішно пропускає операторів через це вікно.

Підсумовуючи, стратегія вибіркової міграції абонентів є розумним підходом до теми переходу HFC до FTTx. Перехід вищих рівнів на FTTx може придбати HFC додаткові десятиліття для 80 - 95% передплатників у флагманських базових/економічних рівнях. Tmax домінує протягом наступних 5-7 років, тому важливіше збільшити потужність HFC принаймні до 1 ГГц спектру, а не розділити вузли. Однак Tavg нарешті наздоганяє через 8-10+ років; і зменшення розміру SG повертається в моду. Оператори повинні просувати Fibre Deep, щоб за запитом увімкнути Selective FTTx для верхніх рівнів та бути готовими до наступного етапу поділу SG.

А який FTTx є найкращим варіантом — це ще одна цікава дискусія. DOCSIS продовжує розвиватися, працюючи над повним дуплексом (FDX) і DOCSIS з розширеним спектром. Деякі з цих досліджень були висвітлені в. Ці нові технології обіцяють зробити для DOCSIS і кабелю те, що G.fast намагається зробити для DSL і витої пари.

Висновок. Підсумовуючи, стратегія вибіркової міграції абонентів є розумним підходом для переходу з HFC до FTTx. Перехід вищих рівнів на FTTx може придбати HFC додаткові десятиліття для 80-95% передплатників у флагманських базо-вих/економічних рівнях. Tmax домінує протягом наступних 5-7 років, тому важливіше збільшити потужність HFC принаймні до 1 ГГц спектру, а не розділити вузли. Однак Tavg нарешті наздоганяє через 8-10+ років; і зменшення розміру SG повертається в моду. Оператори повинні проштовхувати волокно достатньо глибоко, щоб увімкнути селективний FTTx для вищих рівнів за запитом, і бути готовим до наступного раунду розподілу SG.

УДК 681.142 (043.2)

О.Ю. Лавриненко
Національний авіаційний університет, м. Київ

ФОРМУВАННЯ МЕРЕЖІ ZIGBEE МОНІТОРИНГУ РУХОМОГО ОБ'ЄКТУ

Для формування мережі перший вузол який виконує функції координації починає формувати мережу і є координатором мережі PAH. Коли інший вузол хоче приєднатися до ран координатора, він відправляє запит до нього, якщо координатор мережі має можливість прийняти даний вузол, він відправляє відповідь про згоду прийняття. Якщо вузол бажає вийти з мережі він відправляє запит про вихід, до координатора ("батьківського вузла"). Він може покинути мережу після отримання відповіді "видалення". Більше того вузол, який залишає мережу, повинен видалити всі зв'язки з іншими вузлами мережі, якщо він має дочірні вузли.

Для організації нової мережі ZigBee є три типи пристроїв:

- координатор формує топологію мережі і встановлює з'єднання з іншими мережами (в кожній ZigBee-мережі є тільки один координатор);

- маршрутизатор необхідний як проміжна ланка, передає в потрібному напрямку дані від інших пристроїв;

- кінцевий пристрій передає дані координатору або машрутизатору і не може зв'язуватися з подібними йому пристроями.

За організацію нової мережі і призначенням адрес новим пристроям відповідає мережевий рівень NWK.

У специфікації стандарту IEEE 802.15.4 визначається можливість трьох ти-пів передачі даних:

а) передача від пристрою до мережевого координатора;

б) передача даних від мережевого координатора до пристрою;

в) передача даних між двома одноранговими пристроями.

У випадку якщо пристрій збирається передати дані координатору, виконує пошук маячка. Коли він знайдений, даний вузол підлаштовується до структури суперфрейма. Використовуючи слотовий механізм CSMA / CA пристрій передає дані координатору. У відповідь координатор відсилає фрейм повідомлення про отримання. Цикл обміну закінчується.

Структура кадру забезпечує надійну передачу. Побудований відповідно до моделі OSI, кожен наступний рівень додає до протоколу свій заголовок. Стандарт передбачає чотири типи фреймів:

а) фрейм маячка;

б) фрейм даних;

в) фрейм повідомлення про отримання;

г) фрейм команд MAC-підрівня.

Фрейм даних (рисунок 1) використовує для синхронізації преамбулу і поле "Старт". Поле "Довжина" містить довжину поля MAC підрівня в 8-бітових байтах (октетах). Службову Інформацію про управління фреймами містить поле "Управління". Інформацію про порядковий номер даних містить поле "Номер", адресну інформацію, а саме 16-бітний короткий або 64-бітний розширений містить поле "Адреса". Фрейм завершується полем контрольної суми КС.

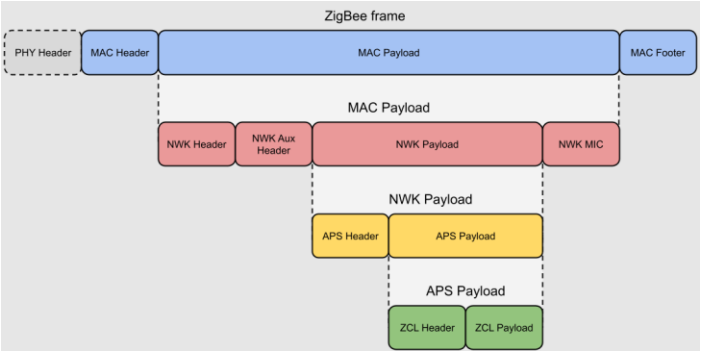

Рис. 1. Формат фрейма даних протоколу ZigBee

Пакет даних складається з деякої кількості бітів переданих в певному форматі. Приймач повинен мати механізм визначення помилок при відновлення вихідного повідомлення. IEEE 802.15.4 використовує 16-бітну перевірку кадру (FCS) на основі надлишкового циклічного коду (CRC) для виявлення можливих помилок в пакеті даних. При цьому мережа може вибрати для використання 16-бітну або 64-бітну адресацію. Топологія ZigBee мережі може мати форму зірки (рисунок 2), дерева (рисунок 3) або комірчастої мережі (рисунок 4).

У топології типу" зірка " мережа контролюється координатором. При цьому він відповідає за ініціалізацію і обслуговування мережевих пристроїв і всіх кінцевих пристроїв, безпосередньо взаємодіючих з

ним. Всі мережі зоряної топології функціонують незалежно одна від одної. Мережевий ідентифікатор не використовується іншими мережами, що знаходяться в межах радіусу дії даної мережі (рисунок 2).

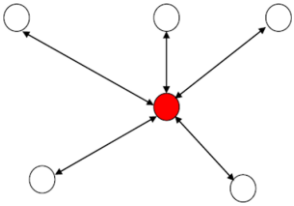

Рис. 2. Топологія мережі ZigBee "зірка"

У комірчастої (рисунок 4) і деревоподібної структури (рисунок 3) мережі координатор відповідає за організацію мережі і вибір деяких ключових параметрів, але мережа може бути розширена за допомогою ZigBee маршрутизаторів. У мережі з деревоподібною топологією маршрутизатори переміщують дані і Керуючі повідомлення по мережі, використовуючи ієрархічну стратегію маршрутизації. Деревовидні мережі можуть використовувати маячкову стратегію маршрутизації.

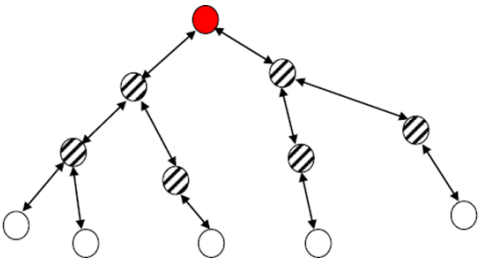

Рис. 3. Деревоподібна топологія мережі ZigBee

Комірчаста мережа - це однорангова комунікація пристроїв, в даній мережі немає пристроїв різних рангів (всі пристрої рівноправні).

Кілька мереж можуть взаємодіяти. Для цього кожна мережа має унікальний мережевий ідентифікатор. Таким чином, повна адреса пристрою для доступу з іншої мережі складається з адреси мережі та короткої адреси пристрою.

В однорангової мережі будь-які пристрої, що знаходяться в зоні досяжності радіозв'язку можуть обмінюватися даними один з одним.

Дана мережа дозволяє передавати інформацію між вузлами мережі використовуючи окремі вузли в якості ретрансляторів (рисунок 4).

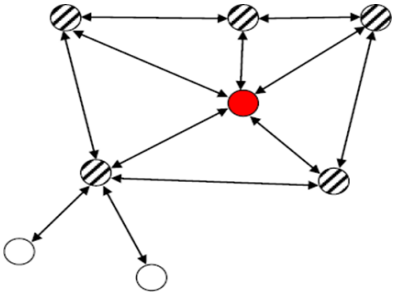

Рис. 4. Комірчаста (mesh) топологія мережі ZigBee

Для побудови бездротової мережі (наприклад, мережа з топологією "зірка") на основі технології ZigBee розробнику необхідно придбати принаймні один мережевий координатор і необхідну кількість кінцевих пристроїв. При плануванні мережі слід враховувати, що максимальна кількість активних кінцевих пристроїв, приєднаних до мережевого координатора, не повинна перевищувати 240. Крім того, необхідно придбати у виробника ZigBee-чіпів програмні засоби для розробки, конфігурування мережі і створення призначених для користувача додатків і профілів. Практично всі виробники ZigBee-чіпів пропонують на ринку цілу ліній-ку продукції, що відрізняється, як правило, тільки об'ємом пам'яті ROM і RAM. Наприклад, чіп зі 128 Кбайт ROM і 8 Кбайт RAM може бути запрограмований на роботу в якості координатора, маршрутизатора і кінцевого пристрою.

Перерахуємо додатки, в які може бути інтегрована технологія ZigBee:

- система моніторингу на жвавих шосе;
- системи з перемикання світлофорів на перехрестях при великому скупченні машин.

Висновок. технологія ZigBee є перспективною технологією в області, в якій потрібно застосувати, а саме фіксації рухомих об'єктів і моніторинг міських вулиць. Технологія ZigBee має ряд переваг перед іншими технологіями, що не вимагають високої передачі даних і є енергозберігаючою технологією, що дозволяє використовувати велику кількість часу. Також в ній присутня технологія CSMA-CA (виявлення колізій).

Можливість побудови мережі простої і складної топології, отже, можливо застосовувати в розгалужених вулицях і будівлях складної структури.

УДК 621.396 (043.2)

Д.О. Павленко, В.П. Климчук
Національний авіаційний університет, м. Київ

СПОСІБ ВИЗНАЧЕННЯ МОДУЛЯЦІЙНИХ ХАРАКТЕРИСТИК СИГНАЛУ

Характерною особливістю сучасних систем і мереж зв'язку є використання різних методів адаптації, в результаті застосування яких у каналах зв'язку з різних причин можуть змінюватися вид модуляції та параметри сигналів, що використовуються протягом одного і того ж сеансу зв'язку. Найбільш показовим прикладом є зміна швидкості передачі даних залежно від якості каналів зв'язку. Проте трапляються й складніші методи адаптації.

Крім того, в умовах неповних апріорних відомостей про параметри прийнятого сигналу розв'язання ряду задач його обробки, таких як установка смуг основної селекції приймача, налаштування демодулятора, прийняття демодулятором правильного рішення про передане значення модуляційного параметра, вимагає можливо більш точного знання модуляційної структури сигналу, що надходить з ефіру. Ці фактори зумовлюють необхідність включення в тракти обробки засобів автоматичного визначення параметрів та видів модуляції сигналів, що приймаються.

Визначення апріорно невідомих модуляційних параметрів широкого класу сигналів, що приймаються, в загальному випадку є складним завданням, що вимагає значних обчислювальних ресурсів. Це створює труднощі при реалізації автоматичних процедур розпізнавання виду та параметрів модуляції, що працюють у реальному масштабі часу. Однак у ряді випадків реалізація таких процедур можлива шляхом застосування відповідних математичних методів та сучасних засобів обчислювальної техніки.

Розв'язання задачі аналізу модуляційної структури сигналу передбачає визначення сукупності ознак, що характеризують необхідні види модуляції та їх параметри, виділення даної сукупності ознак із прийнятої суміші сигналу та перешкод та обробку ознак з метою прийняття рішення про модуляційні параметри аналізованого сигналу.

Розглянемо деякі практичні питання розпізнавання виду та модуляційних параметрів низки різновидів сигналів із частотною та фазовою маніпуляцією. З точки зору розтину модуляційної структури вся

значуща інформація про такі сигнали міститься в їх фазових та частотних параметрах. Інакше висловлюючись, вона міститься у значеннях миттєвої частоти f(nT) і фази p(nT) сигналу. Миттєва амплітуда a(nT) при аналізі модуляційних параметрів FSK- та PSK-сигналів у загальному випадку не є інформаційним параметром, хоча облік її значень в алгоритмах частотного та фазового детектування дозволяє компенсувати завмирання сигналу, що приймається.

Для визначення виду та параметрів модуляції FSK та PSK сигналів необхідно оцінювати миттєву кутову фазу сигналу, яка може бути представлена у вигляді

$$p(nT) = 2\pi f0 + 2\pi f(nT) + p0(nT),$$

де f0 - центральна частота сигналу, параметри f(nT) та p0(nT) - відповідно миттєва частота та миттєва початкова фаза сигналу.

Ці параметри можуть, наприклад, приймати такі значення:

• для FSK сигналів без стрибка фази $f(nT) = (i - M) f + \Delta f/2$, $p0(nT) = const$;

• для PSK-сигналів $p0(nT) = (2\pi(I - M)/M)nT$, $f(nT) = 0$ де i = 1,..., M, M - число позицій модуляції.

Для оцінки способу модуляції будується гістограма значень початкової фази. Для прийняття рішення про спосіб модуляції можна використати методи розпізнавання образів.

Розташування піків отриманої гістограми різниці фаз, що віддаляються на певній відстані один від одного, залежить від наявності та значень постійного стрибка фази аналізованого сигналу і дозволяє приймати рішення про використовуваний вид модуляції та кількість її позицій. Цей факт ілюструється на відповідних рисунках, де наведені обчислені гістограми різниці фаз PSK-2, PSK-4-сигналів та сигналу FSK.

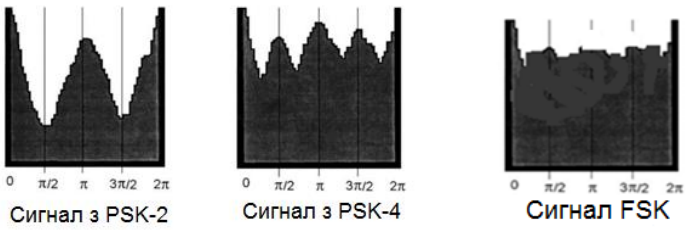

Рис.1. Гістограми значень початкової фази для різних сигналів

Список використаних джерел

1. Теория обнаружения сигналов / П. С. Акимов, П. А. Бакут, В. А. Богданович и др.; Под ред. П. А. Бакута. - М.: Радио и связь, 1984.— 440 с.

2. Фомин Я. А., Тарловский Г. Р. Статистическая теория распознавания образов. - М.: Радио и связь, 1986.

3. Тихонов В. И. Оптимальный прием сигналов. - М.: Радио и связь, 1983.

4. Френке Л. Теория сигналов. - М.: Сов. Радио, 1974.

УДК 004.056.53

М. В. Панченко, С. Ю. Даков
Київський національний університет імені Тараса Шевченка, м. Київ

ВИЯВЛЕННЯ АТАКИ PASSWORD SPRAYING ШЛЯХОМ АНАЛІЗУ ЖУРНАЛУ АВТОРИЗАЦІЇ НА БАЗІ ЕНТРОПІЇ

Одним із видів атак на паролі є password spraying. Під час цієї атаки зловмисник підбирає невелику кількість паролів для великої кількості користувачів. Наприклад, він може проаналізувати діяльність деякої організації та згенерувати декілька імовірних паролів, перед цим отримавши список імен її співробітників для входу в інформаційну систему. Крім того, зловмисник може підбирати найбільш розповсюджені або стандартні паролі для сервісів, які використовує організація. Якщо ця організація не веде контроль за паролями та не має політики безпеки щодо паролів, тоді деякі користувачі можуть забути, або не встигнути змінити стандартний пароль і зловмисник зможе легко його підібрати.Аналіз випадків порушення безпеки показав, що атака password spraying може бути успішною навіть проти великих організацій. Наприклад, у 2019 році зловмисники отримали доступ до внутрішньої мережі Citrix та мали змогу завантажити ділові документи [1].

Зазвичай для захисту від перебору паролів встановлюється обмеження кількості невдалих спроб входу для одного користувача. Але проти цієї атаки такий захист не буде результативним, бо кількість невдалих спроб входу буде невеликою. Зловмисник, наприклад, може підбирати лише один або два паролі для багатьох користувачів. Якщо встановити обмеження неправильних спроб входу для всіх користувачів одночасно, тоді атака password spraying може перетворитись на DoS атаку, бо вхід буде заблоковано для всіх користувачів. Дієвим захистом від цієї атаки є багатофакторна автентифікація, але вона пов’язана із додатковими складнощами, а також може бути недоступною для деяких сервісів.

Якщо організація не використовує багатофакторну автентифікацію, але виконується ведення журналу авторизації користувачів, тоді атака password spraying спричинить появу великої кількості записів про невдалий вхід. Аналіз журналу авторизації на базі ентропії дає змогу ви-

явити описану атаку та вчасно виконати дії для її зупинки та знешкодження наслідків.

Ентропія журналу авторизації розраховується з використанням методу рухомого вікна [2], який дозволяє обчислювати ентропію для певного діапазону повідомлень, який називається вікно. Розмір вікна необхідно визначати з урахуванням того, яка кількість неуспішних спроб входу вважається допустимою. Значення ентропії залежить від кількості різних повідомлень у вікні. Ідентифікація різних записів в журналі виконується таким чином: повідомлення про успішний вхід та вихід – за іменем користувача, а про неуспішний вхід – за кодом події, або її назвою. Якщо в журналі авторизації є інші повідомлення, то в межах цих розрахунків їх можна не враховувати. За нормального стану системи кількість неуспішних спроб входу буде невисокою, на відміну від кількості інших повідомлень, пов'язаних із авторизацією користувачів. У такому випадку, здебільшого, повідомлення в журналі авторизації будуть різними, адже вхід в систему виконують різні користувачі, тому ентропія буде близька до максимальної, бо ці повідомлення будуть майже рівноймовірними [3, с. 33]. Якщо в журналі буде багато повідомлень про неуспішний вхід користувачів, тоді вони будуть ідентифікуватись як однакові, їх імовірність буде близька до 1, тому це суттєво вплине на значення ентропії – воно буде близьке до нуля [3, с. 33]. За описаним алгоритмом атака password spraying може бути виявлена навіть якщо зловмисник використовує велику кількість IP адрес, із яких виконуються спроби входу. Обійти цей алгоритм можна лише якщо одночасно виконують вхід багато легітимних користувачів та атакуючий робить достатні паузи між кожною спробою входу, щоб у журналі не переважали повідомлення про невдалий вхід.

Список літератури

1. Black S. Citrix investigating unauthorized access to internal network. Citrix Blogs. 2019. URL: https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/ (accessed 28.05.2022).

2. Gudkov O. Calculation algorithm for network flow parameters entropy in anomaly detection. IT security for the next generation, international round. (11.05.2012). Delft University of Technology, 2012. URL: https://silo.tips/download/calculation-algorithm-for-network-flow-parameters-entropy-in-anomaly-detection (accessed 25.05.2022).

УДК 621.39 (043.2)

А.Д. Пінчук, В.В. Самойленко, Р.С. Одарченко
Національний авіаційний університет, м. Київ

РЕАЛІЗАЦІЯ ПРОЄКТІВ ДЛЯ МЕРЕЖ 5G НА ОСНОВІ OPEN SOURCE РІШЕНЬ

Більшість комерційного програмного забезпечення має, так званий, закритий код. Користувачі ніяк не можуть взаємодіяти з кодом програми. В такому випадку код є комерційного таємницею і взаємодіяти з ним можуть лише компанії даного програмного забезпечення (ПЗ). Тому зараз все більшої популярності набирають Open Source рішення.

Open Source — це цілий рух, що підтримує розробку й просування відкритого програмного забезпечення. Простіше кажучи, Open Source — це, наприклад, безліч проєктів на GitHub чи GitLab, з якими кожний з нас хоч раз у житті зіштовхувався, щоб знайти потрібне рішення для тієї чи іншої задачі. Open Source — це ще й Linux, улюблена ОС більшості розробників програмного забезпечення [1].

Open Source надає можливість користувачам використовувати вже готовий код, змінювати його та покращувати, інтегрувати у власні проєкти або створювати нові на основі оригіналу. Важливо, що це все повністю безкоштовно та при цьому не відбувається порушення авторських прав розробників початкового ПЗ, а саме рішення поширюється під ліцензіями GNU/Linux, MIT та інші.

Серед найбільш відомих продуктів з відкритим вихідним кодом є CMS WordPress — система керування контентом на сайтах. Всі можливості продукту надаються користувачу безкоштовно. В якості мови програмування використовувався PHP, БД — MySQL.

Безкоштовна альтернатива Microsoft Office — OpenOffice. Можливості ПЗ ідентичні, а сам інтерфейс досить схожий.

GIMP надає собою альтернативу комерційному продукту Adobe Photoshop. Функції та можливості повністю ідентичні комерційному рішенню [2].

Насправді Open Source рішення та проєкти в цілому є дуже важливими для розвитку технологій [3].

Поширення знань між однодумцями — головна мета Open Source платформ. Наприклад, розробник з України створює новий додаток, потім інший програміст у Мюнхені вивчає додаток і знаходить способи

його поліпшення. Інформація поширюється, а спільнота отримує вигоду від колективних інновацій.

Таким чином, Open Source сприяє вільному обміну ідеями в спільноті, чим стимулює творчий, науковий і технологічний прогрес.

Open Source рішення знайшли свої місце і в нашому проєкті — запуск тестової мережі 5G в Національному авіаційному університеті. Для цього, на основі відкритих кодів, потрібно буде підняти ядро мережі та програмну базову станцію.

Звісно за кожним таким проєктом стоїть спільнота, тобто community, яка розробляє, підтримує та вдосконалює його. Тому це гарний приклад ефективності командної роботи.

Open Source проєкти та рішення є безцінним ресурсом для розробників та людей, які працюють в IT-сфері. Вони надають можливість реалізувати велику кількість різноманітних проєктів безкоштовно, покращити свої знання та навички в даній сфері. Такі проєкти абсолютно не поступаються в якості та безпеці перед комерційним ПЗ, а в більшості випадків, завдяки постійній взаємодії з кодом, навіть перевищують їх. В процесі реалізації проєктів з відкритим кодом, компіляція використовуваного модуля і створення для нього потрібної робочого середовища вимагає певних навичок IT-фахівця.

[1] *Pletnov O. Open source: що це, для чого і як розпочати. ДОУ. URL: https://dou.ua/lenta/articles/open-source-reasons-to-join/ (дата звернення: 25.05.2022).*

[2] *Open Source: что это, значение термина, особенности и примеры ПО. ITGLOBAL.COM - Managed IT and Business Cloud services. URL: https://itglobal.com/ru-ru/company/glossary/open-source/ (дата звернення: 25.05.2022).*

[3] *Проекти в Open Source: чому розробники викладають код у відкритий доступ і дають змогу безкоштовно його використовувати | AI CONFERENCE KYIV 2020. AI Conference Kyiv 2021. URL: https://aiconference.com.ua/uk/news/proekti-v-open-source-pochemu-razrabotchiki-vikladivayut-kod-v-otkritiy-dostup-i-razreshayut-besplatno-ego-ispolzovat-98530 (дата звернення: 25.05.2022).*

УДК 004.383.3:004.623 (043.5)

О. Ю. Пузиренко
Національний авіаційний університет, м. Київ

ЕФЕКТИВНІСТЬ СТЕГАНОГРАФІЧНОЇ ОБРОБКИ АУДІОПРОГРАМ ЦИФРОВОГО МОВЛЕННЯ

Для стеганообробки (СО) цифрових аудіосигналів запропоновано чимало методів і алгоритмів, огляд яких може бути знайдений в [1]. Актуальними є питання ефективності того чи іншого методу або алгоритму в контексті СО аудіоконтенту (АК) цифрового мовлення (ЦМ) [2], зважаючи на те, що загальнонаціональну мережу радіомовлення в Україні передбачається будувати на основі стандарту *DAB+*.

У *DAB+* обробка АК здійснюється згідно *MPEG-4 HE-AAC v2* (*ISO/IEC 14496-3:2019*) з технологією *SBR* (*Spectral Band Replication*), що дозволяє «зберегти» високі частоти (ВЧ) при кодуванні з низькими бітрейтами. Завдяки апріорній похибці відновлення ВЧ складових, *SBR* обрана основою створення стеганографічного каналу (СК) передавання додаткової інформації (ДІ) у складі АК *DAB+* з урахуванням властивих слуху ефектів часового і частотного маскування.

ДІ, відповідно до її пов'язаності з АК ЦМ і рівнем доступу до неї з боку споживачів, розділено на 4 класи — рис. 1.

Додаткова інформація	ПОВ'ЯЗАНА з аудіоконтентом	БЕЗУМОВНИЙ допуск	клас **ПБ**	*PAD*, анотації
		УМОВНИЙ допуск	клас **ПУ**	ЦВЗ, цифрові відбитки
	НЕПОВ'ЯЗАНА з аудіоконтентом	БЕЗУМОВНИЙ допуск	клас **НБ**	службова інформація
		УМОВНИЙ допуск	клас **НУ**	передплачена інформація

Рис. 1. Класифікація повідомлень ДІ, передаваних СО аудіопрограм ЦМ

За схильністю до активних атак метод СО класу «ПУ» оцінений на ймовірність руйнування стеганограм шляхом спотворень АК перекомпресією і додаванням білого шуму. Результати дозволяють вважати досліджуваний метод стійким до зазначених атак у межах, обумовлених достатністю кореляційного зв'язку (більшим за рівень 0,7) між оригіналом і видобутою копією стеганограм.

За схильністю до пасивних атак метод СО усіх класів і, передусім, СО класу «НУ» оцінено за стійкістю до виявлення стеганошляху через перевищення рівня акустичної прихованості елементів стеганограми. Результати обчислень відомих показників акустичного спотворення [1]

АК, заповнених ДІ, підтвердили вплив на рівень акустичної невідчутності стеганограми сталої довжини величини R бітрейту АК (а, відповідно, і кількості бітів, виділених на кодування субсмугових відліків). Навіть за вбудовування до всіх кодованих субсмуг, рівень прихованості лишався високим. Найкращі результати одержані при одночасному відборі контейнерів за довжиною кодів і частотним діапазоном субсмуг.

Рівень стійкості методів СО класу «НУ» до видобування елементів стеганограми, якщо противнику відомо про її існування, визначається комбінаторною кількістю можливих комбінацій заповнених елементів АК під час їх перебирання, яка становить близько $4 \cdot 10^{41}$.

Значення Θ_i прихованих пропускних здатностей (ППЗ) СК для різних бітрейтів R_i АК, порогових значень довжин n_i кодів відліків і частот їхніх субсмуг f_i, можуть вважатися гранично досяжними для будь-яких методів СО на базі i-х *MPEG*-стиснутих АК, незважаючи на принципи побудови останніх, і лежать в межах 2...20% від R_i.

Завдяки зміні стандартних конфігурацій ансамблів й стеганографічного усунення з їхнього складу потоків передавання ДІ та приєднання об'єму звільненого при цьому каналу до складу аудіопотоків програм на 5–75% зростає спектральна ефективність ЦМ. За аналогічних дій, але без зміни конфігурацій *DAB*-ансамблів, на 12–14% зростає середня якість звучання окремих програм або на 1–2 пункти зростає потужність завадостійкого кодування захищуваних ним чутливих до помилок полів *MPEG*-аудіокадрів *DAB*-потоків.

Очікуваний приріст доходу, як відношення сумарної ППЗ СК *DAB*-ансамблю в цілому (Θ_Σ) до сумарної швидкості передавання ансамблю (R_Σ) становить 13–20%.

Отже, стеганографічне вбудовування мультимедійного супроводу аудіоконтенту вбачається цілком перспективним до застосування, шляхом модифікації наземних, супутникових і кабельних систем цифрового радіо- і телевізійного мовлення.

Список літератури

1. Конахович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.

2. Пузиренко О.Ю. Комп'ютерні системи стеганографічної обробки і захисту інформації у цифровому звуковому мовленні : дис. на здоб. наук. ступеня кандидата техн. наук : 05.13.05. — К., 2012. — 162 с.

УДК 621.391 (043.2)

В.В. Пульний, В.П. Климчук
Національний авіаційний університет, м. Київ

ЕНЕРГОЕФЕКТИВНИЙ РАДІОПЕРЕДАВАЧ ЦИФРОВОЇ РАДІОСТАНЦІЇ

VHF Datalink (VDL) – це засіб передачі інформації між повітряними суднами і наземними станціями. В даний час, VDL-2 є основною версією VDL, і єдиним режимом, що підтримує Controller-Pilot Data Communications Link (CPDLC). Мережі VDL-2, мережі цифрового зв'язку високої швидкості і високої ємності забезпечують приблизно в 20 разів більшу ємність повідомлень, ніж зазвичай використовують сьогоднішні системи ACARS. Збільшені швидкість і ємність підтримують CPDLC, в якому визначені набори текстових інструкцій і повідомлень замінили звичайні обміни інформації. Ці набори інструкцій призначені для полегшення управління повітряним рухом при радіоперевантаженнях. В VDL-2 використовується модуляція D8PSK і метод управління множинним доступом з контролем несної (CSMA).

Цифровий канал передачі даних VDL-2 є одним з каналів мережі авіаційного електрозв'язку (ATN), що має в основі 7-рівневу модель взаємодії відкритих систем (OSI) ISO.

Канал VDL-2 виконує функції трьох нижчих рівнів моделі OSI.

Рівень 1 (фізичний) забезпечує управління частотою передачі, модуляцію і демодуляцію сигналу, а також функції сповіщення.

Рівень 2 (канальний) забезпечує надійну передачу пакетів даних і доступ до фізичного каналу, він розділяється на два підрівні і об'єкт управління. Підрівень управління доступом до середовища передачі (MAC) використовує метод множинного доступу з контролем несної (CSMA).

Рівень 3 (мережевий) забезпечує доступ до підмережі ATN і визначається ISO 8208. Цей протокол також відповідає за передачу пакетів в мережі, відновлення в випадку помилок, управління потоком даних, фрагментацію і зборку пакетів, а також управління зв'язками.

Основною рисою VDL-2 є значне підвищення пропускної здатності каналу і ефективності використання радіочастотного спектру. Ця перевага дозволила замінити існуючі системи або покращити їхню роботу завдяки використанню фізичного каналу VDL-2.

Для вирішення існуючих задач великий практичний інтерес складає розробка mesh-мережі. Здатність таких мереж ретранслювати повідомлення, використання різноманітних алгоритмів підтримки зв'язку і невеликий об'єм службових даних дозволить скласти мережу повного зв'язку (кожен з кожним), де кожен вузол може вести передачу даних з будь-яким ПС, використовуючи для цього інші вузли. Також це дозволить вирішити проблему втрати радіовидимості і зв'язку з диспетчером через особливості місцевості. Наприклад: здійснюється виліт літака з аеропорту, в цей же момент до аеропорту наближається інший літак для заходу на посадку. Припустимо, що через погану радіовидимість диспетчер не може зв'язатись з ПС, що заходить на посадку. За відсутності мережі це може призвести до зіткнення, якщо літак здійснює аварійну посадку. Якщо ж ми маємо повну мережу зв'язку, тоді диспетчер зможе одночасно помітити ПС і дати коректуючи команди для безпечного приземлення судна.

Для перевірки доцільності розробки mesh-надстройки для режиму VDL Mode 2 необхідно провести попередній аналіз структури. Для цього були проведені розрахунки необхідної дальності радіозв'язку і розрахунки ймовірності пропускної здатності мережі. Всі розрахунки враховують вплив умов середовища поширення радіосигналу.

Радіомережа є зв'язковою тоді, коли між будь-якою парою радіостанцій існує маршрут, котрий, в загальному випадку, може включати декілька ретрансляцій. Для оцінки зв'язковості використовуються наступні допущення:

– для зв'язності радіостанцій необхідна дальність радіозв'язку повинна бути не менше ніж R; система, яку аналізують пропонується як однорідна, тобто значення R для всіх радіостанцій однакове;

– територіальний розподіл радіостанцій є пуассонівським;

– при поширенні радіохвиль враховуються середні втрати поширення, повільні та швидкі завмирання;

– в якості антени використовується кругова антенна решітка.

Метою аналізу є оцінка такого значення дальності радіозв'язку R, яке за заданої густини радіостанцій системи передачі даних λ_S забезпечуватиме зв'язок радіостанцій з ймовірністю $P_{\text{CON}} \geq P_{\text{CON\_ТРЕБ}}$, де $P_{\text{CON\_ТРЕБ}}$ – необхідна ймовірність зв'язку радіостанцій.

Під зв'язком радіостанцій розуміють ситуацію, яка з визначеною вірогідністю P_{ISO} виключає наявність ізольованих радіостанцій в системі зв'язку. Ізольованою вважається така радіостанція, яка з визначе-

ною імовірністю P_{ISO} виявляється поза зоною радіопокриття інших радіостанцій. Зона радіопокриття визначається дальністю радіозв'язку R.

На графіках (рис. 1) представлена залежність дальності радіозв'язку від площі радіопокриття і кількості радіостанцій.

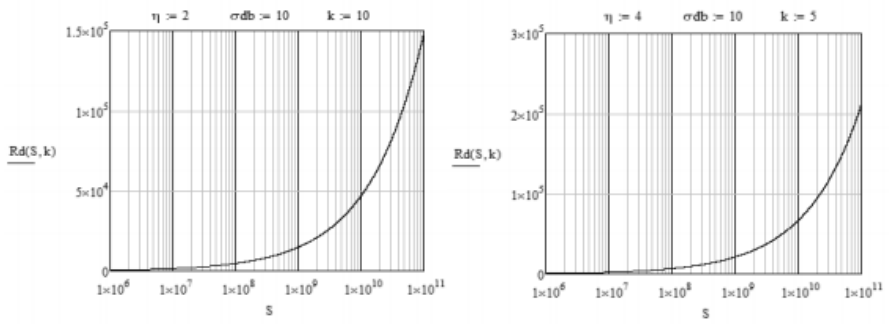

Рис. 1. Залежність дальності радіозв'язку від площі радіопокриття і кількості радіостанцій

Проаналізувавши графіки можна зробити висновок, що зі збільшенням показника середніх втрат поширення, необхідна дальність радіозв'язку R збільшується, а зі збільшенням числа вузлів мережі k, необхідна дальність зменшується.

Ще одна відмінна особливість ДВЧ лінії передачі даних режиму 2 полягає в тому, що існує можливість не тільки контроля повідомлень на рівні цілісності, але й прямого виправлення помилок. Дана перевага забезпечує кодування кадра даних кодом Ріда-Соломона, що дозволяє не усі пошкоджені повідомлення передавати повторно, і, в кінцевому рахунку, збільшує ефективність використання радіоканала.

Завдання оцінки пропускної здатності радіостанцій самоорганізованої радіомережі вирішується використанням методики оцінки пропускної здатності імовірнісним способом. Методика враховує апріорну невизначеність територіального розподілу радіостанцій, умови поширення радіохвиль і імовірність передачі радіостанції. Отримані співвідношення дозволяють в явному виді визначити пропускну здатність радіостанцій мережі при використанні ненаправлених антен.

На графіках (рис. 2) представлені залежності пропускної здатності від імовірності передачі радіостанції та від кількості сусідів радіостанції, для випадку ненаправлених антен.

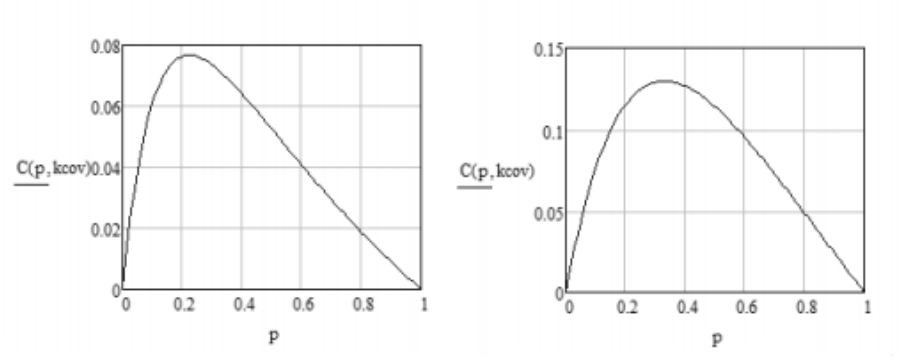

Рис. 2. Залежності пропускної здатності від імовірності передачі радіостанції та від кількості сусідів радіостанції

Аналіз графіків вказує на зменшення пропускної здатності при збільшенні сусідніх вузлів.

Представлена модель показує, що використання алгоритма самоорганізації дозволяє здійснювати видимість між всіма об'єктами мережі, а значить з використанням протоколів передачі даних здійснювати зв'язок між ними. Розрахунок зв'язку дозволяє дати оцінку стійкості взаємозв'язків між вузлами.

Отже, VDL-2 забезпечує сумісну з авіаційною телекомунікаційною мережею (ATN) лінію передачі даних «повітря-земля» і передбачає використання методів цифрового радіозв'язку. Номінальна швидкість передачі даних в 31,5 кбіт/с сумісна з характеристиками зв'язку при частотному розносі каналів в 25 кГц, що використовується при аналоговому надвисокочастотному зв'язку. VDL-2 дозволяє використовувати набори протоколів ATN для різноманітних експлуатаційних прикладних процесів, забезпечуючи, тим самим, значне підвищення ефективності використання високочастотного канала. Необхідно відмітити, що D8PSK (що використаний в VDL-2) був рекомендований ICAO, щоб уникнути амплітудних спотворень від різних схем модуляції в каналах «повітря-земля».

УДК 621.396.969.1

І.С. Пятін
Хмельницький політехнічний фаховий коледж національного університету «Львівська політехніка»
Ю.М. Бойко
Хмельницький національний університет

ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ МОБІЛЬНИХ ТЕЛЕКОМУНІКАЦІЙ

Розвиток телекомунікаційних систем рухається по шляху підвищення пропускної спроможності. Сучасні мобільні телекомунікації підтримують гнучку смугу пропускання каналу. Параметри, які впливають на пропускну спроможність наступні:

- пропускна здатність каналу;
- конфігурація антени MIMO;
- схема завадостійкого кодування і модуляції;
- умови радіозв'язку (відношення сигнал-шум, якість каналу)
- дуплексний режим роботи, наприклад FDD, TDD.

Пропускна спроможність каналу визначається законом Шеннона:

$$C = W \cdot n \cdot \log_2(1 + SNR),$$

де W - ширина спектра каналу; n - кількість антен MIMO; SNR - відношення сигнал-шум.

LTE використовує турбо-коди і згорткові коди для забезпечення стійкості від завад, а системи зв’язку наступного покоління будуть використовувати полярні і LDPC коди [1]. Для підвищення пропускної спроможності важливо використовувати коди, які при низьких відношеннях сигнал-шум (SNR) забезпечують якомога менший коефіцієнт бітових помилок (BER) багатопозиційних видів модуляції. У доповіді розглядається Simulink модель системи зв’язку (рис. 1), що використовує завадостійкий LDPC код, багатопозиційну 16-QAM модуляцію і просторово-часовий кодер з трьома передаючими і двома приймальними антенами (MIMO). Використовується канал зв’язку з завмираннями, до якого додається адитивний білий гаусів шум (AWGN). Рознесене кодування підвищує надійність передачі, надсилаючи сигнали різними шляхами між декількома передавальними і приймальними антенами. Об'єднання отриманих даних дає підсилення сигналу на шляху розповсюдження.

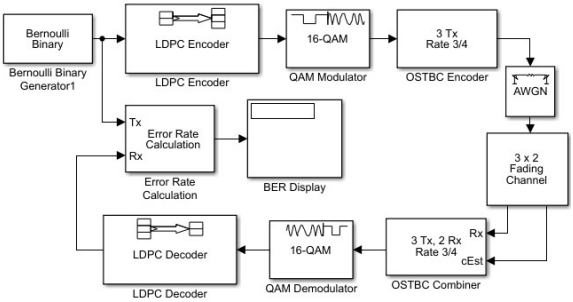

Рис. 1. Simulink модель системи зв'язку

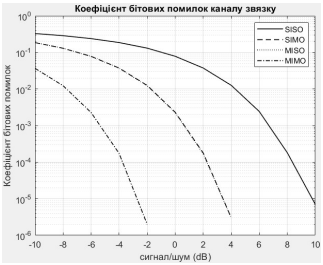

Рис. 2. Залежність BER від SNR для систем: один вхід-один вихід (SISO); один вхід-багато виходів(SIMO); багато входів-один вихід(MISO); багато входів-багато виходів (MIMO)

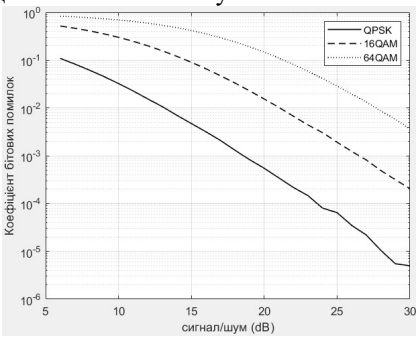

Рис. 3. Залежність BER від SNR системи MIMO і модуляцією QPSK, 16-QAM, 64-QAM

Система SIMO забезпечує підсилення від антен приймача, а система MISO забезпечує підсилення від антен передавача, система MIMO в межах прямої видимості отримує підсилення від масиву передачі, так і від прийому. За рис. 2, можна зробити висновок, що система MIMO на 12 дБ енергетично ефективніша за систему SISO.

При збільшенні позиційності модуляції, для отримання заданого коефіцієнту бітових помилок необхідно підвищувати відношення сигнал-шум (рис.3). Модуляція QPSK передає 2 біта на символ, 16-QAM – 4 біта на символ, 64-QAM – 6 бітів на символ. Для збільшення швидкості передачі з 2 біт/символ до 6 біт/символ при BER=1e-5, необхідно збільшити відношення сигнал-шум на 13 дБ.

1. Boiko J. Design and Evaluation of the Efficiency of Channel Coding LDPC Codes for 5G Information Technology /J. Boiko, I. Pyatin, O. Eromenko //Indonesian Journal of Electrical Engineering and Informatics (IJEEI). – 2021. – Vol. 9, nr. 4. – P. 867-879.

УДК 621.391

А. Романов, М. Романов, студенти
Національний авіаційний університет, м. Київ
Науковий керівник – Г. Конахович д.т.н., проф.

ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЯХ

Сьогодні перед IT-службами виникають важливі питання: як уніфікувати безліч серверів і робочих станцій; як забезпечити сумісність додатків, операційних систем і апаратного забезпечення; як ізолювати одні сервіси і додатки від інших для зниження числа конфліктів; як оптимально завантажити нові потужні сервера.

Одним з підходів до вирішення цих проблем є віртуалізація. Серед безлічі запропонованих рішень по віртуалізації, найбільший розвиток в комерційному застосуванні знайшли:

віртуалізація представлень;

віртуалізація операційної системи;

віртуалізація додатків.

Технологія віртуалізації представлень є доцільною для додатків, чия архітектура має серйозні обмеження на роботу в мережі, і в свою чергу може вирішувати завдання ізоляції користувача від фізичного комп'ютера, розміщення на одному фізичному комп'ютері декількох робочих місць, так як архітектура сучасних серверів x86 передбачає виконання тільки однієї ОС на сервері. Подолати таке структурне обмеження можна за допомогою віртуалізації серверів.

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.

Віртуалізація додатків - процес використання програми, яка не вимагає її установки в операційну систему, но створюється необхідне спеціалізоване середовище для віртуалізуємого додатку і, тим самим, забезпечується ізольованість роботи цього додатка

УДК 614.842.435:643.62

Є.В. Соловйов
Національний авіаційний університет, м. Київ

СИСТЕМИ ПРОТИПОЖЕЖНОЇ БЕЗПЕКИ

Пожежа – неконтрольоване горіння поза спеціальних вогнищем, що розповсюджується в часі і просторі. Знищує матеріальні цінності, створює загрозу для життя людей, тварин, негативно впливає на навколишнє середовище. Проблема пожежної безпеки на сьогоднішній день не тільки на території України, але й у світі, залишається актуальною. В умовах високої швидкості руху, особливо сухого повітря актуальність проблеми зростає. Велике занепокоєння викликає організація протипожежного захисту місць збирання, переробки та зберігання врожаю; недотримання пожежної безпеки у лісах та парках; неохайне відношення до роботи з інвентарем. Гасіння пожежі вимагає значних матеріальних засобів і людських ресурсів. Актуальним завданням у пожежної безпеки є розвиток уявлення про можливі перспективні напрями розвитку систем протипожежного захисту. забезпечення пожежної безпеки підприємств ґрунтується на ефективному функціонуванні систем протипожежного захисту, а також принципах раннього виявлення пожеж шляхом застосування сучасних систем пожежної сигналізації. Перспективи розвитку в окресленій проблематиці мають базуватися на застосуванні сучасних технологій, досконалості нормативно-технічної бази, а також застосуванні новітніх підходів до організації системи протипожежного захисту.

Установки і системи пожежної сигналізації, оповіщення та управління евакуацією людей при пожежі повинні забезпечувати автоматичне виявлення пожежі за час, необхідний для включення систем оповіщення про пожежу з метою організації безпечної (з урахуванням допустимого пожежного ризику) евакуації людей в умовах конкретного об'єкта. Системи пожежної сигналізації, оповіщення та управління евакуацією людей при пожежі повинні бути встановлені на об'єктах, де вплив небезпечних факторів пожежі може призвести до травматизму та загибелі людей.

Отже, для збереження людських життів, запобігання знищення матеріальних цінностей та усунення негативного впливу на навколишнє середовище необхідно активно розвивати системи охоронно-пожежної сигналізації та системи автоматичного пожежогасіння.

УДК 004.77 (043.2)

А.В. Степанюк, В.Є. Курушкін
Національний авіаційний університет, м. Київ

КОРПОРАТИВНА VOIP МЕРЕЖА НА БАЗІ ASTERISK IP PBX

Комп'ютерні мережі, телефонія, телекомунікаційні системи на сьогоднішній день мають величезне значення в нашому сучасному суспільстві. В останній час виражаються тенденції до об'єднання різного роду мереж таких як: мережі Інтернет і локальних мереж, телекомунікаційних мереж, і інших мереж зв'язку: як телефон-них, так і радіомереж. Технологічне об'єднання різнорідних мереж обумовлено передавців цифрової інформації за мережами різного виду. IP-телефонія, або VoIP – Voice Over IP – це такий вид голосового зв'язку, де на передачу аудіо-інформації по цифрових каналах зв'язку, застосовується протокол IP. У цей час скрізь помічається заміна старих телефонних технологій на нові технології по IP-телефонії.

Asterisk IP-PBX - це рішення для комп'ютерної телефонії с відкритим вихід-ним кодом від компанії Digium. Даний додаток працює в операційних системах Linux, FreeBSD і Solaris. Назва цього проекту походить від назви символу "*" зірочка, Астеріск.

Рис. 1. Логотип проєкта Asterisk

Система Asterisk в сукупності с необхідним користувацьким обладнанням має всі можливості стандартної АТС, що підтримує множину VoIP протоколів і надає множину функцій управління дзвінками: голосову пошту; відео-конференції; інтерективне голосове меню IVR; центр обробки викликів поставок дзвінків в чергу і розподілення їх по абонентам застосовуючи різні алгоритми; запис CDR;

При створенні додаткового функціонала можна користуватися власною мовою Asterisk при написанні плану нумерації, написанні модулю мовою CI++, або скориставшись AGI - гнучким і універсаль-

ним інтерфейсом для інтеграції з зовнішніми системами обробки даних. Модулі, що виконуються через AGI, можуть бути написані на будь-якій мові програмування.

Програма Asterisk розподіляється при умові подвійної ліцензії, при якій одночасно з основним кодом, що розповсюджується у відкритій ліцензії GNU GPL, можна створити закриті модулі, що містять ліцензований код: наприклад, модуль для підтримки кодека G.729.

З-за вільної ліцензії програма Asterisk швидко розвивається і підтримується тисячами людей зі всієї планети.

Програма Asterisk працює і з аналоговими лініями FXO/FXS модулі, і з цифровими ISDN BRI і PRI - потоками T1/E1. Прі допомозі певних комп'ютерних плат найбільше відомими виробниками яких є Digium, Sangoma, OpenVox, Rhino, AudioCodes, Asterisk можна підключити до високопропускних ліній T1/E1, які дозволяють працювати паралельно з десятками і сотнями телефонних з'єднань.

FXO/FXS модулі - це назви портів, до яким підключаються аналогові телефонні лінії ТМЗК. Інтерфейс FXS - це порт, він дає можливість підключення користувача до аналогової телефонної лінії. Інтерфейс FXO - це роз'єм, в який включається аналогова телефонна лінія. Це роз'єм на телефонному або факсимільному апараті або роз'єм на аналогової міні-АТС. Такий порт має індикацію стану трубка знята і трубка на телефоні за-микання ланцюга. Шлюз FXO. Прі підключенні аналогових телефонних ліній до IP міні-АТС потрібен шлюз FXO. Це дозволить підключити порт FXS до порту FXO, наявно-го на шлюзі, який перетворює сигнал аналоговий телефонної лінії в виклик VOIP. Шлюз FXS застосовується при підключенні однієї або більше традиційних аналогових міні-АТС до VOIP міні-АТС або провайдеру послуг. Шлюз FXS потрібен при з'єднанні портів FXO, зазвичай з'єднуються телефонні компанії з мережами Інтернет або VOIP міні-АТС.

Підтримуються наступні протоколи: SIP; H.323; IAX2; MGCP; Skinny SCCP; XMPP Google Talk; UNIStim; Skype через комерційний канал. Можна передавати текст і сигнали відео, наприклад, застосовувати відеофон. Крім цього, реалізована робота з іншими комп'ютерними протоколами: DUNDi - протокол, також розроблений Digium; OSP; T.38, підтримується передача факсів. Підтримка великого спектра терміналів і комп'ютерних протоколів дозволяє організовувати велику кількість сценаріїв взаємодії мереж, відправки, отримання та обробки інформації.

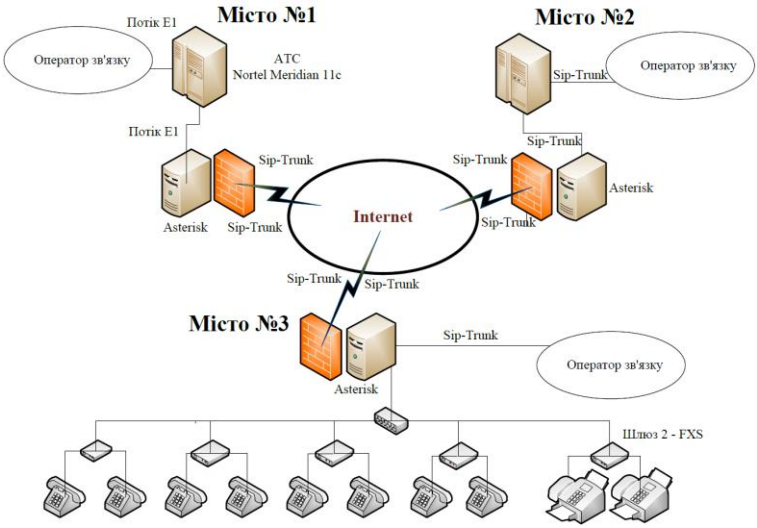

Рис. 2. Проєктована мережа

Програмна маршрутизація з використання спеціалізованого ПЗ для маршрутизаторів, і у випадку, коли апаратні методи не застосовуються, наприклад, при організації тунелів, або ПЗ на комп'ютері. В цілому, кожен комп'ютер виробляє маршрутизацію своїх вихідних пакетів. При маршрутизації чужих пакетів IP, і при побудові таблиць маршрутизації застосовуються різні ПЗ такі як: сервіс RRAS, routing and remote access service, в Windows Server; демони routed, gated, quagga, в Unix-подібних ОС, Linux, FreeBSD і тд.

Висновок. У результаті розробки даної дипломної (кваліфікаційної) роботи, загалом переглянута система роботи зв'язку, яка забезпечує трансляцію мовного і відео сигналів в мережі Інтернет, для зменшення вартості на міжміські і міжнародні дзвінки, досягнута в процеси використання нових інноваційних технологій. Далі, розроблений проєкт VoIP мережі на базі IP- PBX Asterisk між філіями, які знаходяться в різних містах України, яка виконує такі функції як: об'єднання філій компанії в одну корпоративну телефонну мережу; зменшення собівартості для компанії, при міжміських дзвінках; відео-дзвінки; аудіо-конференції; визначення додаткових найкоротших маршрутів при виході з ладу проєктованої корпоративної VoIP мережі.

УДК 621.396.933.4

М.І. Стожко
Національний авіаційний університет, м. Київ

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМ РАДІОЗВ'ЯЗКУ

Особливим питанням для стабільної та безвідмовної роботи авіаційних систем радіозв'язку (СРЗ) є заходи спрямовані на боротьбу із завадами, що забезпечують необхідну завадозахищеність.

Враховуючи значне різноманіття факторів виникнення завад в СРЗ, відповідно існують специфічні методи боротьби з ними, узагальнена класифікація яких показана на рис.1. Вони використовуються для досягнення високих параметрів завадозахищеності та стабільності роботи СРЗ в умовах складної радіообстановки.

Рисунок 1 – Основні методи боротьби з завадами.

Виходячи з фізичної природи виникнення завад та особливостей їхніх параметрів, будуються й методи боротьби з ними.

Схемотехнічні методи полягають у використанні особливих схемних рішень, що дозволяють зменшити вплив внутрішніх завад. Вони спрямовані на компенсацію паразитних зв'язків, що виникають усередині апаратури СРЗ, зокрема від генераторів та пристроїв електроживлення, і на стабілізацію робочих параметрів електронних модулів.

Системотехнічний метод полягає у застосуванні дієвих організаційних підходів, що дозволяють зменшити взаємні впливи різних радіосистем. Це може бути частотне та часове рознесення або вибір просторової орієнтації діаграм направленості антен.

Математичні методи базуються на розробці та використанні нових адекватних математичних моделей сигналів та завад, нового ефективного математичного апарату для обміну даних у СРЗ. Вони здатні значно знизити імовірність впливу різноманітних завад на

корисні сигнали і дозволяють здійснювати оптимальний прийом цих сигналів.

Конструктивні методи мають за мету правильну інженерну розробку конструкцій блоків СРЗ, розташування елементів таким чином, щоб зменшити влив, який ці елементи можуть чинити один на одного в процесі роботи системи.

Зазвичай, при аналізі завадостійкості, у першу чергу розглядають технічні методи зменшення рівня завад на виході пристроїв, а саме: екранування, заземлення, узгодження каскадів, фільтрація сигналів, придушення (частотна або часова) завад, рознесення антен СРЗ, вибір відповідних комунікаційних кабелів.

Типових прикладів є багато, але основою будь-якого підходу є детальний аналіз можливих факторів та шляхів проникнення завад.

Безпосередньо у процесі обробки прийнятих сигналів суттєвими стають різноманітні методи селекції, що зводяться до виділення сигналів на фоні перешкод на підставі можливих відмінностей їх основних параметрів, а саме: несучої частоти, ширини спектра, фази, напрямку приходу тощо.

Частотна селекція базується на відмінності амплітудно-частотних спектрів корисного сигналу і завади. Якщо завада загороджувального типу (спектр завади істотно ширше спектра корисного сигналу), то смугу пропускання радіоприймача необхідно максимально допустимо звужувати, узгоджуючи її зі спектром сигналу. Якщо ж спектр завади значно вужчий спектру сигналу, то доцільним є здійснення режекції (видалення) спектральних складових завади за допомогою відповідно налаштованого режекторного вузькосмугового фільтру, частота та смуга якого визначаються параметрами завади.

Розглядаючи завади радіоприйому, слід особливо відмітити завади від сусідніх за частотою радіостанцій. Цей вид завад характеризується тим, що їх усунення повністю в нашій владі; причина їх утворення – погані технічні засоби і організація каналів радіообміну. Для усунення взаємних перешкод між СРЗ необхідно:

1) суворо дотримуватися встановленого частотного розподілення хвиль між користувачами;

2) фільтрувати радіосигнали так, щоб ширина спектра не перевищувала половини інтервалу між несучими частотами сусідніх СРЗ;

3) усувати паразитні гармоніки несучої частоти.

Використання зазначених методів є корисним не тільки для СРЗ, а й для покращення завадостійскості інших типів радіоелектронних систем – локаційних, навігаційних, космічних, у яких інформація передається по сильно зашумлених каналах.

УДК 004.75

M. Suzdaltsev, PhD, assoc. prof. I. Ye. Terentieva
National Aviation University, Kyiv

CONCEPT AND GENERAL PROVISIONS OF THE INTERNET OF THINGS AND CLOUD COMPUTING

1. Introduction. Right now, many smart devices (laptops, smartphones, tablets) communicate with each other using Wi-Fi. By transferring these capabilities to ordinary household gadgets - refrigerators, washing machines, microwave ovens - and equipping them with computer chips, software, Internet access, you can make everyday life more comfortable, and the industry better and more profitable.

2. The concept and definition of the Internet of Things

IoT connects millions of smart objects, which leads to increased data traffic and the need for large processors and storage. Based on the above, IoT faces problems in the quality of service, data protection and security. Thus, the IoT architecture must take into account a number of issues, such as compatibility, scalability, QoS, reliability, and so on. However, each of the proposed architectures has a number of common shortcomings and does not cover all the features of IoT.

3. The architecture of the IoT system

The simplest architecture is the three-tier architecture. This was introduced in the early stages of research in this area. It has three levels, namely the detection level, network and application.

1. Perception layer is the physical level that sensors have for detecting the environment and collecting information. Detects some physical parameters or identifies other intelligent objects in the environment.

2. The network layer is responsible for connecting to other smart things, network devices and servers. Its functions are also used to transmit and process sensor data.

3. The application layer is responsible for providing program-related services to the user. It identifies a variety of programs in which you can deploy the Internet of Things, such as smart homes, smart cities, and smart healthcare.

At each level, the nodes are grouped into domains, where a single IoT domain consisting of Nodes-Fog-Cloud agents can execute a program. The following is a computing node and a cloud server for communicating and

interacting with each other; first, the IoT node transmits its tangible data directly to the nebula node belonging to its domain program. As a result, the fog node processes the received data directly or sends it to another fog node or cloud server in the same domain to return a response to the associated IoT node.

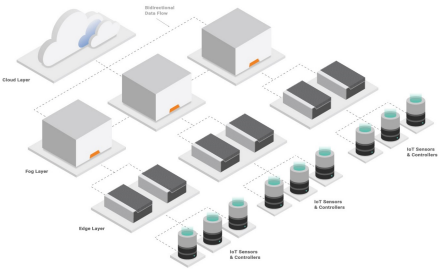

Fig.1 Example of typical structure of IoT

Advantages of the Internet of Things: communication; control and automation; monitoring; cost; a higher standard of living.

Weakness of the Internet of Things: security issue; compatibility; complexity.

4. Conclusion: In the long run, not only houses will become "smart", but also cities and even (some) states. But at this stage of technology and society, the Internet of Things is being actively implemented not on a global scale, but within companies engaged in the production of goods, energy, transportation, etc. - where new technologies are expected to increase productivity and competitiveness. The difficulty of scaling this experience is due to the fact that it is necessary to integrate many systems from different suppliers, and to establish their coordinated work.

References

1. R. Pratim, "A survey on Internet of Things architectures," Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 3, pp. 291-319, 2016.
2. Internet of Things: Architectures, Protocols and Standards Simone Cirani, Gianluigi Ferrari, Marco Picone, Luca Veltri

УДК 004.75

Topala R, PhD, assoc. docent. Tkalich O. P.
National Aviation University, Kyiv

Research of security systems of corporate networks and their problems

Nowadays, building a secure network is one of the most common problems for engineers. Since at the stage of designing and implementing a project, various problems may arise that both indirectly and directly affect the security of the network. In this section, corporate networks and their problems will be considered. Types of networks and ways to build them will be given, the difficulties that may arise with them and how to deal with them as far as possible. The main pros and cons of networks and ways to implement them are also considered

1. Principles of building corporate networks

Corporate data networks are one of the most useful tools for the development of medium and large businesses. Since such networks are very helpful in establishing business infrastructure and providing communication between different departments. They also reduce the delay in processing various requests and solving problems.

One of the main requirements for networks of this kind is that they must provide all types of telecommunications and information services. Also, the costs of creating and maintaining the network should not exceed the optimal ones.

The networks under consideration are for different purposes. For example, local and global, the main differences between these networks, as the name implies, is the unification of local units that are located on the same territory or units located at a certain distance from each other. Depending on the type of network we have chosen, the need to rent communication lines or build a virtual communication line between two departments is determined.

Also, an important nuance in the construction of the networks under consideration is the choice of equipment. As you know, equipment can be divided into two classes: main and peripheral. Backbone equipment is installed in those cases when leased communication lines are involved, or they create their own access nodes. In other situations, global means of information transfer take on this role. It is also necessary to pay attention to the fact that the backbone equipment is always subject to increased re-

quirements in terms of reliability, scalability and performance. As for the peripheral equipment for this class of special tools, the requirements are much lower, which affects some nuances of building a network.

Especially important is the definition of the topology on which the network will be built. At the moment, there are only four types of topologies. Some key features depend on the choice of topology, for example, the cost of building a network and its location.

2. The main cyber threats to the corporate network

To begin with, we should understand what is, all the same, responsible for security. Security responsibility refers to an action or event that can represent the destruction, distortion, or unauthorized use of network resources, including stored, perceived and processed information and software and hardware. Threats are divided into:

- Unintentional or accidental;
- Intentional.

Let's take a closer look at these threats. To begin with, Random threats arise as a result of errors in software, hardware failure, incorrect actions of users or a network administrator, etc. But Deliberate threats are aimed at causing damage to users and subscribers of the network and, in turn, are divided into active and passive.

Passive threats are aimed at unauthorized network information resources but do not affect their functioning. An example of a passive threat is receiving information circulating in the network channels through listening. In turn, active threats aim to disrupt the normal functioning of the network through a targeted impact on its hardware, software and information resources. Operational hazards include, for example, destruction or electronic jamming of communication lines, disablement of a computer or operating system, distortion of information in user databases or system information, etc. The main security threats include:

- disclosure of confidential information;
- information compromise;
- unauthorized exchange of information;
- refusal of information;
- denial of service;
- unauthorized use of network resources;

Threats of disclosure of confidential information are implemented through unauthorized access to databases. Information is compromised by

making unauthorized changes to databases. The unauthorized use of network resources means disclosing or compromising information and harms users and network administration. Erroneous use of resources is a consequence of local area network software errors. The unauthorized exchange of information between network subscribers makes it possible to obtain information to which access is prohibited, i.e., it essentially leads to information disclosure. Refusal of data consists of non-recognition by the recipient or sender of this information of the facts of its receipt or sending. Denial of service is a common threat that originates from the network itself. Such a failure is hazardous in cases where a delay in providing network resources can lead to severe consequences for the subscriber.

3. Methods for protection corporate network

The key to a successful fight against unauthorized access to information and data interception is a clear understanding of the channels of information leakage. Integrated circuits, on which computers are based, create high-frequency changes in the level of voltages and currents. Oscillations propagate through wires and can not only be transformed into an understandable form but also intercepted by particular devices. For example, devices can be installed on a computer or monitor to block information displayed on the monitor or entered from the keyboard. Interception is also possible when data is transmitted via external communication channels, for example, via a telephone line. In practice, several groups of protection methods are used, including:

- An obstacle in the way of the alleged kidnapper, which is created by physical and software means;
- Management, or influencing the elements of the protected system;
- Masking, or data transformation, usually by cryptographic means;
- Regulation, or the development of rules and a set of measures aimed at encouraging users interacting with databases to behave appropriately;
- Coercion, or the creation of such conditions under which the user will be forced to comply with the rules for handling data;
- Inducing or creating conditions that motivate users to behave appropriately.

Each of the methods of information protection is implemented using various categories of means. Fixed assets - organizational and technical.

Organizational means of information protection. The development of a set of organizational information security tools should be within the competence of the security service. Most often, security professionals:

Deploy documentation that establishes the rules for working with computer equipment and confidential information;

Conduct training and screening procedures for personnel; initiate the signing of additional provisions to the employment contract, which specifies liability for disclosure or misuse of evidence that has become permissible at work;

Delimit coverage areas to cover situations where the most common data available to one of the employees is most common; organize work in large workflow programs and track to get important files not stored outside of using disks;

Implement software products that protect data from sale or destruction by individuals, including top management of the organization;

System recovery plans in case of an outage from a building around the world.

If the company does not have a dedicated information security service, the way out will be to invite a security specialist to outsource. A remote employee will be able to audit the company's IT infrastructure and give recommendations on how to protect it from external and internal threats. Outsourcing in information security also involves the use of special programs to protect corporate information. The group of technical means of information protection combines hardware and software. Main of them:

- Backup and remote storage of the most important data arrays in a computer system - on a regular basis;
- Duplication and redundancy of all network subsystems that are important for data safety;
- Creation of an opportunity to redistribute network resources in cases of malfunction of individual elements;
- Ensuring the ability to use backup power systems;
- Ensuring safety from fire or water damage to equipment;
- Installing software that protects databases and other information from unauthorized access.

The set of technical measures also includes measures to ensure the physical inaccessibility of computer network objects, for example, such practical methods as equipping a room with cameras and alarms

Conclusion: Based on the above and having considered in more detail the topologies that are used in the construction of networks, a mixed topology was chosen.

Mixed topology is a network topology that prevails in large networks with arbitrary connections between computers. In such networks, it is possible to single out separate arbitrarily connected fragments (subnets) that have a typical topology; therefore, they are called networks with a mixed topology.

Also, after analyzing the market for XDR products, the cortex XDR was chosen to protect our network, namely its endpoints.

The Cortex XDR from Palo Alto Networks is, according to the manufacturer, the first system in the world that natively integrates network, end device and cloud data to prevent sophisticated attacks. It uses behavioral analytics (Behavioral IOC), and profiling identifies unknown and hard-to-detect threats to the network. Sandbox integration is available for dynamic and non-mediated (bare-metal) analysis. Machine learning and artificial intelligence models that work locally identify threats from any source, including managed and unmanaged devices, enabling rapid investigations. Several specialized technologies prevent the exploitation of vulnerabilities on endpoints, and the focus rules of behavioral analysis protect against ransomware. Cortex XDR prioritizes threats and assists in incident response by providing a complete picture of each danger, automatically identifying its root cause, and providing a wide range of actions against the station under attack.

References

1. https://www.dnsstuff.com/what-is-network-topology
2. https://www.britannica.com/technology/telecommunication
3. https://www.cisco.com/c/en/us/products/security/what-is-xdr.html

УДК 004.732 (043.2)

Д.Р. Устенко, В.В. Антонов
Національний авіаційний університет, м. Київ

МУЛЬТИСЕРВІСНА МЕРЕЖА КОМПАНІЇ

Сучасні потреби клієнтів у нових послугах є відправною точкою у визначенні стратегії розвитку мережевої інфраструктури. Попит на нові послуги – пакетної телефонії, передачі даних, відеоконференцзв'язку, голосової та універсальної пошти, теленавчання, VPN, а також додаткові інформаційні сервіси – розвивається у всьому світі стрімкими темпами. Мультисервісні мережі на підприємстві забезпечують можливість надання користувачам більш широкого спектра якісних послуг при ефективному використанні передавальних ресурсів мережі й універсальному способі обробки навантаження, що генеруються різними застосуваннями.

Усе більше організацій і підприємств приходять до висновку про необхідність створення мультисервісної мережі, що дозволяє використовувати увесь потенціал інформаційних технологій, значно підвищити їх ефективність і швидкість роботи. Такі зміни в структурі трафіку ускладнюють, а іноді і взагалі виключають, застосування аналітичного моделювання для створюваних алгоритмів і процесів. Альтернативним рішенням може служити імітаційне моделювання, яке дозволяє створювати моделі і умови роботи мережі найбільш наближені до реальності. Проблема проектування мультисервісних мереж є актуальною, внаслідок неможливості застосування старих підходів і відомих методик.

Задача проекту була в тому, щоб побудувати мультисервісну мережу підприємства використовуючи проводову і безпроводову мережу передачі даних. В даному завданні основною проблемою було підібрати комутаційне обладнання, яке б витримувало навантаження та функціонувало без жодних проблем і збоїв.

Проаналізувавши ринок інформаційних технологій вибір був зупинений на таких виробниках обладнання:

- для захисту мережі – WatchGuard;
- для комутаційної мережі – Hewlett-Packard;
- для бездротової мережі Ubiquiti UniFi та Linksys;
- для серверної частини також Hewlett-Packard.

Дані виробники є досить відомими і надійними компаніями, які вже давно стали світовими лідерами на ринку інформаційних технологій.

При побудові мережі було використано два інтернет канали, які ідуть через мережний захисний екран WatchGuard в два коммутатори Hewlett-Packard 1810-24 та Hewlett-Packard 2620-48 PoE+. Комутатор Hewlett-Packard 1810-24 повністю розрахований на серверну частину мережі. До нього було підключено шість серверів та одне мережне сховище даних. В свою чергу коммутатор Hewlett-Packard 2620-48 PoE+ використовується для комутації робочих станцій та оргтехніки.

В розрахунковій частині проекту були розраховані затримки та черги на Hewlett-Packard 2620-48 PoE+, розрахунок ймовірності збоїв та розрахунок надійності серверів. Також була побудована безпроводова мережа на обладнані Ubiquiti UniFi та Linksys. Програмно-апаратний комплекс Ubiquiti UniFi дозволяє побудувати безшовну Wi-Fi мережу, що складається з великої кількості безпроводових точок. Можливість підключити до одної майстер-точки, підключеної по кабелю, до 4-х точок по Wi-Fi. Завдяки цій можливості не довелося до кожної Wi-Fi точки підключати мережевий кабель. Було побудовано власну безпроводову мережу таким чином, щоб Wi-Fi мережа покривала повністю все приміщення.

З активним розвитком мультисервісних мереж стає важливим питання про їх кваліфіковану розробку. Адже від грамотного створення проекту мережі залежить ефективність її подальшого функціонування. У проекті в результаті проведеної роботи була спроектована мультисервісна мережу для офісу. Мережа було побудована двома способами: як проводовим так і безпроводовим, що повністю задовольнило всіх користувачів. Зробивши розрахунки черг і ймовірностей збоїв стає зрозумілим, що вибране обладнання повністю підходить для побудови офісів малого розміру.

УДК 004.75

A.Frolkov, PhD, assoc. prof. I. Ye. Terentieva
National Aviation University, Kyiv

TELECOMMUNICATION TECHNOLOGIES FOR THE VANET NETWORKS FUNCTIONING

What is transport in the automotive network of the future? In this network, vehicles will exchange between themselves (V2V) and with external infrastructure (V2I) a huge amount of data. This is data collected from GPS, cameras, radars, leaders that keep track of the state of the road, transport, driver, etc. To interact with the network, vehicles will be equipped with devices that support wireless communication (3GPP, IEE 802.11p, Bluetooth, etc.).

1. Automotive network data

There are two types of vehicular communications in such a network: V2V and V2I. Vehicles, roadside infrastructure can collect environmental information for processing and sharing (within reach). V2V means direct connection between vehicles. Such a message allows the exchange of information between vehicles regardless of the infrastructure. Such a connection is useful for extending the communication range of an automobile network.

In this case, the following types of interactions are distinguished:

1. Vehicle - Vehicle (V 2 V) – machine-machine interaction, used for information exchange between traffic-related applications [1];
2. Vehicle - Roadside (V 2 R) – vehicle-base station interaction, used to unload the network by declaring a part of the functionality for relaying, stationary base stations;
3. Vehicle - Infrastructure (V 2 I) is a subtype of interaction V 2 R , when mobile nodes are provided with access to an external network (Internet) through a connection to a base station.
4. Infrastructure - Infrastructure / Roadside - Roadside (I 2 I / R 2 R) - used to connect fixed stations into a single network, in order to plan the infrastructure for the tasks of any services.

2. The structure of a typical station ITS

Any ITS subsystem is built on the basis of interconnected ITS stations. In turn, each station consists of a set of components that communicate with each other through an internal network, as shown in Figure 1.

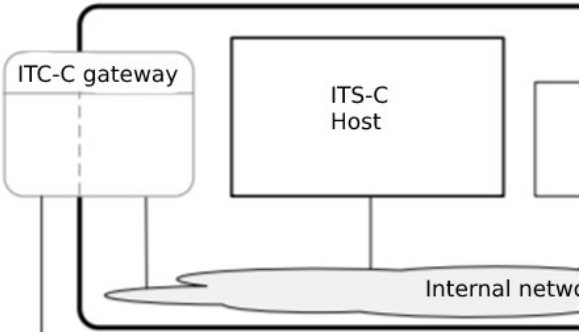

Fig. 1 Component composition of RSU

According to the EN 302 636-3 standard, the total mass of components is differentiated according to the functional feature into:

− hosts;
− gateways;
− routers;
− edge routers.

ITS-C hosts implement the minimum required functionality to support the underlying applications [3].

Conclusion

Wireless communication between vehicles is an object of research both in the scientific community and in the automotive industry. Automotive networks are developing more and more, creating a large field for new developments and discoveries.

In addition to security issues, there are also problems related to the speed of communication and the delay in transferring data from one vehicle to another. In the future, it is planned to develop the topic and achieve a minimum delay in data transmission through the use of unmanned aerial vehicles.

References

1. https://ru.wikipedia.org/wiki/Сети_VANET
2. https://en.wikipedia.org/wiki/Vehicular_ad_hoc_network
3. https://www.iec.ch/about/

УДК 621.396.967.2

А.І. Харченко
Національний авіаційний університет, м. Київ

ШЛЯХИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ РЛС ВІД ПАСИВНИХ ЗАВАД

Пасивні завади виникають за рахунок відображення електромагнітної енергії, що випромінюється РЛС, як від організованих перевипромінювачів (металізованих стрічок, ниток, скловолокна, спеціальних куточків), так і від хмар, опадів, земної поверхні та місцевих предметів.У радіолокації під пасивними завадами прийнято розуміти ехосигнали, виявлення яких не є завданням РЛС. Це відображення від поверхні, що підстилає об'ємно-розподілених природних і штучних утворень, а також сигнали, виникнення яких пов'язане з певними умовами поширення радіохвиль. Залежно від причини їх утворення пасивні завади можна розділити на три класи: поверхнево-протяжні, об'ємно-протяжні та просторово-дискретні. На індикаторі пошуку РЛС пасивні перешкоди спостерігаються як засвічені плями і ділянки (рис. 1.1), але в індикаторі дальності – як ділянки чи смуги сигналів великої амплітуди.

Рисунок 1.1 Вигляд пасивної завади на екрані індикаторі пошуку

Яскравість і амплітуда перешкод досить велика, внаслідок чого важко або неможливо на цьому фоні виділити позначку мети, що перебуває у хмарі. При дослідженні щільності розподілу ймовірностей амплітуди зазвичай беруть модель перешкоди у вигляді безлічі незалежних елементів, що відбивають, хаотично розподілених в елементі дозволу.

Труднощі виділення сигналів і натомість пасивних завад обумовлена тим, що перешкода, як і корисний сигнал, є відображення ЗС. Тому основна проблема розробки ефективних систем захисту пов'язана з вибором параметра або групи параметрів, в межах яких сигнал і пасивні перешкоди мають найбільші відмінності.

В даний час основна увага приділяється швидкісним (частотним) та просторово-часовим відхиленням сигналу від пасивних завад. Цей метод називають методом СДЦ. Для виявлення сигналу на тлі відбиття від метеоутворень у деяких РЛС як додатковий методу захисту застосовують поляризаційну селекцію. Загалом складне завдання підвищення захищеності перспективних РЛС від пасивних завад до рівня необхідної може бути вирішена лише за допомогою комплексу заходів, що передбачаються при їх проектуванні та забезпечують :

1. Зменшення потужності перешкоди на вході приймача. Потужність пасивних завад, що впливає на вхід приймача, дорівнює сумі потужностей відбитків від сукупності відбивачів даного обсягу, що дозволяється. Звичайно, чим менший обсяг, тим менше буде потужність пасивних завад. При цьому передбачається, що розміри мети менші за дозволений обсяг і потужність корисного сигналу залишається незмінною. . Тому підвищення роздільної здатності можливості РЛС по дальності та кутовим координатам є дієвою мірою підвищення їх захищеності від ПП. Якщо можливості підвищення роздільної здатності оглядових РЛС по азимуту вже практично вичерпані, то за дальністю та кутом місця ще досить великі.

Для забезпечення високої роздільної здатності по дальності у РЛС малої дальності дії доцільно застосовувати короткі «гладкі» імпульси, тому що вони не дають побічних максимумів на виході СФ і простіше у формуванні та обробці. В РЛС з великою дальністю дії, де потребується велика енергія зондуючих сигналів забезпечити яку при коротких імпульсах важко, застосовуються довгі широкосмугові сигнали з роздільною здатністю по дальності близько десятка метрів;

2. звуження спектра флюктуацій перешкоди;

3. оптимізацію системи обробки сигналів і натомість пасивних завад.

УДК 621.396 (043.2)

В.Р. Хіврич, В.В. Антонов
Національний авіаційний університет, м. Київ

ОПТИЧНА МЕРЕЖА МІСТА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ NG-PON2

В даний час спостерігається «вибуховий» попит на мультимедійні послуги, а в майбутньому – на надширокосмугові послуги, такі як послуги ультраякісного телебачення у форматі 3D. Послуги «хмарних» обчислень і зберігання інформаційного контенту, що динамічно розвиваються, а також стрімке зростання бездротових методів передачі і все більші запити на пропускну спроможність мереж вимагають швидких і ефективних рішень для забезпечення зростаючих інформаційних потреб, що призводить до зближення та конвергенції бездротових та дротових мереж. Також необхідно враховувати нові напрями розвитку телекомунікаційних та інформаційних систем, наприклад, технологію M2M (machine-to-machine), або по-іншому IoT (Internet of things – «Інтернет речей»). За прогностичними оцінками в найближчому майбутньому кількість пристроїв класу M2M буде значно більше, ніж кількість людей, що населяють нашу планету. Очікується, що термінали M2M передаватимуть відеоінформацію. Обмін цією інформацією між терміналами здійснюватиметься мережами доступу. Зростає роль мереж доступу у забезпеченні телекомунікаційними послугами бізнес-користувачів, великих підприємств та опера-торів бездротового зв'язку, що вимагають швидкісну симетрію у напрямках передачі. Важливою вимогою є гарантоване виділення ресурсів мережі доступу кожному із споживачів послуг.

Стандарт NG-PON2 дозволяє об'єднувати мережі з кількома службами в один ODN. Це призводить до значного зниження сукупної вартості володіння, водночас дозволяючи впроваджувати нові ефективні архітектури, глибоко адаптовані до но-вих потреб абонентів. Рисунок 1 ілюструє основні будівельні блоки NG-PON2. Вони включають:

Optical Line Terminals (OLT) - Лінійні карти OLT підтримують сумісні плани довжини хвилі. Лінійні карти надають прийомопередавачі, що підключаються, специфічні для лямбди (λ1 ... λ4); Optical Networking Units (ONU) - ONU з лазерами, фільтрами і приймачами, що перебудовуються, для підтримки сумісних планів довжин хвиль, що забезпечує їх мобільність; Wavelength Multiplexer (WM1) - хвильовий мультиплексор - це пристрій MUX з пасивною довжиною хвилі, який поєднує 4 довжини хвилі NG-PON2 в одно-му волокні (з майбутньою підтримкою 8 довжин хвиль);

Co-existence Element (CE) - це пристрій MUX з пасивною довжиною хвилі, який поєднує більшість технологій доступу в одному волокні.

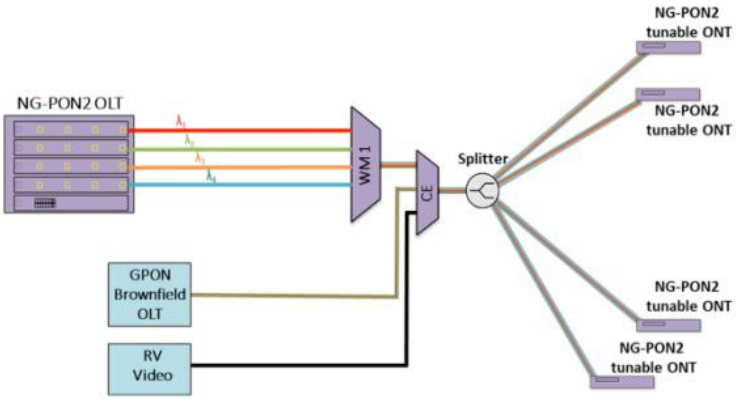

Рис.1. Основні будівельні блоки NG-PON2

NG-PON2 використовує мультиплексування з поділом за часом і довжиною хвилі (TWDM) і підтримує щонайменше одну довжину хвилі, яка може зростати до 4 довжин хвиль (λ1…λ4) або до 8 довжин хвиль (у майбутньому) в моделі з оплатою в міру зростання на кожному волокні, що робить його першим у галузі стандартом доступу до кількох довжин хвиль. Кожна довжина хвилі в одному волокні може забезпечувати симетричну швидкість 10 Гбіт/с (висхідний і низхідний), що забезпечує пропускну здатність 40 Гбіт/с оптоволоконному з'єднанню. Стандарт допускає максимум вісім довжин хвиль, що дозволяє NG-PON2 забезпечувати швидкість до 80 Гбіт/с.

Висновок. Технологія NG-PON2 пропонує багато переваг для забезпечення постійної ро-боти в мережі. Вона забезпечує швидкості, необхідних використання широкого спектра додатків, інтенсивно використовують пропускну спроможність. NG-PON2 на-дає перспективну архітектуру, яка підвищує ефективність та гнучкість та знижує експлуатаційні витрати. Оновлення можуть виконуватися без проблем, без шкоди абонентським послугам, а мережа може бути розширена з використанням підходу з оплатою в міру зростання. Більше того, смуга пропускання може бути легко перебалансована в мережі за необхідності, призначаючи користувачів різним довжинам хвиль. Завдяки можливості доставки 10 Гбіт/с (і вище) окремому абоненту, NG-PON2 відкриває нові бізнес-можливості для постачальників послуг.

УДК 621.392. (043.2)

Чорний М.С., студент
Національний авіаційний університет, м. Київ
Науковий керівник – Зуєв О.В., к.т.н., доц.

ПИТАННЯ ПІДВИЩЕННЯ ВІРОГІДНОСТІ КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ РАДІОЕЛЕКТРОННИХ СИСТЕМ

Контроль – це процес установлення відповідності між об'єктивним станом об'єкта і заздалегідь заданою нормою на можливі стани об'єкта, що здійснюється шляхом сприйняття сукупності контрольованих параметрів, обробки отриманої інформації, формування та видачі рішення про результати встановлення відповідності [1].

Технологічна операція контролю – одна з основних з усіх технологічних процесів експлуатації радіоелектронних систем (РЕС). Слідом за встановленням відповідності між об'єктивним технічним станом РЕС і тим технічним станом, який є відмінним, виконуються ті або інші керувальні впливи, наприклад, регулювання, настроювання, поточний ремонт, плановий ремонт, позаплановий обліт об'єктів і т. ін.

Операторну схему контролю технічного стану РЕС показано на рис.

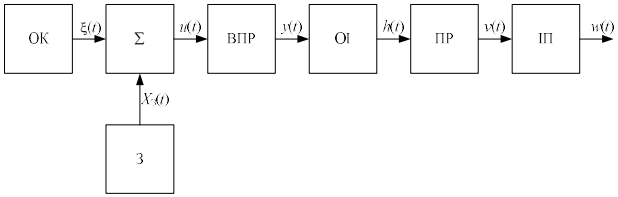

Рисунок - Схема контролю технічного стану РЕС: ОК – об'єкт контролю; ВПР – оператор, який визначає роботу вимірювального приладу; ОІ – оператор обробки інформації; ПР – оператор прийняття рішення; ІП – оператор, який визначає роботу індикаторного пристрою; З – оператор завад вимірювання

Для розв'язання завдань синтезу і аналізу операторної схеми необхідно деталізувати узагальнений вигляд уведених операторів, приз-

начити показники ефективності операцій контролю технічного стану РЕС.

Вірогідність контролю є кількісною мірою об'єктивності прийнятих у результаті контролю технічного стану РЕС рішень. Кількісно вірогідність контролю визначається відношенням ймовірності прийняття правильного рішення до суми ймовірностей прийняття правильних і помилкових рішень [1,2].

У науково-технічній літературі [1,2] розглядають два основні способи підвищення наведених вірогідностей – удосконалення методичної складової контролю і удосконалення інструментальної складової контролю.

Методична складова контролю здебільшого пов'язана з організацією контролю і технологією (алгоритмами) контролю технічного стану РЕС. Інструментальна складова контролю передбачає найчастіше вдосконалення апаратурного забезпечення процесу контролю технічного стану РЕС.

Детальну класифікацію методів підвищення методичної складової вірогідності контролю наведено в літературі [1] .

До основних методів підвищення інструментальної складової вірогідності можна віднести :

– підвищення безвідмовності та поліпшення ремонтопридатності контрольно-вимірювальної апаратури;

– зменшення похибок контрольно-вимірювальних операцій;

– зменшення рівня завад у вимірювальних ланцюгах контролю технічного стану РЕС і т. ін.

Зокрема, для підвищення вірогідності вводять контрольний допуск на додаток до гарантійного допуску, визначеному в технічних умовах.

Зі звуженням контрольного допуску порівняно з гарантійним допуском зменшується ризик замовника і збільшується ризик виготовлювача.

Удосконалюючи алгоритми первинної обробки вимірювальної інформації про параметри РЕС застосовують мажоритарні алгоритми. При цьому робиться n вимірюваь контрольованого параметра. Порівнюючи значення параметра з допусками маємо, наприклад, m наслід-

ків – результат вимірювань у межах допусків і $(n\text{-}m)$ наслідків – результат вимірювань поза допусками. Якщо $m \geq k$ (де k – задане граничне значення), то приймається рішення про те, що РЕА за даним визначальним параметром ”придатна”, інакше вважають, що РЕА за даним визначальним параметром ”непридатна”.

Для первинної обробки вимірювальної інформації з одного визначального параметра РЕС та вторинної обробки сукупності даних про визначальні параметри всього виробу можна застосовувати такі два методи.

Це метод багаторазової перевірки з відбраковуванням і метод з багаторазовою повторною перевіркою контрольованих параметрів. Багаторазову перевірку з відбраковуванням можна застосовувати як до комплектуючих деталей, вузлів РЕС, так і стосовно всього виробу.

Об’єкти контролю, визнані придатними за результатами першої перевірки, підлягають вторинній перевірці. Далі ОК, визнані придатними під час другої перевірки, перевіряють утретє і т. ін. Використовуючи таку процедуру контролю технічного стану ОК у тих виробах, які приймаються замовником, можна скоротити частку непрацездатних виробів. Тим самим зменшується ”ризик замовника” і підвищується вірогідність результату ”придатний”. Але при цьому ”ризик виготовлювача” збільшується і знижується вірогідність результату ”непридатний”.

Список використаних джерел

1. Системи експлуатації авіаційних радіоелектронних систем та комплексів: Конспект лекцій / О.В.Соломенцев, М.Ю. Заліський, О.В. Зуєв, С.В.Рудий. – Кривий Ріг: КК НАУ, 2017. – 62 с.

2. Зуєв О.В. Ситуативний аналіз прийняття рішень та реалізації керуючих впливів в процесах технічного обслуговування радіотехнічних систем / Вісник державного університету інформаційно-комунікаційних технологій. – 2009. – Том 7, №2. – с. 183–187.

УДК 004.4’2 (043.2)

Ю.Є. Яремчук, А. В. Грицак
Вінницький національний технічний університет, м. Вінниця

УДОСКОНАЛЕНИЙ МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Вимоги до рівня захисту інформації почали зростати зі збільшенням кількості атак від зловмисників не тільки на великі технологічні компанії, але і на рядових користувачів. Після викриття Сноуденом фактів прослуховування спецслужбами пересічних громадян США все, хто користуються мобільними мессенджерами, відразу стали приділяти увагу особистій безпеці даних і захисту інформації. Саме тому на ринку з'явився ряд месенджерів, які використовують повне або часткове шифрування повідомлень, файлів, фотографій або відео, які ви пересилаєте іншим людям.

Крім власне шифрування, також з'явилася опція самознищення повідомлень і цілих чатів і навіть блокування можливостей для скріншотів. Месенджери Wickr, Wiper і ряд аналогів пропонують саме такі суперможливості.

Прототипом для методу побудови генераторів псевдовипадкових послідовностей оберемо MTProto Mobile Protocol v.1.0 [1]. Порівняно з прототипом внесемо зміни:

1. Змінені вхідні та вихідні дані методу. На вході приймаються і обробляються наступні дані: повідомлення M, інформацію про ідентифікатор користувача та ідентифікатор сесії S, інформацію про час відправлення і довжину повідомлення ID та порядковий номер повідомлення PD. На виході тільки отримуємо $mHash$ – геш значення DB ($DB = \left(S, ID, M\right)$) та $EncP$ – зашифроване повідомлення P.

2. Замість використання геш функції SHA-1 введено використання певної криптостійкої геш функції F_{hash}. Слід

зауважити, що у якості F_{hash} може бути використана функція гешування.

3. Замість використання блокового шифру AES введено використання функції F_{enc}. Слід зауважити, що у якості F_{enc} може бути використаний певний криптостійкий алгоритм шифрування, побудований на основі блокових, потокових шифрів чи геш функцій тощо.

4. У якості $authKey$, ввдено використання заздалегідь узгодженого секретного ключа користувачів, наприклад за допомогою протоколів асиметричної криптографії.

Отже, провівши дослідження ми бачимо що удосконалений метод, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в інформаційно-комунікаційних системах. Для використання на практиці даного методу потрібно визначитись/зафіксувати функцієї гешування F_{hash} та функцію шифрування F_{enc}.

[1] *Майзаков К.Д., Алгоритмическая оптимизация вычисления прообразов необратимых хэш-функций MD5 И MD4. [Електронний ресурс] / К.Д. Майзаков, Д.А. Эдель, В.А. Новосядлый // URL: http://docplayer.ru/39360691-K-d-mayzakov-d-a-edel-v-a-novosiadliy-algorithmic-optimization-of-inverse-image-computation-for-md5-and-md4-digest-algorithms.html*

[2] *Daum Magnus, Cryptanalysis of Hash Functions of the MD4-Family / M. Daum. — B.: Electronic edition, 2005. — P. 23-34.*

[3] *Debaert C. The RIPEMDL and RIPEMDR Improved Variants of MD4 Are Not Collision Free/ Debaert C., Gilbert H. // L.:LNCS, 2002. — P. 52–65.*

[4] *Dobraunig Christoph, Analysis of the Kupyna-256 Hash Function. [Electronic recourse] /C. Dobraunig, M. Eichlseder, F. Mendel // URL: https://eprint.iacr.org/2015/956.pdf*

УДК 004.056.5

Ю.Є. Яремчук, І.О. Бондаренко, І.С. Каплун
Вінницький національний технічний університет, м. Вінниця

ПІДВИЩЕННЯ СТІЙКОСТІ АВТЕНТИФІКАЦІЇ ДО АТАК ТИПУ SHOULDER SURFING

Одним із перших етапів контролю доступу та основною перешкодою від несанкціонованого доступу до інформаційних ресурсів є автентифікація. Автентифікація – процедура перевірки достовірності суб'єкта, яка дозволяє впевнитися у тому, що суб'єкт, пред'явивши свій ідентифікатор, дійсно є саме тим суб'єктом, ідентифікатор якого він використовує, тобто підтверджується відповідність суб'єкта ідентифікатору. Метод парольної автентифікації найбільш поширений та простий серед звичайних користувачів. Більшість користувачів із збільшенням облікових записів використовують одні й ті ж самі текстові паролі, які легко вгадати, або записують паролі, які важко запам'ятовувати, тим самим, не притримуючись парольної політики. Збільшуються випадки ризику злому та отримання конфіденційної інформації зловмисниками. Існують альтернативні методи автентифікації для вирішення даної проблеми – автентифікація на основі біометричних даних та на основі графічних паролів.

Графічні паролі мають ряд переваг, так і недоліків. Основні переваги графічних паролів над іншими методами автентифікації наступні:

- легкість запам'ятовування;
- стійкість до більшості атак;
- потенційно більший простір для паролів;
- скомпрометований графічний пароль легко замінити;
- порівняно невелика вартість розробки;

Основними недоліками для більшості графічних паролів є час введення пароля та вразливість до атаки типу shoulder surfing.

Атака типу shoulder surfing – це одна з форм злому, за допомогою якої зловмисник може отримати несанкціонований доступ до даних користувача.

Виділяють три типи основних засобів атаки типу shoulder surfing:

- Тип I: неозброєними очима;
- Тип II: одноразова відео фіксація процесу автентифікації;
- Тип III: багаторазова відео фіксація процесу автентифікації.

Вразливість методу автентифікації до атаки Типу I, доводить, що метод автентифікації вразливий і до атак Тип II та Тип III. Наприклад, традиційний текстовий пароль та PIN-код, розкривають паролі зловмисникам, як тільки користувач вводить його за допомогою клавіатури або натисканням певних елементів на екрані. Інші схеми, навпаки, можуть протистояти Типу I, але є вразливими до атак Типу II та Типу III. Багаторазова відео фіксація вимагає від зловмисника більших зусиль і прийомів. Якщо парольна автентифікація протистоїть атакам Тип III, то вона буде захищена від атак Тип I та Тип II.

Прототипом обрано схему Triangle. Основним недоліком даної схеми є час реєстрації та кількість повтору сесій введення пароля. Через можливі проблеми із запам'ятовуванням довгих паролів, запропоновано обрати оптимальну довжину з 5 парольних зображень, на відміну від прототипу. Оскільки, генерується випадковий набір із P зображень, який включає і парольні зображення, виникає можливість проведення частотного аналізу попадання парольних зображень в згенерований набір модуля автентифікації. Тому для усунення даної вразливості запропоновано генерувати випадковий власний набір для кожного користувача із 20-30 зображень, які будуть мати більш високу ймовірність попадання в згенероване зображення і рівномірно розподілені поміж інших зображень. Збільшення кількості парольних зображень дає можливість отримання додаткових комбінацій паролів. Під час кожної сесії буде проведено рандомний вибір *3* із *5* парольних зображень. Зміна довжини парольних зображень дозволить зменшити кількість сесій вводу пароля та ймовірність його вгадування.

Проаналізувавши значення ймовірності випадкового попадання в область трикутника, запропоновано контролювати та обмежувати розмір площі згенерованого трикутника. Якщо область трикутника занадто велика – збільшується ймовірність вгадування вірного кліку, а якщо занадто мала – призводить до збільшення помилкових кликів.

Отже, провівши дослідження бачимо, що вдосконалення графічного пароля за схемою Triangle, за рахунок вибору оптимальної довжини парольних зображень, генерації випадкового набору для кожного користувача та їх рівномірного розподілення, а також визначення граничних меж області згенерованого трикутника, дозволило підвищити стійкість та рівень безпеки даного методу автентифікації до атак типу shoulder surfing.

НАУКОВЕ ВИДАННЯ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 ЧЕРВНЯ 2022 Р.

М. КИЇВ

ГОЛОВНИЙ РЕДАКТОР ОДАРЧЕНКО Р.С.

КОМП'ЮТЕРНА ВЕРСТКА ЛАВРИНЕНКО О.Ю.

КОНТАКТНИЙ E-MAIL: conference@tks.nau.edu.ua

ВІДПОВІДАЛЬНІСТЬ
ЗА ЗМІСТ ТА ФОРМУ ВИКЛАДЕННЯ НАУКОВИХ РЕЗУЛЬТАТІВ
НЕСУТЬ АВТОРИ МАТЕРІАЛІВ ТЕЗ.

ЕЛЕКТРОННА ВЕРСІЯ ТЕЗ КОНФЕРЕНЦІЇ ЗРОБЛЕНА СПЕЦІАЛЬНО ДЛЯ РОЗМІЩЕННЯ НА САЙТІ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ
http://tks.nau.edu.ua