МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

XIV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

5 – 7 червня 2024 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, 5 – 7, 2024
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»

5 – 7 червня 2024 р.
м. Київ, Україна

УДК 621.39: 004.9 (082)

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 5 – 7 червня 2024 р., Національний авіаційний університет. – К.: Вид-во НАУ, 2024. – 144 с.

ISBN: 978-611-01-0740-2

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова:

Гнатюк С.О.	в.о. проректора з наукової роботи Національного авіаційного університету, доктор технічних наук, професор;

Члени оргкомітету:

Гнатюк В.О.	кандидат технічних наук, доцент, 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;
Одарченко Р.С.	доктор технічних наук, професор, в.о. декана Факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету;
Бахтіяров Д.І.	кандидат технічних наук, доцент, заступник декана Факультету аеронавігації, електроніки та телекомунікацій Національного авіаційного університету;

Секретар:

Лавриненко О.Ю.	кандидат технічних наук, доцент, доцент кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету.

ЗМІСТ

УДК 621.391:004.8 (043.2)

Андрій ОСИПЧУК, Юлія ПЕТРОВА
Національний авіаційний університет, м. Київ

ДИСКРЕТНА СИСТЕМА СКУД НА БАЗІ GSM КОНТРОЛЕРА

У сучасному світі важливо забезпечувати безпеку об’єктів різного призначення, що зумовлює розвиток систем контролю і управління доступом (СКУД). Однією з перспективних технологій є використання GSM-контролерів, які дозволяють здійснювати віддалений контроль і управління доступом на об'єкти з використанням мобільних мереж. Це особливо актуально для об'єктів, які знаходяться в складних умовах або віддалених місцях, де традиційні системи можуть бути неефективними.

Традиційні системи СКУД, хоча і ефективні, мають низку недоліків, таких як обмеження щодо віддаленого доступу, висока вартість монтажу та обслуговування, необхідність у спеціалізованій інфраструктурі. Використання GSM-контролерів може значно знизити ці недоліки, забезпечуючи гнучкість, доступність та надійність системи. Однак, інтеграція GSM-технологій у СКУД потребує ретельного підходу до проєктування, врахування особливостей безпеки передачі даних та зручності користування.

Технологія та принцип роботи. GSM-контролер є пристроєм, що використовує мобільну мережу для передавання даних між контролюючими та контрольованими елементами системи СКУД. Він містить GSM-модуль, що забезпечує зв’язок через стільникову мережу, мікроконтролер для обробки команд та управління периферійними пристроями, такими як електронні замки, датчики, зчитувачі карт тощо.

Переваги використання GSM-контролерів:

- Віддалений доступ: адміністратор системи може контролювати та керувати доступом до об'єкту з будь-якої точки світу, використовуючи мобільний додаток або веб-інтерфейс.
- Легкість встановлення: не потребується прокладання спеціальних кабелів для передачі даних, що знижує витрати на монтаж і обслуговування.
- Гнучкість: система може бути легко масштабована та адаптована до різних типів об'єктів та умов експлуатації.

• Надійність: використання мобільних мереж забезпечує високу надійність передачі даних навіть у віддалених районах.

Основні компоненти системи:

• GSM-контролер: центральний елемент системи, який здійснює зв'язок з іншими компонентами через GSM-мережу.

• Електронні замки та зчитувачі: пристрої, що безпосередньо здійснюють контроль доступу до приміщень.

• Сервер управління: програмне забезпечення для централізованого управління системою, зберігання даних про доступ та налаштування.

• Мобільний додаток: інтерфейс для користувачів та адміністраторів системи для керування доступом та моніторингу.

Одним із прикладів застосування дискретної системи СКУД на базі GSM-контролера є організація контролю доступу на склади, офіси, паркувальні зони та житлові комплекси. Наприклад, в офісних будівлях можна легко керувати доступом співробітників і відвідувачів, надаючи або скасовуючи доступ у режимі реального часу.

Висновок. Використання дискретних систем СКУД на базі GSM-контролерів є ефективним рішенням для забезпечення безпеки об'єктів різного призначення. Вони поєднують у собі надійність, гнучкість і зручність, забезпечуючи віддалений доступ та управління. Це дозволяє оптимізувати витрати на встановлення та обслуговування, одночасно підвищуючи рівень безпеки об'єкта. Перспективи розвитку таких систем відкривають нові можливості для інтеграції з іншими технологіями, що робить їх ще більш привабливими для широкого кола користувачів.

Література

1. Смирнов, І. К., "Системи контролю і управління доступом", Видавництво "Безпека", Київ, 2020.

2. Петров, О. В., "GSM-технології в сучасних системах безпеки", Журнал "Технології захисту", 2021.

УДК 336.7:[330.34+004]
Ф-60

С.О. Асмолов, О.Г. Саітгареєва
Криворізький фаховий коледж
Національного авіаційного університету»,
м. Кривий Ріг

ФІНТЕХ: ІННОВАЦІЇ ТА КІБЕРБЕЗПЕКА

Фінансові технології відіграють ключову роль у сучасному світі, прагнучи вдосконалити та автоматизувати надання і використання фінансових послуг. Вони охоплюють програмне забезпечення, мобільні додатки та інші технології, спрямовані на покращення і автоматизацію фінансових процесів [1, с. 96].

В Україні функціонує понад 80 286 FinTech-компаній, більшість з яких були засновані протягом останніх трьох років. Після фінансової кризи 2008-2009 років з'явилися перші FinTech-стартапи, які зосереджувалися на платежах і переказах [2, с. 4]. Кількість таких стартапів досягла близько 60 до кінця минулого року. Наразі 84% українських FinTech-стартапів (див рис. 1), вже отримують прибуток від продажу своїх продуктів і послуг [2, с. 20].

Штучний інтелект відіграє важливу роль у цифровізації економіки, знижуючи витрати та забезпечуючи доступ до споживачів. Це дозволяє новим учасникам у фінансовій сфері, таким як мобільні оператори та електронна комерція, розвиватися. Використання штучного інтелекту в фінансовому секторі також відіграє важливу роль у кібербезпеці, захищаючи дані клієнтів [3, с. 301].

Використання чат-ботів в українських компаніях FinTech забезпечує швидку підтримку клієнтів у фінансовому секторі та інших галузях, роблячи їх важливим інструментом для будь-якого бізнесу, де є потреба в оперативному зв'язку та розв'язанні питань [4].

Перевага над конкурентами за різними параметрами дозволяє організації пропонувати товари або послуги вищої якості і/або за нижчими цінами. Це зміцнює ринкові позиції, забезпечує прибуток вище середнього рівня і позитивно впливає на конкурентні переваги (див. табл. 1). Технічні заходи, такі як захист даних і впровадження шифрування, необхідні для забезпечення конфіденційності та відповідності регулятивним вимогам [5].

Фінансові технології визначають сучасний світ, впливаючи на розвиток та автоматизацію фінансових процесів. В Україні активно зростає кількість компаній у секторі FinTech, підтверджуючи його значущість і потенціал. Використання штучного інтелекту і чат-ботів у фінансовому секторі допомагає не лише знизити витрати, а й підвищує рівень безпеки та якості фінансових послуг для клієнтів.

Література:

1. Фаренюк Н.В. «Неофінанси світової економіки»: монографія. Київ: Навчально-науковий інститут міжнародних відносин Київського національного університету імені Тараса Шевченка, 2023. 240 с.
2. “Фінтех в Україні: тенденції, огляд ринку та каталог “ URL: https://data.unit.city/fintech/fgt34ko67mok/fintech_in_Ukraine_2018_ua.pdf (дата звернення 21.05.24).
3. Єфремова К.В. «До питання застосування штучного інтелекту у сфері фінансових послуг» https://ndipzir.org.ua/wp-content/uploads/2020/09/Tezy_25_06_20/Tezy_25_06_20_300-305.pdf (дата звернення 29.05.24).
4. Демчишак Н. Б., Гудима Р. П. «Розвиток фінтеху в Україні та світі на основі використання технологій блокчейну і штучного інтелекту». *Ефективна економіка.* 2021. № 6. URL: http://www.economy.nayka.com.ua/pdf/6_2021/4.pdf (дата звернення: 29.05.2024).

Шпиг.Ф.І. Конкурентоспроможність банку: фактори та критерії оцінки. *Проблеми і перспективи банківської системи України збірник наукових праць*. - Суми: Українська академія банківської справи Національного банку України, 2006 .- Т. 16. – С. 57-63.

УДК 004.7:004.056 (043.2)

Максим БЕРДИЛО, Денис БАХТІЯРОВ, Віталій КУРУШКІН
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VIRTUAL PRIVATE NETWORK

У сучасному світі телекомунікаційні мережі відіграють ключову роль у забезпеченні зв'язку та обміну інформацією між різними користувачами та організаціями. Однією з найбільш ефективних технологій для захисту даних у таких мережах є Virtual Private Network (VPN). Використання VPN дозволяє створювати захищені канали зв'язку поверх відкритих мереж, забезпечуючи конфіденційність, цілісність та автентичність переданої інформації. Ця стаття розглядає принципи побудови телекомунікаційної мережі з використанням технології VPN, акцентуючи увагу на її перевагах, архітектурних рішеннях та практичних аспектах впровадження для підвищення безпеки та ефективності мережевих комунікацій.

Традиційна технологія та вимоги «в повітрі» передбачають високу пропускну здатність, значення затримки та високу гнучкість. Тим не менш, поточні обставини на ринку вимагають нових правил гри. Для мережі вашого провайдера послуг тепер недостатньо просто отримати доступ до магістралі Інтернету. Доступ до вбудованих мережевих сервісів, організації віртуальної приватної мережі (VPN) і багатьох інших інтелектуальних функцій є важливими компонентами модифікованого користувача. Збільшення попиту на більшу кількість послуг, які можна продавати за допомогою легкого доступу до IP, передбачає, що інтернет-провайдери отримають значні прибутки.

Архітектура кабельних компаній передбачає створення мережі з практично нескінченними масштабованими можливостями, підвищеним трафіком, швидкістю обробки та безпрецедентною гнучкістю в плані організації додаткових послуг. Крім того, оскільки у кабельних компаній немає технології, яка дозволяє інтегрувати IP і ATM мережі, постачальники послуг не тільки зможуть заощадити гроші на закупівлі обладнання асинхронного передавання, але й зможуть усунути надлишковий розподіл вигод, пов’язаних із цими протоколами.

Група маршрутизації IETF має однойменну робочу групу, яка відповідає за розробку архітектури, яку кабельні компанії не використовують. Представники найбільших постачальників обладнання та ме-

режевих рішень активно брали участь у заходах. Ця архітектура була розширена з використанням даних системи, запропонованих Cisco Systems; однак деякі концепції були перенесені на паралельну технологію IP-комутації Ipsilon і продукт IBM Aris. Завдяки зусиллям IETF кабельні компанії перетворять на стандартний інтернет, оскільки їхній дизайн не зібрав найвдаліших елементів з усіх заходів. Крім того, самі компанії не зацікавлені у швидкому просуванні технології на ринок.

Класична технологія VPN дозволяє передачі даних через мурашині тунелі. Немає VPN і шифрування в кабельних компаніях. Кабельні компанії не маркують пакети, щоб вони залишалися непомітними, оскільки вони перевозяться на час. Маршрутизатори LSR (Label Switch routers) розташовані на позначеному сліді можуть читати трафік певних символів. Для кабельних компаній, які не мають власної мережі, звичайний метод IP-маршрутизації не використовується; трафік маршрутизується лише по слідах міток. Кабельні компанії можуть продовжувати використовувати не сам пакет, якщо це необхідно (рисунок 1). Кабельні компанії не мають VPN-інфраструктури, яка включає програмне забезпечення та створення розподіленого клієнта всередині IP-мережі. Таким чином, віртуальна приватна мережа гарантує обмін пакетами між IP-мережами.

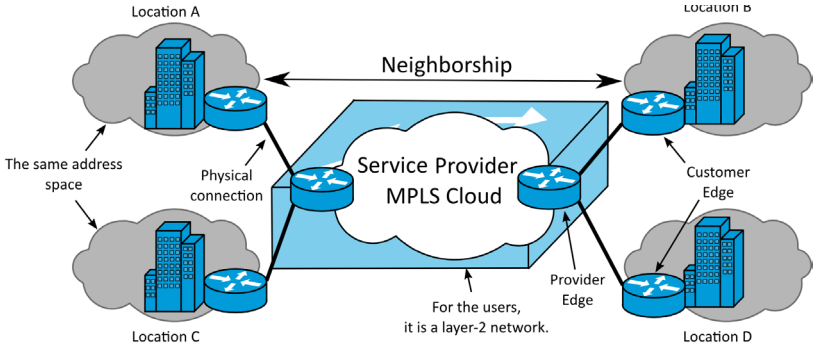


Рис. 1. Мережа MPLS VPN

Висновок. Загалом, перехід до нових технологій, таких як IP-комутація та VPN, забезпечить кращу продуктивність, гнучкість і можливість надання додаткових послуг, що, в свою чергу, призведе до зростання прибутків інтернет-провайдерів.

УДК 621.391 (043.2)

Дмитро БОЙКО, Веніамін АНТОНОВ
Національний авіаційний університет, м. Київ

СУБСМУГОВИЙ МЕТОД ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ВЛАСНИХ ВЕКТОРІВ

У сучасному світі зростаючий попит на швидке та ефективне передавання інформації стимулює розвиток нових методів і технологій в галузі зв'язку. Одним з перспективних напрямків є субсмуговий метод передавання інформації на основі власних векторів. Цей підхід дозволяє значно підвищити ефективність використання смуги пропускання та покращити стійкість до перешкод, що є критично важливим для сучасних систем зв'язку. Субсмуговий метод передавання інформації використовує математичний апарат власних векторів для оптимізації процесу модуляції і демодуляції сигналів. Це дозволяє зменшити рівень шумів і спотворень, а також забезпечити високу точність відновлення переданої інформації. Застосування даного методу відкриває нові можливості для розвитку телекомунікаційних систем, зокрема в умовах обмеженої смуги частот і високих вимог до якості зв'язку. У цій роботі розглянуто основні принципи субсмугового методу передавання інформації на основі власних векторів, проведено аналіз його ефективності та визначено основні переваги й недоліки у порівнянні з традиційними методами. Основна увага приділяється застосуванню цього методу в різних умовах експлуатації та його потенціалу для майбутніх досліджень і розробок у сфері зв'язку.

У дослідженні було використано п’ять каналів з різними характеристиками, включаючи різну кількість променів (від одного до п’яти променів) і посилення каналу зв’язку в децибелах. Крім того, було використано десять стандартних каналів, щоб імітувати різні типи місцевості з різними типами променів. Змодельовані канали відповідають специфікації 3GPP TS.45.005 v7.9.9 (2007-2).

Канал зв’язку передає послідовність біт інформаційного вектору розмірністю J. На вході реєструється N значень, а потім виконується перемноження на відому транспоновану матицю власних векторів.

Інформаційний вектор у вигляді нулів і одиниць передається каналом зв’язку Cost207RAx4, який використовується зі-каналом стандартної бібліотеки MATLAB.

Coc207RAx4 вектор, 4 промені представлено на рисунку 1.

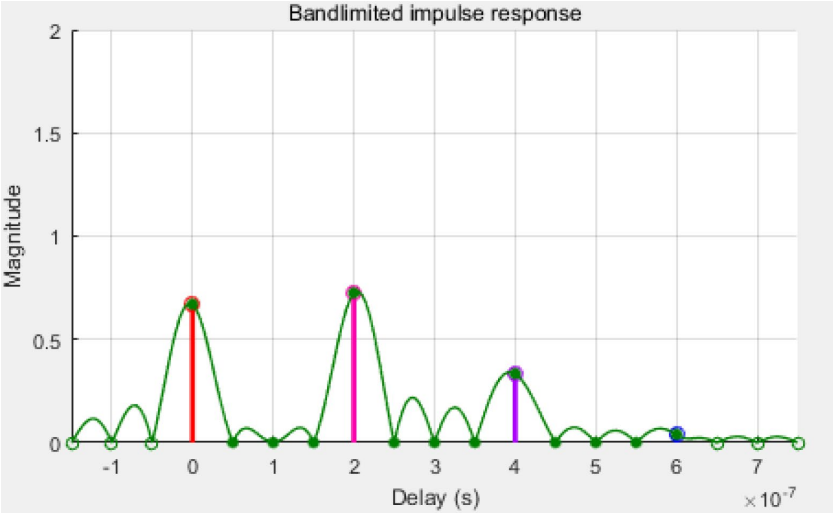
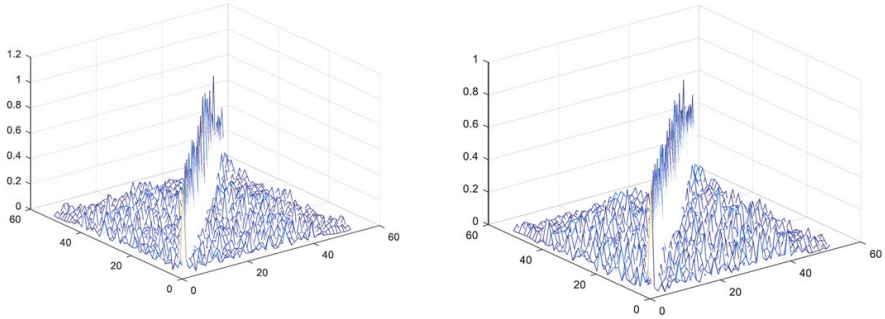


Рис. 1. Амплітуда і затримка променів поширення каналу cost207RAx4

а) **б)**



$P_{пом}$=51.5%

Рис. 2. Скалярний добуток власних векторів: а) до каналу б) після каналу

На приймальній стороні є N значень. Після цього проводиться перемноження на транспоновану матрицю власних векторів, яка вже відома. Це дозволяє відновити сигнал, використовуючи його властивості. Таблиця 1 містить скалярний добуток власних векторів. Рисунок 2 показує скалярний добуток власних векторів. У цьому прикладі ймовірність помилки становить 51,5%.

Таблиця 1

Скалярний добуток власних векторів

0,7482	0,1267	0,0530	0,0795	0,0190	0,1878	0,0778	0,0394	0,1569	0,0734	0,0975
0,1267	0,6668	0,1449	0,1075	0,1369	0,1744	0,0699	0,0378	0,0448	0,0451	0,0864
0,0530	0,1449	0,7251	0,0491	0,0692	0,1022	0,0572	0,0337	0,1020	0,0428	0,1532
0,0795	0,1075	0,0491	0,8482	0,0274	0,0694	0,0346	0,0666	0,0783	0,0620	0,0495
0,0190	0,1369	0,0692	0,0274	0,7096	0,0163	0,0660	0,0129	0,0609	0,0607	0,0354
0,1878	0,1744	0,1022	0,0694	0,0163	0,8453	0,0223	0,0928	0,0900	0,1266	0,1684
0,0778	0,0699	0,0572	0,0346	0,0660	0,0223	0,7253	0,0664	0,1029	0,0973	0,1191
0,0394	0,0378	0,0337	0,0666	0,0129	0,0928	0,0664	0,7379	0,1354	0,1106	0,0699
0,1569	0,0448	0,1020	0,0783	0,0609	0,0900	0,1029	0,1354	0,8450	0,0297	0,0244

Висновок. Сучасний світ вимагає високої швидкості та ефективності передавання інформації, що стимулює розвиток нових методів і технологій у галузі зв'язку. Одним із перспективних напрямків є субсмуговий метод передавання інформації на основі власних векторів. Цей підхід значно підвищує ефективність використання смуги пропускання і покращує стійкість до перешкод, що є критично важливим для сучасних систем зв'язку. Використання математичного апарату власних векторів для оптимізації процесів модуляції та демодуляції сигналів дозволяє зменшити рівень шумів і спотворень та забезпечити високу точність відновлення інформації.

Дослідження підтвердили, що субсмуговий метод відкриває нові можливості для розвитку телекомунікаційних систем, особливо в умовах обмеженої смуги частот і високих вимог до якості зв'язку. Проведений аналіз показав ефективність цього методу та його переваги над традиційними методами. Використання різних каналів зв'язку з різними характеристиками продемонструвало, що даний підхід є універсальним і може застосовуватися в різних умовах експлуатації. Зокрема, змодельовані канали відповідно до специфікації 3GPP TS.45.005 v7.9.9 (2007-2) підтвердили здатність методу забезпечувати високий рівень якості зв'язку.

Таким чином, субсмуговий метод передавання інформації на основі власних векторів має значний потенціал для майбутніх досліджень і розробок у сфері зв'язку, що дозволить подальше вдосконалення телекомунікаційних систем і задоволення зростаючих вимог ринку.

УДК 621.396.96:13

І.О. Василецький
І.П. Омельчук
Національний авіаційній університет, м. Київ

СТІЙКІСТЬ РЛС ДО ІМПУЛЬСНИХ ЗАВАД

Дослідження були спрямовані на підвищення завадо-захищеності первинних диспетчерських радіолокаційних станцій (РЛС). Згідно концепції розвитку CNS/ATM вони обов'язково входять до комплексу систем спостереження повітряного простору, і ефективність їх роботи напряму впливає на безпеку та регулярність польотів літаків цивільної та військової авіації.

Вочевидь, для виконання належних завдань необхідно, щоб РЛС була захищена від дії завад та забезпечувала високу імовірність виявлення цілей не нижче 0,9. Основна увага приділяється питанню придушення хаотичних – інакше несинхронних імпульсних завад. Їх вилучення на попередньому етапі є необхідним, щоб уникнути суттєвих збоїв при подальшій обробці радіолокаційної інформації. Імпульсні завади можуть бути віднесені до активних імітуючих завад, що можуть мати природнє або штучне походження.

Попередня просторова та поляризаційна селекція завад забезпечується безпосередньо вузькою діаграмою спрямованості антени РЛС та можливістю керування її поляризацією.

Частотна селекція – це функція радіоприймача, котрий повинен бути налаштований на спектр корисних сигналів. Але імпульсні завади мають широкий спектр, частина якого буде проходити через фільтри приймача. Тому необхідні додаткові заходи для їх вилучення. Ця проблема вирішується за допомогою часового методу компенсації.

Принцип цього методу полягає у наступному. Обробка здійснюється після детектування, тобто над відеосигналами. У різних періодах зондування імпульси, відбиті від цілі, залишаються на незмінному часовому інтервалі від імпульсів зондування РЛС, а положення імпульсів завад суттєво випадкове. Тому після схеми збігу імпульсів двох сусідніх зондувань будуть залишатися тільки корисні імпульси цілей.

Основною задачею технічної реалізації є створення каналу затримки квантованого відеосигналу точно на період повторення зондуючих імпульсів та їх компенсація.

На рис. 1 зображена схема подавлювача-компенсатора. До її складу входять: оперативний запам'ятовуючий пристрій (ОЗП), генератор адресів, схема генерації та схема управління і обробки.

Аналоговий відеосигнал надходить на схему обробки, де відбувається його квантування, перетворення в імпульси однакової амплітуди і полярності та прив'язка до просторових кілець дальності. Там же відбувається селекція і нормалізація за тривалістю імпульсів. Відеосигнали, що пройшли перевірку по амплітуді та тривалості, подаються на вхід ОЗП, який здійснює затримку сигналу на один період зондування, після чого сигнали піддаються відніманню в схемі обробки.

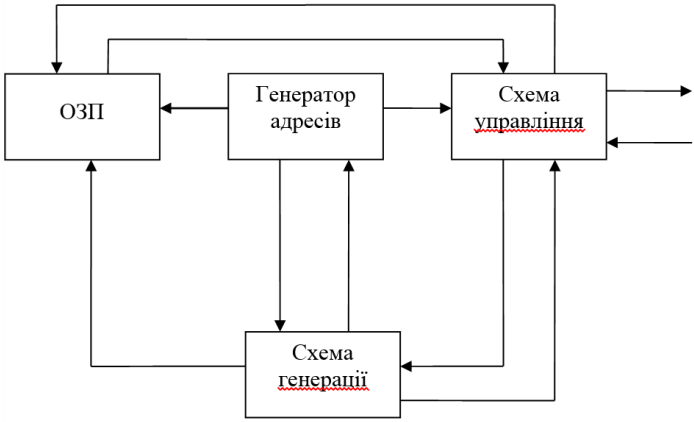


Рисунок 1 – Структурна схема придушувача імпульсних завад РЛС.

У запам'ятовуючому пристрої здійснюється збереження квантованих сигналів двох поточних суміжних розгорток РЛС по кожному кільцю дальності.

Генератор адресу працює як генератор, і як лічильник. Він видає імпульси управління до ОЗП, згідно запускаючих імпульсів РЛС, та виробляє тактові імпульси, що поділяють розгортку на кільця дальності. Генератор тактових імпульсів після кожного запускаючого імпульсу генерує послідовність прямокутних імпульсів з частотою 1 МГц, які подаються на генератор адресу. У генераторі тактових імпульсів також формується імпульс «запис - зчитування» з частотою 2 МГц.

Застосування принципу компенсації детектованих імпульсних сигналів у суміжних парах періодів зондування дозволить, практично, вилучити усі хаотичні імпульсні завади.

УДК 656.7

М.О. Вороненко
А.Г. Тараненко
Національний авіаційний університет, м. Київ

ІНФОРМАЦІЙНІ СИСТЕМИ ДЛЯ ПІДТРИМКИ ПОСЛУГ АВІАКОМПАНІЙ

Інформаційні системи відіграють ключову роль у сучасному світі, забезпечуючи ефективне управління та підтримку різних бізнес-процесів. У галузі авіації, де точність, оперативність і безпека є критичними факторами, інформаційні системи стають незамінними інструментами для забезпечення високого рівня обслуговування пасажирів та оптимізації операційної діяльності авіакомпаній.

Метою створення інформаційної системи для підтримки послуг авіакомпаній є покращення якості обслуговування пасажирів, підвищення ефективності внутрішніх процесів та забезпечення конкурентоспроможності авіакомпаній на ринку. Ця система має включати різноманітні функціональні можливості, що дозволяють оптимізувати управління розкладом рейсів, резервуванням квитків, обробкою багажу та іншими ключовими аспектами діяльності авіакомпаній.

На сьогодні найбільш поширеними системами GDS (Global Distribution Systems) є Amadeus, Travelport GDS (включає такі системи як Apollo, Galileo та Worldspan), Sabre, TameliaRES, Avantik PSS, Abacus, AccelAero, Axess, Internet Booking Engine, KIU, Mercator, Navitaire, Patheo, Radixx, akeflite, Travel Technology Interactive, WorldTicket Sell-More- Seats, Сирена та ін. Як альтернативу системам GDS розробники позиціонують Інтернет системи бронювання (Internet Distribution Systems, IDS) чи альтернативні системи бронювання (Alternative Distribution Systems, ADS), які з'явилися вкінці минулого сторіччя і мають цілу низку переваг над GDS системами.

Для прикладу, система обслуговування пасажирів Navitaire - це удосконалена система New Skies, яка була впроваджена у 2005 р. Navitaire надає технологічні послуги для авіаційної та залізничної галузей. Компанія зазвичай працює з лоукостерами та гібридними авіакомпаніями і є провідним постачальником систем обслуговування пасажирів на ринку лоукостерів. Станом на 2014 рік фірма обслуговувала 43% зі 100 найбільших лоукостерів та 47% з 30 найбільших лоукостерів за кількістю проданих місць на тиждень. Серед клієнтів - авіако-

мпанії Wizz Air, Jetstar, Spirit Airlines, Azul Brazilian Airlines, HK Express, і Volaris.

В системі запроваджено такі функції, як пошук низьких тарифів та бронювання між містами. Система забезпечує бронювання через Інтернет, колл-центри та через глобальні розподільчі системи (GDS), використовуючи безквиткову модель, а також уможливлюючи електронний продаж квитків. Вона також дозволяє інтегруватися з іншими туристичними послугами, такими як туристичне страхування та оренда автомобілів, а також укладати код-шерінгові угоди з іншими авіакомпаніями. Це дозволяє пасажирам легко та швидко оформлювати свої подорожі, а авіакомпаніям — ефективно керувати своїми продажами.

Технічні аспекти інформаційної системи також відіграють ключову роль. Вибір правильної архітектури (модульна, мікросервісна) та технологій (хмарні рішення, бази даних) є критично важливим для забезпечення гнучкості та масштабованості системи. Система повинна включати механізми захисту даних від несанкціонованого доступу та кібератак, забезпечуючи конфіденційність інформації про пасажирів. Крім того, система має бути надійною, забезпечувати безперервну роботу та мати можливість масштабування відповідно до зростаючих потреб авіакомпанії.

Використання інформаційних систем у сфері авіації надає значні переваги, зокрема покращення якості обслуговування пасажирів, підвищення ефективності операцій, скоротити час обробки операцій, зменшити кількість помилок та зменшення витрат. Зрештою, оптимізація процесів та зниження операційних витрат сприяє підвищенню рентабельності авіакомпаній. Тож загалом, інвестиції в інформаційні системи є важливим кроком для авіакомпаній, які прагнуть залишатися конкурентоспроможними та забезпечувати високий рівень обслуговування. Рекомендується ретельно планувати впровадження та експлуатацію таких систем, враховуючи специфіку кожної авіакомпанії та вимоги ринку.

УДК 681.5 (004)

O.V. Hryshko
National Aviation University, Kyiv

INFORMATION TECHNOLOGIES OF MULTIMEDIA IN MODERN SOCIETY

Multimedia technologies are one of the most promising and popular areas of computer science. They are aimed at creating a product containing "collections of images, texts and data accompanied by sound, video, animation and other visual effects (Simulation), including an interactive interface and other control mechanisms".

It is hard to imagine modern life without multimedia. Tens of thousands of people use multimedia technologies every day. Nowadays, it is almost impossible to overestimate the importance of these technologies. This is due to the fact that multimedia technologies are increasingly penetrating all spheres of life. The main advantage of their use is that they open up new opportunities for us that we could only dream of before. The development of multimedia has been going on for several decades, and it is impossible to predict what the same interactive whiteboard will look like and whether it will exist at all or be replaced by something more advanced.

Basic tools for creating multimedia projects may include one or more tools for editing text, images, sounds, and video sequences. The tool set of multimedia tools is quite wide and may include hardware and software solutions of information technologies.

Software solutions for multimedia tools can be divided into the following main groups as a graphic editor, video editors, multimedia players, audio editors, computer games.

Multimedia finds its application in various fields, including advertising, art, production, entertainment, development, medicine, mathematics, business, and scientific research.

Multimedia technologies are needed all over the world, they dominate through various visual technologies, in which it is necessary to select information from the surrounding reality, analyzing it against the background of one's experience, knowledge, interpreting it from the angle of suitability, and using it to enrich and develop the educational component of the individual.

Further development and improvement of multimedia technologies is obvious.

Experimental remote surgical operations are being conducted on a regular basis. NASA, with the cooperation of specialists from the University of Nebraska, will train astronauts so that they can use robotic surgeons in orbit. At the same time, the robot's actions will be controlled by a team of experienced doctors who will be thousands of kilometers away from the patient.

The constant integration of multimedia into educational processes is undeniable and obvious. No one will be surprised by multimedia foreign language courses anymore. Net-worked academies using multimedia online courses are widely used. A striking example is the CISCO network academy, which has branches in many countries around the world. The educational process consists of remote study of materials, and even certain laboratory work can be done remotely with the help of virtual device programs that simulate the behavior of real technical means.

The advertising industry is constantly influenced by the development of multimedia, adopting the latest solutions such as light boxes, bank terminals, etc.

Multimedia technologies are not only about education, science, research, entertainment, games, art and advertising, but also about saving lives.

The integration of artificial intelligence in multimedia technologies is shaping the future of digital content creation and consumption. As the capabilities of AI continue to evolve, we can expect to see even more innovative developments in this field, with AI driving the next wave of advancements in multimedia technologies.

As we stand on the cusp of 2024, the future of multimedia is a canvas painted with the brushstrokes of innovation, creativity, and technological prowess. From spatial computing to emotionally intelligent AI, these emerging trends are set to redefine the way we perceive and engage with multimedia content. As audiences, creators, and technologies converge, the journey into the multimedia frontier promises a thrilling ride into uncharted territory, where the boundaries of imagination are continually expanded.

УДК 043.2

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

СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЙНОГО КОНТЕНТУ

У сучасному світі інформаційні технології та телекомунікаційні мережі є невід'ємною частиною нашого повсякденного життя, забезпечуючи швидкий та надійний зв'язок і передачу даних. Однак, стрімкий розвиток цих технологій супроводжується зростанням загроз у сфері інформаційної безпеки.

Конфіденційність, цілісність та автентичність даних стають все більш вразливими до атак зловмисників, що вимагає нових підходів до їх захисту. Стеганографія, яка дозволяє приховати сам факт передачі секретної інформації, представляє собою перспективний метод забезпечення безпеки інформаційного контенту. Використання цифрових водяних знаків як стеганографічного інструменту дозволяє забезпечити додатковий рівень захисту даних у телекомунікаційних мережах.

У світі цифрових технологій інтелектуальна власність зустрічається з рядом проблем захисту від копіювання. Це одна з основних проблем, коли контент використовується без дозволу правовласника. Розповсюджене копіювання ліцензованого контенту може призвести до широкого розповсюдження піратських копій, що призводить до падіння якості та прибутковості контенту, а також наносить фінансові збитки авторам та власникам прав.

Піратство в інтернеті є розповсюдженою проблемою. Нелегальні сайти та сервіси забезпечують доступ до піратського контенту, що сильно впливає на прибутковість та легальне його розповсюдження.

Інтелектуальна власність піддається ризику незаконного використання, коли користувачі використовують контент, що порушує авторське право без відповідних ліцензій або дозволів.

Стеганографія відіграє важливу роль у захисті інтелектуальної власності шляхом приховування важливої інформації так щоб сторонній спостерігач не помітив її наявності.

Таким чином можна вбудувати інформацію про право власність у контент без зміни його зовнішнього вигляду. Застосування стенографії дозволяє надати додатковий рівень захисту, адже навіть прихова-

ної інформації у випадку несанкціонованого доступу до контенту, ця інформація залишається непомітною для незаконного користувача.

Також одним ефективним методом захисту інтелектуальної власності є використання цифрових водяних знаків. Ця технологія дозволяє вбудовувати унікальну ідентифікаційну інформацію, логотип, назву, ім'я безпосередньо в контент. Відмінність цифрових водяних знаків від стеганографії полягає в тому, що вони не тільки приховують інформацію, але і надають можливість однозначно ідентифікувати власника або автора контенту. Зазвичай водяний знак накрадається поверх контенту та може перекривати якусь його частину.

У світі високих технологій, де інформація швидко перетворюється на валюту та постійно змінюється, захист інтелектуальної власності став критичною проблемою.

Стеганографія та цифрові водяні знаки можна використовувати як ефективні інструменти безпеки для запобігання несанкціонованому доступу до конфіденційних даних і для визначення прав власників вмісту.

Ці технології допомагають підтримувати цілісність і автентичність інформації та захищати творчість та інтелектуальну власність. Використання скорочених і цифрових водяних знаків у телекомунікаційних мережах відображає здатність до інновацій та визначення нових стандартів безпеки в епоху цифрових технологій.

УДК 629.053 (043.2)

Я.І. Дорошенко
Національний авіаційний університет, м. Київ

ДОСЛІДЖЕННЯ РОБОТИ АВТОМОБІЛЬНОГО АВТОПІЛОТА НА ОСНОВІ ВИКОРИСТАННЯ ШІ

У сучасному світі, де технології стрімко розвиваються, штучний інтелект трансформує багато аспектів життя, особливо у автомобільній промисловості з впровадженням автопілотів. Ці системи, що використовують датчики та алгоритми машинного навчання, обіцяють і головне вже впроваджують підвищення безпеки на дорогах, роблять поїздки комфортнішими та оптимізують транспортні потоки. Автопілоти здатні адаптуватися до різноманітних дорожніх ситуацій, передбачати дії інших учасників руху та зменшувати затори, що сприяє економії часу та покращенню екологічного стану. Проте, існують виклики, такі як забезпечення надійності та питання того, хто буде нести відповідальність за дії безпілотних авто, які потребують подальших досліджень та розробок для повної інтеграції автопілотів у транспортну систему.

Автопілот – це складна система, яка інтегрує сенсори, потужні комп'ютери та передові алгоритми штучного інтелекту, здатний самостійно керувати автомобілем, покращити ефективність транспортної системи, зменшуючи кількість ДТП та викиди шкідливих речовин. Ця інноваційна технологія, що колись була лише фантастичною ідеєю, сьогодні стає реальністю, яка стрімко наближається завдяки постійному розвитку та вдосконаленню. Автопілоти класифікуються за рівнями автономності від 0 (без автоматизації) до 5 (повна автоматизація). Кожен рівень характеризується ступенем самостійності системи у керуванні автомобілем. Наразі більшість комерційно доступних автопілотів знаходяться на рівні 2 або 3, забезпечуючи часткову або умовну автоматизацію. Проте, компанії активно працюють над розробкою та впровадженням автопілотів вищих рівнів, які зможуть повністю взяти на себе керування автомобілем у будь-яких умовах. Однією, мабуть найголовнішою, з ключових переваг автопілотів є підвищення безпеки дорожнього руху. За статистикою, більшість аварій спричинені людським фактором, таким як помилки водіїв, втома, неуважність та вплив алкоголю чи наркотиків. Автопілоти, не схильні до цих недоліків, здатні суттєво знизити ризик ДТП та врятувати тисячі

життів. Крім того, вони можуть зробити поїздки зручнішими, звільняючи водіїв від рутинних завдань та дозволяючи їм зосередитися на інших справах чи просто відпочити під час подорожі. Завдяки здатності підтримувати оптимальну швидкість та дистанцію, автопілоти можуть зменшити кількість заторів та покращення екологічного стану навколишнього середовища. Це особливо актуально в умовах зростаючої урбанізації та збільшення кількості автомобілів на дорогах. Проте, незважаючи на всі переваги, розвиток та впровадження автопілотів пов'язані з низкою викликів. Одним з головних є забезпечення надійності та безпеки систем, особливо в складних дорожніх умовах, таких як негода, погане освітлення чи непередбачувана поведінка інших учасників руху. Іншим важливим аспектом є правове регулювання використання автопілотів та вирішення етичних питань, пов'язаних з відповідальністю за дії автономних транспортних засобів у разі аварії. Незважаючи на всі сьогоденні проблеми, зв’язані з автопілотами, їх перспективи розвитку вражають. Від безпілотних таксі та громадського транспорту до інтеграції з розумними містами, автопілоти відкривають перед нами нову еру транспорту, яка обіцяє бути безпечнішою для кожного, як водія з пасажирами так і пішоходів, комфортнішою та безпечнішою для навколишнього середовища. Розвиток цієї технології вимагає подальшого вдосконалення алгоритмів штучного інтелекту, розробки нових сенсорів, створення відповідної інфраструктури та вирішення правових та етичних питань. Проте, потенційні переваги автопілотів настільки значні, що їх впровадження є лише питанням часу.

На практиці було успішно розроблено та реалізовано систему виявлення автомобілів на відео в режимі реального часу. Для цього було використано мову програмування Python в середовищі Jupyter Notebook, бібліотеку комп'ютерного зору OpenCV та алгоритм машинного навчання "каскад Хаара". Розроблена система виявлення автомобілів на відео в режимі реального часу є важливим кроком у розвитку технологій автономного керування та інтелектуальних транспортних систем. Вона демонструє практичну цінність штучного інтелекту та машинного навчання для вирішення реальних завдань у сфері транспорту. Завдяки своїй ефективності та універсальності, ця система може знайти застосування в різних галузях, сприяючи підвищенню безпеки та ефективності дорожнього руху.

УДК 004.8:621.391 (043.2)

Н.Д. Єгоров
Національний авіаційний університет, м. Київ

МЕТОД ВИЯВЛЕННЯ ДЕТЕРМІНОВАНОГО СИГНАЛУ НА ФОНІ ШУМУ НА ОСНОВІ ВИКОРИСТАННЯ НЕЙРОННОЇ МЕРЕЖІ

Тема актуальна через зростаючий інтерес до штучного інтелекту та нейронних мереж у різних сферах. Нейронні мережі стали потужним інструментом для обробки і аналізу даних, що потенційно робить їх ефективними для вирішення завдань виявлення сигналів на фоні шуму, зокрема у таких галузях як: радіолокація, телекомунікації та радіозв'язок.

Об'єктом дослідження є нейронна мережа, як інструмент виявлення детермінованих сигналів. Предметом дослідження є вплив рівня шуму на ефективність виявлення детермінованих сигналів. Мета роботи – розробити та експериментально дослідити метод виявлення детермінованих сигналів на фоні шуму з використанням нейронної мережі.

Для реалізації мети, розроблено блок-схему задач експерименту.

Задача виявлення сигналів формулюється як задача класифікації, де на вхід нейронної мережі подаються відліки сигналів, а на виході отримується ймовірність належності сигналу до одного з класів (відсутність сигналу або наявність одного з детермінованих сигналів).

Приймаючи категоріальні рішення, можливі помилки: α – хибна гіпотеза про наявність сигналу, і β – хибна гіпотеза про відсутність сигналу. При виявленні одного детермінованого сигналу можливі чотири ситуації: вірна гіпотеза про відсутність сигналу (H_{00}), хибна гіпотеза про наявність сигналу (H_{01}), хибна гіпотеза про відсутність сигналу (H_{10}), вірна гіпотеза про наявність сигналу (H_{11}). При виявленні декількох сигналів додається ще один вид помилки – хибна класифікація виявленого сигналу. Загальна ефективність нейронної мережі характеризується матрицею неточностей.

Змодельована у експерименті нейронна мережа є багатошаровим персептроном, що складається з трьох шарів (вхідний, прихований, вихідний). Розмір вхідного шару залежить від розміру сигналу (1024). Розмір прихованого у ході експерименту змінювався поки не залишився на оптимальному «швидкість/точність» значенні як чверть від вхідного (256). Розмір вихідного залежить від кількості сигналів, які повинні виявлятися (4).

Для прихованого шару використана функція активації – sigmoid, а для вихідного softmax. Функція sigmoid є диференційованою та неперервною, що робить її підходящою для використання у градієнтних методах навчання;

також у процесі проведення експерименту з даною функцією параметри точності нейронної мережі були найкращими.

Функція softmax обрана через її здатність нормалізувати вихідні значення вектору відповідей у вигляді ймовірностей. Це особливо важливо для багатокласової класифікації, де кожен клас має власну ймовірність належності. Вона дозволяє зручно порівнювати ці ймовірності та приймати рішення щодо класифікації вхідних даних.

Для експерименту обрано функцію втрат Categorical Cross-Entropy Loss (CCEL) через її здатність точно визначити, наскільки добре модель класифікує вхідні дані при багатокласовій класифікації. Вона порівнює прогнозовані ймовірності з вірними класифікаційними мітками у форматі «one-hot». CCEL використовує логарифмічні обчислення, і тому надає більш виразний показник втрати при великих відхиленнях від очікуваних значень, і малий показник при невеликих.

З методів оптимізації, які можуть використовуватися для коригуванні параметрів при backpropagation (а це методи градієнтного спуску), обрано стохастичний градієнтний спуск (SGD). Він вимагає менші обчислювальні потужності обладнання, але при цьому може довше збігатися. Також при використанні SGD, точність була більшою ніж при використанні наприклад Adam, хоча кількість епох при використанні Adam була набагато меншою.

Загалом навчання нейронної мережі зайняло 144 епохи. Точність класифікації сигналів з тестового датасету із різним рівнем шуму (приблизно від -35дБ до 10дБ) склала 65.1%. Отримана матриця неточностей зображена на рис. 1.

Графіки історії навчання відображають, що у перших епохах навчання присутнє швидке зменшення значення функції втрат і збільшення точності моделі, оскільки параметри оновлюються в напрямку, який зменшує втрати та покращує точність передбачень. Однак, з часом, цей процес сповільнюється, оскільки модель наближається до оптимальних значень параметрів. Також це говорить про оптимальний підбір параметрів моделі НМ, що забезпечив ефективне навчання, та не допустив перенавчання.

Отримані при проведенні експерименту результати, свідчать про високу ефективність використаної методики виявлення детермінованого сигналу на фоні шуму при значеннях відношення сигнал/шум не нижче -20дБ, про це свідчить приклад графіку характеристики виявлення одного з сигналів (рис. 2). Він має таку форму через те, що будувався на статистичних даних.

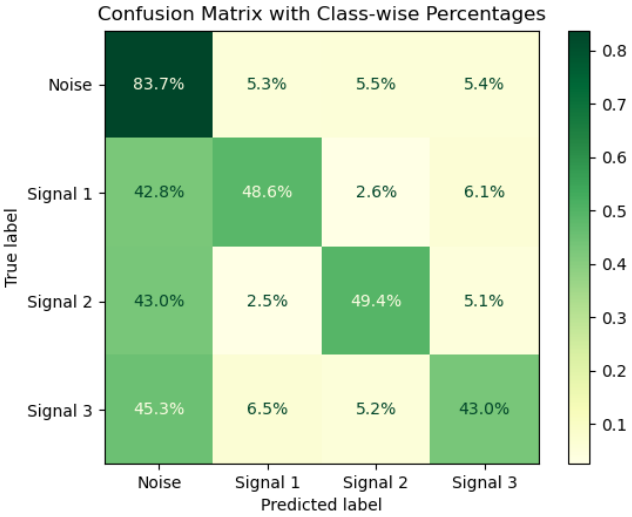


Рис. 1 Матриця неточностей класифікації тестових даних

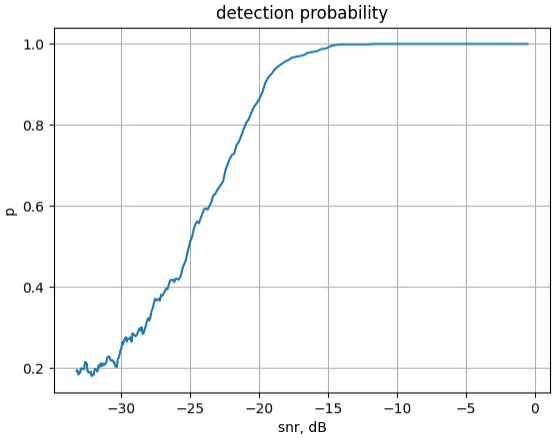


Рис. 2 Характеристика виявлення першого сигналу

Нейронна мережа може виявляти більше одного детермінованого сигналу, що робить цей метод перспективним. З удосконаленням обладнання на якому проводиться навчання нейронної мережі, можливе збільшення кількості параметрів моделі та подальше покращення її точності при малому відношенні сигнал/шум. Таким чином, дане дослідження має потенціал для подальшого розвитку та покращення результатів.

УДК 004.7 (043)

Д.М. Іщенко, Ю.В. Петрова
Національний авіаційний університет, м. Київ

МОДЕРНІЗАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Модернізація інформаційно-комунікаційної системи підприємства є важливим кроком у підвищенні ефективності роботи, конкурентоспроможності та інноваційного розвитку організації. В сучасних умовах глобалізації та швидкого розвитку технологій підприємства стикаються з необхідністю вдосконалення своїх інформаційно-комунікаційних систем, щоб забезпечити більш ефективне управління ресурсами, покращення якості обслуговування клієнтів та оптимізацію внутрішніх процесів.

Інформаційно-комунікаційні технології відіграють ключову роль у сучасному середовищі, оскільки вони забезпечують швидкий доступ до інформації, сприяють автоматизації процесів та полегшують комунікацію як всередині підприємства, так і з зовнішніми партнерами. В умовах зростаючої конкуренції, своєчасна модернізація цих систем дозволяє підприємствам зберігати свою конкурентну перевагу, адаптуватися до нових вимог та зменшувати витрати на управління і захист інформації.

Стара система може бути неефективною через застаріле обладнання, повільну обробку даних, відсутність інтеграції з новими технологіями та низьку рівень безпеки. Це може призводити до втрат часу, ресурсів і зниження якості обслуговування клієнтів.

Впровадження нових технологій та оновлення існуючої інфраструктури допомагає вирішити ці проблеми, забезпечуючи безперебійну роботу підприємства та підвищуючи його продуктивність. Важливою складовою модернізації є також забезпечення захисту даних та інформаційної безпеки, що стає більш актуальним у зв’язку зі зростанням кіберзагроз.

Модернізація інформаційно-комунікаційної системи підприємства включає кілька ключових етапів та завдань. Першим кроком є детальний аналіз існуючої інформаційно-комунікаційної системи, визначення її сильних і слабких сторін, виявлення основних проблем та недоліків.

Це дозволяє сформувати чітке розуміння того, які аспекти потребують модернізації. Наступним етапом є визначення основних цілей

модернізації та вимог до нової системи. Це можуть бути підвищення продуктивності, зменшення витрат, покращення безпеки даних, інтеграція з новими технологіями тощо.

На основі визначених цілей і вимог здійснюється вибір відповідних технологічних рішень та програмного забезпечення. Важливо враховувати сучасні тенденції в іт-сфері та обирати ті технології, які забезпечать максимальну ефективність та гнучкість. На цьому етапі розробляється детальний план впровадження нової інформаційно-комунікаційної системи. План включає аналіз старого обладнання терміни виконання, бюджет, необхідні ресурси та етапи впровадження.

Реалізація проекту модернізації включає встановлення нового обладнання та програмного забезпечення, міграцію даних, налаштування системи та навчання персоналу. Важливо забезпечити безперервність процесів під час впровадження.

Після впровадження системи необхідно провести її тестування для виявлення та усунення можливих помилок і недоліків. На основі результатів тестування здійснюється оптимізація системи для забезпечення її максимальної ефективності. Завершальний етап передбачає оцінку результатів модернізації. Аналізуються досягнуті цілі, ефективність та вплив нової системи на роботу підприємства. на основі отриманих даних робляться висновки про доцільність подальших вдосконалень.

У результаті проведеної модернізації інформаційно-комунікаційної системи підприємства було досягнуто значного підвищення ефективності роботи, зниження витрат та покращення якості опрацювання інформації та обслуговування клієнтів.

Нові технологічні рішення забезпечили кращу інтеграцію, швидке реагування на зміни в середовищі та підвищення безпеки даних. Модернізована система стала надійним інструментом для подальшого розвитку підприємства та його успішного функціонування в умовах сучасного середовища.

УДК 004.9
І-74

А.В. Капелюшна, О.Г. Саітгареєва
Криворізький фаховий коледж
Національного авіаційного університету,
м. Кривий Ріг

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ: СУЧАСНІ ТЕНДЕНЦІЇ

Сучасні технології щодня стають більш популярними, використовуються більшим числом людей, і ці тенденції набирають все більших обертів.

Поняття «інформаційні технології» (ІТ) - багатогранне та різнобічне. Наприклад, М Монахов висвітлює поняття «інформаційні технології», як «процес збору, передачі, зберігання і обробки інформації у всіх можливих формах: текстовій, графічній, візуальній і усній» [1, с. 179].

Швидке збільшення новітніх інформаційних технологій в повсякденному житті людей викликало деякі наступні тенденції:

1. *Хмарні послуги, сервіси і новітні технології*. Цей ідеальний задум з'явився, коли американський вчений Джон Маккарті розповів свою пропозицію [2, с. 91]. Хмарні технології (англ. cloud technologies) – це «кардинально новий сервіс, який дозволяє віддалено використовувати засоби обробки і зберігання даних». [3, с. 4]. Використання цих новітніх технологій звільняє від залежності від робочого місця і завдяки цьому методу можна розробити нові можливості на ринку праці.
2. *«Інформаційна екологія людини».* Базується на «складних взаємовідносинах між людьми та технологіями під час використання інформації у суспільстві та організаціях» [4, с. 33]. Водночас з посиленням джерел інформації актуалізується питання забруднення інформаційного середовища, втома людини від надмірного інформаційного потоку [2, с. 93].
3. *Інформаційна безпека* – це «невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку та здійсненні національної інформаційної політики відповідно до чинних правових актів країни, міжнародного права». [5, с. 14].

4. *Інформаційна свідомість.* Створено концептуальну парадигму інформаційної свідомості. Доктор Джо Діспенза - один з перших почав досліджувати вплив свідомості на реальність. [2, с. 92].
5. *Штучний інтелект*. За штучним інтелектом майбутнє і можна окреслити її природу як «розділ комп'ютерної лінгвістики та інформатики, що формалізує завдання, які нагадують справи, що виконує людина» [2, с. 92].

Інформаційні технології тісно ввійшли в життя людей, набираючи обертів у повсякденному використанні. Тенденції розвитку сучасного технологічного простору демонструють і підкреслюють вагомий внесок технологій в поліпшення людського життя.

Література:

1. Романишина О. Огляд інформаційних технологій та засобів їх реалізації у вищих навчальних закладах. *Науковий вісник Ужгородського національного університету. Серія : Педагогіка. Соціальна робота.* 2013. Вип. 29. С. 179-183.
2. Мар'яненко Г.І. Інформаційно-технологічний простір сучасного світу: перспектива високотехнологічного майбутнього. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління.* 2018. № 29 (68). С. 90-95.
3. Вакалюк Т.А. Хмарні технології в освіті. Навчально-методичний посібник для студентів фізико-математичного факультету. Житомир: ЖДУ, 2016. 72 с.
4. Сердюк І.А. Організаційні засади публічного управління інформаційною безпекою суспільства в умовах загроз ментальному здоров'ю. Дисертація. Київ: 2023. 256 с. URL : https://maup.com.ua/assets/files/dis/serdyuk/serdyuk-disertaciya.pdf (дата звернення: 30.06.2024).
5. Федорова Н.Є і Смєсова В.Л. 2020. Інформаційна безпека та шляхи її забезпечення на етапі інформаційно-технологічної революції. *Причорноморські економічні студії.* 2020. № 57. С. 13-16.

УДК 621.397-047.26(043.2)

Д.Ю. Коваленко
Національний авіаційний університет, м. Київ

СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ ВИРОБНИЧОГО ПІДПРИЄМСТВА

Головна мета використання систем відеоспостереження полягає в підвищенні рівня безпеки. Основною функцією таких систем є нагляд за певними об'єктами або суб'єктами, а також виявлення подій, які трапляються на місці спостереження. Візуальний контроль є ефективним засобом здійснення контролю над територією і дозволяє детально розглядати різні ситуації з різних точок зору.

На сьогоднішній день системи відеоспостереження відіграють важливу роль у багатьох сферах людської діяльності. Вони є невід'ємною частиною організацій і підприємств, забезпечуючи їх безпеку. Присутність відеокамер надає впевненість власникам приватних будинків і магазинів, але також викликає страх перед можливістю потрапити до рук злочинців. Навіть у випадку вчинення злочину записи з камер можуть стати корисними для слідства та упіймання злочинців.

Потреба у забезпеченні безпеки власності та сім'ї спонукає до використання передових систем безпеки. Однак використання таких систем не обмежується лише сферою безпеки. Інтеграція відбувається і в інших галузях, де розвивається потреба в централізованих системах управління процесами і людьми.

Розвиваючи цю галузь, системи відеоспостереження знайшли своє застосування в медицині для нагляду за пацієнтами у важких станах. Також їх використовують у сфері дорожнього руху для фіксації порушень та розпізнавання автомобільних номерів. Крім того, вони можуть бути корисними для запобігання шахрайства на іспитах чи вступних тестах.

Слово "відеоспостереження" стало неабиякою складовою нашого словника ще у минулому столітті, і його значення лише зростає і у наш час. Сьогодні майже неможливо знайти організацію, завод або магазин, де б не було камер відеоспостереження. Крім того, в

сучасному світі системи відеоспостереження активно входять і в приватне життя. Тож для чого саме потрібне відеоспостереження?

По-перше, воно стало невід'ємною складовою сучасних систем безпеки. З розвитком суспільства зростає і рівень злочинності. Люди все частіше прагнуть захистити себе від небажаних вторгнень і посягань на їхнє життя або майно. Без камер відеоспостереження важко уявити собі надійну систему безпеки.

Зовнішні камери відеоспостереження дозволяють охороняти периметр і територію, прилеглу до об'єкта: будь то склад, завод, магазин чи приватне володіння. Сучасні камери відеоспостереження можуть виявляти і навіть розпізнавати людину на велику відстань, а інфрачервоне підсвічування, що використовується у більшості вуличних відеокамер, дозволяє бачити навколишнє середовище навіть у повній темряві.

За допомогою внутрішніх відеокамер керівник підприємства може стежити за ходом роботи в офісі або цеху, навіть з будь-якої точки планети через систему відеоспостереження через Інтернет. Сучасні IP-камери відеоспостереження забезпечують можливість аудіозв'язку між об'єктом спостереження та оператором, спрощуючи процес керівництва персоналом.

Відеоспостереження стало не лише різноманітною складовою нашого словника, але й невід'ємною частиною нашого повсякденного життя. Відеокамери, монітори та відеореєстратори стали невід'ємними помічниками в багатьох сферах життя. Ця стаття допоможе вам прийняти позитивне рішення щодо встановлення системи відеоспостереження у вашому підприємстві чи офісі.

УДК 004.453 (043.2)

Т.В. Корнієнко
Національний авіаційний університет, м. Київ

СИСТЕМА РОСПІЗНАВАННЯ ЗВУКОВИХ СИГНАЛІВ НА ОСНОВІ ВИКОРИСТАННЯ ШІ

Здатність класифікувати різні звуки має критичне значення для різних галузей, особливо безпеки, телекомунікацій та сфер громадського контролю. Розпізнавання звукових сингалів за допомогою нейромереж дозволяє ефективно використовувати людський ресурс, надаючи можливість та пришвидшити процес прийняття рішень.

Сучасні системи, що використовують штучний інтелект (ШІ), надають можливість адаптації під різні завдання, що дозволяє враховувати різні особливості конкретних умов застосування змінюючи та доповнюючи вже існуючі рішення.

Універсальність та ефективність таких систем обґрунтовує необхідність дослідження даної теми, особливо зараз, коли відбувається якісний перехід сфери систем прийняття рішень на новий рівень, де рішення приймає високоточна модель.

Метою роботи є дослідження можливостей використання нейронних мереж для ефективної класифікації звукових сигналів що характерні для систем оборони та безпеки.

Для досягнення мети дослідження було виконано ряд завдань, що включають побудову нейронної мережі для класифікації звукових сигналів на основі штучного інтелекту, аналіз отриманих метрик та побудова репрезентативних графіків. Практична частина роботи спрямована на створення моделі нейронної мережі, яка здатна розпізнавати звуки дронів, пострілів та шуму.

Об’єктом дослідження є процес класифікації звукових сигналів. Предметом дослідження є методи та модель нейронної мережі, що застосовуються для класифікації звукових сигналів.

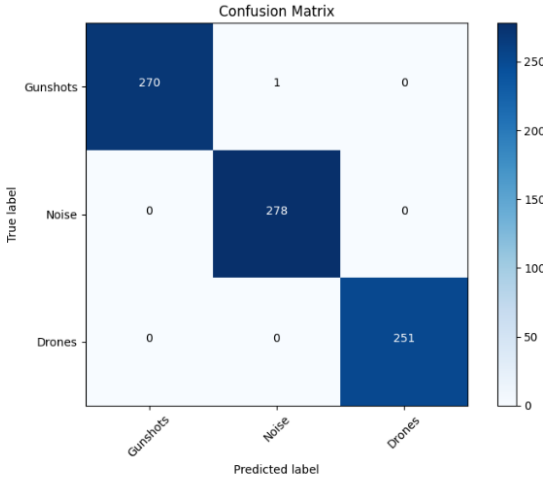
Методи досліджень включають аналітичні методи та математичні абстракції для теоретичного вивчення нейронних мереж, а також експериментальні підходи для побудови та тестування нейромережі, що виконує класифікацію звукових сигналів.

Практичне значення отриманих результатів. Отримані результати можуть бути використані для розробки систем моніторингу звукових сигналів у реальному часі, що знайде застосування в багатьох галу-

зях, включаючи безпеку та промисловість. Результати досліджень можуть бути впроваджені у системи, що виявляють незвичайні звуки, такі як вибухи або крики, з великою варіативністю класів допомагаючи вчасно реагувати на небезпеку або аварійні ситуації.

В роботі обирається мова програмування та бібліотеки обробки та візуалізації аудіоданих. Підготовлюються набори даних класів пострілу, шуму та дронів. Аналізуються та графічно зображаються середні спектрограми оброблюємих звуків. Далі розглядаються дві типи мереж та на основі даних експериментів та обирається найліпший варіант типу мережі. Цим типом мережі є ргорткова нейронна мережі (CNN), що побудована на основі згорткових шарів (Conv2D) і повнозв'язних шарів (Dense).

Розглядаються представленість класів в наборах навчань. Отриманим з навчань мережі результати надається характеристика. Далі надано матрицю плутанини найкращого типу мережі, що розглядається в роботі.



Отримані результати показують високу ефективність обраної архітектури нейромережі і способу обробки та трансформації даних для вирішення поставленого завдання.

УДК 004.8:621.391 (043.2)

О.В Кошуба
Національний авіаційний університет, м. Київ

СИСТЕМА БЕЗПЕКИ ВИРОБНИЧОГО ПІДПРИЄМСТВА

Сучасні системи безпеки та охорони використовують різноманітні методи та засоби для захисту життя, здоров'я та майна. Електронні пристрої та сенсорні технології дозволяють виявляти порушення безпеки на ранніх стадіях.

Системи контролю та управління доступом (СКУД) обмежують доступ до території або об'єкта. Відеоспостереження забезпечує візуальний контроль. Для ефективної роботи системи безпеки важливо врахувати всі вимоги та характеристики, що відповідають завданням охорони. Системи безпеки постійно вдосконалюються, використовуючи новітні технології, такі як штучний інтелект, машинне навчання та блокчейн, для підвищення ефективності та надійності. Системи контролю доступу інтегрують новітні технології, такі як бездротові технології та інтеграція з іншими системами безпеки, для створення єдиної інтегрованої системи безпеки та управління будівлями.

Розвиваються нові методи аутентифікації та ідентифікації користувачів, такі як біометричні технології. Розробляються нові стандарти та протоколи для систем контролю доступу, що забезпечують більшу сумісність та інтероперабельність. Захист систем безпеки підприємства включає комплекс організаційних та технічних заходів для виявлення і протидії різноманітним загрозам. Важливо забезпечити надійний захист ресурсів підприємства.

Апаратні компоненти використовуються в комплексних системах безпеки та пожежної безпеки для захисту об’єктів і забезпечення протипожежного захисту. Радіоелектронні системи безпеки (РЕСБ) є частиною загальної системи безпеки об'єкта, яка спрямована на виявлення, протидію та ліквідацію різноманітних загроз. Охоронні системи включають систему сигналізації, відеоспостереження, контролю доступу, безпекового освітлення, резервні джерела живлення та засоби зв'язку.

Шлейф сигналізації (ШС) забезпечує зв'язок між сповіщувачами та приймально-контрольним приладом (ППК) у системі охоронної сигналізації (СОС). Методи контролю шлейфу сигналізації дозволяють виявляти проблеми в шлейфі. Системи відеоспостереження

забезпечують безпеку об'єктів. Система надзвичайного оповіщення та керування евакуацією використовує мережу динаміків та світлових індикаторів для керування евакуацією людей.

Системи контролю доступу (СКУД) контролюють доступ до приміщень або територій, використовуючи різні методи ідентифікації. Вони можуть бути автономними, централізованими (мережевими) та універсальними. Електропостачання для СКУД повинне бути надійним та мати резервне джерело живлення.

Система охоронної сигналізації складається з трьох основних частин: сповіщувачів, системи збору, обробки, відображення та документування інформації (СЗОД) і виконавчих пристроїв. Сповіщувач – це пристрій, який автоматично виявляє порушника і генерує сигнал із заданими параметрами під час вторгнення порушника в зону дії пристрою. СЗОД – це сукупність апаратно-програмних засобів, призначених для збору, обробки, реєстрації, передачі та подання оператору даних від сповіщувачів. Вона також використовується для контролю стану та працездатності сповіщувачів, каналів передачі, складових частин та виконавчих пристроїв. СЗОД керує виконавчими пристроями та надсилає інформаційні сигнали на інші системи безпеки.

Функція системи виявлення полягає в виявленні несанкціонованого доступу до захищеної зони. Ця система складається з двох підсистем, системи виявлення вторгнення з використанням лазера та системи управління.

Ці дві підсистеми синхронізуються разом, щоб отримати найкращі результати виявлення. Чотири системи виявлення вторгнення з використанням лазера синхронізуються з системою управління таким чином, що процес виявлення стає більш ефективним. Система безпеки використовує чотири пари лазерних передавачів та приймачів для створення сітки невидимих променів на відстані 0,5 м один від одного. При перетині будь-якого променя системою управління реєструється вторгнення.

УДК 004.092 (043.2)

В. Т. Крамаренко
Національний авіаційний університет, м. Київ

СТВОРЕННЯ РОБОЧОЇ ІМІТАЦІЙНОЇ МОДЕЛІ САМОПОДІБНОГО МУЛЬТИМЕДІЙНОГО ТРАФІКУ В СЕРЕДОВИЩІ NETWORK SIMULATOR 2

На даний момент мережі на стільки сильно зайняли місце у повсякденні кожної людини на різних її рівнях, що вони мають забезпечувати передачу великої кількості різних швидкісних пакетів між клієнтами по всьому світу в мережі інтернет. Багато різних експериментальних досліджень по всьому світу показують, що потоки в сучасних мережах не є найпростішими, мають значну післядію та самоподібність. Необхідність забезпечення мережевими процесорами високої якості обслуговування різних категорій мережевих додатків, облік періодично виникаючих затримок у передачі даних та втрати пакетів при недостатній продуктивності та обмежених ресурсах пам'яті роблять вивчення властивостей самоподібного трафіку актуальним завданням навіть сьогодні. Метою даного дослідження є створення робочої імітаційної моделі самоподібного мультимедійного трафіку в середовищі Network Simulator 2, дослідження поведінки трафіку

Багато сучасних досліджень інтернет трафіку показують нам те що він має властивістю самоподібності. Під самоподібністю мається на увазі повторення розподілу навантаження на мережу в часі, незалежно від масштабу а бо місця в самій мережі. Тобто якщо набір значень з самоподібної функції, що має ознаки самокореляції, поділити на рівні частини, а після вивести сумму значень кожної, ми дізнаємося, що весь цей набір буде мати таку ж кореляційну функцію як і початкові дані.

На відміну від Пуассонівського процесу який моделює кількість випадкових подій, що стались, тільки якщо вони відбуваються зі сталими середнім значеннями інтервалів між наставанням, самоподібним процесам характерно наявність наслідків. Іншими словами імовірність настання наступної події залежить не тільки від часу інтервалів між ними, але і безпосередньо від минулих подій. Це також може означати що дана кількість подій у даний момент часу, повністю може залежати від кількості подій у віддалених проміжках часу. Саме через це однією

з найважливіших властивостей самоподібного процесу є повільно зникаюча залежність від об'ємів трафіку в різні проміжки часу.

Network Simulator 2 – це мережевий симулятор, по своїй суті інструмент для моделювання процесів, що відбуваються в комп'ютерних мережах. Його сильна сторона полягає в тому, що він дозволяє змоделювати та описати багато речей, такі як: топологію, конфігурацію компонентів по типу джерела та приймача трафіку, параметри з'єднання, параметри трафіку, візуальні налаштування, тощо. При моделюванні є можливість керувати параметрами буферів, моніторити пакети, прийняті, відправленні, загубленні, в черзі. Також є можливість витягти інформацію про стан мережі, стан з'єднання між об'єктами, роботу протоколів, динаміку трафіку, скільки компонент отримав пакетів від усіх інших, тощо.

Сам самоподібний мережевий трафік створюється з великою кількістю незалежних його джерел. Найпростіша модель On/Off передбачає, що ці самі джерела трафіку постійно переходять із одного стану, коли постійно генерується трафік зі сталою швидкістю, до стану коли пакети зовсім не посилаються. Саме об'єднання такого трафіку і дає це саме навантаження що ми зазвичай спостерігаємо на мережевому обладнанні.

Сама суть подібних імітаційних моделей полягає в тому щоб спростити або навіть вирішити проблеми по типу: планування, оптимізація безпосередньо існуючих чи потенційно існуючих мереж, створення та перевірка аналітичних моделей мережі, навіть створення чи перевірка протоколів зв'язку, тощо. Тому значимість подібних проектів дуже велика і може сильно спростити чи навіть уникнути багатьох проблем по всьому світу при створенні внутрішніх та зовнішніх мереж. А завдяки властивостям самоподібності трафіку подібні імітаційні моделі дозволяють не тільки оптимізувати роботу мережі, а і зробити трафік в будь який час в будь якому її місці рівномірним.

УДК 621.391.825.5 (043.2)

Олександр ЛАВРИНЕНКО
Національний авіаційний університет, м. Київ

МОДЕЛЮВАННЯ ВПЛИВУ ВУЗЬКОСМУГОВИХ ЗАВАД НА СИГНАЛЬНО-КОДОВІ КОНСТРУКЦІЇ В СИСТЕМІ WIMAX

У сучасних бездротових комунікаційних системах, таких як WiMAX, забезпечення надійності та якості передачі даних є критично важливим завданням. Однією з основних проблем, що впливають на якість зв'язку, є вузькосмугові завади, які можуть суттєво погіршити продуктивність системи. Дослідження впливу таких завад на сигнально-кодові конструкції дозволяє розробити ефективні методи їхньої мінімізації та підвищити стійкість передавальних систем.

У даній роботі проводиться моделювання впливу вузькосмугових завад на сигнально-кодові конструкції в системі WiMAX. Метою є аналіз ефективності різних методів кодування та модуляції в умовах наявності перешкод, а також розробка стратегій для зниження їхнього негативного впливу. Вивчення цього питання є важливим кроком до покращення якості зв'язку в сучасних і майбутніх телекомунікаційних мережах.

Багатотональні завади, які представляють суму гармонійних коливань рівної потужності з випадковими фазами, є одним із найпоширеніших типів моделей вузькосмугових завад (рис. 1).

Багатотональна перешкода виду $\zeta = (\zeta_1, \zeta_2, .., \zeta_N)^T$ формується відповідно до:

$$\zeta_n = \sum_{k=1}^{K} U_n \cos(2\pi f_k t_n + \varphi_k),\ n = 1,...,N, \quad (1)$$

де f_k - частота гармонійної складової (контрольна частота), φ_k - випадкова фаза, $(...)^T$ - операція транспонування, U_n - амплітуда k - тієї складової.

Різноманітні варіанти частотно-часового розподілу вузькосмугової багатотональної завади можуть виникати залежно від кількості частотних складових вузькосмугової завади, як показано на рисунках 1–4.

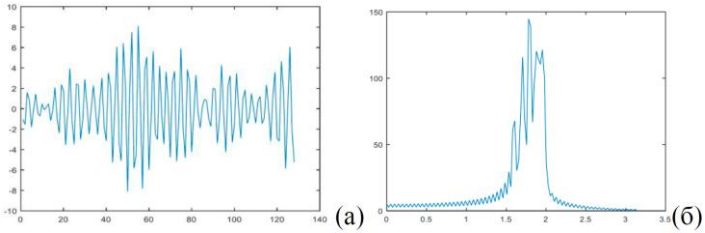


Рис. 1. Багатотональна перешкода (сума 16 косинусоїд): а) графік функції; б) спектр вузькосмугової перешкоди (нормована до π частота)

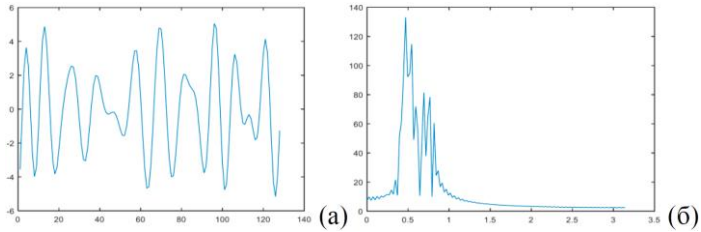


Рис. 2. Вузькосмугова перешкода: а) графік функції; б) спектр (нормована частота), $\pi/8$

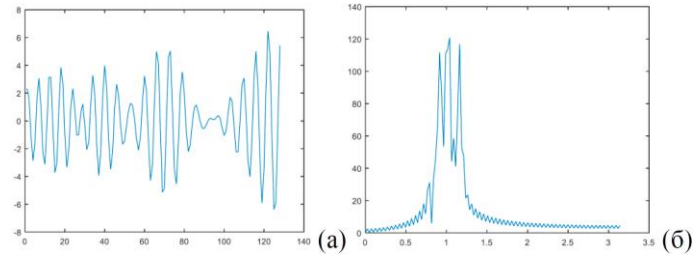


Рис. 3.3. Вузькосмугова перешкода: а) графік функції; б) спектр (нормована частота), $\pi/4$

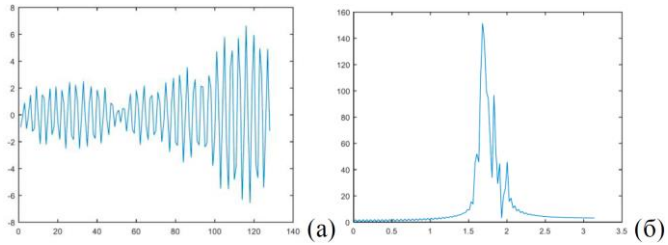


Рис. 3.4. Вузькосмугова перешкода: а) графік функції; б) спектр (нормована частота), $\pi/2$

Далі в роботі буде розглянуто адитивну модель впливу на СКК:

$$\vec{\tilde{x}} = \vec{x} + h_0 \cdot \vec{\zeta}, \quad (2)$$

де h_0 - відношення сигнал/шум, $\vec{\zeta}$ - вузькосмугова перешкода, енергія якої унормована $|\vec{\zeta}| = 1$.

Висновок. Дослідження впливу вузькосмугових завад на сигнально-кодові конструкції в системі WiMAX виявилося ключовим для забезпечення надійності та якості передачі даних у бездротових комунікаційних системах. Зокрема, виявлено, що вузькосмугові завади можуть значно погіршити продуктивність системи, що підкреслює важливість розробки ефективних методів їхньої мінімізації та забезпечення стійкості передавальних систем.

Моделювання впливу вузькосмугових завад на сигнально-кодові конструкції в системі WiMAX дозволило провести аналіз ефективності різних методів кодування та модуляції у врахуванні наявності перешкод. Результати дослідження становлять важливий крок у напрямку розробки стратегій для зниження негативного впливу вузькосмугових завад на якість зв'язку в бездротових комунікаційних мережах.

Багатотональні завади виявилися одним із найпоширеніших типів моделей вузькосмугових завад. Різноманітні варіанти їхнього частотно-часового розподілу можуть виникати в залежності від кількості частотних складових, що підкреслює необхідність подальших досліджень у цьому напрямку.

Список використаних джерел

1. S. Aditya, O. Dizdar, B. Clerckx and X. Li, "Sensing Using Coded Communications Signals," in IEEE Open Journal of the Communications Society, vol. 4, pp. 134-152.
2. D. B. Kurka and D. Gündüz, "DeepJSCC-f: Deep Joint Source-Channel Coding of Images With Feedback," in IEEE Journal on Selected Areas in Information Theory, vol. 1, no. 1, pp. 178-193.
3. H. -Y. Lin and M. R. Bell, "A Time-Frequency Modulation and Coding Scheme for Communications in the Presence of LFM Chirp Radar," 2023 57th Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 2023, pp. 202-209.

УДК 621.396.98:004.738.5 (043.2)

Максим КУДРИЦЬКИЙ, Веніамін АНТОНОВ
Національний авіаційний університет, м. Київ

МУЛЬТИСЕРВІСНА МЕРЕЖА ЗВ'ЯЗКУ З ВПРОВАДЖЕННЯМ ТЕХНОЛОГІЇ VLAN НА ОСНОВІ IPV6

В сучасному світі мережі зв'язку відіграють ключову роль у забезпеченні надійного обміну даними між різними пристроями та системами. Однак із зростанням обсягів передачі даних і розвитком нових сервісів виникає потреба у мультисервісних мережах, які здатні ефективно передавати різноманітні типи трафіку. Впровадження технології VLAN (віртуальних локальних мереж) на основі IPv6 є одним з способів покращення функціональності та ефективності мультисервісних мереж зв'язку. Це дозволяє створювати віртуальні мережі з обмеженим доступом для різних типів трафіку, що сприяє забезпеченню безпеки, оптимізації ресурсів та підвищенню продуктивності.

У даній роботі проводиться аналіз можливостей та переваг використання технології VLAN на основі IPv6 в мультисервісних мережах зв'язку. Розглядаються основні аспекти впровадження, методи реалізації та потенційні вигоди для різних типів мереж та обслуговуваних послуг.

Для моделювання мереж використовується Riverbed Modder, який дозволяє створювати моделі мереж і показувати параметри, такі як пропускна спроможність на вузлі, час затримки проходження пакета, завантаження серверів тощо.

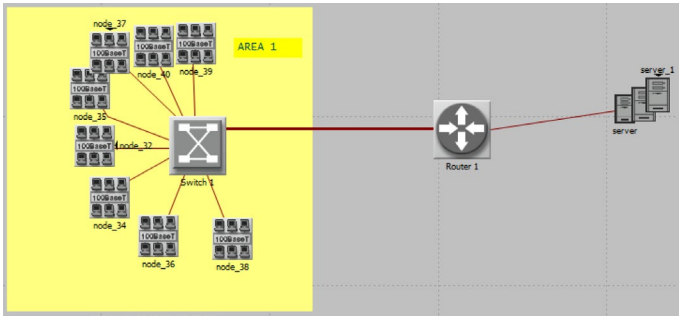


Рис. 1. Схема моделі для початкового сценарію

У першій моделі є до 1000 абонентів і один маршрутизатор, який передає трафік до серверів клієнтів, які надають різні послуги, такі як

Інтернет, VoIP, відео та аудіо трансляції, серед інших. Були задані стандарти генерації трафіку з інтенсивністю 100 пакетів на секунду від підключеного пристрою відповідно до певних законів. Кожній частині мережі було надано унікальну IP-адресу. Спочатку мережа працювала за протоколом IPv4. Потім маршрутизатори та робочі станції були переведені на роботу за протоколом IPv6.

Було отримано результати досліджуваних характеристик через 15 хвилин симуляції роботи мережі. Середній час перебування пакета в мережі з кількома вузлами комутації, з'єднаними між собою дуплексними лініями зв'язку з пропускною здатністю dk,l байт/с між k і l вузлами, використовується як показник для оцінки продуктивності мережі. Кожен вузол комутації містить буфер необмеженої ємності, а середня довжина пакета дорівнює Lp =1/μ байт. Найпростіший потік даних має середню інтенсивність пакетів/с λi,j. Формула для визначення загальної середньої інтенсивності мережі:

$$\lambda = \sum_{i=1}^{N}\sum_{j=1}^{N}\lambda_{ij}, \quad (1)$$

де N: - загальне число вузлових комутаторів. Вираз середньої затримки пакета виглядає таким чином:

$$T = \frac{1}{\lambda}\sum_{k=1}^{N}\sum_{j=1}^{N}\gamma_{kl}t_{kl}, \quad (2)$$

де tkl- середня тривалість зберігання повідомлень на лінії.

$$\gamma_{kl} = \sum_{i=1}^{N}\sum_{j=1}^{N}\lambda_{ij}x_{kl}^{(i,j)}, \quad (3.3)$$

де x(i,j) - частка потоку по лінії (k,l). Крім часу затримки, порівняння проводяться за допомогою результатів пакетного завантаження серверів послуг і кількості біт, оброблених.

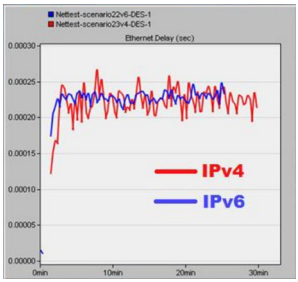


Рис. 1. У першому сценарії затримка пакетів

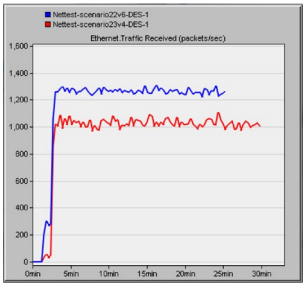


Рис. 2. Кількість пакетів, які були оброблені сервером у першому сценарії

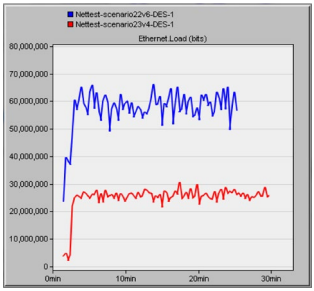


Рис. 3. Кілька байт, які обробляє сервер у першому сценарії

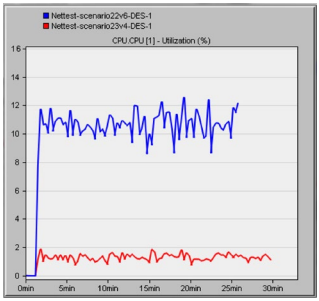


Рис. 4. Завантаження процесора маршрутизатора в першому сценарії

На отриманому графіку можна побачити, скільки часу витрачається пакетом (у секундах) під час проходження всього шляху. На час затримки проходження пакета в малих мережах суттєво не впливає різниця між версіями протоколу IP. У певні моменти роботи мережі модель мережі IPv4 працює швидше за IPv6. Маршрутизатор може обробляти велику кількість пакетів, не витрачаючи багато часу на затримування пакетів у черзі. Це досягається завдяки тому, що пакети збе-

рігаються в пам’яті маршрутизатора. Тим не менш, на графіку, який показує завантаження сервера на обробку запитів і передачу послуг, видно, що протокол IPv6 навантажує сервер більше біт інформації, ніж протокол IPv4. Таким чином, кількість пакетів даних, оброблених у двох досліджуваних протоколах, однакова на графіку.

Розробники передбачили протокол IPv6, оскільки він дозволяє створювати великі пакети даних завдяки новітнім технологіям передавання даних. Це зменшує кількість пакетів у мережі, а також кількість бітів технічної інформації, переданої через канал передачі даних. Як показано на графіку завантаження процесора, це призводить до збільшення навантаження на маршрутизатори. Щоб зберігати великі пакети, які очікують на обробку, потрібна велика ємність буфера маршрутизатора.

Висновок. В роботі було розглянуто важливі аспекти розвитку сучасних мереж зв'язку, зокрема потребу у мультисервісних мережах, що забезпечують ефективну передачу різноманітного трафіку. Впровадження технології VLAN на базі IPv6 було розглянуто як один із шляхів оптимізації функціональності та ефективності таких мереж.

Аналіз можливостей використання даної технології в мультисервісних мережах дозволив визначити переваги та можливі шляхи оптимізації ресурсів. Моделювання мереж за допомогою Riverbed Modder відображає вплив технології на різні параметри мережі. Отримані результати підтверджують переваги протоколу IPv6 в порівнянні з IPv4 у великих мережах, зокрема, збільшення потужності передачі даних та зниження кількості пакетів. Проте, важливо враховувати збільшення навантаження на маршрутизатори та необхідність великої ємності буфера для зберігання великих пакетів. Таким чином, робота спрямована на покращення якості та продуктивності мультисервісних мереж зв'язку за допомогою використання технології VLAN на базі IPv6, що є актуальним напрямком в розвитку телекомунікаційних систем.

Список використаних джерел

1. A. A. Fauzan, E. A. Juanda, S. Elvyanti, N. F. Arief Hakim, A. M. Ridwan and Hasbiyallah, "Performance Analysis of Rapid PVST+ Technology (Per VLAN Spanning Tree) On LAN Networks Using Redudancy Link Systems," 2023 9th International Conference on Wireless and Telematics (ICWT), Solo, Indonesia, 2023, pp. 1-6.

УДК 05.12.02 (043.2)

С.О. Кузнєцов
Національний авіаційний університет, м. Київ

МУЛЬТИСЕРВІСНА МЕРЕЖА ДОСТУПУ БІЗНЕС-ЦЕНТРУ НА БАЗІ ТЕХНОЛОГІЇ FTTB

У сучасному динамічному світі бізнес-центри стикаються з постійно зростаючими потребами у надійному та високошвидкісному підключенні до мережі. Для підтримки безперебійної роботи, що включає доступ до Інтернету, IP-телефонію, IPTV та системи відеонагляду, їм необхідні рішення, які гарантують не лише високу пропускну здатність, але й гнучкість та масштабованість.

Мультисервісні мережі доступу на базі технології FTTB (Fiber to the Building) з'являються як оптимальний вибір для задоволення цих потреб. Завдяки прокладці оптоволоконного кабелю безпосередньо до будівлі, FTTB забезпечує безпрецедентні рівні пропускної здатності, надійності та гнучкості, роблячи її ідеальною платформою для підтримки широкого спектру послуг, що необхідні сучасним бізнес-центрам.

Переваги FTTB для бізнес-центрів:

- Висока пропускна здатність. FTTB пропонує значно більшу пропускну здатність, порівняно з традиційними технологіями, такими як DSL та кабельний Інтернет. Це робить її ідеальною для бізнес-центрів, де одночасно працює багато користувачів, які потребують доступу до ресурсів, що потребують великої кількості даних.
- Надійність. Оптоволоконні кабелі, що використовуються в FTTB, стійкі до перешкод та несприятливих погодних умов, що гарантує надійне та стабільне з'єднання. Це критично важливо для бізнес-центрів, де перебої в роботі мережі можуть призвести до значних фінансових втрат.
- Гнучкість та масштабованість. FTTB легко масштабується, що дозволяє додавати нових користувачів та послуги без значних додаткових витрат. Це робить її ідеальним рішенням для бізнес-центрів, які постійно розширюються або оновлюють свої потреби в мережі.

- Безпека. Оптоволоконні кабелі FTTB значно безпечніші, ніж мідні кабелі, що використовуються в традиційних мережах. Це робить їх більш стійкими до несанкціонованого доступу та крадіжки даних.
- Якість обслуговування. FTTB забезпечує низькі затримки та високу якість обслуговування (QoS), що необхідно для таких програм, як VoIP та відеонагляд.

Впровадження FTTB-мережі в бізнес-центрі не лише покращує поточні можливості підключення, але й готує його до майбутніх потреб. Зростаюча залежність від хмарних сервісів, штучного інтелекту та інших ресурсів, що потребують великої кількості даних, робить FTTB необхідною інвестицією для будь-якого бізнес-центру, який прагне залишатися конкурентоспроможним у динамічному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Engelen and N. Weling, "PLC-xDSL Dynamic Interference Mitigation," 2021 IEEE International Symposium on Power Line Communications and its Applications (ISPLC), Aachen, Germany, 2021, pp. 25-30.

2. V. G. Sannikov, A. V. Alyoshintsev and A. N. Sak, "Advanced DMT Modem as an Element of the PON / xDSL System," 2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Arkhangelsk, Russian Federation, 2022, pp. 1-4.

3. M. Sharma, M. Moonen, Y. Lefevre and P. Tsiaflakis, "MIMO Time Domain Equalizer Design for Long Reach xDSL MIMO Channel Shortening," in IEEE Access, vol. 8, pp. 203468-203477, 2020.

4. P. Jares, J. Vodrazka and P. Lafata, "Experimental verification of a simulation model for extra-fast communication on twisted pair lines," 2020 19th International Conference on Mechatronics - Mechatronika (ME), Prague, Czech Republic, 2020, pp. 1-4.

5. N. Keukeleire, B. Hesmans and O. Bonaventure, "Increasing Broadband Reach with Hybrid Access Networks," in IEEE Communications Standards Magazine, vol. 4, no. 1, pp. 43-49, March 2020.

УДК 621.396 (043.2)

А.В. Курінний
Національний Авіаційний Університет Київ

ДОСЛІДЖЕННЯ ТА ВИКОРИСТАННЯ НАД ШИРОКОСМУГОВИХ ІМПУЛЬСНИХ СИГНАЛІВ ДЛЯ ДАЛЬНЬОГО РАДІОЗВ'ЯЗКУ

В теперішній час дослідження використання над широкосмугових імпульсних сигналів для дальнього радіозв'язку є надзвичайно актуальною темою з декількох причин:

Можливість збільшення обсягів передачі даних. У сучасному світі використовуються все більші швидкості передачі даних та більший обсяг інформації, яку можуть обробляти комунікаційні системи. Тому дослідження та розвиток над широкосмугових технології, які забезпечують велику пропускну здатність є критично важливим етапом розвитку технологій передачі даних для різних застосувань;

Потреба у завадостійкості. В теперішній час розробка та встановлення нових радіоелектронних пристроїв та систем є актуальним питанням забезпечення надійності радіозв'язку. Так наприклад над широкосмугові сигнали мають високу завадостійкість, що дозволяє ефективно використовувати їх в складних умовах електромагнітного середовища;

Розвиток та застосування в життєвих сферах (військовій, цивільній): У військовій сфері над широкосмугові системи можуть бути використані для створення надійних систем зв'язку та радарів, здатних виявляти об'єкти на великі відстані із значно вищою точністю порівняно з теперішніми системами. У цивільному секторі це може означати краще покриття сигналом в регіонах, де традиційний зв'язок є обмеженим;

Значення для науки: над широкосмугові системи відкривають нові можливості для наукових досліджень. Це може призвести до нових відкриттів та технологічних інновацій, які покращать та пришвидшать розвиток технологій в подальшому.

Покращення систем та засобів безпеки: використання над широкосмугових технологій може значно покращити системи безпеки та спостереження через їх здатність передавати значно більші обсяги даних із більш високою швидкістю та меншою затримкою.

Враховуючи ці фактори, можна сказати, що дослідження та розвиток над широкосмугових імпульсних сигналів є важливими для подальшого покращення умов в різних галузях життя та науки. Розглянувши нині існуючі системи, які використовують над широкосмугові імпульсні сигнали для дальнього радіозв'язку можна виділити те що вони стикаються з різного роду проблемами які потребують подальшого виправлення та вдосконалення. Головними проблемами на сьогодні є те, що існуючі системи мають значні проблеми з енергоспоживання (особливо при використанні великої потужності для підтримки стабільності сигналу на дальні відстані); поганою пропускною здатністю (впливає на якість та швидкість передачі даних); недостатньою завадостійкістю (із-за малої завадостійкості ефективність роботи в умовах високого рівня електромагнітних перешкод,); складність введення та впровадження існуючих систем (є значним недоліком, оскільки це вимагає значних вкладень в різному виді). Для виправлення даних не вирішених проблем в майбутньому, можна використовувати підхід, який полягає у застосуванні новітніх технік кодування і модуляції сигналу, що може значно підвищити ефективність використання над широкосмугових імпульсних сигналів та зменшити енергоспоживання, зберігаючи в даному випадку високу пропускну здатність; Також можна використати підхід адаптивних антенних систем і алгоритмів керування потужністю, що дозволить зменшити вплив зовнішніх перешкод та покращити радіочастотний вихід за потребами, тим самим підвищуючи завадостійкість системи, таінше.

З урахуванням даних висновків, важливо підкреслити, що застосування над широкосмугових імпульсних сигналів та розробка новітніх технологій управління спектром можуть істотно сприяти покращенню пропускної здатності та енергетичної ефективності систем. Введення адаптивних антен та розумних алгоритмів керування потужністю не тільки підвищить завадостійкість, але й спростить процес інтеграції та налагодження систем у різних умовах. Таким чином, стратегічне впровадження цих підходів може забезпечити значні переваги для наступних поколінь телекомунікаційних систем, забезпечуючи їх готовність до викликів майбутнього та вимог сучасного цифрового світу. Цей комплексний підхід до аналізу, вдосконалення та впровадження систем дальнього радіозв'язку відкриває нові можливості для розвитку більш ефективних, надійних та економічно вигідних рішень у сфері телекомунікацій.

УДК 043.2

В.Л. Лазаренко
І.О. Козлюк
Національний авіаційний університет, м. Київ

ЗАБЕЗПЕЧЕННЯ ЗАДАНОГО РІВНЯ БЕЗПЕКИ ПЕРЕДАЧІ ІНФОРМАЦІЇ В АРХІТЕКРУРІ IoT З ЕЛЕМЕНТАМИ ТЕХНОЛОГІЙ 5G

Архітектура Інтернету речей (IoT) стає все більш важливою в сучасному світі, де пристрої та датчики забезпечують зв'язок та обмін даними. Однак разом з ростом можливостей IoT з'являються нові виклики щодо безпеки передачі інформації. Особливо це стосується впровадження технології 5G, яка відкриває нові можливості для зв'язку, але також вимагає додаткових заходів безпеки.

У цих тезах ми розглянемо питання безпеки в архітектурі IoT з елементами технології 5G та запропонуємо шляхи забезпечення заданого рівня безпеки передачі інформації. Давайте розглянемо деталі цієї проблеми.

Архітектура IoT складається з різноманітних пристроїв, від сенсорів і акторів до потужних обчислювальних ресурсів. Кожен з цих елементів може бути вразливим до атак, що робить всю систему потенційно небезпечною. Основні аспекти забезпечення безпеки включають:

1. Аутентифікація та авторизація.
2. Конфіденційність даних.
3. Цілісність даних.
4. Відмовостійкість та безперервність роботи.

Технологія 5G має значний потенціал покращити безпеку IoT через свої технічні можливості, такі як:

- висока швидкість передачі даних;
- мала затримка;
- підтримка великої кількості пристроїв;
- розширена функціональність мережі.

Для забезпечення високого рівня безпеки в архітектурі IoT з елементами 5G можуть бути застосовані наступні методи:

- Шифрування даних.
- Використання блокчейну.

- Механізми виявлення аномалій.
- Підтримка оновлень безпеки.

Безпека в архітектурі IoT з технологією 5G є багатовимірним завданням, яке включає технічні, організаційні та процедурні аспекти. Впровадження сучасних технологій шифрування, методів виявлення аномалій та інших заходів безпеки дозволяє забезпечити надійний захист даних та стабільну роботу систем IoT в умовах нової ери цифрових технологій.

Список літератури:

1. I. Analytics, “State of the IoT 2018: Number of IoT devices now at 7B” [Electronic resource] – Mode of access: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iotdevices-now-7b/.

2. Speranzainc, “Security with QoS Optimization in IoT” [Electronic resource] – Mode of access: https://www.speranzainc.com/security-with-qos-optimization-in-iot/.

3. Siemens, “Is 5G already robust enough for industry?” [Electronic resource] – Mode of access: https://new.siemens.com/global/en/products/automation/industrialcommunication/5g.html.

4. Ericsson, “A guide to 5G network security” [Electronic resource] – Mode of access: https://www.ericsson.com/en/security/a-guide-to-5g-network-security.

5. 3GPP, “Security architecture and procedures for 5G system” [Electronic resource] – Mode of access: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

6. A. Alhilal, T. Braud, and P. Hui, “Distributed Vehicular Computing at the Dawn of 5G: a Survey” [Electronic resource] – Mode of access: https://arxiv.org/pdf/2001.07077.pdf.

7. A. Scrase, “3GPP Overview: The Standardization Ecosystem for Global Mobile Systems” [Electronic resource] – Mode of access: https://www.3gpp.org/ftp/Information/presentations/presentations_2018/2018_10_17_tokyo/presentations/2018_1017_3GPP Summit_02_Key.

8. J. S. Walia, H. Hämmäinen, K. Kilkki, and S. Yrjölä, “5G network slicing strategies for a smart factory” [Electronic resource] – Mode of access: https://doi.org/10.1016/j.compind.2019.07.006.

УДК 621.391.15 (043.2)

Олександр ЛАВРИНЕНКО
Національний авіаційний університет, м. Київ

МЕТОД ЗНИЖЕННЯ ПІК-ФАКТОРА OFDM СИГНАЛУ

OFDM (Orthogonal Frequency Division Multiplexing) - це метод модуляції, який широко використовується в сучасних системах зв'язку, таких як Wi-Fi, LTE і 5G. OFDM пропонує ряд переваг, таких як стійкість до багатоканальної інтерференції та вицвітання, що робить його ідеальним для бездротового зв'язку. Однак OFDM сигнали мають високий пік-фактор (PAPR), що може призвести до ряду проблем, таких як: Перевантаження підсилювачів потужності; Нелінійні спотворення; Збільшення шуму в системі. Зниження пік-фактора OFDM сигналу є важливою задачею для покращення продуктивності та ефективності систем OFDM. У цій роботі пропонується новий метод зниження пік-фактора OFDM сигналу, який має ряд переваг перед існуючими методами. Запропонований метод базується на моделюванні і дозволяє зменшити пік-фактор OFDM сигналу без значного погіршення його характеристик. Пропонований метод буде проаналізовано та оцінено, а також буде проведено його порівняння з існуючими методами. Очікується, що результати роботи покращать продуктивність та ефективність систем OFDM.

MATLAB, пакет прикладних програм Communication System Toolbox, був обраний для використання як середовище моделювання для проведення практичних досліджень. Збірник інструментів для систем зв’язку містить додатки та алгоритми, які використовуються для розробки, аналізу та тестування моделей цифрових і аналогових систем, пристроїв зв’язку та передачі інформації. Алгоритми Toolbox включають модуляцію сигналів, MIMO, OFDM і канальне кодування, а також дозволяють створювати модель фізичного рівня проєктованої системи. Побудова діаграм сузір’їв і вічкоподібних діаграм, визначення BER (кількості бітових помилок) і інші можливості для аналізу та перевірки роботи проєктованих систем доступні в наборі інструментів системи Communication System Toolbox. Ці програми дозволяють аналізувати сигнали, створювати візуальні зображення характеристик каналу та отримувати показники продуктивності системи зв’язку.

Для дослідження величини пік-фактора OFDM-сигналу було створено модель, яка перед виконанням ЗШПФ генерує OFDM-сигнал із заданого або випадкового потоку даних (рис. 1).

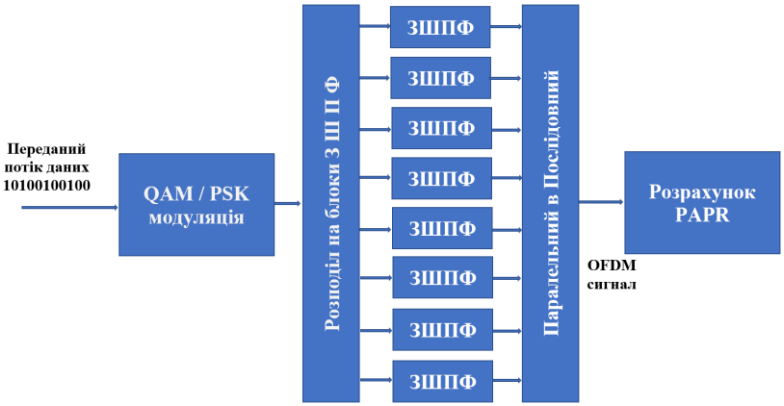


Рис. 1. Функціональна схема експериментальної моделі

Цю модель простого OFDM модулятора було побудовано за допомогою таких стандартних функцій MATLAB і функцій Communication System Toolbox:

randsrc(m, n, alphabet) - повертає матрицю розміром m на n, елементи якої є незалежними випадковими числами, з однаковою ймовірністю обираними з вектора-рядка alphabet. Функція використовувалася як генератор інформаційного потоку на вході QAM/PSK модулятора.

pskmod(x, M, ini_phase) - повертає комплексну обвідну y, отриману в результаті передавання інформаційної послідовності x з використанням фазової маніпуляції. Вхідний параметр M задає розмір алфавіту (число позицій маніпуляції) і має бути ступенем числа 2. Інформаційна послідовність x має складатися з цілих чисел, що лежать у діапазоні від 0 до M-1 включно. Додатковий вхідний параметр ini_phase задає початкову фазу комплексної обвідної в радіанах.

reshape(A, M, N) - повертає масив розміром MxN, сформований з елементів масиву A шляхом їхнього послідовного відбору за стовпчиками. Функція була використана для паралельно-послідовного перетворення з метою розбиття вхідної послідовності на блоки для обробки ОБПФ і зворотного мультиплексування даних після цього перетворення.

ifft(Y, n) - обчислює для масиву даних Y n-точкове дискретне зворотне перетворення Фур'є, використовуючи IFFT-алгоритм зворотного швидкого Фур'є-перетворення. У разі двовимірного вхідного масиву здійснюється дискретне перетворення для кожного стовпчика (що було використано в моделі).

scatterplot(x) - виводить діаграму розсіювання для сигнального масиву x. Інтерпретація масиву залежить від його форми і наявності уявної частини. У розробленій моделі сигнальний масив x являв собою одновимірний комплексний вектор, і здійснювали інтерпретацію його дійсної частини як синфазної, а уявної - як квадратурної складової, внаслідок чого ця функція давала змогу відобразити позиційне сузір'я квадратурної маніпуляції сигналу.

В моделі було три способи формування модулюючої інформаційної послідовності. Вони включали генерування випадкових чисел, повторення певної комбінації символів і завантаження вектора даних, який був збережений у файлі.

```
% 1.Вибір потоку закодованих даних
% 1.1. Випадкова послідовність
data = randsrc(1, N, 0:M-1);

% 1.2 Детермінована послідовність

A=[0 2 1 3];
% idx=randperm(M)-1;
% A=idx;
data=repmat(A,1,N/M);
% disp(A)

% 1.3 Завантаження даних із файлу
load params data
```

Висновок. MATLAB та Communication System Toolbox є ефективними інструментами для дослідження та розробки методів зниження пік-фактора OFDM сигналу. Запропонована модель OFDM модулятора та методи формування інформаційної послідовності можуть бути використані для подальших досліджень в цій галузі.

Список використаних джерел

1. N. Sharan, S. K. Ghorai and A. Kumar, "PAPR reduction using a Precoder and Compander combination in a NOMA-OFDM VLC system," 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 2022, pp. 1-4.

УДК 621.396 (043.2)

D.R. Loienko
National Aviation University Kyiv

STARLINK TERMINAL EQUIPMENT MODULE FOR AERONAUTICAL PURPOSES

Major development of the satellite communication is a highly competitive field that develops everyday, so it is important to follow the evolution of aeronautical communication and sat-based systems to provide connectivity and navigation to private and commercial aircraft.

Here the point is to explore all about new technologies in this field, a comparative analysis of the main sat-based systems and the role that related structures have in improving aeronautical communication with Starlink Terminal Equipment Modules.

The craving for exploring heights shocked people throughout their entire existence. Humanity has dreamed and fantasized that from the tales of flying flying carpets that were woven by the threads of time into mythology, to the insanely daring attempts of inventors that were eventually documented in our history, the desire to soar above the earth's boundaries has never left the human mind. However, remembering the historical event on December 17, 1903, at a place called Kitty Hawk, located in the center of North Carolina, mankind finally achieved the first powered flight thanks to a never-before-seen innovation by Orville Wright. It's hard to believe that in just over 12 seconds, Orville Wright flew thirty-six and a half meters, thus entering the books of modern history, his name inscribed as the first person to accomplish such a daring and revolutionary feat - an event that forever changed the course of our civilization.

Rising 4 meters above the desolate land, this short but momentous flight marked the dawn of change in aviation history like never before. Currently we see advancements, in aviation that have pushed the boundaries of flight to heights.

Through in flight refueling techniques and lightweight aircraft designs we are witnessing flight durations that defy gravity for months on end. The challenging barriers of distance have been overcome, with flights covering distances exceeding 6,000 miles becoming an occurrence.

Additionally aviations expansion, into the stratosphere has revolutionized global travel and connectivity among people. In the days of aviation pilots navigated through skies filled with uncertainty as they

adapted to the intricacies of this groundbreaking mode of transportation. Unaware of the mechanical constraints and nuances inherent in flying machines, pilots often pushed the boundaries of their aircraft beyond safe limits, leading to tragic accidents. Pilots took on maneuvers that ended up causing problems due, to weaknesses and performance limits.

They had to learn how to control aircraft through trial and error while exploring territory. Dealing with spins and stalls required them to be resilient and face challenges head on. Nowadays aviation education has evolved significantly with pilots needing an understanding of aircraft design, controls and operational limits. With the help of instructors aviators undergo training in both theory and practice**.**

The social significance of the development of this project is to change the channel of atmospheric scattering signal, to significantly improve the connection rate of user aircraft ,to optimize the operation efficiency and experience of the flight, which is a major progress in the development of aviation communications technology.

These modules that communicated with Starlink satellites at low angle elevations over the horizon, and were designed to operate on the 10.7-12.7 GHz frequency range, were a remarkable leap in satellite communications saving design scalability issues altogether.

Design rock-solid terminal modules capable of functioning under aviation applications This requires an alternative approach and additional considerations for the atmospheric signal scattering issues**.**

The radio frequency module developed in this work improves the capabilities of the Starlink system, which can provide stable signal without delay under all kinds of bad weather environment, so as to reserve its core competitiveness for satellite communications vehicles.

By solving the key problems of signal scattering in atmosphere and signal amplification in antenna, the satellite realizes stable communication under low satellite altitude angle, making the Starlink aerospace engineering superior than all similar satellite communications systems.

УДК 004.056:621.391 (043.2)

Валентин ЛУК'ЯНИЦЯ, Віталій КУРУШКІН
Національний авіаційний університет, м. Київ

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ CISCO

У сучасному світі інформаційні технології стали невід'ємною частиною діяльності будь-якого підприємства. Забезпечення безпеки інформації є критично важливим для захисту від зловмисних атак, витоку даних та інших кіберзагроз. Особливої уваги потребують підприємства, які працюють з великими обсягами конфіденційної інформації та мають складну мережеву інфраструктуру. Одним із провідних виробників мережевого обладнання, яке забезпечує високий рівень інформаційної безпеки, є компанія Cisco. Використання рішень Cisco дозволяє підприємствам створювати надійні системи захисту, які включають в себе фаєрволи, системи виявлення вторгнень, захищені маршрутизатори та комутатори, а також програмні засоби для управління безпекою. У даній роботі розглядається побудова системи інформаційної безпеки на базі обладнання Cisco, що дозволяє забезпечити ефективний захист інформаційних ресурсів підприємства від сучасних загроз.

Брандмауер PIX працює в режимі прозорого проксі-сервера, визначаючи потреби в автентифікації сеансу зв'язку на основі користувача, надаючи відповідний механізм запиту імені та пароля користувача, а також перевіряючи користувачів за допомогою стандартних баз даних систем TACACS+ і RADIUS. Процес передачі даних між клієнтом і сервером здійснюється безпосередньо через брандмауер PIX після того, як користувач успішно пройшов процес аутентифікації. З іншого боку, брандмауер лише стежить за станом сеансу.

Основним використанням цієї технології є перевірка користувачів, які входять до DMZ-зони Інтернету. Приклад входу користувача на певну URL-адресу для доступу до Web-сервера XYZ показано на рисунку 1. Для цього користувачеві потрібно буде пройти процес авторизації та аутентифікації, у якому він повинен ввести свій ідентифікаційний номер користувача та пароль. Після того, як користувач вводить дані, вони передаються брандмауеру в незашифрованому вигляді. Далі брандмауер передає цю інформацію на AAA-сервер, на якому виконується CSACS. Користувач отримує дозвіл на взаємодію із запитуваним сервером після успішного завершення процесу аутен-

тифікації. Користувач також повинен ввести ці дані, якщо йому потрібен пароль для входу на Web-сервер.

Рис. 1. Робота в режимі прозорого проксі-сервера

Налаштування процесу аутентифікації. Після налаштування програми CSACS у конфігурації брандмауера PIX також потрібно внести налаштування для AAA-сервера. Адміністратор може налаштувати багато параметрів брандмауера та AAA-сервера. Насамперед необхідно визначити протокол аутентифікації AAA-сервера. Після цього вам потрібно створити сервер AAA і додати його до групи AAA. Багато серверів можуть бути AAA в одній групі. Група з AAA-серверами дозволяє отримати більшу загальну надійність системи. Наприклад, якщо один сервер виявляється недоступним (період часу, протягом якого сервер не відповідає на запити, визначається спеціальним таймером, який буде розглянуто пізніше), запит передається наступному AAA-серверу.

Команда aaa-server використовується для створення AAA-груп. У випадку використання брандмауера PIX адміністратор може задавати різні групи серверів TACACS+ або RADIUS, щоб обробляти різні види потоків даних. Наприклад, для потоків даних, які надходять і надходять, можуть використовуватися два різні сервери системи TACACS+. Команда AAA може автентіфікувати, авторизуватися та аналізувати потік даних від певного облікового запису за допомогою певного AAA-сервера.

Адміністратор може керувати шістнадцятьма групами, кожна з яких може включати до шістнадцяти AAA-серверів. У результаті адміністратор має можливість керувати 256 серверами TACACS+ або

RADUIS. Крім того, якщо є кілька AAA-серверів, вони можуть працювати в режимі захисту від збоїв шляхом резервування, щоб система не працювала. Під час входу користувача в систему він опитує кожен сервер, починаючи з першого в групі, доки не отримає першу відповідь від сервера.

За замовчуванням обидва протоколи AAA-серверів працюють. Такі команди дозволяють підтримувати ці протоколи:

```
aaa-server tacacs+ protocol tacacs+
aaa-server radius protocol radius
```

Коли адміністратор працює зі старими версіями операційної системи Cisco OS, не потрібно створювати груп AAA. Створення двох груп виникає в результаті використання за замовчуванням цих двох протоколів. Це означає, що всі інші AAA-команди будуть доступні під час оновлення операційної системи.

Брандмауер PIX використовує порти 1645 і 1646, щоб працювати за протоколом RADUIS. RADIUS-сервер повинен змінити налаштування, щоб використовувати порти 1812 і 1813, щоб він міг працювати.

Синтаксис команди aaa-server:

```
aaa-server група (ім'я) host IP_адреса ключ timeout секунди
aaa-server група protocol протокол_аут
```

Висновок. У цій роботі було розглянуто принципи роботи брандмауера Cisco PIX у режимі прозорого проксі-сервера, особливості його налаштування та використання для автентифікації користувачів у корпоративних мережах. Показано, як брандмауер забезпечує безпеку передачі даних, використовуючи стандартні бази даних систем TACACS+ та RADIUS для перевірки користувачів. Налаштування аутентифікаційного процесу включає створення груп AAA-серверів, які дозволяють забезпечити надійність та безперервність роботи системи навіть у випадку збою одного з серверів. Здатність керувати великою кількістю серверів TACACS+ або RADIUS, а також використання резервування, значно підвищує загальну стійкість системи до збоїв та покращує рівень інформаційної безпеки.

УДК 004.056.55 (043.2)

Олександр ЛАВРИНЕНКО
Національний авіаційний університет, м. Київ

МЕТОД АУТЕНТИФІКАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ НА ОСНОВІ ХЕШУВАННЯ ДАНИХ

У сучасному світі інформаційних технологій питання забезпечення безпеки даних набуває все більшого значення. Аутентифікація користувачів є критично важливим аспектом захисту комп'ютерних систем від несанкціонованого доступу. Одним із ефективних методів аутентифікації є використання хешування даних. Цей метод дозволяє надійно перевіряти справжність користувача без необхідності зберігати його пароль у відкритому вигляді. У даній роботі розглядаються основні принципи та алгоритми хешування, їх застосування в системах аутентифікації, а також аналізуються переваги та недоліки такого підходу в контексті сучасних загроз кібербезпеки.

Ідеальною криптографічною хеш-функцією є така криптографічна хеш-функція, до якої можна віднести п'ять основних властивостей:

1. Детермінованість. За однакових вхідних даних результат виконання хеш-функції буде однаковим (одне й те саме повідомлення завжди призводить до одного й того самого хешу);
2. Висока швидкість обчислення значення хеш-функції для будь-якого заданого повідомлення;
3. Неможливість згенерувати повідомлення з його хеш-значення, за винятком спроб створення всіх можливих повідомлень;
4. Наявність лавинного ефекту. Невелика зміна в повідомленнях має змінити хеш-значення, так широко, що нові хеш-значення не збігаються зі старими хеш-значеннями;
5. Неможливість знайти два різних повідомлення з однаковими хеш-значеннями.

Таким чином, ідеальна криптографічна хеш-функція, яка має довжину n (тобто на виході n біт), для обчислення прообразу має вимагати щонайменше 2^n операцій.

Зловмисник шукатиме прообраз ідеальної хеш-функції таким чином: у нього є число h, і він повинен знайти таке m, що H(m)=h. Зловмиснику залишається лише збирати всі можливі M і перевіряти, чому хеш-функція цього повідомлення дорівнює, якщо це ідеальна хеш-функція. Якщо m перебирається повністю, результат обчислення є

фактично випадковим числом. Якщо число h лежить у діапазоні від 0 до 2^n, то тоді в середньому на пошуки потрібного h зловмисник витрачатиме 2^{n-1} ітерацій. Таким чином, обчислення прообразу займе вдвічі менше ітерацій, ніж в ідеальному випадку.

Обчислення другого прообразу залишиться 2^n. У пошуку колізій оцінка дасть 2^n, причому це не зовсім точний результат. Ця оцінка йде з оцінки так званого "Парадокса днів народження".

Зловмисник повинен спочатку створити словник колізій, якщо він хоче написати програму з пошуку колізій. Таким чином, він далі обчислює хеш-функцію нового повідомлення і визначає, чи належить ця хеш-функція цьому новому повідомленню. Якщо необхідно, колізію знаходять, а вихідне повідомлення з даним хеш-кодом можна знайти за допомогою словника. Якщо ні, це додає до словника. Такий метод неможливий на практиці, оскільки не вистачило б пам’яті для подібного словника.

Висновок. У даній роботі розглянуто основні властивості ідеальної криптографічної хеш-функції. До них відносяться детермінованість, висока швидкість обчислення, неможливість згенерувати повідомлення з його хеш-значенням, наявність лавинного ефекту та неможливість знайти два різних повідомлення з однаковими хеш-значеннями. Зазначено, що ідеальна хеш-функція для обчислення прообразу повинна вимагати щонайменше 2n операцій для хешування даних довжиною n біт. Також оцінено складність обчислення прообразу та пошуку колізій у випадку ідеальної хеш-функції. Враховуючи розглянуті аспекти, виявлено, що практичне застосування таких ідеальних хеш-функцій ускладнюється через обчислювальні та пам'яткові обмеження.

Список використаних джерел

1. M. Obaidat and J. Brown, "Two Factor Hash Verification (TFHV): A Novel Paradigm for Remote Authentication," 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 2020, pp. 1-4.
2. H. Kim, D. Lee and J. Ryou, "User Authentication Method using FIDO based Password Management for Smart Energy Environment," 2020 International Conference on Data Mining Workshops (ICDMW), Sorrento, Italy, 2020, pp. 707-710.

УДК 004.056:621.391

Б.М. Матвеєв
Ю.В. Петрова
Національний авіаційний університет, м. Київ

СИСТЕМА КОНТРОЛЮ ДОСТУПУ ОФІСНОГО ПРИМІЩЕННЯ

Системи контролю доступу до офісних приміщень є невід'ємною частиною сучасних заходів безпеки, спрямованих на захист інформації, життєво важливих ресурсів і персоналу. Ефективність систем контролю доступу особливо важлива в умовах зростаючої загрози кіберзлочинності та фізичних атак. Ці системи дозволяють контролювати відвідування, а також забезпечують безпеку на різних рівнях організації.

Існує кілька типів систем контролю доступу, включаючи механічні, електронні та біометричні системи. Механічні системи, такі як замки та ключі, є найпростішими, але менш безпечними, ніж електронні та біометричні системи. Електронні системи з картами доступу або кодовими панелями забезпечують більш високий рівень безпеки і зручності. Біометричні системи, засновані на унікальних фізичних характеристиках людини, таких як відбитки пальців і розпізнавання осіб, є найбільш надійними і важкими для імітації.

Основні компоненти включають пристрої ідентифікації, контролери доступу, програмне забезпечення для управління системою, а також засоби зв'язку та живлення. Пристрої ідентифікації можуть бути як простими картками, так і складними біометричними сканерами. Контролери доступу здійснюють прийом та обробку даних від пристроїв ідентифікації та приймають рішення про надання чи відмову в доступі. Програмне забезпечення забезпечує моніторинг, управління та звітність.

Сучасні системи контролю доступу забезпечують високий рівень безпеки, зниження ризиків несанкціонованого доступу, автоматизацію процесів контролю, зручність у використанні та інтеграція з іншими системами безпеки (наприклад, відеоспостереженням). Крім того, сучасні системи можуть забезпечувати аналітичні функції, що дозволяють оцінювати потоки людей, виявляти потенційні загрози та оптимізувати безпекові процеси.

Системи контролю доступу часто інтегруються з іншими безпековими системами, такими як відеоспостереження, сигналізація та системи пожежної безпеки. Така інтеграція дозволяє створювати комплексні рішення для забезпечення максимального рівня безпеки. Наприклад, у разі несанкціонованого доступу, система може автоматично повідомити службу охорони та активувати відеозапис з камер спостереження.

Попри численні переваги, впровадження систем контролю доступу може стикатися з певними труднощами. Це включає високу вартість встановлення та обслуговування, необхідність постійного оновлення програмного забезпечення, а також можливі технічні проблеми, такі як збої у роботі або вразливість до кіберзагроз. Важливо також враховувати людський фактор, зокрема навчання персоналу та запобігання зловживанням повноваженнями.

Система контролю доступу офісного приміщення є критично важливим елементом загальної безпеки організації. Вибір відповідної системи залежить від конкретних потреб та ризиків конкретної компанії. Інтеграція з іншими системами безпеки та регулярне оновлення технологій забезпечують надійний захист від різноманітних загроз. Ефективне впровадження та експлуатація системи контролю доступу сприяють захисту матеріальних та інформаційних ресурсів, забезпечуючи безпеку персоналу та збереження бізнес-активів.

У процесі проектування системи контролю доступу до офісного приміщення, було виконано детальний аналіз потреб компанії та оцінку ризиків, що дозволило визначити оптимальну конфігурацію системи. Було обрано сучасні зчитувачі чип-карток HID iCLASS SE R10 та HID Signo Reader 20, які забезпечують високу надійність та зручність в експлуатації. Для управління системою були використані контролери HID VertX EVO V2000 та HID EDGE EVO E400, що дозволяють централізоване та гнучке управління доступом. На основі отриманих даних я розробив схему розміщення обладнання, враховуючи особливості планування офісу та необхідність резервного живлення. Складена проектна документація включала технічні завдання, креслення, схеми та кошторис витрат. Після монтажу та налаштування обладнання, система пройшла комплексне тестування, що підтвердило її функціональність та безперебійну роботу. Для забезпечення ефективного використання системи була розроблена документація для навчання персоналу.

УДК 004.056:621.39:004.932(043.2)

Матвійчук-Юдін О.О.
Національний авіаційний університет, м. Київ

СУЧАСНІ МОДЕЛІ ЗАХИСТУ ВІДЕОДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ УПРАВЛІННЯ

Оскільки зростає значимість відеоданих у телекомунікаційних системах управління, які використовують у різних сферах діяльності, розробка ефективних методів та моделей захисту відеоданих є актуальною проблемою дослідження, Також відображення в постійному зростанні обсягу відеоданих, які транслюються або зберігаються в телекомунікаційних системах управління містить конфіденційну інформацію, яка може бути цінною для користувачів, а також становить значний інтерес для зловмисників. Таким чином, забезпечення надійного захисту відеоданих в телекомунікаційних системах управління є актуальним.

Мета дослідження полягає в огляді існуючих моделей захисту відеоданих в телекомунікаційних системах управління. Визначити переваги та недоліки різних підходів до захисту відеоданих, виявлення загроз.

Використання стандартизованого програмного забезпечення під час передачі інформаційних ресурсів, яке є доступним для безкоштовного використання, має як свої переваги, так і недоліки. На жаль, в Україні бракує власних програмних продуктів для обміну інформаційними ресурсами в інформаційно-комунікаційних мережах, що створює додаткові загрози для конфіденційності та цілісності критичних відеоданих. Наразі телекомунікаційні абоненти використовують операційні системи зарубіжних розробників, таких як Microsoft, Linux, Novell та інших.

Існує ряд моделей захисту відеоданих, які можуть використовуватися в телекомунікаційних системах управління.

- Шифрування: перетворення даних у нечитабельний формат.
- Контроль доступу: обмеження доступу до даних лише авторизованим користувачам.
- Аутентифікація та авторизація: перевірка особистості користувачів та надання їм дозволів на доступ до даних.

- Захист даних у спокої: захист даних, які зберігаються на носіях інформації.
- Захист даних в русі: захист даних, які передаються по мережі.
- Специфічні моделі захисту:
- Шифрування AES: симетричний алгоритм шифрування, який використовується для захисту даних в спокої та в русі.
- Протокол IPSec: протокол безпечного тунелювання, який використовується для захисту даних в русі.
- Система Kerberos: система аутентифікації та авторизації, яка використовується для контролю доступу до даних.
- Система PKI: система управління відкритими ключами, яка використовується для аутентифікації користувачів та шифрування даних.

Фактори, які слід враховувати при виборі моделі захисту: тип відеоданих, рівень чутливості даних, потреби системи управління, технічні можливості системи, витрати на реалізацію та експлуатацію Табл.1.

Таблиця 1

Моделі захисту відеоданих в телекомунікаційних системах управління

Назва моделі	**Спосіб**	**Функції**
Модель шифрування відеоданих	Симетричне шифрування AES (Advanced Encryption Standard)	Швидке та ефективне шифрування великих обсягів відеоданих. Передбачає використання одного ключа для шифрування і розшифрування даних, що може бути як перевагою, так і недоліком через потребу безпечного обміну ключами.
	Асиметричне шифрування RSA	Передбачає використання 2 ключів. Високий рівень безпеки при передачі ключів, але може бути менш ефективним для шифрування великих обсягів даних через високу обчислювальну складність.

Модель автентифікації та контролю доступу	Мультифакторна автентифікація (MFA)	Використовує кілька рівнів перевірки (паролі, біометричні дані, одноразові коди) для забезпечення надійного доступу до відеоданих. MFA значно підвищує рівень безпеки, знижуючи ризик несанкціонованого доступу.
	Рольова модель управління доступом (RBAC)	Обмежує доступ до відеоданих на основі ролей користувачів у системі., що дозволяє чітко визначити, хто і до яких даних має доступ, що допомагає запобігти внутрішнім загрозам.
Модель блокчейн-технологій	Забезпечення цілісності та автентичності відеоданих.	Децентралізований підхід і неможливість зміни даних без виявлення роблять цю модель перспективною для захисту відеоінформації в телекомунікаційних системах.
Модель захисту на основі машинного способу	Штучного інтелекту (AI)	Використовують алгоритми машинної обробки даних для виявлення та запобігання загрозам у реальному часі. Аналізують великі обсяги даних, виявляють аномалії, реагують на кібератаки.
Модель захисту кінцевих точок	Endpoint Security захист кінцевих пристроїв	Захист кінцевих точок є важливим елементом комплексної безпеки відеоданих (камери відеоспостереження і мобільні пристрої, за допомогою антивірусного ПЗ)
Модель гібридного шифрування	Поєднує переваги симетричних і асиметричних методів	Здійснює шифрування відеоданих може використовуватися симетричний алгоритм, тоді як для захисту ключів - асиметричний. Це забезпечує високу продуктивність і надійність

При побудові стеганосистеми необхідно враховувати такі аспекти:

- система повинна мати оптимальну складність обчислень для вбудовування та вилучення повідомлення зі стеганоконтейнера, тобто

вона має виконувати оптимальну кількість арифметико-логічних операцій;

- методи приховування мають забезпечити невидимість вбудованої інформації для зовнішніх спостерігачів, щоб уникнути виявлення стеганографічного каналу;

- система повинна бути ефективною та швидкою у використанні, щоб забезпечити оперативність у вбудовуванні та вилученні даних;

- важливо забезпечити стійкість системи до атак та спроб виявлення стеганографічного використання;

- потенційний порушник повністю усвідомлений про наявність і принцип роботи стеганосистеми. Єдине, про що він не має поняття, це ключ, який дозволяє визначити наявність повідомлення та його вміст;

- порушник повинен бути позбавлений будь-яких (технічних та інших) переваг.

Основними поняттями у стеганографії є повідомлення та контейнер. Повідомлення $m \in M$ - певна закрита інформація, яку необхідно приховати. $M = \{m_1, m_2, ..., m_n\}$ - множина всіх повідомлень [2].

Контейнер $c \in C$ - множина відкритих даних, яка використовується для вбудовування закритої інформації. $C = \{c_1, c_2, ..., c_q\}$ - множина всіх контейнерів, причому $q >> n$.

Висновок: За результатами існуючих моделей захисту відеоданих в телекомунікаційних системах управління, можна констатувати переваги та недоліки різних підходів до захисту відеоданих, виявлення загроз. Розглянуто основні характеристики моделей: шифрування відеоданих, автентифікації та контролю доступу, блокчейн-технологій, захисту на основі машинного способу та гібридного шифрування. Описані моделі захисту відеоданих, які можуть використовуватися в телекомунікаційних системах управління.

Список літератури.

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

. О. Весельська, Р. Зюбіна, О. Фролов «Систематизація та класифікація наявних стеганографічних методів приховування інформації», Наукоємні технології, Том 30, № 2, с.187-194, 2017

УДК 007.304.659.3

Маштепа М.Б.
Національний авіаційний університет, м. Київ

СУЧАСНІ ТЕХНОЛОГІЇ ВДОСКОНАЛЕННЯ ЦИФРОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ В УКРАЇНІ

У роботі представлено комплексне дослідження теоретичних і практичних аспектів цифрового телевізійного мовлення з акцентом на технологіях і методах, які можуть підвищити якість і надійність телемовлення в Україні.

Враховуючи стрімкий розвиток інформаційних технологій і зростання вимог глядачів до якості телевізійного контенту, удосконалення технологій телевізійного мовлення є надзвичайно важливим. У дослідженні розглядаються ключові області подання цифрового сигналу, методи модуляції, методи виправлення помилок і методи обробки цифрового сигналу для підвищення якості та надійності телевізійного мовлення.

Теоретична частина дипломної роботи присвячена фундаментальним поняттям цифрового телевізійного мовлення. Особлива увага приділяється методам кодування цифрового сигналу, які необхідні для забезпечення високоякісної передачі зображення та звуку.

Різні методи модуляції, такі як квадратурна амплітудна модуляція, обговорюються з огляду на їх ефективність у використанні доступного частотного спектру. Крім того, у роботі детально аналізуються методи виправлення помилок, включаючи коди Ріда-Соломона та згорткові коди, які значно знижують ймовірність втрати даних під час передачі. Ці методи підвищують надійність мовлення навіть за несприятливих умов.

Практична частина дослідження присвячена застосуванню цифрової обробки сигналів для покращення якості телевізійного мовлення. Розглядаються різні методи зменшення шуму, включаючи методи часової та просторової фільтрації, які допомагають зменшити шум і підвищити чіткість зображення.

Тимчасове усереднення зменшує випадковий шум шляхом усереднення значень пікселів за послідовними кадрами, використовуючи надмірність у відео-послідовності для створення чіткішого зображення. Просторова фільтрація передбачає застосування таких фільтрів, як Гаусів і медіанний, щоб згладити шум, зберігаючи такі важливі функ-

ції, як границі зображення. Просторова фільтрація ефективно зменшує шум без значного погіршення якості зображення.

Дослідження також розглядає методи підвищення контрастності зображення, такі як вирівнювання гістограми та гамма-корекція, які роблять зображення більш візуально привабливим шляхом регулювання розподілу інтенсивності та рівнів яскравості.

Практичні застосування, які обговорюються, включають використання часової та просторової фільтрації для мінімізації шуму, впровадження вирівнювання гістограми та гамма-корекції для покращення контрастності зображення, а також використання таких методів, як маскування нерізкості, щоб виділити границі та покращити чіткість зображення.

Постійний розвиток і застосування цих технологій відіграватиме ключову роль у подальшому розвитку цифрового телемовлення в Україні. Майбутні дослідження мають бути зосереджені на вивченні нових технологій, таких як машинне навчання та штучний інтелект, для подальшого вдосконалення методів обробки сигналів. Крім того, інтеграція технології 5G з цифровим мовленням може запропонувати нові можливості для підвищення ефективності передачі контенту.

На завершення ця дипломна робота створює міцну основу для розуміння та впровадження передових технологій цифрового мовлення в Україні.

Використовуючи ці методи, галузь телерадіомовлення може досягти значного покращення якості послуг, позиціонуючи Україну як лідера у сфері цифрового мовлення та забезпечуючи чудові враження від перегляду для всіх громадян.

УДК 004.453 (043.2)

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

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПРИЙНЯТТЯ РІШЕННЯ НА ОСНОВІ НАЇВНГО КЛАСИФІКАТОРА БАЙЄСА

Прийняття рішень – це фундаментальний людський процес, який лежить в основі нашої взаємодії зі світом. Люди приймають як хороші, так і погані рішення. Існує багато факторів, що впливають на прийняття рішень, і в інформаційну еру їх стало ще більше. Система прийняття рішень (СПР) – це комп'ютерна автоматизована система, метою якої є допомога людям у прийнятті рішень у складних умовах для забезпечення повного та об'єктивного аналізу. З розвитком технологій системи прийняття рішень почали використовувати методи штучного інтелекту для посилення та покращення підтримки осіб, що ухвалюють рішення. Такі інструменти штучного інтелекту, як нечітка логіка, міркування на основі конкретних ситуацій, еволюційні обчислення, штучні нейронні мережі, машинне навчання та інтелектуальні агенти, у поєднанні зі СПР, надають велику допомогу у вирішенні складних прикладних завдань. Ці завдання часто виконуються в режимі реального часу, включають великі обсяги розподілених даних. Такі системи отримали назву інтелектуальні системи прийняття рішень(ІСПР). Галузі застосування ІСПР простягаються від підтримки охорони здоров'я до ухвалення управлінських рішень, і всі вони здатні покращити процес ухвалення рішень людиною.

Класифікація в інтелектуальних системах прийняття рішень - це важливий процес, який сприяє ефективному прийняттю рішень. Він передбачає розподіл даних на різні групи або класи на основі їхніх характеристик. Цей процес має велике значення в різноманітних областях, таких як бізнес, медицина та інші, де він може сприяти розподілу документів, медичних аналізів або пацієнтів на відповідні групи. Наївний Байєсівський класифікатор є одним з найпростіших та найефективніших алгоритмів машинного навчання для задач класифікації. Він базується на використанні теореми Байєса з припущенням про незалежність ознак, що в реальності рідко є правдивим. Ця теорема описує ймовірність події, заснованої на попередніх знаннях, які можуть бути пов’язані з цією подією. У контексті класифікації, наївний Байєсівський класифікатор обчислює ймовірність належності об’єкта до певного класу на основі його ознак. Наївний Байєсівський кла-

сифікатор називається “наївним”, оскільки він припускає, що всі ознаки є незалежними одна від одної. Однак, незважаючи на це припущення, він часто показує високу продуктивність в різних областях, включаючи фільтрацію спаму, класифікацію тексту та медичну діагностику. Однією з головних переваг наївного Байєсівського класифікатора є його простота і швидкість. Алгоритм вимагає невеликих обчислювальних ресурсів і може бути застосований до великих наборів даних. Він також добре справляється із завданнями, де ознаки дійсно незалежні, що буває рідко, але можливо. Однак, наївне припущення про незалежність ознак є основним обмеженням цього методу. У реальних задачах ознаки часто корельовані, що може знижувати точність моделі. Незважаючи на це, наївний Байєсівський класифікатор часто виявляється досить точним завдяки його стійкості та здатності до узагальнення. Наївна модель Байєса проста у побудові і особливо корисна для дуже великих наборів даних. Окрім простоти, наївний Байєс, як відомо, перевершує навіть дуже складні методи класифікації. Його можна використовувати як для бінарних, так і для багатокласових задач класифікації. Однак, він краще працює з категоричними вхідними змінними, ніж з числовими. Для числових змінних припускається нормальний розподіл.

Прийняття рішень є важливим процесом, що піддається впливу багатьох факторів, особливо в інформаційну еру. Системи прийняття рішень спрямовані на допомогу в ухваленні рішень у складних умовах, а з розвитком технологій вони інтегрують методи штучного інтелекту, утворюючи інтелектуальні системи прийняття рішень , які здатні обробляти великі обсяги даних у реальному часі. Ці системи знаходять застосування в різних галузях, таких як охорона здоров'я та управління. Класифікація даних є важливим аспектом ІСПР, оскільки вона сприяє ефективному ухваленню рішень. Наївний Байєсівський класифікатор, який базується на теоремі Байєса і передбачає незалежність ознак, показує високу продуктивність у різних областях, незважаючи на своє наївне припущення. Його простота, швидкість і ефективність роблять його корисним інструментом для великих наборів даних, хоча залежність ознак у реальних задачах може знижувати його точність. Він знайшов застосування в багатьох реалізованих проєктах, таких як фільтрація спаму, медична діагностика, та класифікація текстів.

УДК 004.55 (043)

Миколюк І.О, Петрова Ю.В.
Національний авіаційний університет, м. Київ

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ПОБУДОВИ СУЧАСНИХ МЕРЕЖ

Побудова мережі доступу за технологією GPON є важливою за кількома причинами. По-перше, технологія GPON забезпечує гігабітні швидкості передачі, що дозволяє підтримувати швидкий інтернет, відеоконференції та інші ресурсоємні додатки. По-друге, пасивна оптична мережа використовує мінімальну кількість активного обладнання, що знижує витрати на електроенергію та обслуговування. По-третє, Оптичні волокна менш схильні до електромагнітних завад та забезпечують стабільне з'єднання навіть на великі відстані. По-четверте, GPON легко масштабується, дозволяючи додавати нових користувачів та послуги без значних змін в інфраструктурі. PON - це технологія пасивної оптичної мережі, яка використовує оптичні сплітери для розподілу сигналу від одного оптичного передавача до кількох приймачів без використання активних елементів між ними. Основна концепція PON полягає в тому, що оптичний сигнал від передавача (OLT - Optical Line Terminal) передається через пасивний сплітер, який розділяє сигнал на кілька оптичних ліній, що ведуть до оптичних мережевих терміналів (ONT - Optical Network Terminal) у кінцевих користувачів. Це забезпечує значну економію витрат на електроенергію та обслуговування, оскільки в мережі немає потреби в живленні проміжних компонентів. GPON (Gigabit Passive Optical Network) - це покращена версія PON, яка забезпечує набагато вищі швидкості передачі даних. GPON підтримує швидкість до 2.5 Гбіт/с на завантаження та 1.25 Гбіт/с на завантаження, що дозволяє забезпечити високоякісний інтернет, відео в реальному часі та голосові послуги через одне оптичне волокно. GPON використовує методи мультиплексування (наприклад, TDM - Time Division Multiplexing) для ефективного управління різними типами трафіку, що підвищує загальну ефективність мережі. Також є основні проблеми при побудові мережі PON які включають обмежену дальність передачі сигналу та загасання сигналу, що впливають на якість з'єднання; загрози безпеці даних через можливість перехоплення; складність обслуговування та діагностики пасивних компонентів; та обмежену масштабованість

через обмежену кількість портів на OLT. Для вирішення цих проблем використовуються високоякісне оптоволокно, потужні передавачі та чутливі приймачі, методи шифрування та автентифікації, спеціалізовані інструменти для моніторингу та діагностики, а також планування додаткових портів або OLT для майбутнього розширення мережі. Проектування PON (Passive Optical Network) мережі включає в себе комплексний підхід до створення оптичної інфраструктури з метою ефективного розподілу інтернет-послуг. Першим кроком є аналіз вимог користувачів, який визначає необхідну пропускну здатність та типи послуг. Після цього вибирається оптимальна топологія мережі (зірка, дерево тощо) з урахуванням географічного розташування користувачів і майбутнього росту мережі. Планування включає в себе розрахунок маршрутів прокладки оптичних кабелів, вибір підходящого обладнання (ONT, OLT) та забезпечення сумісності з існуючими мережевими системами. Надійність мережі забезпечується за рахунок резервних маршрутів та регулярного тестування перед впровадженням у реальні умови. Побудова мережі доступу пропонується на прикладі міста Полонне за технологією GPON (Gigabit Passive Optical Network) має велике значення з різних аспектів, це сприяє розвитку цифрової інфраструктури та забезпечує мешканцям швидкий та надійний доступ до інтернету з високою пропускною здатністю. Для побудови мережі використовувався оптичний термінал GP3600-16B. Він відповідає стандартам ITU-T G.984 / G.988 для GPON OLT. Він підтримує CTC2.0, автоматичне виявлення ОНУ різних виробників і має асиметричну швидкість передачі: uplink 1,25 Гбіт/с і downlink 2,5 Гбіт/с. З коефіцієнтом розподілу до 1:128, тобто дане обладнання дозволяє використовувати коефіцієнт розподілу до 128 абонентів на гілку, в загальному 2048 абонентів, що дає можливість мінімізувати фінансові вкладення при побудові мережі. Пристрій забезпечує ефективне використання Ethernet для надійних послуг. Він підтримує маршрутизацію (RIP, OSPF, BGP), SLA, DBA і застосовує сучасний Ethernet чіпсет, що забезпечує високу якість обслуговування. Така мережа покращить якість життя мешканців, надаючи можливість використовувати сучасні цифрові сервіси, такі як відеозв'язок, стрімінгові послуги та хмарні додатки. Крім того, вона сприятиме розвитку інтернету речей, що може покращити ефективність управління міською інфраструктурою, зменшуючи витрати на енергію та забезпечуючи більшу безпеку та комфорт для мешканців.

УДК 699.81: 654.924

А.С. Молчанов
І.П. Омельчук
Національний авіаційній університет, м. Київ

ІНФРАЧЕРВОНІ КОРДОНИ ОХОРОНИ ОБ'ЄКТУ

Інфрачервоні (ІЧ) кордони є складовими підсистемами інтегрованих систем охорони підприємств та сигналізації про наявність порушників. Зокрема вони застосовуються у аеропортах, де до об'єктів охорони відносяться: радіоелектронні системи, що забезпечують управління повітряним рухом; стоянки та ангари повітряних суден; інші об'єкти підвищеної небезпеки – склади горюче-мастильних матеріалів, зберігання зброї, вибухових речовин.

Зазвичай охоронні системи великих підприємств утворюються як один інтегрований комплекс з функціонально доповнюючими одна одну такими підсистемами: охорони та сигналізації; контролю та управління доступом; охоронно-пожежної та тривожної сигналізації; охоронного відео, ІЧ-бар'єри на окремих об'єктах. Таке об'єднання дає можливість розв'язувати задачі щодо комплексної безпеки підприємства з максимальною ефективністю, саме завдяки їх взаємодії, обміну інформацією та централізованому комп'ютерному мережевому керуванню. Оператор має повну картину про функціонування об'єкта, що охороняється, та стан його підсистем

Основне призначення ІЧ-кордонів – це побудова охоронних периметрів навколо важливих об'єктів, які фіксують перетин порушником їх кордонів. Вони забезпечують максимальну оперативність й точність виявлення місця проникнення порушника, що є вирішальним для оперативного реагування підрозділами охорони.

ІЧ-бар'єр складається з передавача ІЧ-сигналу та ІЧ-приймача, які розташовуються один навпроти одного. Так формується невидимий кордон, перетин якого порушником призводить до переривання променів і, відповідно, видається сигнал тривоги. ІЧ передавачі та приймачі можна встановлювати та маскувати зверху або вздовж огорожі, або над поверхнею землі, або камуфлювати у зовнішніх ліхтарях.

Окремо означимо оптичну систему, завдяки якій створюються дуже вузькі області кордону до 2-3 градусів, що дає змогу із незначною потужністю ІЧ-випромінювання забезпечити дальності охорони 200–250 м із врахуванням всіх заважаючих метеофакторів.

Основні вимоги до ІЧ-кордону насутпні:

– повне покриття лінії периметра без сліпих зон;

– достатня чутливість датчиків для розпізнати всіх спроб порушення периметра;

– можливість зміни параметрів для відокремлення тривожних подій від явищ природи в умовах значного поглинання ІЧ-сигналу в тумані, дощі й снігом;

– мінімальний час затримки передачі даних про порушення у інтегровану систему та на виконавчі пристрої.

Живлення випромінюючого ІЧ-діоду може здійснюватися імпульсним модулюючим сигналом частотою 36 кГц з періодом 5 мс. Інтенсивність випромінюваного ІЧ-світла визначається струмом через діод. Довжина хвилі ІЧ-променю варіюється у різних пристроях і лежить у діапазоні від 0,76 до 1,1 мікрона. Якщо між ІЧ-передавачем та ІЧ-приймачем відсутні перешкоди, то на приймач надходить періодичний сигнал. Коли між ним з'являється порушник, то на цей час сигнал до приймача не поступає, що фіксується у приймачі пристроєм обробки та з невеликою затримкою формується сигнал тривоги. У просторі до ІЧ-сигналу додаються також шум та інші завади.

У ІЧ-бар'єрах невеликої дальності до 10 м можна використовувати звичайні випромінювачі та фотодіоди. Але для потреб до 200 м вже необхідно застосовувати спеціалізовані мікросхеми, де є вбудовані каскади для формування та обробки сигналів. Зокрема, у мікросхемі ІЧ-приймача здійснюється обробка, починаючи з чутливого ІЧ-елемента, далі фільтрація, автоматичне регулювання підсилення, детектування.

Окремо необхідно означити доцільність застосування мікропроцесорів, наприклад типу PIC чи ATtiny, у створенні модулів ІЧ-передавача та ІЧ-приймача. Зазвичай, вони здійснюють управління (реалізацію алгоритму) процесом вимірювання у реальному часі, обробку дослідних даних, зберігання та виведення результатів вимірювання, що є характерним для роботи ІЧ-кордонів. Оскільки уся логіка роботи ІЧ-модулів реалізується мікропроцесорами, то їхні функціональні схеми є достатньо елементарними; неперервну роботу вони починають з моменту включення живлення.

ІЧ-кордони є ефективним технічним засобом охорони периметру віддалених об'єктів підприємств.

УДК 621.396 (043.2)

М.Ю. Паламарчук
Національний авіаційний університет, м. Київ

VIDEO COMPRESSION IN DIGITAL VIDEO BROADCASTING

Video compression plays a crucial role in digital video broadcasting (DVB), facilitating efficient transmission and storage of video content. In a world where high-definition and ultra-high-definition video are becoming standard, the need for effective compression algorithms is paramount. This paper explores the principles of video compression, the various compression standards utilized in DVB, and their impact on video quality and bandwidth requirements.

Let's take a look at Principles of Video Compression

Video compression involves reducing the size of video files while maintaining acceptable quality. The fundamental techniques include:

Spatial Compression: Reduces redundancy within a single frame using methods like the Discrete Cosine Transform (DCT) to compress image data.

Temporal Compression: Exploits redundancies between consecutive frames by encoding only changes from one frame to another, often using motion vectors and predictive coding.

Compression Standards in DVB

Several key standards are used in digital video broadcasting, each offering different benefits and trade-offs:

MPEG-2: One of the earliest and most widely adopted standards, MPEG-2 is known for its balance between compression efficiency and video quality. It is used extensively in DVD and broadcast television.

MPEG-4 AVC (H.264): Provides significantly better compression efficiency compared to MPEG-2, making it ideal for high-definition content. H.264 achieves high quality at lower bit rates, which is crucial for streaming and broadcasting.

HEVC (H.265): The successor to H.264, HEVC offers about twice the compression efficiency of its predecessor, supporting 4K and higher resolutions. Its adoption is growing in contexts where bandwidth is limited but high quality is required.

Impact on Video Quality and Bandwidth

Video compression directly impacts both the visual quality of the video and the bandwidth required for transmission. Key considerations include:

Bit Rate: Lower bit rates reduce bandwidth usage but can lead to noticeable quality degradation if not managed properly.

Resolution and Frame Rate: Higher resolutions and frame rates require more data, thus more efficient compression is essential to prevent excessive bandwidth consumption.

Latency: In live broadcasting, the compression algorithm must also minimize latency to ensure real-time transmission.

Advances in Video Compression

Recent advancements focus on improving compression efficiency and video quality through:

Artificial Intelligence and Machine Learning: AI-driven compression algorithms can adaptively optimize compression settings based on content complexity.

Perceptual Video Coding: Techniques that prioritize areas of the video that are more noticeable to the human eye, thereby improving perceived quality without increasing bit rate.

Versatile Video Coding: The latest standard aims to provide even better compression efficiency than HEVC, catering to future needs such as 8K video and beyond.

Video compression is essential for the effective transmission and storage of digital video, especially in broadcasting where bandwidth is a critical constraint. By understanding and leveraging various compression standards like MPEG-2, H.264, and HEVC, broadcasters can deliver high-quality content efficiently. Ongoing advancements promise to further enhance the capabilities of video compression, ensuring that it continues to meet the evolving demands of the digital video landscape. As technology progresses, the importance of optimizing video compression will only grow, ensuring that viewers receive the best possible experience while conserving valuable bandwidth resources.

References

1. Books:

Richardson, Iain E.G. "H.264 and MPEG-4 Video Compression: Video Coding for Next-generation Multimedia." John Wiley & Sons, 2003.

"Video Coding: An Introduction to Standard Codecs" by Iain E. Richardson. This book provides an overview of various video compression standards and their applications.

2. Academic Papers:

"A Technical Overview of HEVC and AVC" by Gary J. Sullivan, Jens-Rainer Ohm, Woo-Jin Han, and Thomas Wiegand. IEEE Transactions on Circuits and Systems for Video Technology, 2012.

"An Overview of Video Compression Techniques" by Mohamed Elbamby, available on arXiv.

3. Standards Documentation:

MPEG-2: ISO/IEC 13818-1, "Information technology – Generic coding of moving pictures and associated audio information: Systems."

MPEG-4 AVC (H.264): ITU-T Recommendation H.264 and ISO/IEC 14496-10.

HEVC (H.265): ITU-T Recommendation H.265 and ISO/IEC 23008-2.

4. Online Resources:

Digital Video Broadcasting (DVB) Project: The official website for DVB standards.

ITU (International Telecommunication Union): Provides details on various video coding standards including H.264 and H.265.

Wikipedia Articles: These articles often provide a good overview and further references on video compression standards.

5. Industry Articles:

"Understanding Video Compression" on TechSmith's website.

"HEVC Explained" on the Bitmovin blog, providing insights into the HEVC standard and its benefits.

УДК 621.39 (043.2)

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

ТЕСТОВА МЕРЕЖА 5G: АРХІТЕКТУРНЕ РІШЕННЯ ТА РОЗГОРТАННЯ

У контексті мереж п’ятого покоління, розгортання такого тестового стенду є передовим рішенням для українського закладу вищої освіти, оскільки створить унікальні можливості для практичного навчання та дослідження в галузі стільникових мереж зв’язку, що є надзвичайно важливим у контексті підготовки кваліфікованих кадрів для майбутнього розвитку телекомунікаційної галузі в Україні.

Аналізуючи найкращі практики розгортання тестових мереж 5G, було розроблено загальну схему мережі (рис.1), яка включає в себе ядро мережі (CORE), базову станції (RAN), інтелектуальний контролер базової станції (RIC), MEC (Multiaccess Edge Computing) та пристрої користувача (UE).

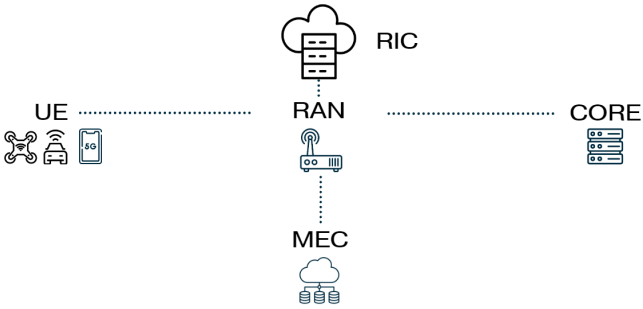


Рис.1. Високорівнева архітектура мережі 5G

Дослідження проєктів з відкритим вихідним кодом, включаючи програмну та апаратну складові мережі, показало, що найбільш оптимальною опцією розгортання тестового стенду, що являє собою MVS рішення, є використання програмних рішень від openairinterface5g (CN + gNB). У якості обчислювальних потужностей можливим варіантом є використання віртуальних машин на серверах, комп’ютерів та програмно-конфігурованих радіо (SDR).

Схема розгортання тестової мережі 5G має наступний вигляд (рис.2).

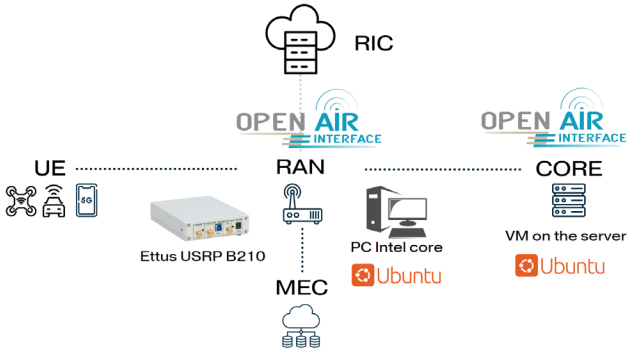


Рис.2. Схема розгортання 5G

Для розгортання тестової мережі п’ятого покоління було обрано end-to-end рішення від openairinterface5g: OAI CN 5G та OAI gNB. Після встановлення всього необхідного програмного забезпечення, налаштування апаратної складової, було відповідним чином запрограмовано SIM-картку для тестового UE. На смартфоні було виконано необхідні налаштування APN для доступу до Інтернету. Після цього було запущено базову станцію та отримано вдалу реєстрацію користувача у мережі (рис.3).

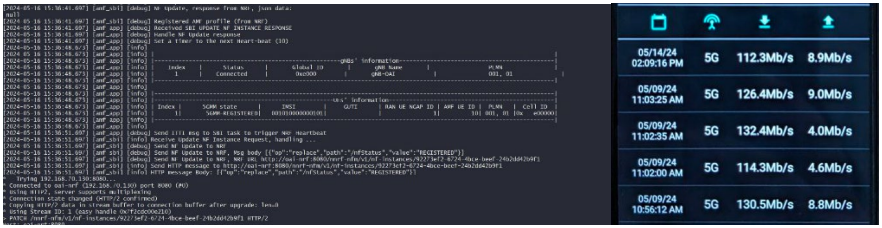


Рис.3. Реєстрація користувача у мережі

Нинішня екосистема open-source зробила 5G відкритими для всіх, хто хоче заглибитися, дослідити і вивчити роботу цих мереж. Реалізація таких тестових стендів стільникових мереж зв’язку дозволить проводити велику кількість різноманітних досліджень, експериментів та окремих наукових проєктів, зокрема у напрямку вдосконалення самих мереж, тестування різного обладнання тощо. Також це створює всі необхідні умови для навчання студентів і їх розвитку як спеціалістів у галузі телекомунікацій та радіотехніки.

УДК 621.396.96:13

М.І. Поляков
А.О. Осіпчук
Національний авіаційній університет, м. Київ

ПРОЦЕДУРА МАШИННОГО НАВЧАННЯ

Машинне навчання, є одним із найкорисніших підмножин штучного інтелекту. Процес машинного навчання починається з введення навчальних даних у вибраний алгоритм. Навчальні дані – це відомі або невідомі дані для розробки остаточного алгоритму машинного навчання. Тип введення навчальних даних впливає на алгоритм. Нові вхідні дані вводяться в алгоритм машинного навчання, щоб перевірити, чи правильно працює алгоритм.

Потім прогноз і результати перевіряються один на одного.Якщо прогноз і результати не збігаються, алгоритм перенавчається кілька разів, доки спеціаліст з даних не отримає бажаний результат. Це дає змогу алгоритму машинного навчання постійно навчатися самостійно та давати оптимальну відповідь, поступово збільшуючи точність з часом.

Машинне навчання складається з різних типів моделей машинного навчання з використанням різних алгоритмічних методів. Залежно від характеру даних і бажаного результату можна використовувати одну з чотирьох моделей навчання: під наглядом, без нагляду, напівпід наглядом або з підкріпленням.

У кожній із цих моделей може бути застосований один або кілька алгоритмічних методів – відносно наборів даних, що використовуються, і очікуваних результатів. Алгоритми машинного навчання в основному розроблені для класифікації речей, пошуку закономірностей, прогнозування результатів і прийняття обґрунтованих рішень. Алгоритми можна використовувати по одному або комбінувати для досягнення найкращої можливої точності, коли задіяні складні та більш непередбачувані дані.

Дослідження були спрямовані на вивченні процедури машинного навчання та застосування у телекомунікаційних мережах. Розглянемо застосування штучного інтелекту у SOC (security operation centre) та автоматизації її процесів. За допомогою методів штучного інтелекту розглянули покращення роботи системи, а саме зменшення витоку

інформації, швидкість і ефективність виконання процесів, значна економія часу аналітиків та запобігання вигорання персоналу.

Використання ШІ для аналізу великих обсягів даних, які не можуть бути ефективно оброблені людиною, відкриває нові можливості для захисту інформаційних систем. Така автоматизація не лише покращує швидкість та точність виявлення загроз, але й дозволяє спеціалістам концентруватися на складніших завданнях, що потребують глибокого аналізу та критичного мислення.

Застосування Ш І у SOC передбачає інтеграцію алгоритмів машинного навчання, які можуть навчатися на базі існуючих даних про інциденти, постійно вдосконалюючись та адаптуючись до нових типів загроз.

Це не лише зменшує час на виявлення та реагування на інциденти, але й дозволяє прогнозувати потенційні загрози на основі аналізу тенденцій та патернів.

УДК 043.2

В.С. Пономарьов
Національний авіаційний університет, м. Київ

СИСТЕМА БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

З розвитком технологій штучного інтелекту та автоматизації, сучасні будинки стають все більш інтегрованими та діджеталізованими. Сучасні будинки обладнуються різноманітними пристроями, що дозволяють автоматизувати багато рутинних процесів, забезпечуючи тим самим комфортне та безпечне середовище для проживання. Однак, разом з широким спектром можливостей, що надається технологіями, виникає потреба в забезпеченні належного рівня безпеки. Наявність численних підключених пристроїв, що взаємодіють між собою та з мережею Інтернет, створює потенційні ризики як для фізичної безпеки мешканців, так і для захисту їх особистих даних. Несанкціонований доступ до таких систем може призвести до значних втрат та шкоди, тому питання безпеки стає неймовірно важливим в контексті нашої сучасності.

Система безпеки розумного будинку - це складний і багатокомпонентний комплекс, що поєднує в собі різні технологічні рішення для забезпечення захисту мешканців та їхнього майна. До нього входять датчики руху, які виявляють несанкціоноване проникнення, камери спостереження, що дозволяють вести відеоспостереження в режимі реального часу, системи контролю доступу, що дозволяють отримати доступ до приміщення за допомогою біометричних даних або електронних ключів, а також розумні замки, якими можна керувати дистанційно за допомогою мобільних додатків. Ключовими особливостями таких систем є автоматичне виявлення загроз, сповіщення користувачів про небезпечні ситуації та інтеграція з іншими домашніми системами для автоматичного реагування на певні події, наприклад, увімкнення сигналізації або замикання дверей. Важливим аспектом є захист персональних даних, оскільки зібрана інформація може стати мішенню для кіберзлочинців, тому використовуються методи шифрування даних і багаторівневі системи аутентифікації. Водночас велика увага приділяється кібербезпеці, оскільки підключення до Інтернету несе в собі додаткові ризики. Сучасні підходи включають використання штучного інтелекту та машинного навчання для аналізу великих обсягів даних і виявлення

аномалій у поведінці системи, що дозволяє завчасно попередити потенційні загрози. Успішне впровадження та функціонування таких систем вимагає комплексного підходу, що включає регулярне оновлення програмного забезпечення, моніторинг потенційних вразливостей та навчання користувачів основам кібербезпеки. Технологія аналізу даних також відіграє ключову роль, дозволяючи системам вчитися на отриманій інформації та підвищувати продуктивність з часом. Використання алгоритмів машинного навчання допомагає більш точно визначити аномалії та потенційні загрози, зменшує помилкові спрацьовування та підвищує надійність системи. Щоб забезпечити безпеку розумного будинку, необхідно враховувати не тільки фізичні вторгнення, а й різні сценарії можливих загроз, таких як техногенні аварії, стихійні лиха та інші непередбачені події. Для цього система може бути інтегрована з іншими важливими побутовими системами, такими як пожежна сигналізація, системи витоку газу і води, і при необхідності може автоматично надавати екстрені служби.

По закінченню цієї роботи було створено детальне креслення системи безпеки для розумного будинку. Проект містить розміщення всіх необхідних компонентів, таких як відеокамери, датчики руху, сигналізації та інші, що забезпечують оптимальне покриття і функціональність системи. Ретельне розміщення кожного елемента відбувалося з урахуванням його функціонального призначення та оптимальних точок установки для максимально ефективної роботи системи безпеки. При розробці креслень враховувалися не тільки технічні аспекти, а й ергономіка та естетика, щоб система безпеки могла бути інтегрована в загальний дизайн будівлі. Увагу також було приділено можливості майбутнього розширення та модернізації системи відповідно до потреб майбутніх користувачів. Даний проект являє собою значний етап на шляху до безпечного та придатного для життя розумного будинку, в якому система безпеки відіграє ключову роль у забезпеченні комфорту та безпеки мешканців.

УДК 004.056:658.5 (043.2)

Анна ПРИЄМСЬКА, Віталій КУРУШКІН
Національний авіаційний університет, м. Київ

ЗАХИЩЕНА ІНФОРМАЦІЙНА СИСТЕМА ПІДПРИЄМСТВА

В сучасному світі інформаційні системи відіграють важливу роль у діяльності підприємств. Вони забезпечують збір, аналіз, зберігання та передачу інформації, що є основою прийняття рішень та успішної діяльності організації. Однак, разом з розвитком технологій зростає і загроза для інформаційних систем підприємств з боку зловмисників. Тому захист інформаційних систем стає надзвичайно важливим завданням для будь-якої організації.

Поняття захищеної інформаційної системи (ЗІС) - це комплекс програмно-апаратних засобів та технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, що обробляється та зберігається в межах підприємства.

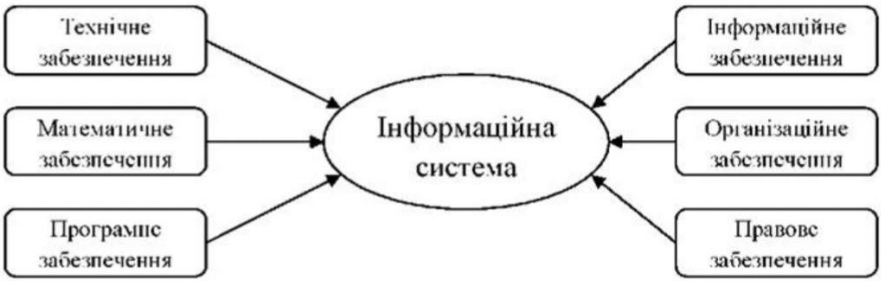


Рис. 1. Структура інформаційної системи

Захист інформаційних систем підприємств базується на комплексному підході, який включає в себе розробку політик безпеки, впровадження технічних та організаційних заходів забезпечення безпеки інформації, а також навчання персоналу.

Одним з основних понять в захисті інформаційних систем є інформаційна безпека. Це стан системи, при якому вона захищена від неправомірного доступу, втрати чи порушення конфіденційності, цілісності та доступності інформації.

Класифікація інформаційних систем. Інформаційні системи підприємств можна класифікувати за різними ознаками. Одна з найпоширеніших класифікацій базується на масштабах застосування ін-

формаційних систем. За цією класифікацією інформаційні системи підприємств можна розділити на такі типи:

1. Системи підтримки операційної діяльності (ОСП). Ці системи використовуються для автоматизації операційних процесів підприємства, таких як замовлення, виробництво, логістика тощо.

2. Системи управління підприємством (СУП). Ці системи використовуються для планування, контролю та прийняття рішень на різних рівнях управління підприємством.

3. Системи підтримки прийняття рішень (СПР). Ці системи надають підтримку прийняття рішень на основі аналізу великих обсягів даних та моделювання ситуацій.

4. Системи електронної комерції (ЕК). Ці системи використовуються для здіійснення електронних торгівельних операцій, здійснення електронних платежів та інших операцій, пов’язаних з електронною комерцією.

Висновок. Створення та підтримка захищених інформаційних систем є необхідною умовою для успішної діяльності сучасного підприємства. Врахування ключових аспектів захисту інформації допомагає забезпечити безпеку, доступність та цілісність даних, що є критичним для збереження довіри клієнтів та відповідності вимогам законодавства.

Список використаної літератури

1. Бєлов О. В. Захист інформації в інформаційно-комунікаційних системах: навч. посіб. / О. В. Бєлов, О. О. Коваленко. – Київ: КНЕУ, 2017. – 332 с.
2. Бондаренко В. Ф. Захист інформації в комп'ютерних системах: навч. посіб. / В. Ф. Бондаренко, В. І. Бондаренко. – Київ: КНЕУ, 2019. – 368 с.
3. Бондарчук О. В. Захист інформації в інформаційних системах: навч. посіб. / О. В. Бондарчук, Н. В. Бондарчук. – Київ: КНЕУ, 2018. – 320 с.
4. Василенко В. О. Захист інформації в інформаційно-телекомунікаційних системах: навч. посіб. / В. О. Василенко, О. В. Коваленко. – Київ: КНЕУ, 2016. – 304 с.

УДК 629.7.01 (043.2)

М.О. Примачок
Національний авіаційний університет, м. Київ

РОЗРОБКА БЕЗПІЛОТНОГО ДИСТАНЦІЙНО-ПІЛОТОВАНОГО ЛІТАЛЬНОГО АПАРАТУ

Безпілотні літальні апарати (БПЛА) зайняли багато важливих ніш в сучасному житті, вони широко використовуються для спостереження, картографії, сільськогосподарській сфері, кінематографії, доставці вантажів, а також в оборонній сфері. Розробка БПЛА різних типів є сучасним та актуальним питанням і потребує подальших досліджень компоновки та систем керування, рушіїв тощо.

Умовно всі БПЛА можна розділити на категорії, наприклад

1. За типом крила;
2. За типом двигуна;
3. За способом управління польотом;
4. За напрямком зльоту/посадки.

Основними складовими частинами БПЛА є наступні компоненти:

1. Корпус – є основою конструкції літального апарату, яка несе на собі всі компоненти та захищає їх від механічних пошкоджень, також забезпечує аеродинамічні властивості.

2. Мотори – виробляє тягу, яка штовхає дрон вперед (або вверх), що дозволяє йому літати.

3. Регулятори обертів (англ. Electronic Speed Controller, ESC) – регулюють швидкість обертання моторів. Впливають на швидкість та маневреність БПЛА.

4. Політний контролер – мозок БПЛА, виконує функції керування польотом, стабілізації, навігації.

5. Радіоприймач – приймає сигнал для керування літальним апаратом від ПДУ або наземної станції.

6. Апаратура керування – це система з декількох пристроїв для керування польотом БПЛА.

7. Джерело живлення – забезпечує енергією всі системи дрона: двигуни, сервоприводи, політний контролер та іншу електроніку.

8. Сервоприводи – використовують для керування рульовими поверхнями, такими як кіль (англ. Rudder), стабілізатор (англ. Elevator), елерони (англ. Aileron).

9. Телеметрія – передає дані про стан БПЛА на пульт дистанційного керування або на наземну станцію.

А також є опціональні складові, наприклад система відеопередачі – складається з камери та відеопередавача, дає змогу спостерігати за місцевістю під час польоту або збирати дані за допомогою специфічних типів камер.

Після аналізу структурних схем БПЛА, будови модулів та особливостей конструкцій БПЛА було запропоновано наступну структурну схему літального апарату, що включає в себе корпус, виготовлений з армованого екструдованого пінополістиролу, двох безщіткових електродвигунів, літієвого акумулятора номінальною напругою 16.8 вольта та ємністю 4 А/г, двох електронних регуляторів обертів, політного контролера, приймача сигналу глобальної системи навігації GPS, чотирьох сервоприводів, радіоприймача системи керування на частоті 2.4 ГГц, передавача телеметрії на частоті 868 МГц, відеокамера та відеопередавача на частоті 5.8 ГГц. Частотна диференціація передавачів різних систем забезпечує стійкий зв’язок та відсутність взаємних завад.

За результатами підбору модулів та компоновки було отримано БПЛА з нерухомим крилом, з дистанційним керуванням з наземної станції, управління відбувається за протоколом ELRS, телеметрія передається за протоколом Mavlink, з запуском з рук оператора. Контроль польоту здійснюється комбіновано, по показникам телеметрії, візуальному спостереженню оператора та по відеоканалу, за допомогою бортової камери БПЛА.

Даний БПЛА може мати широке застосування в різноманітних сферах, таких як навчання, візуальний контроль місцевості, охорона місцевості тощо. Можливості політного контролера допускають підключення додаткових різноманітних датчиків, що може розширити сфери застосування даного літального апарату. Отриманий БПЛА є відносно дешевим, ефективним та технологічним.

УДК 004.056.9.032 (043.2)

Олександр САВЧЕНКО, Веніамін АНТОНОВ, Денис БАХТІЯРОВ
Національний авіаційний університет, м. Київ

СИСТЕМА СТЕГОАНАЛІЗУ ЗОБРАЖЕНЬ НА ПРЕДМЕТ ПРИХОВАНОЇ ІНФОРМАЦІЇ

У цифрову епоху, коли обмін інформацією став надзвичайно широким та швидким, виникає необхідність забезпечення конфіденційності, цілісності та аутентичності передаваної інформації. Одним із методів захисту інформації є стеганографія - наука про таємне приховування інформації в невидимій формі. Як результат, зростає значення розвитку методів стеганалізу, які спрямовані на виявлення та аналіз прихованої інформації у різних типах мультимедійних даних. Особливо актуальною стає проблема стегоаналізу зображень, оскільки зображення є одним із найбільш поширених та важливих типів мультимедійних даних. Засоби стеганографії дозволяють приховувати інформацію у зображеннях, зберігаючи зовнішній вигляд останніх майже без змін. Однак виявлення такої прихованої інформації має важливе значення для забезпечення безпеки та інтегритету даних у різних сферах, включаючи кримінальне розслідування, контррозвідку та цифрове обладнання для захисту авторських прав. В даному дослідженні ми розглянемо систему стегоаналізу зображень, спрямовану на виявлення прихованої інформації. Ми дослідимо різні підходи та методи, що використовуються для аналізу зображень з метою виявлення стеганографічних артефактів. Дослідження включатиме як класичні методи, так і сучасні техніки машинного навчання та обробки сигналів, спрямовані на покращення ефективності виявлення прихованої інформації в зображеннях. Це дослідження має на меті розширення розуміння проблеми стеганографії та стегоаналізу в контексті зображень, а також розвиток ефективних інструментів для виявлення та аналізу прихованої інформації в цьому типі мультимедійних даних. Надійне виявлення та аналіз стеганографічних артефактів у зображеннях відіграє важливу роль у забезпеченні безпеки та конфіденційності інформації в сучасному цифровому середовищі.

Було розроблено таку архітектуру автоматизованої системи на основі розробленої моделі нейронної мережі та завдання:

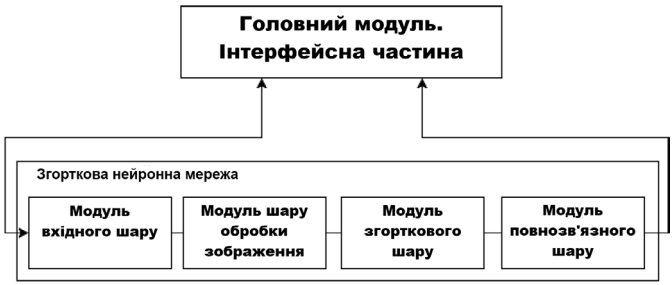


Рис. 1. Архітектура системи

У вікні головного модуля користувач вказує зображення-контейнер або масив зображень, що перевіряється. Наступним кроком є передача зображення модулю вхідного шару нейронної мережі. Після цього він передається модулю обробки шару зображення, де його потрібно буде обробити операцією фільтрації. Наступний модуль описує функції згорткового шару. У ньому застосовуються операції згортання та гауссової нелінійності до карт ознак. Після цього в модулі класифікаційного шару виводиться рішення про класифікацію у вигляді числового значення, яке знаходиться в діапазоні від 1 до 0. Рішення виводяться або у вікно головного модуля, або у файл, який зберігається в домашній директорії користувача, якщо це масив зображень.

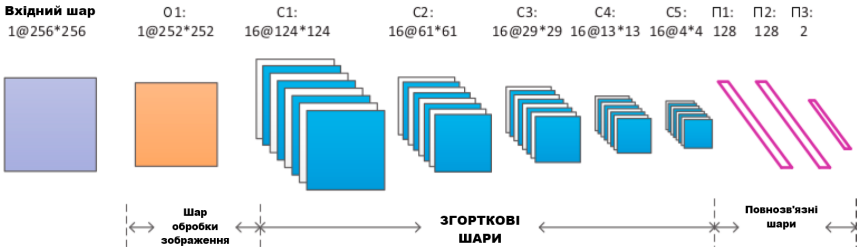


Рис. 2. параметри згорткової нейронної мережі цієї системи. Кількість карт характеристик a і роздільна здатність b * b відповідного шару вказується у формі «a@b*b»

Алгоритм зворотного поширення використовувався для навчання ГЗНМ шляхом мінімізації - log yt, де t ∈ {1,2} позначає цільовий клас. У згорткових і повністю пов’язаних шарах стандартні помилки та ада-

птація до ваги. Процес описано в [3]. Одним словом, усі параметри в рівнях класифікації та вилучення ознак оптимізуються разом.

Вхідне зображення з ядром розміром 5 × 5 фільтрується першим згортковим шаром. З 16 ядрами розміром 5 × 5, другий згортковий шар приймає сигнал першого рівня як вхідний і фільтрує його. П'ятий, четвертий і третій згорткові шари використовують згортки з 16 ядрами розміром 3 на 3. Все вихід другого-п’ятого згорткового шару отримує гаусову нелінійну функцію. Тим часом операція усередненого об’єднання, яка має розмір вікна 3 на 3 і крок величиною 2, виконується за кожним із другого-п’ятого згорткового рівня. Ця операція впливає на кожну карту ознак у відповідному згортковому шарі, що призводить до такої ж кількості карт просторових об’єктів зі зменшеною просторовою роздільною здатністю. Нарешті, 256 ознак, які були витягнуті, передаються в модуль класифікації, який складається з трьох повнозв’язних шарів. У перших двох повнозв’язаних шарах міститься 128 нейронів. Функція Rectified Linear Units (ReLUs) активує вихід кожного нейрона в перших двох повністю зв’язаних шарах ГЗНМ, коли f(x) =max(0, x) [4]. Два нейрони складають останній повнозв’язний шар, і його сигнал передається на двосторонню нормовану нормовану експоненціальну функцію активації.

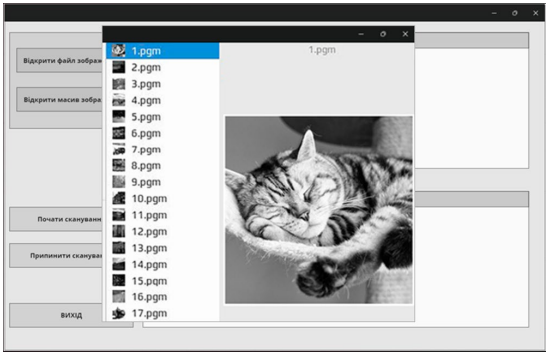


Рис. 3. Діалогове вікно вибору файлу/файлів

Висновок. У даному дослідженні була розроблена архітектура автоматизованої системи, яка базується на моделі нейронної мережі для стегоаналізу зображень. Ця система пропонує ефективний метод виявлення та аналізу прихованої інформації в мультимедійних даних, зокрема в зображеннях. Архітектура системи включає модулі для об-

робки зображень, згорткового шару та класифікації, кожен з яких відповідає за конкретну частину процесу аналізу. Після введення зображення-контейнера або масиву зображень користувачем, система проводить аналіз шляхом передачі даних через вказані модулі та виводить результат класифікації у вигляді числового значення. Застосування алгоритму зворотного поширення у навчанні моделі нейронної мережі дозволяє досягти ефективності та точності виявлення прихованої інформації у зображеннях. Використання стандартних помилок та адаптації до ваги у згорткових і повністю пов'язаних шарах сприяє оптимізації параметрів моделі. У висновку, розроблена система має потенціал для застосування у різних областях, включаючи кримінальне розслідування, цифрову безпеку та захист авторських прав. Подальші дослідження можуть спрямовуватися на вдосконалення архітектури системи та методів аналізу для досягнення ще вищої ефективності та точності виявлення прихованої інформації в зображеннях.

Список використаних джерел

1. N. Nahar, M. K. Ahmed, T. Miah, S. Alam, K. M. Rahman and M. A. Rabbi, "Implementation of Android Based Text to Image Steganography Using 512-Bit Algorithm with LSB Technique," 2021 5th International Conference on Electrical Information and Communication Technology (EICT), Khulna, Bangladesh, 2021, pp. 1-6.
2. Q. AL-Durrah and T. A. AL-Assadi, "Image Steganography Based on Pixel Topology and Threshold on Selected Pixels Differences," 2023 6th International Conference on Engineering Technology and its Applications (IICETA), Al-Najaf, Iraq, 2023, pp. 491-496.
3. K. Vandana and S. K. Kumari, "Improving Security with Efficient Key Management in Public cloud using Hybrid AES, ECC and LSB Steganography comparing with Novel hybrid Cube Base Obfuscation," 2022 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2022, pp. 1-6.
4. W. Peng, T. Wang, Z. Qian, S. Li and X. Zhang, "Cross-Modal Text Steganography Against Synonym Substitution-Based Text Attack," in IEEE Signal Processing Letters, vol. 30, pp. 299-303.

УДК 004.453 (043.2)

В.В. Самойленко
Національний авіаційний університет, м. Київ

РОЗГОРТАННЯ МЕРЕЖЕВИХ ДОДАТКІВ У КОНТЕЙНЕРИЗОВАНОМУ СЕРЕДОВИЩІ З ВИКОРИСТАННЯМ KUBERNETES

Швидкий розвиток інформаційних технологій та поширення мікросервісної архітектури в сучасному програмному забезпеченні вимагає відповідних рішень для підтримки та обслуговування розподілених прогам. З кожним днем ми бачимо, як контейнеризація стає все більш популярним вибором для розгортання додатків, так як вона має ряд переваг над традиційними методами розгортанням програмного забезпечення. Спрощення розгортання, масштабування і керування додатками забезпечується ізольованим та стандартизованим середовищем виконання. Але при збільшенні числа контейнерних додатків постає потреба у ефективному їх управлінні. При вирішенні важливих бізнес-задач або наданні сервісів клієнтам число контейнерних додатків може вимірюватися десятками, тому питання підвищення операційної ефективності залишається і по сей день.

В традиційній серверній архітектурі фізичний комп'ютер, сервер, використовується для розгортання обмеженої кількості аплікацій. Встановлюючи аплікації загального призначення на традиційну серверну архітектуру ми, у більшості випадків, зіткнемося з великою кількістю невикористаних ресурсів, оскільки при потребі розгортанні нової аплікації не відомо, які ресурси потребує саме ця аплікація. Це приводити до додаткових витрат та простою ресурсів, які можна було б виділити іншим аплікаціям. Віртуалізація широко використовується у хмарних технологіях, де реалізується модель «орендування» ВМ. Тобто користувач може орендувати лише ті обчислювальні потужності ВМ, які задовольняють його потребу. Це усуває необхідність у придбанні виділених серверів під окремі аплікації. У будь-який момент користувач має право зупинити оренду таких потужностей, що збільшує економію та підвищує ініціативу використання такої моделі. Контейнеризація є відносно новою технологією, яка намагається розв'язувати проблеми та обмеження віртуальних машин. Разом з появою контейнеризованих аплікації з'являється новий архітектурний стиль взаємодії між собою додатків – мікросервіси. При використанні цього ар-

хітектурного стилю аплікація розбивається на декілька малих сервісів, кожний з яких може існувати незалежно один від одного. ВМ та контейнери обоє є прикладами віртуалізації обчислювальних ресурсів. Головна відмінність контейнерів від ВМ закладається в тому, які саме частини ОС вони віртуалізують. Ядро ОС є посередником, яке дозволяє процесам програмних застосунків безпечно використовувати ресурси апаратного забезпечення комп'ютера. Ядро ОС не віртуалізується контейнерами, замість нього використовується ядро гостьової ОС, що дозволяє полегшити об'єми та час запуску контейнерів. Для оркестрування контейнерів ми можемо використовувати відповідне програмне забезпечення. Провідною технологією в управлінні контейнерами є Kubernetes. Головна ціль програмного забезпечення оркестрації контейнерних додатків Kubernetes полягає саме в автоматизації процесу їх розгортання, управління та масштабування. Це дозволяє оптимізувати низку процесів, які до цього виконувалися вручну. Kubernetes складається з багатьох базових компонентів, такі як кластер, вузол, площина керування, «kube-apiserver», «controller manager» і т.д. Площина керування приймає глобальні рішення щодо стану кластера, а також реагує на різні події всередині кластеру, приймаючи відповідні дії щодо них. Саме ця характеристика Kubernetes надала потужності та популярності даному інструменту. Дана технологія має властивості самозцілення: при раптовій зупинці контейнера Kubernetes буде намагатися відновити контейнер з попередніми конфігураціями.

Підхід розгортання мережевих додатків з використанням контейнеризації та оркестрування останніх дозволить автоматизувати процеси, гарантує відмовостійкість додатків та дозволить динамічно масштабувати інфраструктуру в залежності від трафіку та навантаження на систему. Практичним результатом виконання даної роботи є побудова образу Docker для мережевого застосунку cidr.xyz, створення конфігураційних файлів Kubernetes для даної аплікації та застосування їх на реальному обчислювальному кластеру, створеному за допомогою хмарних обчислювань та побудова і встановлення пакунку Helm у кластер Kubernetes. У результаті ми отримали мережевий додаток cidr.xyz, розгорнутий на платформі Kubernetes, встановлений за допомогою пакетного менеджера Helm, доступ до якого відбувається через доменне ім'я cidr.samoilenko.xyz та з допомогою захищеного протоколу зв'язку HTTPS.

УДК 621.396 (043.2)

A.V. Silin
National Aviation University Kyiv

IMPLEMENTING 5G NETWORKS WITH CLOUD TECHNOLOGIES: OPPORTUNITIES AND CHALLENGES

The role of 5G networks and cloud technologies is key to the current era, significantly impacting how we communicate, share information and manage data. In terms of speed, 5G networks are faster than their predecessors and therefore guarantee efficient streaming along with quick downloads due to their high speed. One notable feature of 5G is its low latency— this means that data is transferred without any delay or time lapse which makes it more reliable especially for applications such as online gaming where even milliseconds matter because of the critical nature of the information being transmitted.Through adoption of cloud services, organizations can significantly reduce costs associated with hardware procurement and maintenance— a more economical approach for small to medium enterprises would be paying for subscription-based usage. In terms of volume used.

The availability to computing resources and data from any location that has an internet connection is the main advantage of cloud computing. For instance, collaboration among remote teams is easier which means it can facilitate remote work and enhance productivity.

If we compare the LTE standard to the new generation of mobile networks we can see that Long Term Evolution uses a band below a 3Ghz to 6Ghz. In the long term, as promised, is going to have from 24Ghz to 100Ghz, which means that 5G can deliver and receive more data than the older generation. Nevertheless, we need considerably more base stations. That is because high frequency can carry more information but have much less travel distance.

One of the major features that 5G brought is the ability to divide a network into applications-specific layers for specific tasks and operations at the same time. Technologies that provide this type of innovation are network functions virtualization(NFV) and software-defined networking(SDN).

NFV is the type of virtualization that changes network components and processes to software functions that can be linked to create a communication service that spans the entire network. Resources of storage, computing and network functions can be virtualized and usually placed on commercial off-the-shelf(COTS) hardware for example servers version x86. A virtual

machine (VM) can run on a single server and extend the free resources it can consume. Also, all resources are more frequently sitting unoccupied. This is done thanks to the sending only part of available resources on servers.

Traditional networks use dedicated hardware devices (such as routers and switches) to control network traffic, but this model is not the same. By using software, you can either create and control a virtual network or control a traditional hardware.

While network virtualization allows organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server.

Software-defined networking offer way to centrally configure and manage network services. These services are routing switching and load balancing. SDN used to dynamically create, secure and connect network to meet need of your apps. Usually enterprises using SDN for application deployment, it will do it faster and lower deployment and operating cost.

The interesting thing about the 5G networks is that they use distributed sophisticated technologies to transmit data at an immense speed and with an incredibly low latency, which will let the networks connect billions of devices. Some of these technologies are the so-called Network Functions Virtualisation (NFV) and Software-Defined Networking (SDN), which contribute to the flexibility and effectiveness of such networks. Moreover, the Cloud can be configured in different ways to provide services, for example, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), according to how larger computational resources need to be manipulated and made available.

Thanks to the implementation of cloud technologies in the infrastructure of 5G networks, their functionality gets a serious boost: you can provide the best or even optimal configuration of resources and more opportunities for scaling. When the cloud infrastructure is used in the framework of 5G networks, it can adapt in real-time to the increased load and use all the capabilities of 5G networks in a more effective and economical way. This cooperation creates a multitude of possibilities, from providing the required conditions for innovative applications such as the abandonment of augmented reality (AR) and virtual reality (VR), to data storage support for IoT devices.

УДК 004.67 (043.2)

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

СИТЕМА ВІДЕОСПОТЕРЕЖЕННЯ КОМЕРЦІЙНОГО ОБ'ЄКТУ

За останні роки відеоспостереження стає невід'ємною частиною комплексної системи безпеки та аналітики комерційних об'єктів, оскільки сучасне обладнання дозволяє не тільки спостерігати і записувати відео, але і виконувати підрахунки та аналіз дій покупців на території комерційного об'єкту.

Системи відеоспостереження знаходять все більш широке застосування у сферах аналізу. До недавнього часу комп'ютерний зір і аналітика були пов'язані тільки з безпекою і захистом, тобто виявленням потенційних крадіжок, загроз для людей і місць відвідування, через обмеженність технологій минулого.

Використання систем відеоспостереження на комерційних об'єктах має велике значення при дослідженні впливів пори року на відвідуваність магазину, при аналізі та розробці маркетингових акцій на магазині, та співвідношенні потоку людей в магазині до популярності проведених акцій у той чи інший період. Такі системи стали зручним інструментом для аналітики віку та статі покупців,

Аналіз точної демографічної статистики відвідувачів за допомогою комплексів відеоспостереження та програмного забезпечення для відеоаналітики допомагає менеджерам з маркетингу та мерчандайзингу виявляти аудиторію, яку вони охоплюють, а також визначати та передбачувати нові цільові аудиторії.

Використовуючи системи відеспостереження можна зрозуміти, як різні вікові категорії покупців зазвичай переміщуються торговими точками, а також скільки часу покупці зазвичай проводять у різних зонах магазину, наприклад поряд з рекламними оголошеннями та біля вітрин з товарами. Також інформація зі звітів про кількість людей можуть бути співвіднесені з даними касових терміналів та даними про продаж, щоб ідентифікувати який відсоток людей які зайшли в магазин купила товарів та на яку суму.

За допомогою цієї дієвої бізнес-аналітики роздрібні продавці можуть приймати стратегічні рішення про заохочення клієнтів магазину,

оптимізувати мерчандайзинг і націлення, як наслідок, збільшувати конверсію.

Через зручність інтеграції системи відеоспостереження у магазин, все частіше організації та підприємства хочуть встановити таку систему та дізнаватися більше з відеокамер.

Зараз світові компанії по виробництву систем відеонагляду та розробці програмного забезпечення націлені на максимальну інформативність, велику відмовостійкість, зручності використання, довготривале зберігання, стійкість до втрати відеозапису під час внештатних відключень світла, та перегляд архівів відео з будь якої точки світу, для подальшого використання.

Зараз такі системи представлені у вигляді сукупності обладнання: відеокамер, мережевих комутаторів, мережевих відеореєстраторів, мережевих сховищь данних, компьютерів для перегляду відео архіву. Для забезпечення високої якості відео камери повинні мати роздільну здатність у форматі FullHD (1920x1080 пікселів) щоб мати можливість забезпечувати чітке зображення, яке дозволяє розпізнавати обличчя, деталі товарів, кількість готівки яку людина передає касиру, які речі передає касир покупцю (товарні чеки, решту, подарункові картки, промо-подарункі).

Камери з високою роздільною здатністю також дозволяють збільшувати окремі частини кадру з малою втратою якості зображення. Також камери відеоспостереження повинні мати функцію широкого динамічного діапазону, щоб ефективно працювати в умовах складного освітлення, наприклад, при яскравому сонячному світлі або в зонах з недостатньою яскравістью.

Завдяки цифровим системам відеоспостереження можна зберігати відео архів у мережевих сховищах, з доступом до них через мережу Інтернет, підбір мережевого сховища данних оснований на великому об’ємі архівів відео, тому для тривалого зберігання відео архіву потрібно встановлювати мережеві сховища з об’ємом від 10 до 30 терабайтів пам’яті.

Також завдяки програмному забезпеченню з широким спектром аналітичних модулів можна виконувати аналіз покупців та їх точний підрахунок.

УДК 004.934: 681.391

М.С. Смілянець
І.П. Омельчук
Національний авіаційній університет, м. Київ

ПАРАДИГМА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ПІДПРИЄМСТВА

Компетентно створена система контролю доступу (СКД) дозволяє запобігти несанкціонованому доступу особи до приміщень та на територію об'єкта і додатково вести облік робочого часу.

Аналіз сучасних СКД доводить, що вони тісно інтегровані із системами загальної та пожежної охорони, системами відеоспостереження, інженерними системами будівлі та інформаційними системами підприємства, як це означено на рис.1.

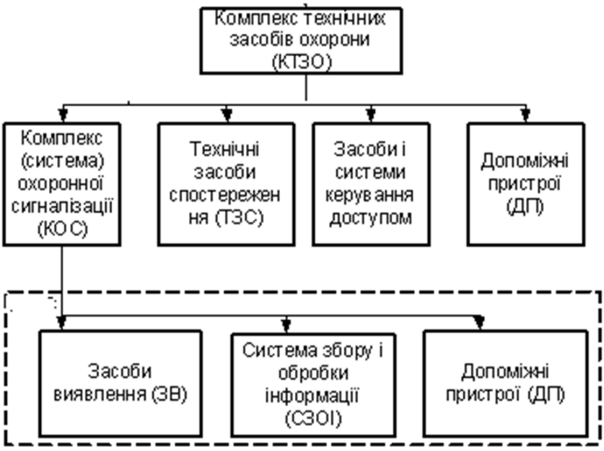


Рисунок 1 – Інтегрований комплекс технічних засобів охорони.

Всі елементи в інтегрованій СКД за допомогою управляючих контролерів поєднані комп'ютерною мережею у інтегрований комплекс (рис. 2). Це надає такі переваги:

– цілісність сприйняття поточної інформації та її збереження;
– оперативність видачі сигналів реагування на факти порушень;
– можливість підключення інших комунікаційних систем.

Одним із основних елементів СКД є мікропроцесорний контролер, який оброблює інформацію, що надходить від різноманітних іде-

нтифікаторів особи, зчитувачів карток, кодових замків, та формує сигнали прийняття рішення та управління виконавчими пристроями.

Для створення ідентифікаційних терміналів доцільно обрати типовий мікропроцесор AT89S51 фірми Atmel із апаратною архітектурою MCS-51, оскільки він має доступну ціну, відносно простий у програмуванні, а можливостей цілком достатньо для функціонування термінального пристрою.

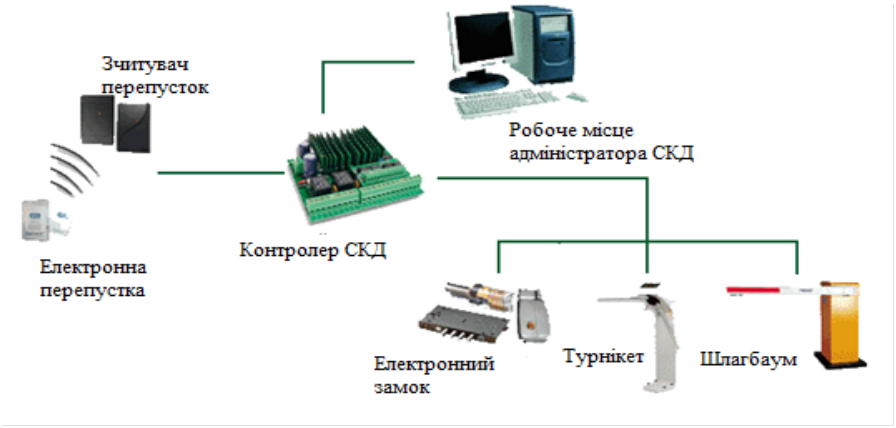


Рисунок 2 – Складові СКД на основі комунікаційної комп'ютерної мережі.

Електронні кодові замки мають істотну перевагу перед механічними, бо це високотехнологічні пристрої, що управляються мікропроцесором. Характеризуються простотою застосування, надійністю, високим рівнем захисту та легкістю зміни контрольного коду в базі.

Технологічно найбільш сучасними є системи із електронними перепустками (картками) та біометричними технологіями. Основна різниця між ними полягає у тому, що біометричні термінали ідентифікують не технічний засіб, а безпосередньо людину, і тому мають великий рівень надійності результатів.

Для поточного контролю стану вхідних дверей служить контактний датчик, сигнал якого оброблюється у мікропроцесорі.

Автоматизована система контролю доступу підприємства повинна створюватися як інтегрована складова комплексу технічних засобів охорони, а термінальні її пристрої ідентифікації працюють під керуванням мікропроцесорних контролерів.

УДК 621.39.005 (043.2)

А.П. Совгиря
Національний авіаційний університет, м. Київ

ТРАНКІНГОВА СИСТЕМА ЗВ'ЯЗКУ СТАНДАРТУ MPT1327

MPT1327 – це стандарт сигналу для транкінгових приватних наземних мобільних радіосистем. Він визначає правила протоколу зв'язку між контролером транкінгової системи (TSC) та радіоблоком користувачів. Стандарт можна використовувати для реалізації різних систем, від невеликих систем всього з кількома радіоканалами (навіть одноканальних систем), аж до великих мереж, які можуть утворюватися шляхом з'єднання TSC. Протокол пропонує широкий спектр можливостей користувача і системних опцій. Однак, немає необхідності реалізовувати всі наявні можливості. Протокол може бути реалізований відповідно до вимог користувача. Також є простір для адаптації до особливих вимог, а також передбачено подальше стандартизовані кошти, які будуть додані до протоколу у майбутньому.

Стандарт визначає лише ефірний сигнал та встановлює лише мінімальні вимоги до обмеження проектування системи. Додаткові специфікації будуть потрібні для конкретних реалізацій, наприклад, для:

- об'єктів, які необхідно реалізувати
- значення параметрів
- план каналу
- для мережі, коли радіопристрій має реєструватися.

Протокол MPT 1327 передбачає наступні види зв’язку:

- голосовий зв’язок - індивідуальний, груповий, пріоритетний; забезпечуються режими загальної розмови й оповіщення (говорить абонент, який викликає, інші слухають);
- передача даних - необмежена довжина, пріоритетна передача, груповий обмін (додаткові специфікації містяться в документі MAP 27);
- аварійний виклик - виклик із максимальним пріоритетом, голосовий зв'язок, передача даних, груповий виклик із можливістю відповіді;
- зв'язок із підключенням - сеанс двох абонентів, у якому забезпечується можливість групового виклику; може

застосовуватися для організації конференцзв'язку і переадресування викликів;

- статусні повідомлення - до 30 статусних повідомлень довжиною 5 біт (не забезпечується передача статусних повідомлень групам абонентів системи, абонентам відомчої АТС або міських АТС);
- короткі блоки даних - цифрові повідомлення до 184 біт, які передаються по каналу керування;
- у багатьох системах на базі МРТ 1327 реалізована можливість передачі по каналу керування (Extended Data Messages) розширених блоків даних, скомпонованих у чотири короткі блоки загальним розміром до 736 біт.

За багатьма параметрами, які є часом головними для відомчих, корпоративних мереж, системи зв'язку на базі протоколу МРТ 1327 перевершують функціональні можливості стільникових мереж. Наприклад, велика дальність зв'язку, що часто є одним з головних вимог корпоративних клієнтів, можливість створення груп, мінімальний час доступу до системи, мінімальний час встановлення зв'язку, динамічна перегрупування і т. д. Абонентське обладнання, що використовується в мережах МРТ 1327, має великий ресурс і високу надійність. Простіші системи транкінгового зв'язку, наприклад Smartrunk поступаються системам протоколу МРТ 1327, оскільки призначені для здійснення індивідуальних викликів і виходу в ТМЗК, а не для оперативного (групового) технологічного зв'язку. Однією із самих великих систем, розроблених на базі МРТ 1327, є мережа Chekker Network, що належить Deutsche Telekom. У цій мережі використовується устаткування ACCESSNET фірми Rohde & Schwarz; сьогодні вона нараховує приблизно 900 каналів, 160 БС і приблизно 62 тис. абонентів (у її складі - декілька транкінгових систем). Як правило, транкінгові системи на базі протоколу МРТ 1327 створюються для охоплення 1...2 тис. абонентів і розраховані на 3...5 базових станцій із 3...8 каналами на кожній із них.

УДК 621.396.67 (043.2)

Олександр ЛАВРИНЕНКО
Національний авіаційний університет, м. Київ

СИСТЕМА ШИРОКОСМУГОВОГО РАДІОДОСТУПУ НА БАЗІ АРХІТЕКТУРИ SDR

У сучасному світі, де бездротовий зв'язок стає все більш важливим для різноманітних застосувань, виникає необхідність у розвитку ефективних та гнучких систем радіодоступу. Одним із ключових напрямків в цьому контексті є використання архітектури SDR (Software-Defined Radio), яка надає можливість програмно змінювати параметри та функції радіоприймачів та передавачів. Системи широкосмугового радіодоступу на базі архітектури SDR відкривають нові перспективи у сферах зв'язку, телекомунікацій, безпеки, медичних технологій та багатьох інших. Ці системи забезпечують гнучкість та адаптивність, що дозволяє їм пристосовуватися до різних умов зв'язку та виконувати різноманітні завдання, від передачі даних до виявлення сигналів у шумному середовищі. В даному дослідженні ми розглядаємо систему широкосмугового радіодоступу, побудовану на базі архітектури SDR. Ми досліджуємо принципи роботи цієї системи, її можливості та переваги, а також розглядаємо різноманітні застосування в різних галузях технологій та комунікацій. Це дослідження спрямоване на розширення розуміння принципів та потенціалу систем радіодоступу на базі архітектури SDR, а також на сприяння подальшому розвитку цих технологій у майбутньому.

Для передавання сформованого сигналу SDR необхідно вибрати найкращий частотний інтервал, а сформований сигнал має мати найвищу концентрацію енергії в цьому частотному інтервалі та не мати великого пік-фактора. Це випливає зі складних сучасних умов передавання радіосигналів. Таким чином, було розроблено алгоритм вибору придатного для передавання, формування та обробки сигналу для вибраного частотного інтервалу. Метод, заснований на формуванні сигналу за допомогою базису власних векторів субсмугових матриць, був обраний для вирішення задачі формування сигналу з найкращою концентрацією енергії. Середовище MatLAB використовувалося для моделювання. Через те, що найважливіша вимога, яку висувають до систем радіозв’язку, є те, щоб одержувач отримав правильну інформацію від передавача. Щоб оцінити вплив завади на переданий сигнал, використовується ймовірність помилки на біт (BER).

Значення піків факторів для сигналу, сформованого за допомогою базису власних векторів субсмугової матриці, і сигналу, сформованого за класичним методом за допомогою базису Фур'є, також були порівняні. Рівень просочування енергії сигналу за межами вибраного частотного інтервалу для передачі є ще однією мірою оцінки того, наскільки запропонований метод відрізняється від традиційного.

Графіки сигналів, які були створені за допомогою базису Фур'є та власних векторів субсмугової матриці, показані на рисунку (1) і (2). Сигнал, створений за допомогою перетворення Фур'є, матиме 64 піднесучих, оскільки тривалість і частота сигналу, створеного за допомогою базису власних векторів, залишаться рівними. Сигнал, створений за допомогою базису Фур'є, було інтерпольовано за допомогою інтерполяційної формули Котельникова та відновлено до 256 піднесучих, щоб зробити порівняння отриманих сигналів більш наочним.

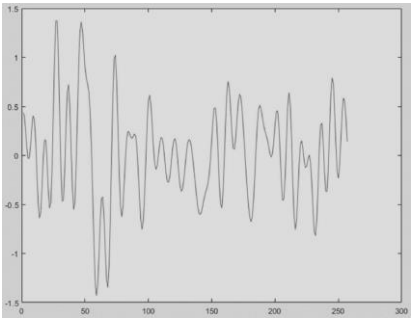


Рис. 1. Графік сигналу, створений базою власних векторів субсмугових матриць

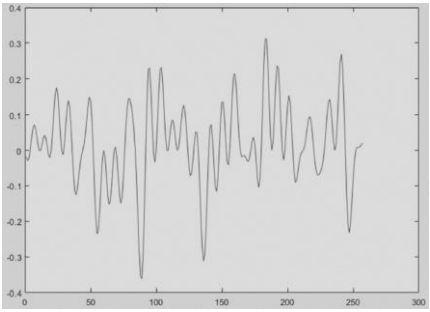


Рис. 2. Графік сигналу, створеного за допомогою базису Фур'є та інтерпольованого за формулою Котельникова

Після цього з кожним із сформованих сигналів створювався різновид перешкод із певним співвідношенням амплітуди до шуму. У цьому випадку було досліджено, як білий Гауссовський шум впливає на сигнали. Рисунок (3) і рисунок (4) показують результати моделювання.

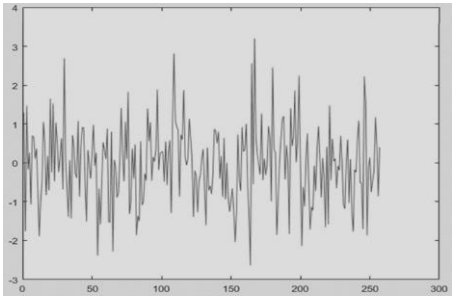


Рис. 3. Графік зашумленого сигналу, сформованого за допомогою базису власних векторів субсмугових матриць

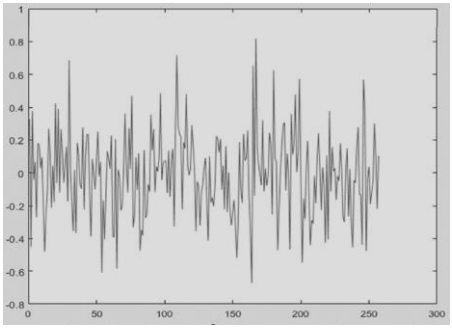


Рис. 4. Пафік зашумленого сигналу, створений за допомогою базису Фур'є

Демодулювали зашумлені сигнали та обчислювали відношення помилки на один біт прийнятого сигналу до переданого сигналу. Для демодуляції використовується пряме дискретне перетворення Фур'є. Властивості ортогональності піднесучих дозволяють реалізувати демодулятор у цифровій формі. Це дозволяє простій демодуляції сигналу OFDM за допомогою БПФ. Імовірність помилки на один біт визначали, діючи кількість помилково прийнятих біт на кількість експериментів.

Висновок. У даному дослідженні розглянуто алгоритм вибору, формування та обробки сигналу для передавання у системах радіодоступу на базі архітектури SDR. З метою досягнення оптимальної ефективності передавання, розроблено метод формування сигналу з найвищою концентрацією енергії в обраному частотному інтервалі, що враховує складні умови сучасного передавання радіосигналів. Використано алгоритм, заснований на формуванні сигналу за допомогою базису власних векторів субсмугових матриць, який дозволив досягти бажаної концентрації енергії в передаваному сигналі. Використання середовища моделювання MatLAB дозволило ефективно відтворити та дослідити характеристики сформованих сигналів. Основною метою систем радіозв'язку є забезпечення коректного прийому інформації одержувачем. З цією метою проведено оцінку впливу шуму на переданий сигнал за допомогою ймовірності помилки на біт (BER), а також порівняно значення пік-факторів для різних методів формування сигналу. Дослідження показало, що використання методу на базі власних векторів субсмугових матриць дозволяє досягти кращих результатів щодо концентрації енергії та оптимізації впливу шуму на переданий сигнал у порівнянні з класичними методами, заснованими на базисі Фур'є. Отримані результати можуть бути використані для подальшого розвитку та вдосконалення систем радіодоступу на базі архітектури SDR з метою підвищення їхньої ефективності та надійності.

Список використаних джерел

1. L. Nanna, R. Andreotti, M. Andrenacci and N. Alagha, "VDE-SAT Link ID 20 performance assessment under different random access conditions," 39th International Communications Satellite Systems Conference (ICSSC 2022), Stresa, Italy, 2022, pp. 241-247.
2. S. Dörner, J. Clausius, S. Cammerer and S. t. Brink, "Learning Joint Detection, Equalization and Decoding for Short-Packet Communications," in IEEE Transactions on Communications, vol. 71, no. 2, pp. 837-850.
3. S. Kumar et al., "OpenAirInterface as a platform for 5G-NTN Research and Experimentation," 2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 500-506.

УДК 004.056.55 (043.2)

Олександр ЛАВРИНЕНКО
Національний авіаційний університет, м. Київ

МЕТОД ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ ДАНИХ

У сучасному інформаційному суспільстві забезпечення конфіденційності та цілісності даних є критично важливим завданням. Потокове шифрування, яке базується на використанні псевдовипадкових послідовностей, є одним із ефективних методів захисту інформації під час її передачі. Ця робота присвячена розробці методу формування псевдовипадкових послідовностей, який підвищує криптографічну стійкість потокового шифрування, забезпечуючи надійний захист даних від несанкціонованого доступу та атак.

Для використання в задачах шифрування даних кожен генератор ПВП повинен мати здатність відтворювати послідовність, яка має певний початковий стан — породжувальний елемент. Цей стан дозволяє генератору відтворювати послідовність чисел, не змінюючи його алгоритм роботи.

Крім того, генератори ПВП мають період повтору послідовності, який зазвичай указується у співвідношенні ступеня двійки. Для прикладу, параметри деяких поширених генераторів ПВП, алгоритми яких реалізовано в програмному пакеті MATLAB, наведено в таблиці 1.

Таблиця 1

Параметри генераторів ПВП у MATLAB

Алгоритм	Тип генератора	Мульти-поточність	Період повтору послідовності
mt19937ar	Вихор Мерсенна	Ні	2^{19937}-1
dsfmt19937	Вихор Мерсенна типу SIMD	Ні	2^{19937}-1
mcg16807	Конгруентний мультиплікативний	Ні	2^{31}-2
mlfg6331_64	Мультиплікативний метод Фібоначчі із запізненням	Так	2^{124}
mrg32k3a	Комбінований багаторекурсивний генератор	Так	2^{127}
shr3cong	Генератор зсувних регістрів, модифікований лінійним конгруентним генератором	Ні	2^{64}
swb2712	Модифікований відніманням із генератором запозичень	Ні	2^{1492}

Крім того, генератори мають здатність працювати з кількома потоками, що дозволяє використовувати мультипотокові обчислювальні алгоритми для обчислення числової послідовності. Для створення криптостійких методів формування ПВП для шифрування цей параметр є важливим. Крім того, багато сучасних систем підтримують апаратне опрацювання мультипотоку, тому мультипоточність є важливим параметром для сучасного генератора ПВП.

Продуктивність алгоритму — це ще один важливий параметр, який визначає кількість ресурсів, необхідних для розрахунку послідовності довжиною 10 000 000 одиниць.

Під час розрахунку послідовності кожен генератор має певний набір коефіцієнтів. Підбір цих коефіцієнтів дозволяє суттєво змінити властивості генератора.

Розроблений метод формування ПВП базується на послідовності, отриманій за допомогою мультипліактивного конгруентного генератора. У послідовності є *k* векторів, довжини яких є простими числами. Таким чином, неповторювані числа, або унікальні, повинні бути обрані. Таким чином, потрібно знайти найменше спільне кратне їхніх довжин N_0, що дорівнює їхньому добутку. Ми отримуємо період повторення. Кожен вектор подовжується циклічно до найменшого спільного кратного N_0. В результаті ми складаємо k векторів довжиною N0 за модулем 2, щоб отримати потрібну послідовність. Збільшення мірності векторів k може покращити ефективність методу. Це означає, що ми розбиваємо послідовність на квадратні матриці, довжини сторін яких є простими числами, у двовимірному контексті. Після цього ми циклічно розширюємо кожну матрицю до матриці розмірністю $N_0 x N_0$. За допомогою модуля два ми складаємо отримані матриці, щоб отримати кінцеву послідовність. Крім того, можна знайти формулу для визначення і-го елемента в створеній послідовності, тривалістю N елементів:

$$Z_i = B1(x_1, y_1) \oplus B2(x_1, y_1) \oplus \ldots \oplus B_k(x_j, y_j) \quad (1)$$

де $i = 1 \ldots N$, $j = 1 \ldots k$, $B1$ та $B2$ - сформовані послідовності мультиплікативним конгруентним методом, l - вектор розмірностей матриць.

$$x_j = \left((i-1) \bmod l_j\right) + 1, \quad (2)$$

$$y_j = \left(\left(\left\lceil \frac{i}{No} \right\rceil - 1\right) \bmod l_j\right) + 1, \quad (3)$$

Таким чином, ця послідовність модифікується до криптостійкого рівня шляхом застосування принципу життєвого циклу цикад.

Блок-схема алгоритму пропонованого методу генерації ПВП представлена на рисунку 1.

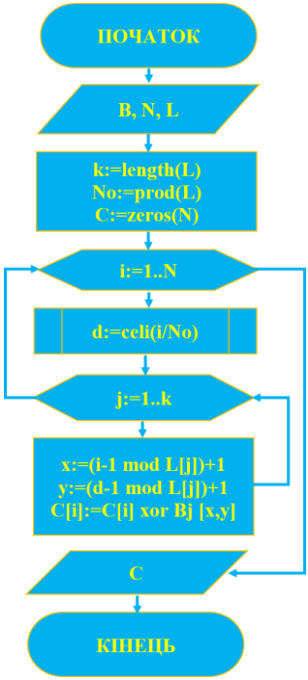


Рис. 1. Блок схема алгоритму формування ПВП

Висновок. Розроблено та досліджено метод формування псевдовипадкової послідовності. Його характеристики дозволяють використовувати послідовності, які були створені, для потокового шифрування даних. Такі методи, як Вихор Мерсенна, Мультиплікативний конгруентний метод і Розроблений метод формування ПВП, пройшли порівняльні дослідження.

На основі даних досліджень можна зробити висновок, що два методи для формування ПВП, які використовують випадкові числа від фізичного генератора або отримані за допомогою вихору Мерсенна, і вихор Мерсенна, який обмежений через те, що він не відповідає всім вимогам криптостійкості.

УДК 621.396.8:004.7 (043.2)

Вадим ТУРОВСЬКИЙ, Денис БАХТІЯРОВ, Віталій КУРУШКІН
Національний авіаційний університет, м. Київ

МЕРЕЖА ПЕРЕДАЧІ ДАНИХ НА БАЗІ ТЕХНОЛОГІЇ CWDM

Мережі передачі даних безперервно розвиваються, адаптуючись до зростаючих вимог до швидкості передачі даних та обсягу інформації. Однією з технологій, що набула популярності в сфері оптичних мереж, є курсова дільнична мультиплексація з використанням різних довжин хвиль (CWDM, Coarse Wavelength Division Multiplexing). Ця технологія дозволяє ефективно використовувати волоконно-оптичні лінії, збільшуючи їх пропускну здатність без значних капіталовкладень в нове обладнання .

CWDM є методом волоконно-оптичної передачі, що дозволяє передавати кілька сигналів одночасно через одне волокно за допомогою використання різних довжин хвиль світла. Відмінною особливістю CWDM є використання більших інтервалів між каналами у порівнянні з DWDM (Dense Wavelength Division Multiplexing), що дозволяє використовувати менш дороге та менш складне обладнання .

Переваги CWDM:

1. Економічність. Нижча вартість компонентів порівняно з DWDM.
2. Простота впровадження та обслуговування. CWDM не вимагає активного охолодження та може використовувати стандартне волоконно-оптичне обладнання.
3. Гнучкість. Можливість додавання та відключення каналів без перерви в роботі мережі.

Недоліки CWDM:

1. Обмежена пропускна здатність. Через більші інтервали між довжинами хвиль кількість каналів, які можуть бути мультиплексовані, менша, ніж у DWDM .
2. Чутливість до температурних змін. Температурні коливання можуть впливати на стабільність довжин хвиль.

CWDM часто застосовується у міських мережах, де потреба в дуже великих пропускних здатностях нижча, але важлива економічність та простота установки. CWDM може використовуватися для розширення пропускної здатності існуючих волоконно-оптичних мереж без додавання нових волокон.

Завдяки своїй здатності ефективно передавати дані на великі відстані, CWDM використовується для зв'язку між головними офісами компаній та їхніми віддаленими філіями або підрозділами [4].

Для реалізації CWDM використовуються спеціальні мультиплексори та демультиплексори, які можуть об'єднувати кілька довжин хвиль на одному волокні та розділяти їх на приймачі. Також необхідні оптичні передавачі та приймачі, настроєні на відповідні довжини хвиль.

CWDM регулюється рядом стандартів, таких як ITU-T G.694.2, який визначає сітку частот для довжин хвиль від 1270 нм до 1610 нм з кроком у 20 нм, що дозволяє використовувати до 18 каналів у мережі. Очікується, що CWDM буде інтегруватися з іншими технологіями, такими як DWDM та оптичні мережі нового покоління, для створення більш гнучких та масштабованих мережевих рішень .

Постійний розвиток стандартів та удосконалення технологічного обладнання допоможуть подолати існуючі обмеження CWDM, зокрема, збільшити кількість каналів та покращити їх стабільність у різних умовах.

Технологія CWDM є важливим інструментом у портфелі технологій оптичної передачі даних, що забезпечує економічну ефективність та гнучкість при розгортанні мереж зі збільшеною пропускною здатністю. Хоча вона має певні обмеження у порівнянні з більш дорогими та складними системами, як DWDM, її переваги роблять її ідеальним вибором для певних застосувань. Майбутнє CWDM залежить від подальших технологічних інновацій та інтеграції з іншими мережевими рішеннями, що відкривають нові можливості для вдосконалення та розширення оптичних мереж.

Список використаної літератури

1. Галущак С.М. "Модернізація та оптимізація волоконно-оптичних систем зв'язку", Одеса, Україна: Астропринт, 2021.

2. Іваненко В.І., Козирєв О.А. "Оптичні мережі передачі даних", Київ, Україна: Наукова думка, 2020.

3. Кравчук С.А., Литвиненко І.Л. "Волоконно-оптичні мережі: від теорії до практики", Харків, Україна: ФОП Яновський, 2019.

4. Петренко А.Г., Сергієнко М.П. "Технології широкополосного доступу", Львів, Україна: Видавництво Львівської політехніки, 2022.

5. Тараненко В.Б. "Сучасні технології у телекомунікаціях", Дніпро, Україна: Балаєв П.Ю., 2023.

УДК 699.81: 654.924

Д.С. Хомяк
Ю.В. Петрова
Національний авіаційній університет, м. Київ

РОЗУМНИЙ БУДИНОК

Задум розумного будинку почалось в середині 20ст. Люди фантазували нові будинки, де все буде працювати завдяки технологіям на автоматі та життя стане комфортнішим. Головним питанням на той час було знаходженням методу передачі декількох сигналів по одному кабелю з задачею управління групою приладів.

Тому саме на початку 70-х років з'явився термін «Розумний Будинок», коли це стало йти на зустріч прогресу та визначати, що це будівля, яка може забезпечувати продуктивне та ефективне користування робочого простору.

З кожним роком спорядження будинків вдосконалювалась, набирала кількість пристроїв та робило робоче середовище більш комфортним для життя, доручаючи техніці виконувати автоматично все більше задач.

Розумний будинок можна створити за допомогою професійних компаній, які займаються проектами smart house. Всі програми, які входять в систему розумного будинку, розподіляють на певні вимоги, потреби мешканців та ситуацій, які можуть пов'язуватись зі зміною середовища або безпеки.

Основними положеннями концепції інтелектуального управління будівлею є:

1) Створення інтегрованої системи управління будівлею:
Впровадження системи, що забезпечує комплексну роботу всіх інженерних систем будівлі, таких як освітлення, опалення, вентиляція, кондиціонування, водопостачання, контроль доступу та інші.

2) Передача функцій контролю і прийняття рішень підсистемам:
Ліквідація традиційних обслуговуючих підрозділів будинку з передачею їх функцій інтелектуальним підсистем. Ці підсистемами є «мозком» будівлі, що реагує на зміни параметрів датчиків та інші події, включаючи надзвичайні ситуації.

3) Механізм негайного відключення і передачі керування людині:

Забезпечення можливості швидкого переходу будь-якої підсистеми інтелектуальної будівлі на ручне управління за потреби. Людині має бути наданий оперативний доступ до управління та моніторингу всіх підсистем і компонентів «розумного будинку».

4) Незалежність окремих підсистем:

Гарантія коректної роботи окремих підсистем навіть при виході з ладу загальної системи керування або інших частин системи.

5) Мінімізація витрат на обслуговування і модернізацію:

Використання загальних стандартів у побудові підсистем, автоматичне налаштування і виявлення нових пристроїв та модулів при їх додаванні до системи для зниження витрат на обслуговування та модернізацію будівельних систем.

6) Комунікаційне середовищем для підключення пристроїв:

Забезпечення будівлі комунікаційним середовищем для підключення пристроїв та модулів системи. Використання різних типів фізичних каналів як середовища зв’язку в системі управління: слабкострумові лінії, лінії електропередач, радіоканали.

На основі методів та аналізу передачі даних у системі "розумного будинку" пропонується апаратно-програмна реалізація адаптивного методу вибору каналів зв'язку для розумного будинку. . Розроблено структурну та електричну принципову схему блоку управління розумним будинком разом із вибором апаратної платформи для реалізації конкретного методу, який дозволяє адаптивний вибір каналів зв'язку для розумного будинку.

На основі обіцяного методу система розробляє алгоритм роботи основного модуля розумного будинку та розробляє програмне забезпечення на його основі. Описує загальну структуру системи «розумний дім» із застосуванням адаптивного методу вибору каналів зв'язку та його функціональних модулів, а також розробляє експериментальний макет системи.

УДК 621.396 (043.2)

M.V. Chernyak
National Aviation University, c. Kyiv

STARLINK BASED NAVIGATION AIDS SYSTEM

Since the beginning of the planet, people have always dreamed of navigating through space, regardless of time, weather, or location. Long before the advent of modern technologies, to which people are already accustomed.

As technology advanced humans started improving navigation techniques. The evolution of navigation systems, from star based methods to GPS, Galileo, Starlink, etc. These innovations have made life on Earth more convenient and modern.

However, not all navigation systems can always provide a stable and clear signal, especially in hard-to-reach places. In order to overcome this problem, every day humanity generated a lot of small pieces of information, which over time became a major technological breakthrough. And this, in turn, started a big race between companies to provide the best services.

The Starlink system is divided into various parts, including satellites in low Earth orbit (the so-called LEO) and in very low Earth orbit (the abbreviation VLEO) by ground control means for both gateways and user terminals. Currently, there are almost 12,000 approved satellites for deployment, which is twice the number of satellites that have ever been launched into space according to the UN Office for Space.

However, launched into space about 6000. The FCC has established its own requirements for license users, in the case of Starlink it is SpaceX. Companies can run so operate only half of their satellites within six years of approval.

The bandwidth of this system is not as great as the terrestrial Internet (fiber optics), but this is understandable, because the principle of operation is completely different, but the speed is better than that of satellites of higher orbits. Starlink offers speeds up to 200 Mbps for each user and up to 20 Gbps for each of the thousand constellation companions.

The Starlink satellite network was originally designed to connect to the Internet. Its versatility and wide range have attracted the attention of mankind. With its high-speed data capabilities and global reach, Starlink offers a choice for integration into various navigation systems. The study of

the significance of Starlink in navigation contexts and its potential contribution to the development of navigation systems through domains is crucial.

1) Global coverage:

Is one of the most important features of this system, which makes Starlink attractive for use in navigation systems. Thanks to its own satellite network, which includes thousands of satellites, Starlink can provide coverage of almost the entire planet Earth. This means that navigation services that use signals from Starlink can be available absolutely throughout the planet, even at its most remote points, where the systems familiar to us can limit their work, or not work at all.

2) Low signal delay:

An equally important aspect is the low signal delay in the Starlink network. Since the satellites of this system are on low orbital systems, the signal delay is much smaller compared to satellites whose location is in large geostationary orbits.

3) Maximum throughput:

Starlinks' impressive bandwidth is a serious feature of the network. Unlike satellite systems, which have long been used by mankind, Starlink can provide much higher bandwidth speeds.

The Starlink system, created by SpaceX, demonstrates promising potential by offering navigation based on an array of satellites in low orbit, which provide minimal signal delays and high data transfer rates.

Starlink-based navigation can be effectively used in sectors such as aviation, maritime transport, land transportation and agriculture, because increased positioning accuracy allows for increased capabilities that not only reduce accidents, but also improve operational efficiency, in some cases without human help.

Of the minuses, one can note the rather high cost of implementing and maintaining the Starlink system, but the benefits that it brings easily cover all costs. Integrating Starlink into navigation systems can reduce the cost of serving end users in the transportation and logistics industries.

Based on the research results, it is obvious that the Starlink system has a perspective in the development of navigation technologies, and it is definitely possible to compete with existing systems, and in some aspects Starlink will be better.

УДК 004.056.5 (043.2)

Олександр ЧМУТ, Георгій КОНАХОВИЧ
Національний авіаційний університет, м. Київ

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ ДРУГОГО КЛАСУ

В сучасному цифровому світі, де автоматизовані системи стають все більш розповсюдженими, захист конфіденційності та цілісності інформації стає надзвичайно важливою проблемою. Автоматизовані системи другого класу особливо вразливі, оскільки містять значну кількість конфіденційної та важливої інформації. У цій статті ми розглянемо процес розробки та впровадження комплексної системи захисту інформації для таких систем.

Аналіз Вимог та Загроз. Перший крок у розробці комплексної системи захисту інформації - аналіз вимог та загроз. Це включає в себе докладне вивчення потенційних загроз безпеці, які можуть виникнути для автоматизованої системи. Зокрема, враховується можливість несанкціонованого доступу до даних, витоку інформації, впливу шкідливих програм тощо. Аналіз вимог також охоплює визначення потреб у захисті та встановлення пріоритетів щодо застосування заходів безпеки.

Вибір Засобів Захисту. Після аналізу вимог і загроз визначається набір засобів захисту, які будуть використовуватися в системі. Це можуть бути як технічні засоби (наприклад, антивірусне програмне забезпечення, файерволи, системи виявлення вторгнень), так і організаційні заходи (навчання персоналу, встановлення процедур контролю доступу). Важливо вибрати засоби, які найбільш ефективно відповідають конкретним вимогам та загрозам, а також урахувати вартість та складність впровадження.

Розробка та Тестування. На цьому етапі розробляється комплексна система захисту інформації з урахуванням вибраних засобів захисту. Після розробки система піддається тестуванню для перевірки її ефективності та надійності. Тестування включає в себе симуляцію різних сценаріїв загроз та перевірку реакції системи на них.

Впровадження та Підтримка. Останнім етапом є впровадження комплексної системи захисту інформації в автоматизовану систему та надання підтримки. Це включає в себе налагодження системи, навчання персоналу, встановлення процедур моніторингу та підтримки.

Важливо також забезпечити регулярне оновлення та підтримку системи з метою забезпечення її ефективності в умовах постійно змінюючихся загроз.

Висновок. Розробка та впровадження комплексної системи захисту інформації для автоматизованих систем другого класу - це складний процес, який вимагає докладної аналітики, вибору відповідних засобів захисту та підтримки на всіх етапах. Проте це вкрай важливо для забезпечення безпеки та цілісності інформації в сучасному цифровому світі.

Список використаних джерел

1. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб" від 23 лютого 2002 р. № 9.
2. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України "Про Положення про державну експертизу в сфері технічного захисту інформації" від 29 грудня 1999 р. № 62.
3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 1.1-004-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
6. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
7. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
8. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

УДК 004.056.9.032 (043.2)

Дмитро СИВОХА, Веніамін АНТОНОВ
Національний авіаційний університет, м. Київ

ТЕХНОЛОГІЯ PON ДЛЯ ПІДПРИЄМСТВА

В останні роки мережі доступу (МД) є найбільш динамічним сегментом телекомунікаційної галузі. Вони безпосередньо пов'язані з наданням операторських послуг абонентам, тому МД добре окупаються навіть в умовах несприятливої економічної ситуації. Тут постійно вдосконалюються технології для задоволення нових потреб користувачів, з'являються нові, характерні тільки для цих мереж, технічні рішення. На відміну від транспортних мереж (міжстанційних, міжміських т.ін.), в МД тільки починається перехід на оптичні технології в фіксованому зв'язку. Тому можна з упевненістю сказати, що МД знаходяться у фазі розвитку, що робить їх технічно і фінансово привабливими.

Передача і прийом в обох напрямках проводяться, як правило, по одному оптичному волокну, але на різних довжинах хвиль. У прямому потоці (від абонента до станції) використовують довжину хвилі 1310 нм, а в зворотному (від станції до абонента) - 1490. Оптична потужність з виходу OLT у вузлах мережі ділиться (рівномірно або нерівномірно) таким чином, щоб рівень сигналу на вході всіх ONU був приблизно однаковий. Досить часто одна з довжин хвиль виділяється для передачі всім абонентам телевізійного сигналу. Тоді на станції встановлюється оптичний мультиплексор WDM для об'єднання переданих сигналів 1310 нм (голос, дані). Всього можливе підключення до 64 і більше абонентів при максимальній дальності зв'язку - до 20 км.

Access PON продовжує розвиватися, щоб забезпечити більшу пропускну здатність для кінцевого користувача. Однак переважаючий спосіб еволюції призводить до заміни або нового встановлення нових кінцевих оптичних мереж (ONT) із більшою шириною смуги або оптичних каналів «точка-точка». Це означає, що постачальники послуг перебувають у стані постійної заміни обладнання або мають неокуплені інвестиції, які потрібно постійно старіти, перш ніж вони зможуть розглянути можливість заміни на розширену пропускну здатність і послуги.

Усі відомі сценарії на даний момент призводять до необхідності заміни ONT для отримання вищих можливостей пропускної здатності,

головним чином обмежених фактом доступної ширини смуги в нижній частині каналу, яка має бути спільною для кількох кінцевих терміналів (тобто ONT). Наприклад, поточні пропозиції PON наступного покоління (NGA) включають 10G PON і WDM PON. 10GPON зосереджується на тому, щоб ONT 10G і ONT 1G могли спільно використовувати той самий PON, але для того, щоб отримати можливості 10G, потрібен новий ONT. Подібним чином, WDM PON, які були запропоновані, в основному зосереджені на забезпеченні унікальних довжин хвиль для кожного ONT. Як зазначено, кожне з відомих рішень вимагає зміни деяких або всіх ONT на PON, щоб збільшити пропускну здатність PON. Це потрібно, навіть якщо потрібне лише збільшення пропускної здатності вниз за течією (переважний випадок).

Тому потрібні система та метод, які долають проблеми та обмеження, описані вище.

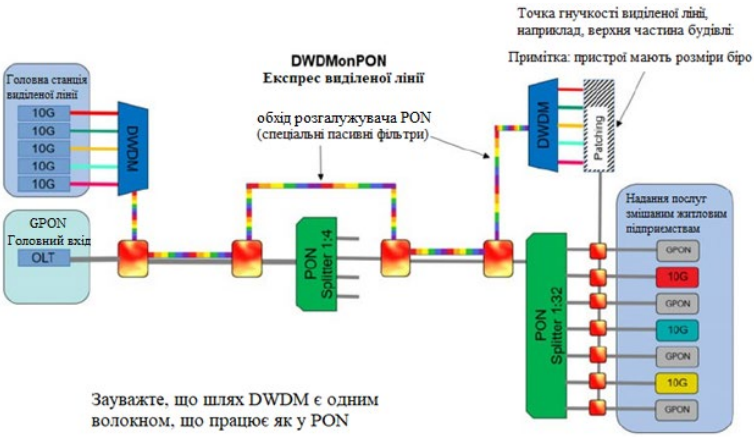


Рис.1.Щільне мультиплексування за довжиною хвилі (PON)

DWDM-PON — це фундаментальна концепція, яка має потенціал для уніфікації в технології нового доступу до транзитного зв'язку майбутнього, перенесення даних від побутових, комерційних і оптичних операторів, підключених до єдиної платформи.

Використовуючи мультиплексори DWDM, оптоволоконним кабелем можна передавати до 64 або 96 каналів DWDM . Наприклад, кожен канал можна підключити додаток зі швидкістю 400 Гбіт/с , у

результаті загальна швидкість передачі становитиме 25,6 Тбіт/с однією оптоволокно.

Висновок: Об'єднання технологій PON (Passive Optical Network) і DWDM (Dense Wavelength Division Multiplexing) є ключовим кроком у розвитку оптичних мереж доступу. Ця інтеграція відкриває нові можливості для швидкісного та надійного передавання великої кількості даних на великі відстані. Застосування DWDM у PON дозволяє збільшити пропускну здатність мережі, зменшити витрати на її будівництво та експлуатацію, а також забезпечити масштабованість і гнучкість в реагуванні на зростаючі потреби користувачів. Такий поєднання технологій відкриває нові перспективи для розвитку сучасних телекомунікаційних інфраструктур, що забезпечують швидкий та надійний доступ до Інтернету та інших цифрових сервісів для користувачів у всьому світі.

Список використаних джерел

1. A. García, «Comunicaciones por Fibra Óptica», [En línea]. Available: http://www.telnetri.es/fileadmin/user_upload/preventa/presentaciones/Comunicacio nes%20por%20Fibra%20%D3ptica.pdf. [Último acceso: enero 2018].
2. Pulse-Link, «CWave MDU (Multi Dwelling Unit) Broadband Solutions», [En línea]. Available: http://www.pulselink.com/cwave-mdu-multi-dwelling-unit-broadbandsolutions. [Último acceso: marzo 2018].
3. Silex Fiber, «Conectores de Fibra Óptica», 2018. [En línea]. Available: http://silexfiber.com/conectores-fibra-optica. [Último acceso: marzo 2018].
4. FribreMex, «Materiales y equipos para fibra óptica», [En línea]. Available: https://fibremex.com/fibraoptica/index.php?mod=showroom&id=14&ext=allinfo. [Último acceso: agosto 2018].
5. Farmacem, «Cajas térmicas ópticas/Caja terminal óptica», [En línea].Available:https://www.fibracem.com/wp-content/uploads/2018/05/caja-terminal-optica-napr04.pdf. [Último acceso: agosto 2018].

УДК 004.62:621.391 (043.2)

Софія ПОНОМАРЕНКО, Віталій КУРУШКІН, Денис БАХТІЯРОВ
Національний авіаційний університет, м. Київ

БЕЗДРОТОВА СЕНСОРНА МЕРЕЖА НА БАЗІ ПРОТОКОЛУ ZIGBEE

Бездротові сенсорні мережі (БСМ) стають все більш важливими в сучасних технологічних рішеннях, зокрема в Інтернеті речей (IoT), розумних будинках та промисловій автоматизації. Одним із найбільш популярних протоколів для реалізації БСМ є ZigBee, завдяки його низькому енергоспоживанню, високій надійності та можливості створення великих мереж. У цій статті розглядаються основні аспекти бездротової сенсорної мережі на базі протоколу ZigBee, її особливості, переваги та застосування.

Постановка завдання. Основною метою цієї роботи є дослідження можливостей та переваг використання протоколу ZigBee у бездротових сенсорних мережах. Для досягнення цієї мети необхідно розглянути архітектуру ZigBee, його ключові особливості, принципи роботи та типові сценарії застосування. Також важливо оцінити переваги та недоліки даного протоколу в порівнянні з іншими технологіями, такими як Wi-Fi, Bluetooth та інші.

Протокол ZigBee розроблений для створення низькошвидкісних бездротових мереж з низьким енергоспоживанням, що є критично важливим для сенсорних мереж. ZigBee працює на основі стандарту IEEE 802.15.4, який визначає фізичний рівень та рівень доступу до середовища (MAC). ZigBee доповнює цей стандарт, забезпечуючи мережеві, транспортні та прикладні рівні.

Архітектура ZigBee. Архітектура ZigBee складається з трьох основних компонентів: координатор, маршрутизатор та кінцевий пристрій. Координатор відповідає за ініціалізацію та управління мережею, маршрутизатори забезпечують передачу даних між вузлами, а кінцеві пристрої збирають та передають дані. Особливості та принципи роботи. ZigBee працює на частотах 2,4 ГГц,

868 МГц та 915 МГц, що забезпечує високу стійкість до перешкод та можливість використання у різних регіонах світу. Протокол підтримує різні топології мереж, такі як зірка, дерево та сітка, що дозволяє адаптувати мережу під конкретні вимоги та умови експлуатації. ZigBee використовує механізм CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) для уникнення колізій при передачі даних, а також підтримує шифрування даних для забезпечення безпеки.

Переваги та недоліки. Основними перевагами ZigBee є його низьке енергоспоживання, можливість створення великих мереж з великою кількістю вузлів, висока надійність та простота інтеграції. Протокол підтримує до 65 000 вузлів у мережі, що робить його ідеальним для розгорнутих інфраструктур IoT. Однак, ZigBee має деякі обмеження, такі як низька швидкість передачі даних (до 250 кбіт/с) та обмежена дальність зв'язку (до 100 метрів без ретрансляторів). Це робить його менш придатним для застосувань, що вимагають високих швидкостей передачі або великої дальності.

Застосування ZigBee. ZigBee широко використовується в різних галузях, включаючи розумні будинки, промислову автоматизацію, моніторинг стану навколишнього середовища, медичні додатки та енергоменеджмент. Наприклад, у розумних будинках ZigBee дозволяє контролювати освітлення, опалення, безпеку та інші системи з єдиного інтерфейсу. У промисловості ZigBee використовується для моніторингу та управління процесами, що дозволяє знизити витрати на кабельні мережі та забезпечити гнучкість у розташуванні сенсорів. У медичних додатках ZigBee дозволяє створювати бездротові мережі для моніторингу стану пацієнтів у реальному часі.

Висновки та рекомендації. Протокол ZigBee є потужним інструментом для створення бездротових сенсорних мереж завдяки його низькому енергоспоживанню, високій надійності та гнучкості. Він ідеально підходить для застосувань, де критичними є енергозбереження та можливість створення великомас-

штабних мереж. Однак, при виборі ZigBee необхідно враховувати його обмеження щодо швидкості передачі даних та дальності зв'язку. Рекомендується використовувати ZigBee у проектах, де потрібна висока надійність і низьке енергоспоживання, таких як розумні будинки, промислова автоматизація та медичні додатки. Для сценаріїв, що вимагають високої швидкості передачі або великої дальності, слід розглянути інші технології, такі як WiFi або LoRaWAN.

Таким чином, ZigBee є відмінним вибором для багатьох сучасних додатків, що вимагають гнучкості, надійності та енергоефективності, і продовжує залишатися важливим компонентом у розвитку бездротових сенсорних мереж.

УДК 621.396.4

В.Д. Радченко
Національний авіаційний університет, м. Київ

ОПТИМІЗАЦІЯ РОБОТИ ПРИЙМАЛЬНО-ПЕРЕДАВАЛЬНИХ БЛОКІВ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ РАДІОРЕСУРСАМИ В МЕРЕЖАХ LTE/LTE-A

Вступ. Управління радіоресурсами (RRM) є фундаментальною складовою ефективного функціонування гетерогенних мереж LTE/LTE-A. RRM включає в себе стратегії розподілу та керування радіочастотним спектром, спрямовані на забезпечення високої якості зв'язку та максимальної ефективності використання ресурсів.

Основна частина. Один із підходів RRM для фемтосотових мереж полягає у розподілі ресурсних блоків (PRB) для мобільних користувачів (MUE) та фемтокористувачів (FUE) на основі таких параметрів, як якість каналу та рівень перешкод. Цей підхід є простим у реалізації та ефективним для мереж з одноканальним або ортогональним розгортанням.

Для мінімізації міжрівневих та інших видів перешкод кожен базовий блок (HeNB) визначає найкращі PRB на основі показників якості каналу (CSI) для кожного FUE. Потім HeNB розподіляє найкращі PRB відповідно до обмежень якості обслуговування (QoS) та потужності.

Оптимізація роботи приймально-передавальних блоків у мобільних телефонах є ключовою для забезпечення ефективного управління радіоресурсами. Вдосконалення алгоритмів RRM та їх адаптація до конкретних умов і технологічних можливостей приймально-передавальних блоків дозволяє значно підвищити загальну ефективність роботи мереж, зменшити затримки та покращити якість зв'язку.

Заключна частина. Подальші дослідження та розвиток методів оптимізації приймально-передавальних блоків, включаючи інноваційні підходи до RRM, є необхідними для забезпечення високої якості зв'язку та ефективного використання спектру в гетерогенних мережах LTE/LTE-A. Ці заходи допоможуть впроваджувати нові стандарти і технології, підвищуючи загальну продуктивність і надійність телекомунікаційних мереж.

УДК 621.39 (043.2)

Ілля ВОЙТЮК, Роман ОДАРЧЕНКО
Національний авіаційний університет, м. Київ

ТЕСТОВА МЕРЕЖА 4G/5G. СИСТЕМА МОНІТОРИНГУ МЕРЕЖІ

У сучасному світі стрімкий розвиток телекомунікаційних технологій створює необхідність у розвитку та впроваджені стабільних і ефективних мереж 5G. Останнє покоління стільникових мереж відзначається кращими технічними параметрами пропускної здатності та затримки, що дозволяє впроваджувати кращі інноваційні практики в реалізації Інтернету речей, автономних керованих будинків, обладнання, машин тощо. Для поглибленого розуміння основних технологічних ривків варто детально досліджувати усі складові, що впливають на фінальні технічні показники. Оглянемо архітектурну складову мережі 5G: вона включає інфраструктуру мережевих елементів з базової станції gNodeB, ядра мережі 5G Core, та пристрою-споживача User Equipment, які взаємодіють між собою. Ці компоненти використовують передові технологічні підходи, зокрема: Massive MIMO, завдяки чому більша кількість антен обслуговує більшу кількість користувачів, активно перерозприділяючи ресурси, покращуючи покриття, швидкості та енергоефективність; Beamforming, яка фокусує сигнал в необхідному напрямі користувача, покращуючи його якість та зменшує інтерференцію в мережі; Network Slicing, яка дозволяє «нарізати» ресурси фізичного мережевого обладнання під конкретні задачі, оптимізовано релокувати ці ресурси за необхідності.

Формування якісної методології та обрання ключових показників ефективності мережі 5G має фундаментальну цінність, оскільки напряму є механізмом для якісної оптимізації мережі. Серед наукової та практично-експериментальної спільноти в результаті тисяч досліджень найбільш впливовими на кінцевий результат мережі метриками вважають пропускну здатність, затримку, надійність та стабільність підключення, якість обслуговування, та ємність користувачів. Використання аналітичних інструментів і технологій збору даних дозволяють глибоко аналізувати роботу мережі, забезпечуючи постійне вдосконалення і відповідність міжнародним стандартам і очікуванням споживачів.

Система моніторингу мережі 5G на основі open-source рішень дозволяє налаштовувати систему моніторингу під конкретні потреби

мережі, що важливо для тестування і розробки нових функціональних можливостей мережі. Завдяки гнучкості та масштабованості, модульна система моніторингу, яка складається за багатьох компонентів, сприяє швидкому виявленню і усуненню проблем у мережі, забезпечуючи стабільність і високу якість сервісу для кінцевих користувачів, також дозволяє в потрібний момент замінити мережеві чи програмні компоненти. Такий підхід не тільки оптимізує обслуговування та управління поточним станом мережі, але й допомагає в прогнозуванні майбутніх вимог та можливостей масштабування.

Висновок. У цій роботі було проведено детальне дослідження архітектури та ключових показників ефективності мережі 5G, а також розглянуто важливість моніторингу для забезпечення стабільної та ефективної роботи стільникових мереж нового покоління. Обгрунтоване використання відкритих технічних рішень для створення систем моніторингу: NodeJS та фреймворк Express для серверного додатку; InfluxDB OSS для зберігання та роботою з даними; Grafana для візуалізації даних, відстеження поточного стану та гнучкої системі сповіщень. Ці інструменти цілком задовільняють вимоги, сформовані в ході аналізу.

Дослідження в напрямку розробки та оптимізації систем моніторингу мають першорядний пріоритет, оскільки подальша робота з впровадження технології на теренах України матиме багато технічних викликів, а правильно підібраний аналітичний підхід дозволить на етапі проєктування відсіяти зайві перешкоди.

Список використаних джерел

1. Singh, S., & Kapoor, D. S. (2019). "5G Wireless Systems: Performance Measures and Connectivity Solutions." *Wireless Personal Communications*.
2. Akyildiz, I. F., & Jornet, J. M. (2020). "The Internet of Things: A Survey from the Connectivity and Network Management Perspective." *IEEE Internet of Things Journal*.

УДК 004.056.9.032 (043.2)

Богдан МИХАЛЬЧЕНКО, Веніамін АНТОНОВ
Національний авіаційний університет, м. Київ

КОРПОРАТИВНА МЕРЕЖА ДОСТУПУ НА БАЗІ xPON ТЕХНОЛОГІЇ

Сучасне суспільство – інформаційне суспільство. Життя та діяльність людини нерозривно пов'язана з інформацією, її зберіганням, передачею та обробкою, Обсяг даних передаються каналами зв'язку постійно зростає. Необхідна смуга пропускання для одного користувача стрімко збільшується.

Швидкість та якість інтернет-з'єднання мають велике значення для користувачів у сферах як особистого використання, так і бізнесу. Завдяки стрімкому розвитку технологій, вимоги до мереж доступу постійно зростають. Однак, варто відзначити, що в різних регіонах та для різних типів користувачів можуть бути застосовані різні рішення з метою оптимізації мережевих ресурсів та забезпечення оптимального рівня обслуговування.

Мережа доступу - це сегмент телекомунікаційної мережі, орієнтований на абонента. Історично мережа доступу розвинулася з єдиної доступної на той час двопровідної мережі. Згодом двопровідна мережа була оцифрована (ISDN та ін.), а разом з нею розвивалися нові технології передачі (Wi-Fi, мобільна телефонія та ін.), альтернативні форми інфраструктури. Наприклад оптоволокно окремо (ВОЛЗ) або в різних комбінаціях з наявними технологіями (кабель, VDSL тощо).

Рис. 1. Мережа доступу між магістраллю та абонентським розподілом

1. Платформа: надає послуги з передачі даних абонентам;
2. Магістраль: також називається backhaul, передає дані від платформи до різ-них мереж доступу;
3. Мережа доступу: «остання миля», мережа перед абонентами;
4. HVA: будинкова розподільча система, розподіл у будинку;

5. WVA: житлова розподільча система, доступ у квартирі.

Якщо раніше мережа доступу використовувалася виключно для телефонії, а згодом для факсимільного зв'язку та передачі даних через голосовий модем, то Інтернет з його потребою в пропускній здатності привів до появи набагато більшої пропускної здатності, а отже, і нових технологій. Це, в свою чергу, уможливило передачу телевізійних програм через IP. Можна передбачити, що швидкість передачі даних 10 Гбіт/с і більше незабаром стане звичним явищем

RFoG (Radio Frequency over Glass, HFC на основі топології PON, Cisco: D-PON) була розроблена як міграційне рішення для переходу від мережевої технології HFC до нової технології на основі оптоволокна.

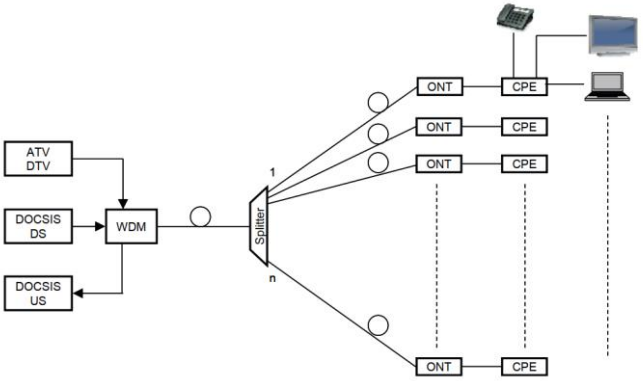


Рис. 2. RFoG через пасивну оптичну мережу

RFoG використовує центральні платформи, вже доступні для мережі HFC, від центру обробки даних до CMTS з абонентськими пристроями включно, як це вже використовується для HFC. Це забезпечує плавний перехід від аналогової мережі HFC до волоконно-оптичних структур і підготовку до переходу на цифрову мережу PON. Зокрема, заміна мережі може бути гнучко розподілена географічно, а інвестиції розподілені на багато років. Сприйняття клієнтами, маркетинг і забезпечення залишаються незмінними.

Система оптичного волокна до будинку (FTTH) дозволяє підключати оптичне волокно безпосередньо до окремих будівель, таких як житлові будинки та квартири. Перш ніж абоненти почали використовувати оптичні волокна замість мідних ліній для отримання широкосмугового доступу до Інтернету, розгортання FTTH займало багато ча-

су. Активна оптична мережа (AON) і пасивна оптична мережа (PON) є двома основними методами створення високошвидкісних мереж FTTH. Тоді в чому різниця між мережами AON і PON і як зробити правильний вибір?

AON (активна оптична мережа) — це структура мережі типу «точка-точка», в якій кожен абонент має власну волоконно-оптичну лінію, яка закінчується на оптичному концентраторі. Мережа AON використовує електричне комутаційне обладнання, як-от маршрутизатор або комутатор-агрегатор, щоб контролювати розподіл і направлення сигналів до конкретних абонентів.

На відміну від мереж AON, **PON (пасивна оптична мережа)** складається з багатьох точок і використовує пасивні оптичні розгалужувачі для розділення та збору оптичних сигналів. Волоконно-оптичні розгалужувачі дозволяють мережам PON обслуговувати кілька абонентів в одному оптичному волокні, не розгортаючи окремих волокон між концентратором і кінцевими користувачами. Як видно з назви, мережа PON розділяє оптоволоконні нитки на частини мережі та не містить обладнання для комутації з електричним живленням. Обладнання, яке потребує електроенергії, необхідно лише на стороні джерела та приймача сигналу.

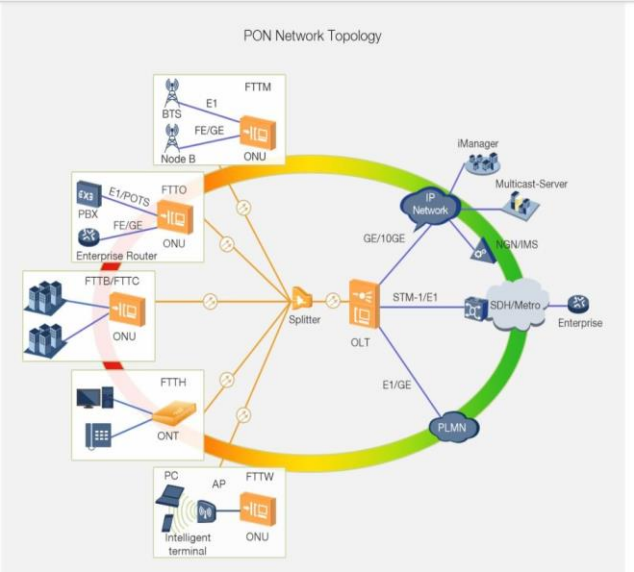


Рис. 3. Схема топології мережі PON

Що стосується вибору між PON і AON, важливо враховувати, які послуги будуть надавати через мережу, загальну топологію мережі та хто буде її використовувати.

Багато операторів використовують комбінацію цих двох мереж у різних ситуаціях. Тим не менш, у світлі зростаючого попиту на інтероперабельність і масштабованість мереж мережева архітектура може дозволити використовувати будь-яке волокно як взаємозамінне в додатках PON або AON. Це буде зроблено, якщо необхідно в майбутньому.

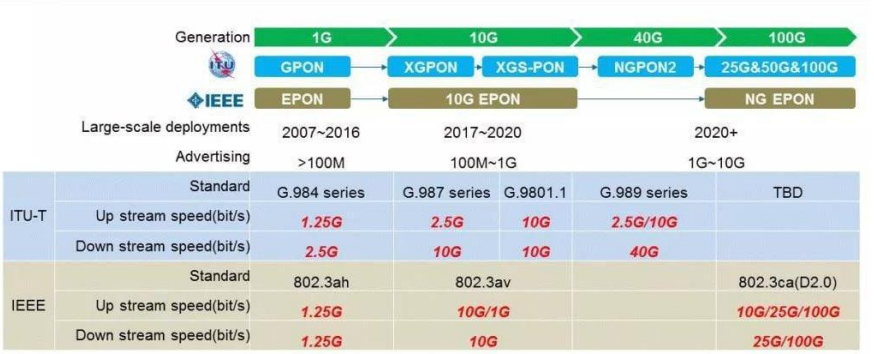


Рис. 4. Дорожня карта стандарту PON та його широкомасштабне розгортання

Висновок. У даному дослідженні були виконані такі завдання:

- Було досліджено різні аспекти архітектури мереж доступу, включаючи визначення топологій, інвестиційні рішення, мережеві архітектури та функціонування мережі доступу, що дозволило нам отримати глибоке розуміння архітектури мереж доступу.
- Було зроблено вибір технології для ділянки абонентського доступу, а також було проведено порівняння технологій PON та вибір між AON та PON мережами, що допомогло нам з'ясувати найкращі технічні рішення для абонентського доступу. Аналіз різних технологій PON, таких як XGPON, XGS-PON дав можливість обрати найбільш підходящу технологію для конкретного випадку.
- Було проведено технічний розрахунок мережі доступу XGS-PON, включаючи розрахунок параметрів оптичного волокна, робочої довжини абонентської ділянки та реального навантаження, створюваного абонентами мережі доступу XGS-PON у ГНН. Ці розрахунки на-

дають цінну інформацію для розгортання та ефективного використання мережі XGS-PON.

Загалом, робота дозволила глибше зрозуміти архітектуру та технічні аспекти мереж доступу, а також вибрати та розрахувати оптимальні технології для реалізації мережі доступу XGS-PON. Ця інформація може бути корисною для подальших досліджень та розробки мереж доступу в майбутньому.

Список використаних джерел

1. Breitbandkabel und Zugangsnetze. Technische Grundlagen und Standards. Bearbeitet von Andres Keller/ 2., vollst. bearb. Aufl. 2011. Buch. xv, 486 S.
2. Nachhaltigkeitsvergleich der Zugangsnetz-Technologien FTTC und FTTH/TECHNISCHE HOCHSCHULE MITTELHESSEN/ Verfasst von: Prof. Dr.-Ing. Kristof Obermann. 13 Mai 2020
3. Kim, H., Won, Y., Moon, S. et al. (2017). "NG-PON2 Technology for Next-Generation Mobile Fronthaul and Access Networks." Journal of Lightwave Technology, 35(1), 1-8.
4. Szcześniak, M., Bujnowski, M., & Marciniak, M. (2019). "FTTH Access Networks Evolution Towards XGS-PON Technology." In 2019 24th International Conference on Optical Network Design and Modeling (ONDM) (pp. 1-6). IEEE.
5. Oliveira, D. H., & Graciano, L. M. (2020). "Evaluation of XGS-PON and NG-PON2 as Technological Options for 5G Fronthaul and Backhaul Networks." In 2020 22nd International Conference on Transparent Optical Networks (ICTON) (pp. 1-4). IEEE.

УДК 004.056.53 (043.2)

Олександр МОРОЗ Георгій КОНАХОВИЧ
Національний авіаційний університет, м. Київ

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПЕРШОГО КЛАСУ

Забезпечення інформаційної безпеки в сучасному світі є критично важливим завданням для будь-якої організації. Комплексні системи захисту інформації (КСЗІ) включають технічні, програмні та адміністративні заходи, які спрямовані на захист інформаційних ресурсів від різноманітних загроз. Дана робота розглядає основні компоненти КСЗІ, їх функції та важливість у забезпеченні цілісності, конфіденційності та доступності інформації.

Технічні засоби захисту інформації включають міжмережеві екрани, системи виявлення та запобігання вторгнень, а також апаратні засоби криптографічного захисту. Вони є важливими для захисту від несанкціонованого доступу та атак на мережевому рівні. Апаратні засоби захисту від вірусів та шкідливого програмного забезпечення доповнюють програмні рішення, забезпечуючи додатковий рівень захисту кінцевих точок та серверів.

Програмні засоби захисту інформації, зокрема антивірусне програмне забезпечення, є ключовими інструментами для виявлення, блокування та видалення шкідливих програм. Системи управління ідентифікацією та доступом забезпечують контроль доступу користувачів до інформаційних ресурсів, підвищуючи безпеку та управління правами доступу. Системи шифрування забезпечують конфіденційність даних, захищаючи їх під час зберігання та передачі. Системи управління інформацією та подіями безпеки збирають та аналізують дані для виявлення та реагування на інциденти безпеки.

Адміністративні заходи захисту інформації - це невід'ємна частина комплексної системи захисту інформації. Політики інформаційної безпеки встановлюють загальні принципи, правила та вимоги до захисту інформаційних ресурсів. Контроль і аудит забезпечують перевірку дотримання політик, процедур та регламентів інформаційної безпеки,

а управління доступом та ідентифікацією забезпечує контроль доступу до інформаційних ресурсів, використовуючи надійні методи автентифікації та авторизації.

Комплексні системи захисту інформації поєднують технічні, програмні та адміністративні заходи для забезпечення всебічного захисту інформаційних ресурсів. Вони є ключовими для підтримання високого рівня безпеки в організації, захищаючи інформацію від різноманітних загроз. Ефективне впровадження та використання КСЗІ дозволяє організаціям зберігати конфіденційність, цілісність та доступність своїх інформаційних ресурсів на високому рівні, забезпечуючи таким чином стабільну та безпечну роботу.

Список використаної літератури

1. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки, 2013. 34 с.
2. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки. Вінниця: ВНТУ, 2018. 317 с.
3. Рижиков В. С. Класифікація загроз при інформаційній безпеці. актуальні питання права та соціально-економічних відносин Збірник наукових статей, 155 с.
4. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. Інформація і право, (3 (9)), 2013. С. 105-112.
5. Jendrian K. Der Standard ISO/IEC 27001:2013. Datenschutz und Datensicherheit - DuD. 2014. Vol. 38, no. 8. P. 552–557. URL: https://doi.org/10.1007/s11623-014-0182-x (date of access: 05.06.2024).

УДК 004.056.9.032 (043.2)

Олександр ТУЗІНКЕВИЧ, Веніамін АНТОНОВ
Національний авіаційний університет, м. Київ

ТРАНСПОРТНА МЕРЕЖА З ВИКОРИСТАННЯМ ОПТОВОЛОКОННОГО КАБЕЛЮ

Порівняння технологій CWDM, MWDM, LWDM та DWDM.

CWDM (грубе мультиплексування з поділом по довжині хвилі) – це технологія, яка використовується на рівнях доступу до міської мережі. Вона має 18 різних каналів довжини хвилі, кожен із яких розділений на 20 нм, і охоплює довжини хвиль від 1270 до 1610 нм. Ці довжини хвиль охоплюють діапазони O, E, S, C та L одномодових волоконних систем. Використовуючи CWDM, міські мережі можуть підвищити пропускну здатність оптоволоконної передачі та покращити використання ресурсів, що, як наслідок, знижує експлуатаційні витрати.

DWDM (щільне мультиплексування з поділом по довжині хвилі) дозволяє пакувати більше довжин хвиль в одне оптичне волокно. Завдяки рознесення каналів всього 1,6/0,8/0,4 нм (200 ГГц/100 ГГц/50 ГГц) DWDM може обробляти до 160 хвиль на волокно, що значно збільшує пропускну здатність порівняно з однохвильовими системами рис. 1.1. Таке ефективне використання волоконно-оптичних ресурсів знижує витрати на будівництво оптичних мереж.

Нижче наведено основні відмінності між CWDM та DWDM:

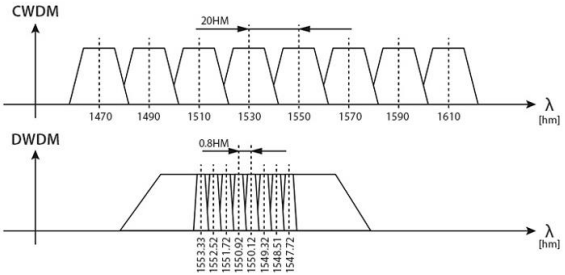


Рис. 1.1. Діаграма довжин хвиль CWDM та DWDM

• CWDM має більш просту архітектуру. Система CWDM не включає OLA (лінійний оптичний підсилювач). Більше того, оскільки відстань

між каналами CWDM ширша, немає необхідності турбуватися про балансування потужності, як у випадку з DWDM.

• CWDM споживає менше енергії. У системах CWDM використовуються лазерні діоди без охолоджувачів, що призводить до зниження енергоспоживання, що вигідно для мережних операторів за рахунок економії витрат.

MWDM проти LWDM

У 2019 році Китайський інститут дослідження телекомунікацій (China Telecom Research Institut) запропонував рішення щодо спектрального ущільнення в O-діапазоні, назвавши його MWDM (METRO WDM). У своїй розробці вчені орієнтувалися на потреби обладнання для мереж 5G. Використання швидкостей 10G стало стандартом в епоху 4G, але бездротовий зв'язок нового покоління 5G висуває великі вимоги (як мінімум у 1,5 рази) до ширини смуги пропускання магістральних каналів. Зараз на ринку доступні оптичні трансівери, що підтримують швидкість 25G, а згідно з прогнозними оцінками розробників, поява більш швидкісних трансіверів очікується вже найближчим часом.

На відміну від технології LWDM, в якій переважно використовується тільки 4 довжини хвилі, MWDM дозволяє передавати до 12 довжин хвиль в діапазоні 1270 - 1370 нм, а також використовувати довжини хвиль, що залишилися, 1390 - 1610 нм в гібридних системах ущільнення CWDM і DWDM.

MWDM (MetroWDM) – це технологія мультиплексування з поділом каналів на середній довжині хвилі, яка розширює можливості CWDM за рахунок використання перших шести хвиль. Він стискає довжину хвилі CWDM із довжиною хвилі 20 нм до 7 нм та використовує технологію контролю температури Thermal Electronic Cooler (TEC) для розділення однієї хвилі на дві рис.1.2. Це означає, що відхилення в 3,5 нм вліво та вправо розпадається на 12 хвиль.

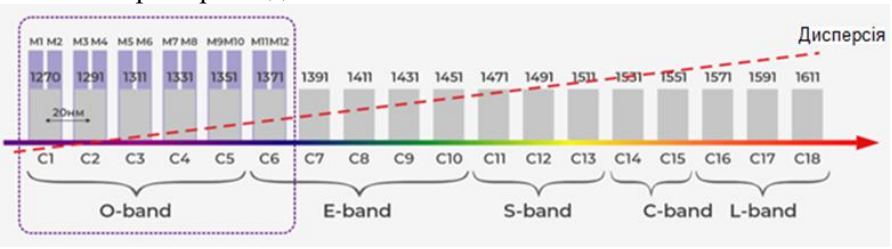


Рис. 1.2. Вплив дисперсії на каналах MWDM

Використовуючи існуючу інфраструктуру CWDM та виконуючи вимоги до дальності передачі 10 км, MWDM забезпечує підвищення пропускної спроможності при подальшій економії ресурсів оптичного волокна. Ще однією істотною відмінністю технології MWDM є можливість виробляти пасивні компоненти в такому самому виробничому циклі, що й для CWDM-компонентів.

LWDM (мультиплексування з поділом по довжині хвилі в локальній мережі) - це чудова технологія WDM, що зазвичай зустрічається в оптичних модулях 100G. Вона працює в діапазоні довжин хвиль, визначеному стандартом IEEE 802.3 для LANWDM, із рознесенням каналів від 200 до 800 ГГц. LWDM використовує 12 довжин хвиль О-діапазоні (від 1260 до 1360 нм), зокрема в діапазоні від 1269 до 1332 нм. Ці довжини хвиль мають такі характеристики, як майже нульова дисперсія, низька дисперсія і чудова стабільність при відстані один від одного 4 нм. Сітка частот LWDM (LAN-WDM) найчастіше використовується в оптичних трансіверах QSFP28 100G. Передавальна частина модулів побудована на базі чотирьох несучих TOSA з 1295/1300/1305/1310 нм, які мультиплексуються в одне волокно рис. 1.2. Довжини хвиль, що відповідають другому вікну пропускання оптичного волокна, а також май-же нульова дисперсія, дозволяють використовувати такі трансівери на дистанції до 40 км.

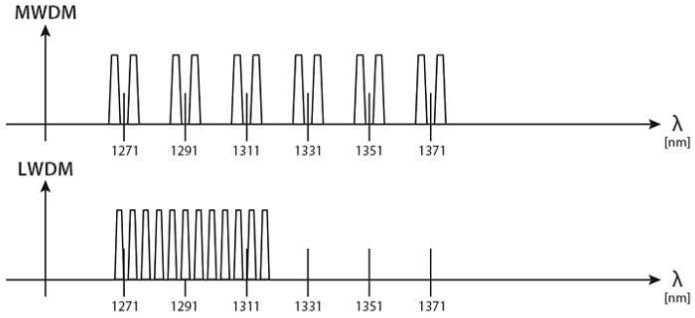


Рис. 1.3. Діаграма довжин хвиль MWDM та LWDM

Технологія LWDM не знайшла широкого застосування через складність та дорожнечу збірок TOSA, а також складність виготовлення пасивних компонентів, однак трансівери, створені на основі цієї техно-

логії, успішно зайняли нішу якісних та надій-них оптичних модулів – QSFP28 100G. LWDM зазвичай використовується на відстані до 10 км, що знаходиться між розносами каналів DWDM (100 ГГц або 50 ГГц) та CWDM (приблизно 300 ТГц).

Нижче наведено основні відмінності між MWDM та LWDM:

• MWDM зазвичай використовується для зв'язку на помірній відстані, наприклад, у міських районах. З іншого боку, LWDM найкраще підходить для зв'язку на коротких відстанях, наприклад, у корпоративних або локальних мережах (LAN).

• LWDM забезпечує велику економію коштів та ефективність використання ресурсів. LWDM часто використовується для більш коротких відстаней зв'язку, пропонуючи нижчі витрати на обладнання та розгортання. І навпаки, MWDM, який підходить для більших діапазонів зв'язку, потребує більшого обладнання та інвестицій у ресурси.

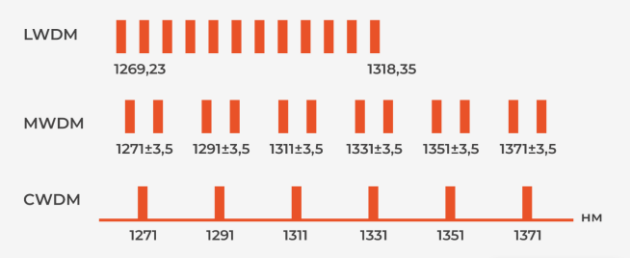


Рис. 1.4. Робочі довжини хвиль для різних технологій

Сценарії застосування CWDM, DWDM, MWDM та LWDM

CWDM знаходить широке застосування у різних мережевих середовищах, включаючи мережі кабельного телебачення та оптоволоконні системи зв'язку. У мережах кабельного телебачення CWDM використовується для використання різних довжин хвиль для висхідних та низхідних сигналів, покращуючи якість сигналу та зме-ншуючи перешкоди. Крім того, CWDM зазвичай інтегрується в трансівери, такі як перетворювачі гігабітного інтерфейсу (GBIC) і оптику, що підключається CWDM малого форм-фактора (SFP). Ці трансівери використовують стандартизовані довжини хвиль CWDM для передачі оптоволокном з мультиплексуванням по довжині хвилі.

DWDM відрізняється своєю здатністю ефективно передавати великі обсяги даних на великі відстані, що робить його ідеальним для передачі великих обсягів даних. Використовуючи існуючі оптоволоконні

мережі, DWDM збільшує пропускну спроможність передачі, що особливо корисно для корпоративних мереж. Більш того, незалежність DWDM від швидкості передачі даних і протоколу у поєднанні з мінімальними перешкодами дозволяє передавати різні типи даних по одному оптоволоконному кабелю, забезпечуючи цілісність даних та полегшуючи поділ користувачів.

MWDM підходить для регіональних мереж з вимогами передачі даних на середні відстані, наприклад, для мереж, що з'єднують міста або кілька об'єктів в межах великої географічної області. Порівняно з високою пропускною здатністю DWDM та простотою CWDM, MWDM забезпечує баланс між ними. Об'єднавши переваги обох, MWDM може задовольнити потреби передачі середні відстані без значного збільшення витрат за розгортання, що робить його економічно ефективним вибором.

LWDM зазвичай використовується в різних умовах, таких як корпоративні інтрамережі (LAN), офіси та мережі кампусів, для підвищення ефективності внутрішнього зв'язку. Використання технології LWDM дозволяє ефективно використовувати ресурси оптоволоконної мережі, забезпечуючи швидку передачу даних між декількома пристроями та гнучко адаптуючись до різних топологій та вимог локальної мережі.

У цілому нині технологія WDM, включаючи CWDM, DWDM, MWDM і LWDM, грає вирішальну роль сучасних системах оптоволоконного зв'язку. Кожна з цих технологій пропонує унікальні переваги та сценарії застосування, задовольняючи широкий спектр комунікаційних потреб. Вони забезпечують ефективні та надійні рішення для передачі даних на різні відстані та в мережевих середовищах. Для використання в якості транспортної мережі для міжміського сполучення найбільш підходить технологія DWDM.

можуть спрямовуватися на вдосконалення архітектури системи та методів аналізу для досягнення ще вищої ефективності та точності виявлення прихованої інформації в зображеннях.

Список використаних джерел

1. ITU-T Recommendation G.694.1: Spectral grids for WDM applications: DWDM frequency grid. International Telecommunication Union (ITU), 2020.

УДК 004.8:621.39 (043.2)

Denys BAKHTIIAROV
National Aviation University, Kyiv

A METHOD FOR DETECTING FAULTS IN A TELECOMMUNICATIONS NETWORK BASED ON ARTIFICIAL INTELLIGENCE

In recent years, the telecommunications industry has experienced rapid growth and transformation, driven by the increasing demand for high-speed internet, reliable connectivity, and advanced digital services. Ensuring the uninterrupted operation of telecommunications networks is paramount, as faults and disruptions can significantly impact both service providers and customers. Traditional fault detection methods often fall short in managing the complexity and scale of modern networks. This article explores a novel method for detecting faults in telecommunications networks based on artificial intelligence (AI), offering a more efficient and proactive approach to network management.

The complexity of telecommunications networks, characterized by a multitude of interconnected devices and systems, presents a significant challenge for maintaining optimal performance. Faults can arise from various sources, including hardware failures, software bugs, and environmental factors. Conventional fault detection techniques typically rely on rule-based systems and manual monitoring, which can be time-consuming and prone to errors. Additionally, these methods often only detect faults after they have occurred, leading to reactive rather than proactive maintenance.

Artificial intelligence, particularly machine learning (ML), offers promising solutions for overcoming these challenges. AI-based fault detection methods leverage large volumes of network data to identify patterns and anomalies indicative of potential faults. By applying machine learning algorithms to historical and real-time data, these systems can predict faults before they occur, enabling proactive maintenance and reducing downtime.

A detailed overview of the problem reveals several key issues in traditional fault detection methods. Firstly, the scalability of rule-based systems is limited. As networks grow and become more complex, the number of rules required to detect faults increases exponentially, making the system difficult to manage and maintain. Secondly, these systems often

struggle to adapt to new types of faults or changes in network behavior, requiring constant updates and manual intervention. Lastly, traditional methods usually lack the ability to provide insights into the underlying causes of faults, limiting their effectiveness in preventing future occurrences.

To address these challenges, the proposed AI-based fault detection method involves several key components: data collection, feature extraction, machine learning model training, and real-time fault detection. The process begins with the collection of network data from various sources, including logs, performance metrics, and user reports. This data is then preprocessed to remove noise and irrelevant information, ensuring that the machine learning models are trained on high-quality data.

Feature extraction is a crucial step, as it involves identifying the most relevant characteristics of the data that can indicate potential faults. This step often requires domain expertise and advanced statistical techniques to ensure that the extracted features capture the underlying patterns in the data. Once the features are extracted, the data is used to train machine learning models, such as neural networks, support vector machines, or decision trees. These models learn to recognize patterns associated with normal network behavior and those indicative of faults.

Real-time fault detection is achieved by continuously monitoring the network and applying the trained models to incoming data. When the models detect an anomaly or pattern that matches known fault signatures, they trigger alerts, allowing network operators to take preemptive action. Advanced AI systems can also provide diagnostic information, suggesting potential causes and remedies for the detected faults, further enhancing the efficiency of network management.

In conclusion, the integration of artificial intelligence into fault detection methods for telecommunications networks offers a transformative approach to network management. By leveraging machine learning algorithms and real-time data analysis, AI-based systems can predict and identify faults more accurately and efficiently than traditional methods. This proactive approach not only reduces downtime and maintenance costs but also enhances the overall reliability and performance of telecommunications networks. As AI technologies continue to evolve, their application in fault detection is expected to become even more sophisticated, paving the way for more resilient and adaptive network infrastructures.

НАУКОВЕ ВИДАННЯ

ТЕЗИ

XIV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

5 – 7 ЧЕРВНЯ 2024 Р.

М. КИЇВ

ГОЛОВНИЙ РЕДАКТОР ГНАТЮК В.О.

КОМП'ЮТЕРНА ВЕРСТКА ЛАВРИНЕНКО О.Ю.

КОНТАКТНИЙ E-MAIL: pezix@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