МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 червня 2023 р.

м. Київ

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

PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

«OPERATIONAL AND SECURITY PROBLEMS OF INFORMATION AND COMMUNICATION SYSTEMS»

June, 7 – 9, 2023
Kyiv, Ukraine

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

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 червня 2023 р.
м. Київ, Україна

УДК 621.39: 004.9 (082)

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 7 – 9 червня 2023 р., Національний авіа-ційний університет. – К.: Вид-во НАУ, 2023. – 123 с.

ISBN: 978-611-01-0740-2

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

ЗМІСТ

УДК 621.3

М.Ю. Андрієвський, В.В. Антонов
Національний авіаційний університет, Київ

ДОСЛІДЖЕННЯ ВОЛОКОННО-ОПТИЧНА МЕРЕЖИ ДЛЯ GIGABIT ETHERNET

Пасивна оптична мережа (PON) була винайдена в British Telecom наприкінці 1980-х років. Початкова концепція полягала у використанні мультиплексування з часовим поділом для розподілу доступної смуги пропускання між багатьма абонентами. Оптоволоконна мережа між обладнанням центрального офісу та обладнанням клієнта буде повністю пасивною. На той час це було значною мірою мотивовано відносно високою вартістю лазерів (на той час вони коштували значно більше 1000 доларів США) і низькою пропускною спроможністю користувачів (телефонія була основним застосуванням). З цієї причини було розпочато велику кількість досліджень для вивчення PON. PON вже давно розглядається як важлива частина багатьох стратегій Fibers to the Home (FTTH). Перш за все, PON є привабливими, тому що вони економлять на волокнах, що ведуть від центрального офісу до обслуговуваних громад, і зменшують кількість оптоелектроніки в центральному офісі, забезпечуючи пряму та непряму економію. Пасивна оптична мережа Gigabit Ethernet (GEPON) — це оптична мережа, одна із стандартів технології PON (Passive Optical Network). Вона складається з OLT, розташованого в центральному офісі (CO), і групи кінцевих оптичних мереж (ONT) на віддалених вузлах, розташованих на території клієнта. Він може бути розташований за місцем проживання абонента, в будівлі або на бордюрі зовні. Wavelength Options Coarse (WDM), одне з рішень наступного покоління, крім того, потребує від мереж можливостей збільшення пропускної здатності з низькою вартістю, доступною в WDM. Інтервал довжини хвилі понад 20 нм зазвичай називається грубим WDM (CWDM). Оптичні інтерфейси, які були стандартизовані для CWDM, можна знайти в ITU G.695, у той же час, коли спектральна сітка для CWDM визначена в ITU G.694.2. Якщо включний діапазон довжин хвиль від 1271 нм до 1611 нм, як визначено в ITU G.694.2, використовується з інтервалом 20 нм, то доступними будуть загалом 18 каналів CWDM, як показано на рисунку.

УДК 654.1

Д.Л. Бонз, А.Г. Тараненко
Національний авіаційний університет, м. Київ

СТІЛЬНИКОВА СИСТЕМА ПЕРЕДАЧІ ПАКЕТНИХ ДАННИХ

Принцип стільникового зв'язку, що використовується в мережах мобільного зв'язку, базується на поділі території на окремі географічні зони, які називаються стільниками. Кожна комірка покриває певну територію і має власну базову станцію, яка відповідає за зв'язок з мобільними пристроями, такими як смартфони та планшети. У стільниковій системі мобільні пристрої встановлюють з'єднання з базовою станцією найближчої комірки, коли вони перебувають у зоні покриття. Перебуваючи в русі, він може перемикатися між стільниками для продовження зв'язку. Цей принцип дозволяє користувачам залишатися на зв'язку з мережею незалежно від їхнього місцезнаходження, забезпечуючи таким чином широке покриття і мобільність.

Множинний доступ із кодовим поділом (CDMA) - це ефективний метод передавання даних у бездротових системах зв'язку. Цей метод дає змогу багатьом користувачам одночасно використовувати один і той самий радіоканал, використовуючи різні кодові послідовності.У системі CDMA кожен користувач має унікальний код, який використовується для модуляції переданого сигналу. Ці кодові послідовності мають властивість ортогональності, що дає змогу приймачу розрізняти сигнали різних користувачів, які передаються одночасно. Така ортогональність забезпечує високий ступінь захисту від колізій і дає змогу кільком користувачам передавати дані одночасно без істотного погіршення якості сигналу.

Структура передавача CDMA охоплює модуляцію сигналу з використанням кодової послідовності, узгодження потужності сигналу і поділ каналу між користувачами. Кожен користувач модулює сигнал, використовуючи свій власний код, підсумовуючи всі сигнали перед передачею їх загальним каналом. Цей процес дає змогу багатьом користувачам передавати дані одночасно й ефективно використовувати доступну смугу пропускання каналу.

Побудова приймального механізму системи CDMA включає демодуляцію всіх сигналів і розділення сигналів користувачів з використанням відповідних кодів. Приймач використовує коректори

помилок і методи фільтрації для відновлення переданих даних. Оскільки кожен користувач використовує унікальний код, приймач здатний відрізнити його сигнали від сигналів інших користувачів і успішно відновити дані. Результати щодо пакетних радіоінтерфейсів показують їх важливість у сучасному бездротовому зв'язку. Використання пакетних радіоінтерфейсів дозволяє ефективно передавати дані через бездротові мережі, розбиваючи їх на пакети і передаючи окремо. Це підвищує надійність, масштабованість і швидкість передачі даних. Такий підхід ефективно використовує радіочастотний ресурс і забезпечує швидшу та надійнішу передачу даних у бездротових мережах.

Розподіл частотного ресурсу є важливим аспектом управління радіочастотним ресурсом. Результати розподілу частот показують, що обмежений спектр для бездротових систем зв'язку повинен використовуватися ефективно. Правильний розподіл частотного ресурсу дозволяє уникнути перешкод, максимізувати пропускну здатність мережі і підвищити якість обслуговування. Ефективне управління розподілом спектральних ресурсів є важливим для задоволення зростаючого попиту на бездротовий зв'язок. Підвищення швидкості передачі даних є постійним викликом у розвитку комунікаційних технологій. Результати досліджень щодо підвищення швидкості передачі даних показують важливість пошуку нових технологій та вдосконалення існуючих технологій для забезпечення високошвидкісної передачі даних. Ці методи включають використання ширших частотних діапазонів, поліпшення алгоритмів стиснення і модуляції, а також більш ефективні схеми управління радіоінтерфейсом. Постійні дослідження і розробка нових технологій дозволяють досягати вищих швидкостей передачі даних у бездротових системах зв'язку.

УДК 621.3

М. М. Ганжа, В. П. Климчук
Національний авіаційний університет, м. Київ

СИСТЕМА ПЕРЕДАВАННЯ ДАНИХ ДЛЯ БПЛА НА ОСНОВІ ТЕХНОЛОГІЇ LORAWAN.

На сьогоднішній день розвиток технологій автономного управління дозволяє літальним апаратам самотужки виконувати польотне завдання за допомогою автопілоту, при повній відсутності зв’язку між бортом літального апарату і наземною системою управління. Проте це не дозволяє говорити про можливість виключення зі складу БПЛА командно-телеметричної радіолінії зв'язку. Окрім того, періодично виникає необхідність коригування параметрів польоту.

При створенні невеликих за розміром БПЛА збільшуються вимоги щодо мінімізації розмірів приймально-передавального і антенно-фідерного обладнання.

Також для літального апарату є актуальним завдання передачі даних корисного навантаження на наземну систему управління. В даному випадку часто потрібно забезпечити передачу великого обсягу даних при заданих вимогах по смузі пропускання, ймовірності бітової помилки, наявності захисту каналу зв’язку та інших параметрах. Для чого доцільно використовувати протоколи передачі даних з великою пропускною здатністю.

Вибір робочого частотного діапазону для командної лінії зв'язку зумовлюється кількома факторами: вимогами до маси, габаритів та споживання приймального пристрою БПЛА; необхідною дальністю роботи за заданої ймовірності бітової помилки; можливістю отримання ліцензії на роботу у необхідному діапазоні або можливістю роботи без ліцензії.

Для систем зв'язку невеликих за розміром БПЛА вирішальними факторами при виборі робочого діапазону є маса та габарити бортового приймача та антенно-фідерного пристрою. Доцільним є вибір діапазону надвисоких частот (НВЧ), при цьому антену можна розмістити у профілі крила за рахунок її невеликих розмірів.

В цьому діапазоні частот працюють декілька протоколів зв’язку, один з яких LoRaWAN – мережевий протокол із низьким

енергоспоживанням та широкою зоною покриття, розроблений для бездротового підключення пристроїв з автономним живленням до глобальної мережі і відповідає ключовим вимогам Інтернету речей.

LoRaWAN складається з запатентованої технології модуляції на фізичному рівні LoRa (1 рівень моделі OSI), що дозволяє здійснювати передачу даних на великі відстані з малими енерговитратами та власне LoRaWAN – що представляє рівень MAC (2 рівень моделі OSI), який було додано для стандартизації та розширення рівня фізичного зв'язку LoRa на мережі Інтернет для керування зв'язком між шлюзами LPWAN і пристроями кінцевих вузлів як протоколу маршрутизації. Зазвичай максимальна відстань покриття складає від 5 до 15 км.

Даний протокол також включає кілька ключових функцій бездротових мереж, таких як наскрізне шифрування (E2E), керування частотами зв'язку та адаптивна оптимізація швидкості передачі даних, якість обслуговування та інші передові програми зв'язку. Специфікація LoRaWAN дещо відрізняється від регіону до регіону на основі різних регіональних розподілів спектру та нормативних вимог.

LoRaWAN має три класи кінцевих пристроїв: A, B та C. Серед них клас C є найкращим для реалізації системи зв'язку БПЛА, оскільки він зменшує затримку на низхідній лінії, тримаючи приймач кінцевого пристрою відкритим увесь час, коли пристрій не передає (напівдуплекс), але при цьому компромісом є енергоспоживання (до 50 мВт).

LoRa базується на технології модуляції з розширеним спектром LoRa Chirp Spread Spectrum (CSS), вона дозволяє знизити рівень вихідної потужності передавача, зберігаючи сталу швидкість передачі сигналу та аналогічний бюджет зв'язку. У модуляції LoRa розширення спектру сигналу досягається шляхом генерації chirp-сигналу, частота якого постійно змінюється.

Проаналізувавши інформацію вище можна дійти висновку, що: командно-телеметрична лінія зв'язку з БПЛА має бути невеликою за габаритами та забезпечувати потрібну дальність роботи, бути енергоефективною, мати гарну завадостійкість та наявність шифрування. Для вирішення поставлених задач пропонується розробити систему зв'язку на основі технології LoRaWAN.

УДК 629.3.025

І.А. Гінетов, М.М. Малоєд
Національний авіаційний університет, м. Київ

СТАБІЛІЗАЦІЯ МОБІЛЬНИХ АНТЕН СУПУТНИКОВОГО ЗВ'ЯЗКУ

Системи стабілізації різних видів застосовуються сьогодні у навігаційних пристроях і системах управління кораблів, літальних апаратів, автомобілів, а також у системах орієнтації антен, телескопів та інших приладів, що встановлені на рухомих об'єктах. У зв'язку з тим, що необхідна точність подібних пристроїв безперервно підвищується, ростуть і вимоги щодо точності, які ставляться до комплексів стабілізації.

Перспективним застосуванням систем інерційної стабілізації платформ є їх використання в системах керування антенами мобільного супутникового зв'язку [1].

З використанням нових супутників, які можуть забезпечити роботу невеликих супутникових терміналів, можна збільшити швидкість передачі даних і знизити витрати. Прикладами типових застосувань для таких терміналів є некомутовані захищені корпоративні мережі та доступ до Інтернету в сільській місцевості.

Зараз мобільний зв'язок охоплює практично весь світ, але для деяких додатків швидкості передачі даних все одно недостатньо.

Антени для супутникового зв'язку з невеликими мобільними пристроями повинні поєднувати в собі такі характеристики, як мала апертура, висока пропускна здатність, висока швидкість передачі даних і доступні ціни на послуги.

За інших рівних умов двовісна платформа стабілізації по азимуту та висоті жорсткіша, менш дорога та компактніша, ніж триосьова конфігурація. Перевага двовісної платформи, на перший погляд, полягає в наявності напівсферичного поля зору, вирівняного в площині горизонту. Однак істотним недоліком двовісної платформи є проблема монтажу ортогональних підвісних рам. Ця проблема виникає, коли кут підйому становить 90°, тобто лінія візування орієнтована під прямим кутом та збігається з віссю азимута кріплення.

При цьому переміщення азимутального підвісу не впливає на вирівнювання лінії візування, а платформа має лише один ступінь свободи.

У статичному випадку коригування зображення не є проблемою, оскільки лінія візування може бути точно вирівняні в напівсферичному полі зору. Однак режими стеження та стабілізації є динамічними та вимагають швидкої зміни кутів рами підвіски. У той же час, явище складання підвісних рам може призвести до вимкнення системи.

Цю проблему можна вирішити шляхом введення третьої осі. Існує чотири конфігурації тривісних кріплень супутникових антен мобільного зв'язку, які забезпечують наведення та стабілізацію за такими параметрами [1]: азимут, кут місця, поперечний кут місця; азимут, горизонт, кут місця; азимут, нахил горизонту, кут місця; нахил, азимут, позиційний кут.

Для постійного навантаження апертури прямої видимості зазвичай використовують інерційні системи стабілізації з високошвидкісними контурами керування. При цьому система стабілізації повинна забезпечувати відсутність кутового переміщення лінії візування, оскільки рухоме переміщення антени через відстань від супутника не впливає на положення лінії візування.

Зокрема, система стабілізації повинна гарантувати відсутність компонентів кутового руху в будь-якому напрямку, перпендикулярному до лінії візування. Для цього гіроскопи встановлюють так, щоб осі їх чутливості були перпендикулярні до лінії зору, що дозволяє безпосередньо вимірювати кутове переміщення лінії зору.

Такий підхід дозволяє реалізувати простий закон керування, який полягає у підтримці нульових сигналів на виході гіроскопів.

Цей метод має дві переваги: по-перше, гіроскопічний пристрій дозволяє безпосередньо вимірювати кутовий рух як збурення в широкому діапазоні частот і забезпечує його швидку компенсацію без перетворення координат; по-друге, точність масштабного коефіцієнта гіроскопа не є критичною, оскільки гіроскопи працюють близько до нуля.

В роботі, проаналізовано стан актуальних проблем інерційної стабілізації мобільних антен супутникового зв'язку

СПИСОК ЛІТЕРАТУРИ

1. Сущенко О. А. Багатокритеріальний параметричний синтез робастних систем гіроскопічної стабілізації інформаційно-вимірювальних пристроїв / О. А. Сущенко, С. Г. Єгоров // Механіка гіроскоп. систем : наук.-техн. зб.. - 2017. - Вип. 33. - С. 5-15.

УДК 004.55 (043)

В.А. Гінько, Ю.В. Петрова
Національний авіаційний університет, м. Київ

ДОСЛІДЖЕННЯ КОСМІЧНИХ ТА НАЗЕМНИХ СИСТЕМ РАДІОМОВЛЕННЯ

Тема "Дослідження космічних та наземних систем радіомовлення" є важливою за кількома причинами.

По-перше, вдосконалення систем радіомовлення дозволяє забезпечити ефективний зв'язок з космічними апаратами та передавати важливі дані.

По-друге, дослідження в цій галузі сприяють розвитку швидкого та надійного інтернет-зв'язку.

По-третє, радіомовлення має важливе значення для наукових досліджень космосу та інших галузей.

По-четверте, системи радіомовлення впливають на комунікацію, безпеку та розвиток нових технологій. Враховуючи постійний розвиток космічних технологій та потребу у надійній комунікації, дослідження цієї теми залишаються дуже актуальними, особливо в контексті безпекових потреб нашої країни.

Супутникові системи зв'язку, започатковані у 1960-х, розвиваються в різних напрямках. Вони поділяються на внутрішні, національні та міжнародні, а також на багатофункціональні і спеціалізовані системи. Супутникові системи зв'язку складаються з супутників-ретрансляторів, які отримують сигнали від земних станцій, підсилюють їх і передають до наземних станцій. Основними компонентами супутника є ретранслятор з антенними системами та космічна платформа. Супутникові системи зв'язку забезпечують широкий охоплюючий зв'язок на різних рівнях і дозволяють передавати різні види інформації. Вони є важливими для сучасного світу, дозволяючи спілкуватися на великі відстані, незалежно від географічних обмежень.

За орбітальним підходом, супутникові системи поділяються на геостаціонарні (стаціонарні), середньорбітальні (середньовисотні) та низькоорбітальні (низьковисотні). Геостаціонарні супутники розташовуються на великій висоті над екватором і залишаються практично нерухомими відносно земної поверхні. Середньорбітальні

супутники рухаються на середній висоті над землею. Низькоорбітальні супутники рухаються на низькій висоті, що набагато менше за геостаціонарну та середньорбітальну

Протоколи супутникових систем зв'язку визначають правила обміну даними між супутником і земною станцією. Популярні протоколи, такі як DVB-S, TCP/IP та UDP, забезпечують надійну та швидку передачу даних у супутникових системах зв'язку. У наземному сегменті виділяються ресурси для планування запуску, управління супутниками, керування зв'язком та шлюзові станції. Наземні станції мають обладнання для радіочастотного та каналостворювального зв'язку. Протоколи і наземні ресурси грають важливу роль у забезпеченні ефективної комунікації на великій відстані в супутникових системах зв'язку.

Сучасні системи радіомовлення включають цифрове, супутникове, мобільне та бездротове радіо. Вони забезпечують швидку та надійну комунікацію. Техніки модуляції перетворюють інформацію на передавальний сигнал, а демодуляція відновлює початкову інформацію. Методи множинного доступу, такі як часовий, частотний і кодовий розподіл, дозволяють багатьом користувачам одночасний доступ до супутникового каналу. Синхронізація є важливим аспектом для правильного сприйняття та передачі даних. Підсилювачі сигналу компенсують його втрати, а управління каналами та інтерференцією забезпечує ефективне використання ресурсів та якість комунікації. Керування потоками даних забезпечує ефективне управління даними між вузлами системи.

Отже вдосконалення систем радіомовлення допомагає забезпечити ефективний зв'язок з космічними апаратами, передавати важливі дані та зображення. Швидкий та надійний доступ до Інтернету є необхідним для сучасного суспільства, і дослідження в цій галузі сприяють розвитку передачі даних. Радіомовлення також використовується у наукових дослідженнях космосу та інших галузях. Космічні та наземні системи радіомовлення є важливим елементом комунікації та безпеки в авіації, транспорті, медицині та аварійних службах.

Дослідження в цій галузі сприяють розвитку технологій та покращенню якості зв'язку. З урахуванням розвитку космічних технологій та потреби у надійній комунікації, ці дослідження залишаються актуальними.

УДК 621.39 (043.2)

М.В. Глей
Національний авіаційний університет, м. Київ

АНАЛІЗ СУПУТНИКОВОЇ РАДІОЛІНІЇ STARLINK

Starlink – проект американської компанії SpaceX, що ставить за мету виготовлення супутників зв'язку та запусків великої їх кількості на орбіту для створення мережі, яка покриватиме всю Землю та надаватиме доступ до інтернету в будь-якій точці планети. За мету даної роботи взято проведення розрахунку енергетики супутникової радіолінії Starlink та аналізу доцільності покриття всієї планети.

На відміну від супутникового зв'язку через Iridium Satellite Constellation, сигнал від якого подається безпосередньо у телефон, система Starlink потребуватиме додаткового термінала апертурою 513 мм та коефіцієнтом використання площі апертури 0,7. Антена підтримує зв'язок із супутником в інтервалі приблизно від 3 до 5 хвилин, після чого відбувається перемикання на наступний апарат.

Супутники знаходяться на висоті 550 км та використовують діапазон частот сантиметрових довжин хвиль, що використовуються в супутниковому телебаченні. Він працює на частоті 12 ГГц з довжиною хвиль 2,5 см та коефіцієнтом передачі потужності антенно-фідерного тракту 0,9. Втрати через неточність наведення антен складають 1 дБ.

Одним з факторів впливу на результат є кут місця. Кут місця – це кутом між напрямом на спостережуваний штучний супутник Землі та площиною горизонту. Він залежить від географічних координат розташування терміналу, а також від координат супутника на орбіті. Для супутника була обрана пара координат, що забезпечують кути місця 89,3 та 3,5 градусів.

Також при розрахунку враховуються такі фактори: загасання радіосигналу у кисні 0,02 дБ/км, водяній парі – 0,004 дБ/км, опадах – 3 дБ; еквівалентна товщина шару кисню 6 км та водяної пари 2,2 км.

За результатами розрахунків вхідна потужність наземного терміналу при куті місця 89,3 градуси складає -97,59 дБм, що лежить в межах слабкого сигналу мобільного зв'язку (-85 дБм … -100 дБм) та дуже слабкого WiFi (менше -70 дБм). Вхідна потужність наземного терміналу при куті місця 3,5 градуси становить -112,1 дБм.

При цьому розрахунок був проведений з урахуванням простих погодних умов, що ставить під сумнів використання Starlink в будь-якій точці світу, де умови можуть бути складнішими та вказує на потенційні можливості удосконалення системи. Також вхідна потужність знижується при зменшенні кута місця, що вказує на потребу великої кількості супутників для забезпечення постійного безперебійного сигналу, оскільки супутник має знаходитись в певному діапазоні відхилення від значення кута місця 90 градусів, після чого термінал перемикається на наступний. Така кількість та щільність супутників приводить до ризику зіткнення у разі несправності та ланцюгової реакції. Космічне сміття, що виникло після зіткнення, буде пошкоджувати все більше супутників та накопичуватися на орбіті. Це може мати серйозні наслідки для систем комунікації, навігації, зондів та космічних станцій. Виведення нових космічних апаратів стане ризикованим та складнішим, або взагалі неможливим. Процес очищення може зайняти роки або навіть десятиліття, залежно від складності ситуації та швидкості впровадження технологій. Окрім зазначеного вище, людство уже стикається з деякими викликами через запуск Starlink, а саме у сфері космічних досліджень. Величезна кількість супутників зменшує кількість даних, зібраних наземними телескопами. Коли супутники рухаються по нічному небу, вони створюють смуги світла, які затьмарюють зірки та інші об’єкти. Виходячи з результатів аналізу можна вважати, що система Starlink може бути у подальшому удосконалена та використовувана в окремих важкодоступних регіонах світу з низькою щільністю покриття або його відсутністю.

УДК 004.738(043.2)

Глущенко А.М. Курушкін В.Є
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА НА БАЗІ ТЕХНОЛОГІЇ METRO ETHERNET

Вибір технології Metro Ethernet для побудови мережі базується на ряді факторів, таких як пропускна здатність, вартість, доступність, розширюваність та масштабованість. Технологія Metro Ethernet відповідає цим вимогам та дозволяє підтримувати високі рівні пропускної здатності, швидкості передачі даних. Ми провели це дослідження з метою вивчення можливостей та переваг які може надати дана технологія та її вплив на якість обслуговування.

Мій аналіз розпочався з літературного огляду на інтернет-ресурсах, де було вивчено різні джерела, що стосуються технології Metro Ethernet та телекомунікаційних мереж в цілому. Що допомогло отримати глибше розуміння принципів та практик стосовно цієї теми.

Наступним кроком було дослідження структури телекомунікаційної мережі яка зазвичай включає в себе різноманітні компоненти та обладнання, такі як маршрутизатори, комутатори, мультисервісні платформи, оптичні перетворювачі, кабельні лінії зв'язку, антени, приймачі та інше. Визначення параметрів мережі, дослідження телефонної мережі, існуючої сигналізації та транспортної мережі дали розуміння основних аспектів їхньої роботи, їх недоліки та переваги.

Одним з основних результатів експериментального дослідження було підтвердження ефективності та продуктивності впровадження технології Metro Ethernet. Що може сприяти значному покращенню швидкості, масштабованості, надійності та якості обслуговування існуючої телекомунікаційної мережі.

Ще одним кроком було дослідження сучасних тенденцій та вимог до телекомунікаційних мереж які необхідно врахувати для побудови мережі Metro Ethernet, врахування яких допоможе в побудові мережі яка б задовольняла потреби сучасних користувачів та бізнесу.

Отримані результати дали розуміння які наступні кроки потрібно виконати для успішної реалізації мережі Metro Ethernet та висвітили результати ,що може принести її побудова. Висвітливши необхідні аспекти для визначення технологій необхідних для побудови, описали деякі з них які можуть бути використані.

Досліджуючи технологію Metro Ethernet визначили загальні відомості необхідні для проектування мережі та основні характеристики, що навели нас на критичні елементи, які необхідно врахувати при побудові мережі та виборі обладнання.

Наступним кроком стало дослідження етапів проектування мережі Metro Ethernet, що включає в себе визначення параметрів та ресурсів ,необхідних для задоволення потреб користувачів. Важливими етапами якого є визначення навантажень від абонентів ADSL одного вузла, міжміське та міжнародне навантаження, а також до інформаційної мережі Internet. Що допоможе операторам мережі забезпечити адекватну пропускну здатність та якість обслуговування користувачів у контексті зростаючого обсягу даних та вимог до швидкості передачі.

Крім того, ми дослідили вихідне навантаження від абонентів ADSL, навели аспекти необхідні для розрахунку вихідного навантаження від ЛОМ ,а також описали фактори необхідні для розрахунку міжміського та міжнародного навантаження від ТА абонентів ЛОМ. Навантаження на інформаційну мережу Internet, визначення кількості цифрових потоків кожного вузла, кількість користувачів на сектор мережі Metro Ethernet є важливими етапами проектування мережі Metro Ethernet, які були висвітлені в доповіді.

Отримані результати можуть служити довідником для широкого кола зацікавлених осіб, які працюють у галузі телекомунікацій. Вони допоможуть приймати обґрунтовані рішення та врахувати велику кількість аспектів щодо налаштування технології Metro Ethernet.

Висновки

Впровадження технології Metro Ethernet дозволить покращити функціональність, ефективність та якість обслуговування телекомунікаційної мережі. Побудова мережі Metro Ethernet допоможе вирішити проблеми, що присутні в існуючій мережі, такі як недостатня пропускна здатність та обмежена масштабованість. Metro Ethernet є масштабованим, гнучким і забезпечує високу продуктивність завдяки використанню кадрів Ethernet. Його можна використовувати для підтримки трафіку даних, голосу та відео. Технологія Ethernet продовжує розвиватися, з’являються нові стандарти, які забезпечують вищу швидкість, покращену продуктивність і більшу надійність на великих відстанях.

Список використаних джерел:

1. URL: https://www.mef.net/?s=Metro+Ethernet+Forum

УДК 621.396

О.В. Гнатенко, О.В. Зуєв
Національний авіаційний університет, м. Київ

МУЛЬТИСЕРВІСНА МЕРЕЖА МІСТА

Цифрові послуги стали невід'ємною частиною нашого життя, включаючи ранкові новини, розклад транспорту, роботу та школу, а також покупки. Державні служби також використовують цифрові технології. Щоб інтегрувати ці технології в місто, необхідно мати уніфіковану мультисервісну цифрову інфраструктуру. Ця інфраструктура повинна бути економічною, безпечною та перспективною для забезпечення сталості міста. Для досягнення цих цілей необхідна спільна мультисервісна архітектура для цифрових послуг міста, враховуючи екологічну ефективність.

Мультисервісні мережі є важливою складовою інфраструктури для цифрової трансформації міст. Вони дозволяють інтегрувати різноманітні цифрові послуги в одну систему, що забезпечує ефективне та безпечне функціонування міста, надають широкий спектр послуг, таких як телефонний зв'язок, передача даних, відеоконференції, телебачення та доступ до Інтернету. Вони також дають можливість створювати віртуальні корпоративні мережі та персоналізовані послуги для користувачів. Мультисервісні мережі є гнучкими та економічними засобами для забезпечення цифрового розвитку міст та покращення якості життя населення. Вони дозволяють інтегрувати різнорідні інформаційні та телекомунікаційні системи в єдине транспортне середовище, забезпечуючи ефективну передачу даних та мовлення. Такі мережі дозволяють знизити витрати на створення та експлуатацію мережі та надають можливість створювати різноманітні накладені сервіси. Використання мультисервісних мереж допомагає покращити ефективність управління підприємством та забезпечує доступ до різноманітних цифрових послуг.

Базовими поняттями для мультисервісних мереж виступають QoS (Quality Of Service) та SLA (Service Level Agreement), тобто якість обслуговування та угода про рівень (якість) надання послуг мережі. перехід до нових мультисервісних технологій змінює саму концепцію надання послуг, коли якість гарантується не лише на рівні договірних угод з постачальником послуг та вимог дотримання стандартів, а й на рівні технологій та операторських мереж.

Архітектурно у структурі мультисервісної мережі можна виділити кілька основних рівнів: магістральний, рівень розподілу та агрегування та рівень доступу. Магістральний рівень є універсальною високошвидкісною і по можливості однорідною платформою передачі інформації, реалізованою на базі цифрових телекомунікаційних каналів. рівень розподілу включає вузлове обладнання мережі оператора, а рівень агрегування виконує завдання агрегації трафіку з рівня доступу та підключення до магістральної (транспортної) мережі. рівень доступу включає корпоративні або внутрішньобудинкові мережі, а також канали зв'язку, що забезпечують їх підключення до вузлів розподілу мережі.

Коло потенційних користувачів мультисервісних мереж дуже широке: бізнес-центри, фірми, які розташовані в одній будівлі. Корпоративним клієнтам необхідно безліч телефонних ліній, високошвидкісний доступ в інтернет, системи аудіо відеоконференц зв'язку, сигналізації та телеметрії, великі холдинги, що мають територіально віддалені філії та підрозділи, компанії, які використовують віддалені автоматичні термінали (банкомати, торгові автомати).

Мультисервісні мережі можна будувати на базі різних технологій, як на платформі IP (IP VPN), так і на основі виділених каналів зв'язку. На магістральному рівні найпопулярнішими сьогодні є технології IP/MPLS, Packet over SONET/SDH, POS, ATM, xGE, DWDM, CWDM, RPR. Більшість магістральних мультисервісних мереж сьогодні будується на основі технологій POS, DWDM, які набули помітного поширення, а також IP/MPLS, які вважаються особливо перспективними при значній широті охоплення і великій кількості споживачів.

На відміну від інших мережевих протоколів, які маршрутизують трафік на основі адрес джерела та призначення, MPLS маршрутизує трафік на основі заздалегідь визначених «міток». Підприємства використовують MPLS для підключення віддалених філій, яким потрібен доступ до даних або додатків, які знаходяться в центрі обробки даних або в штаб-квартирі компанії.

Переваги MPLS полягають у масштабованості, продуктивності, кращому використанні пропускної здатності, зменшеному перевантаженні мережі та кращому досвіді кінцевого користувача.

УДК 654.1

Г.Ю. Дейнека , В.Ю. Курушкін
Національний авіаційний університет, м. Київ

ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ МОБІЛЬНОГО АБОНЕНТА

Дослідження технології мережі доступу FTTB на базі GPON є важливим кроком у розвитку сучасних комунікаційних систем. Використання GPON дозволяє забезпечити високу швидкість передачі даних, зменшити витрати на інфраструктуру та підвищити якість обслуговування для кінцевих користувачів. Розрахунок технічних параметрів та оптимізація мережі FTTB GPON грають важливу роль у забезпеченні стабільної та ефективної роботи мережі.

Моє дослідження підкреслює значущість технології мереж доступу FTTB GPON і надає цінні висновки та рекомендації для практичного впровадження цієї технології. Дослідження показує, що використання мереж FTTB GPON сприяє вдосконаленню комунікаційної інфраструктури, підвищенню якості обслуговування та задоволенню зростаючих потреб сучасного суспільства.

Мережа доступу FTTB передбачає прокладання оптоволоконного кабелю до будівлі, що дозволяє забезпечити високу швидкість передачі даних та стабільність сигналу. Технологія GPON є однією з ключових складових цієї мережі, яка дозволяє ефективно передавати дані на великі відстані та обслуговувати багато користувачів одночасно.

Основною перевагою мережі доступу FTTB на базі технології GPON є її висока пропускна здатність. Завдяки використанню оптоволоконного кабелю та передових методів передачі сигналу, мережа забезпечує велику швидкість передачі даних, що дозволяє користувачам комфортно використовувати інтернет, стрімінгові послуги, відеозв'язок та інші онлайн-додатки.

Технічний розрахунок проєктованої мережі доступу FTTB GPON є важливим етапом при плануванні та впровадженні такої системи. Перед початком розрахунку необхідно визначити технічні вимоги та параметри мережі. Одним з основних параметрів є швидкість передачі даних, яка повинна відповідати потребам користувачів. Враховуючи зростаючу потребу у високій швидкості, проєктована мережа FTTB GPON має забезпечувати гігабітну пропускну здатність. Поті необхідно

визначити довжину та характеристики оптичних кабелів, які використовуватимуться в мережі. Оптичний кабель повинен бути відповідного типу та якості, здатного передавати сигнал на достатню відстань без втрати сигналу. Крім того, необхідно враховувати кількість користувачів та призначення приміщення для розташування обладнання.

Розрахунок пропускної здатності та витрати потоку даних є важливим етапом у процесі проєктування мережі FTTB GPON. Визначення пропускної здатності базується на передбаченому навантаженні та очікуваному обсягу переданих даних. Залежно від потреб користувачів, можуть використовуватися різні методики розрахунку, які допоможуть визначити оптимальну швидкість передачі даних, та забезпечити стабільну роботу мережі. Окрім того, вибір необхідного обладнання та компонентів мережі є важливим аспектом проєктування мережі FTTB GPON. Під час вибору оптоволоконного обладнання, такого як Optical Line Terminal (OLT) та Optical Network Unit (ONU), слід звернути увагу на їхні технічні характеристики, продуктивність та сумісність з іншими компонентами мережі.

Проєктування мережі доступу FTTB GPON вимагає ретельного аналізу потреб користувачів, технічних вимог та особливостей будівлі, в якій буде розгортатися мережа. Визначення необхідного обладнання, кількості портів та кабельної інфраструктури є важливими етапами проєктування. При цьому слід враховувати майбутні потреби та можливості розширення мережі. Технічний розрахунок проєктованої мережі FTTB GPON включає визначення пропускної здатності, довжини оптичних кабелів, розподілу потоків даних та витрати ресурсів.

У висновку можна сказати, що мережа доступу FTTB на базі технології GPON є передовим рішенням, яке дозволяє забезпечити швидкий та стабільний доступ до Інтернету для користувачів. Вона використовує оптичне волокно та передові технології для ефективного передавання даних і вимагає правильного планування та розгортання для досягнення оптимальних результатів. Технічний розрахунок, аспекти безпеки та масштабованість є ключовими факторами, які необхідно враховувати при реалізації такої мережі. Завдяки своїм перевагам і можливостям, мережа FTTB на базі GPON стає надійним засобом забезпечення зв'язку і задоволення потреб сучасного інтернет-користувача.

УДК 621.396

А.С. Дзюба, В.П. Климчук
Національний авіаційний університет, м. Київ

БЕЗПРОВОДОВІ МЕРЕЖІ ДОСТУПУ З ДИНАМІЧНИМ ВИБОРОМ СПЕКТРУ

Зі зростаючим попитом на радіочастотний спектр для підтримки нових бездротових послуг із інтенсивним трафіком, масовими з'єднаннями та різноманітними вимогами до якості послуг, керування спектром сьогодні стає безпрецедентно складним завданням. З огляду на те, що традиційна політика розподілу фіксованого спектру призводить до неефективного використання спектру, динамічне управління спектром пропонується як багатообіцяючий спосіб пом'якшити проблему нестачі спектру.

Радіоспектр є природним, але обмеженим ресурсом, який забезпечує бездротовий зв'язок. Доступ до радіочастотного спектру регулюється державними установами. Зазвичай регуляторні органи приймають політику доступу до фіксованого спектру , щоб розподіляти різні частини радіоспектру з певною смугою пропускання для різних послуг. Завдяки такій статичній та ексклюзивній політиці розподілу спектру лише авторизовані користувачі, також відомі як ліцензовані користувачі, мають право використовувати призначений спектр, а іншим користувачам заборонено доступ до спектру, незалежно від того, зайнятий призначений спектр чи ні. Незважаючи на те, що доступ до фіксованого спектру дозволяє уникати перешкоди між різними програмами та службами, він виснажує радіоресурс із поширенням нових послуг і мереж, що призводить до проблеми дефіциту спектру.

Статистика розподілу спектру в усьому світі показує, що радіоспектр уже майже повністю розподілений, а доступний спектр для розгортання нових послуг досить обмежений. Поява масових підключень пристроїв Інтернету речей прискорює кризу дефіциту спектру. Негнучка політика розподілу спектру призводить до неефективного використання радіочастотного спектру та значною мірою сприяє проблемі дефіциту спектру навіть більше, ніж фізична нестача радіоспектру.

Протиріччя між дефіцитом доступного спектру та недостатнім використанням виділеного спектру зумовлює необхідність зміни парадигми від неефективного доступу до фіксованого спектру до

гнучкого та високоефективного доступу до спектру. У цьому контексті динамічне управління спектром було запропоновано та визнано ефективним підходом до пом'якшення проблеми дефіциту спектру.

Було передбачено, що за допомогою динамічного управління спектром вимоги до спектру для розгортання мільярдів пристроїв Інтернету речей можна різко скоротити з 76 до 19 ГГц.

У динамічному управлінні спектром користувачі без ліцензії, також відомі як вторинні користувачі, можуть отримати доступ до спектру авторизованих користувачів, також відомих як первинних користувачів, якщо основний спектр неактивний, або якщо можуть надати спільний доступ до основного спектру за умови, що послуги первинних користувачів можуть бути належним чином захищені. Таким чином, вторинні користувачі можуть отримати можливість передачі, не вимагаючи виділеного спектру. Ця політика доступу до спектру відома як динамічний доступ до спектру. Відповідно до способу співіснування між первинними та вторинними користувачами існує дві основні моделі динамічного доступу до спектру:

1) модель оппортуністичного доступу до спектру;

2) модель одночасного доступу до спектру.

В останні роки модель одночасного доступу до спектру привертає все більший інтерес з боку наукових кіл та промисловості, основні причини полягають в наступному: по-перше, одному або декільком вторинним користувачам дозволено одночасно передавати на первинному спектрі за умови, що перешкоди для первинних користувачів можна регулювати; по-друге, не потрібні ані запит до бази даних геолокації, ані визначення спектру, тому можна уникнути частої зміни конфігурації спектру; по-третє, одночасний доступ до спектру може досягти вищої спектральної ефективності зони, і, отже, може використовуватися для розміщення щільного бездротового трафіку в зонах хост-споту.

Одночасний доступ до спектру, який дозволяє різним системам зв'язку одночасно передавати в одному діапазоні частот, є одним із найважливіших методів реалізації динамічного керування спектром. Регулюючи перешкоди, які приймаються основними користувачами, вторинні користувачі можуть отримати можливість безперервної передачі. Без необхідності частого виявлення спектру та реконфігурації одночасний доступ до спектру має низьку вартість і легке впровадження на практиці.

УДК 654.1

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

ДОСЛІДЖЕННЯ СУЧАСНИХ СТІЛЬНИКОВИХ МЕРЕЖ 5G

У сучасному світі, де технологічний прогрес швидко розвивається, зв'язок відіграє важливу роль у житті людей і суспільства в цілому. Якщо перші три покоління мобільних технологій були здебільшого орієнтовані на передачу голосу, то розробка, впровадження і поширення мобільних мереж четвертого покоління свідчить про поворот до більш контент-орієнтованої інфраструктури мобільного зв'язку, на що вплинуло, головним чином, масове поширення вимогливих до пропускної здатності додатків і мультимедійних сервісів на дуже широкому спектрі комунікаційних платформ. Однак, однією з найбільш революційних і потужних технологій зв'язку нашого часу - стільникові мережі п'ятого покоління.

5G має три різні послуги для кінцевих користувачів. Перший з них - екстремальний мобільний широкосмуговий зв'язок (eMBB). Він пропонує високошвидкісне підключення до Інтернету, більшу пропускну здатність, помірну затримку, потокове відео у форматі Ultra HD, медіа з віртуальною і доповненою реальністю (AR/VR) та багато іншого. Друга послуга - масовий зв'язок машинного типу (eMTC) забезпечує широкосмуговий зв'язок машинного типу на великі відстані за дуже економічно вигідною ціною з меншим енергоспоживанням. eMTC забезпечує високу швидкість передачі даних, низьке енергоспоживання і розширене покриття завдяки меншій складності пристроїв через мобільних операторів для додатків IoT. Третя - наднадійний зв'язок з низькою затримкою (URLLC), який забезпечує низьку затримку і надвисоку надійність, багату якість обслуговування (QoS), що неможливо в традиційній архітектурі мобільних мереж. URLLC призначений для взаємодії в режимі реального часу на вимогу, наприклад, для дистанційної хірургії, зв'язку між транспортними засобами (V2V), індустрії 4.0, інтелектуальних мереж, інтелектуальних транспортних систем і т.д.

Перш за все, бездротова технологія 5G пропонує підвищену роздільну здатність для щоденного інтенсивного використання мобільного телефону та забезпечує користувачам якісне та надійне з'єднання з Інтернетом. Передбачає заздалегідь встановлені ліміти на тарифікацію

саме тому ця технологія буде більш успішною в сучасну епоху. Надає користувачам мобільних телефонів, мобільні записи легко доступні для кращого завдань друку. Дозволяє передавати величезні обсяги передавати величезні обсяги даних зі швидкістю в гігабітах. Забезпечує більш швидке завантаження та передачу даних швидкість завантаження даних у порівнянні з попередніми поколіннями. Більш точні та надійні результати отримуються завдяки даних, що передаються передачі даних за технологією 5G.

Завдяки своїм характеристикам, 5G може також покращити зв'язок у віддалених та менш розвинутих регіонах, де раніше були обмеження у доступі до швидкого та стабільного Інтернету. Це може сприяти зближенню цифрового поділу та забезпечити рівні можливості для всіх користувачів.

Незважаючи на багато переваг 5G, виникають виклики, такі як проблеми з конфіденційністю та безпекою даних, зростання витрат на інфраструктуру та залежність від технологій. Для досягнення рівного та розумного використання переваг 5G, необхідна активна співпраця та зусилля з боку уряду, промисловості та суспільства. Технологія все ще перебуває на стадії розробки, і дослідження її життєздатності тривають. Швидкість, на яку претендує ця технологія, здається важкодосяжною через некомпетентну технологічну підтримку в більшості частин світу. Багато старих пристроїв не будуть сумісними з 5G, отже, всі вони потребують заміни на нові, що є дорогим задоволенням. Розвиток інфраструктури потребує великих витрат. Питання безпеки та конфіденційності ще не вирішене.

Взагалі, для усунення недоліків та удосконалення стільникових мереж 5G, необхідна постійна співпраця між операторами зв'язку, виробниками обладнання, дослідниками та урядовими органами. Це дозволить ідентифікувати проблеми, виробляти нові технологічні рішення та впроваджувати їх на практиці. Тільки шляхом постійного вдосконалення та інновацій можна досягти оптимальної продуктивності, надійності та задоволення потреб користувачів у мережах 5G.

Мережа 5G активно розгортається і очікується, що в найближчому майбутньому воно стане головним стандартом зв'язку, по всьому світу, що забезпечує зручність, швидкість та стабільність комунікаційних послуг для мільйонів людей.

УДК 628.92/.97

Д.Р. Долгов, В.П. Климчук
Національний авіаційний університет, м. Київ

ПРИНЦИП РОБОТИ ТЕХНОЛОГІЇ LI-FI

Безпроводові мережі зв’язку займають важливе місце в світі телекомунікацій, саме тому питання щодо їх розвитку є дуже актуальним. На сьогоднішній день значний інтерес викликає технологія Li-Fi (Light Fidelity). Li-Fi – це технологія бездротової передачі даних, заснована на використанні інфрачервоного та видимого спектра світла як канал зв'язку для високошвидкісної передачі даних. Li-Fi відноситься до комунікацій через видиме світло (VLC – Visible Light Communication).

Li-Fi – це швидка і більш бюджетна оптична версія Wi-Fi, що використовує видиме світло електромагнітного спектру від 400 до 800 ТГц як оптичний носій для передачі даних. Основні компоненти базової системи Li-Fi містять білий світлодіод високої яскравості, який служить джерелом передачі, і кремнієвий фотодіод з гарним відгуком на видиме світло як приймальний елемент.

Світлодіодні лампочки можна димувати на дуже високих швидкостях, невиразні для людського ока. Короткі імпульси при швидкому димуванні LED-ламп потім перетворюються приймачем в електричний сигнал. Після цього сигнал перетворюється назад в потік двійкових даних, який ми отримуємо у вигляді веб-, відео- та аудіофайлів на наших пристроях з виходом в Інтернет.

Лампи li-fi оснащені чіпом, який трохи модулює світло для оптичної передачі. Дані передаються побутовими світлодіодними (led) лампами та приймаються фото рецепторами. При впровадженні системи li-fi можна досягти швидкостей передачі, які приблизно в 100 разів перевищують швидкості сучасного традиційного wi-fi, що працює на радіохвилях (тобто швидкість може досягати більше 1 гбіт/с).

Характерною особливістю Li-Fi є те, що, на відміну від Wi-Fi, ця система не інтерферує з радіо сигналами, що ставить її на більш вигідні позиції з точки зору стабільності швидкості Інтернету. І це ще без урахування величезної різниці в швидкостях двох видів порівнюваних мереж. Також можна відзначити, що Li-Fi більш безпечна і забезпечує додаткову конфіденційність, оскільки світло блокується стінами, і, отже, забезпечує більш безпечну передачу даних.

Область застосування Li-Fi насамперед знайде своє застосування у підводному середовищі. Інтернет-з'єднання, що зумовлене кардинальними відмінностями між Wi-Fi та Li-Fi. Світло, на відміну від радіосигналів Wi-Fi, може поширюватися у воді. Це може докорінно змінити спосіб комунікації підводних апаратів. Також завдяки своїй вражаючій швидкості Li-Fi може надати великий вплив на Інтернет речей. Оскільки швидкість передачі даних технології Li-Fi набагато вище, ніж у Wi Fi, ще більше підключених до Інтернету пристроїв зможуть взаємодіяти один з одним, тим більше що основне застосування Інтернету речей – саме в приміщеннях при включеному світлі.

Окремо варто виділити дедалі більше актуальну сферу - інформаційна безпеки. У Li-Fi радіус дії менше, ніж у Wi-Fi, і тому ступінь забезпечення безпеки вище, тим більше, що світло не передається через стіни, на відміну від радіосигналу. Варто відзначити, що з точки зору безпеки передачі даних менший радіоус дії та блокування сигналу перешкодами можна розглядати і як позитивні фактори. Це може бути дуже корисним у галузях, де обробляється велика кількість конфіденційних даних, наприклад, охорони здоров'я.

Отже, технологія Li-Fi це, бездротова комунікаційна оптична технологія, яка обіцяє стати більш дешевим та ефективним методом бездротової передачі великих обсягів даних, зберігаючи при цьому високу швидкість, стійкість до перешкод, економічність, а найголовніше безпеку, як екологічну, так і конфіденційну.

УДК 004.4'277.2.056.55

Д.В. Євграфов, Ю.Є. Яремчук
Вінницький національний технічний університет, м. Вінниця

ТЕСТОВІ СИГНАЛИ ДЛЯ МОНІТОРІВ НА РІДИННО-КРИСТАЛІЧНИХ СТРУКТУРАХ

З метою дослідження технічних каналів витоку інформації з екранів моніторів на рідинно-кристалічних структурах через побічні електромагнітних випромінювання (ПЕМВ) необхідно знайти показники якості виявлення ПЕМВ спеціалізованими технічним засобами розвідки противника (СТЗРП).

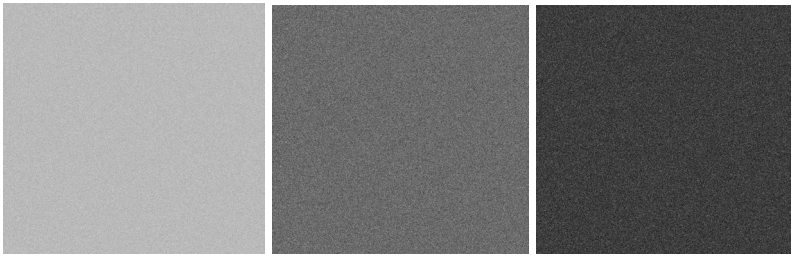
Для «статичної» картинки на екрані монітору СТЗРП повільно накопичує енергію сигналу витоку ПЕМВ на гармоніках, $f_{\text{к}} = \dfrac{k}{T_{\text{к}}}$, де $T_{\text{к}}$ – період слідування кадрової розгортки екрану монітору. Спростимо задачу тим, що розглядатиме сигнал ПЕМВ, для якого $\forall k = 1,2,..,K$, квадратурні складові

$$a_{kc0}^2 + a_{ks0}^2 = a_{k0}^2 = a^2 = \text{const}, \qquad (1)$$

a^2 – потужність сигналу ПЕМВ на будь-якій k- й гармоніці. Сигнал (1) схожий за властивостями на білий гаусівський шум (БГШ), який має постійну спектральну густину потужності N_0. Але на відміну від БГШ, який виглядатиме на екрані чорно-білого монітору як «сніг», цей сигнал виглядає як хаотична за яскравістю, але статична (не змінна) «картинка», вигляд якої змодельовано у середовищі MathCad, для монітору 800×768 пікселів з $T_{\text{к}} = 1/60\,\text{Гц}$. Сформований сигнал нормувався до максимального значення у 255 і перетворювався за допомогою команди WRITEBMP (“data.bmp”) у файл графічного зображення, подане на рис. 1, для різних значень a^2.

Якщо тестовий сигнал з максимально можливою ентропією буде виявленим СТЗРП з деякими показниками якості: ймовірністю хибної тривоги F та правильного виявлення D, будь

який сигнал на екрані монітору буде виявленим з показником, кращим за D для тієї ж ймовірності F (критерій Неймана-Пірсона).



а) *б*) *в*)

Рисунок 1 – Вигляд тестового сигналу на екрані монітору:
а) – для $a^2 = a_1^2$; *б*) – для $a^2 = a_2^2$; *в*) – для $a^2 = a_3^2$, $a_1^2 < a_2^2 < a_3^2$

Список літератури

[1] *Євграфов Д. В. Алгоритми вимірювання частоти кадрової розгортки моніторів для частотно-вибіркового придушення каналів витоку інформації / Д.В. Євграфов, Ю. Є. Яремчук // Вісник Вінницького політехнічного інституту. – № 4, 2022. – С. 83–90.*

[2] *Євграфов Д.В. Фізичні основи захисту інформації в радіоелектронній апаратурі: навч. посіб. / Д. В. Євграфов. – К.: НТУУ «КПІ», 2014. – 176 с.*

[3] *Бакут В. А. Теория обнаружения сигналов* / В. А. Бакут. – *М. : Радио и связь, 1984. – 439 с.*

[4] *Трифонов А. П. Совместное различение сигналов и оценка их параметров на фоне помех* / А. П. Трифонов, Ю. С. Шинаков. – *М. : Радио и связь, 1986. – 236 с.*

[5] Федорюк М. В. *Метод перевала* / М. В. Федорюк. – *М. : Наука, 1977. – 368 с.*

[6] *Yevgrafov D.V. Signal detection by means of electronic intelligence. monograph. Kyiv: Publishing house "Condor", 2020. 152 p.*

[7] *Євграфов Д.В. Розрахункові спектри сигналів витоку інформації з екранів моніторів на рідкокришталевих структурах / Д. В. Євграфов, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 23, №2, 2021. – С. 3–11.*

УДК 004.7:004.62

І.О. Жаворонков, В.В. Антонов
Національний авіаційний університет, м. Київ

МУЛЬТИСЕРВІСНА МЕРЕЖА З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ SDH

Сьогодні, телекомунікаційні мережі розвиваються в напрямі ринку мультисервісних послуг, впровадження нових телекомунікаційних і інформаційних технологій. Впровадження нових послуг, як і підтримка вже існуючих, вимагає значних мережевих ресурсів. Аналіз розвитку сучасних мереж зв'язку показує, що необхідність в передачі трафіка в мережах електрозв'язку, що характеризуються різними видами даних (відео, голос, інформація), зростає швидкими темпами. Такі мережі зв'язку, які отримали назву мультисвісні, викликають інтерес, в першу чергу, своєю пропускною здатністю і можливостями передачі широкого набору послуг як Triple Play (відео, голос, дані). Існуюча мережа побудована за принципом SDH - кільця (STM - 4 і STM - 1). Функції опорно-транзитної станції (ОПТС), вузла спецслужб (ВСС), і вузла відомчих телефонних станцій (ВВТС) виконує АМТС/АТСЕ-32. У ВВТС найімовірніший індекс «39». Абоненти ВВТС виходять на міську мережу за допомогою набору додаткового індексу, що має різні значення. Технологію xDSL (цифрова абонентська лінія) застосовують для надання послуг, що вимагають асиметричного передавання інформації, наприклад, відео за запитом, де потрібно передавати величезний потік інформації користувачеві, а від користувача передають найменший обсяг даних. Технологія SHDSL (стандарт G.991.2) забезпечує симетричну дуплексну передачу даних на швидкостях від 192 Кб/с до 2,32 Мб/с по звичайній мідній лінії зв'язку. 18 Робота по двох парах у симетричному режимі зі швидкістю від 384 Кб/с до 4.6 Мб/с. Для організації доступу за SHDSL технологією необхідний прямий дріт (фізична двопровідна лінія). SHDSL не може зберегти телефонний канал, нова Voice-over-DSL техніка застосовується для передачі оцифрованого голосу. Швидкість доступу при підключенні по SHDSL визначається технічними характеристиками, протяжністю конкретної лінії зв'язку, що з'єднує абонента з провайдером, і конкретною маркою SHDSL модему.

Мультисервісна мережа - це універсальне багатоцільове середовище, призначене для передавання мовлення, зображення і даних із застосуванням технології комутації пакетів. Мультисервісна

мережа на базі IP вирізняється ступенем надійності, характерним для телефонних мереж, і забезпечує низьку вартість передавання.

Головне завдання мультисервісних мереж полягає в забезпеченні роботи різнорідних інформаційних і телекомунікаційних систем і застосунків у єдиному транспортному середовищі, коли під час передавання звичайного трафіку (даних) і трафіку

іншої інформації (мовлення, відео та ін.) використовується єдина інфраструктура.

Головна ідея і основна мета мультисервісних мереж полягає в доступності будьяких сервісів у будь-який час, у будь-якому місці. Така мережа відкриває безліч можливостей побудови різноманітних накладених сервісів поверх універсального транспортного середовища - від пакетної телефонії до інтерактивного телебачення і вебслужб.

Гнучкий комутатор (SoftSwitch) - це основний компонент мультисервісної мережі, що здійснює керування викликами, керування доступом до медіашлюзів, розподіл ресурсів, оброблення протоколів, маршрутизацію, автентифікацію та облік вартості послуг, а також надання користувачам основних мовленнєвих послуг зв'язку, мобільних послуг, послуг мультимедіа, а також інтерфейсів програмування додатків. «Технологія Fast Ethernet є еволюційним розвитком класичної технології Ethernet. Fast Ethernet називається 100BaseT. Це пояснюється тим, що: 100BaseT є розширенням стандарту 10BaseT з пропускною спроможністю від 10 М біт/с до 100 Мбіт/с. Стандарт 100BaseT містить у собі протокол обробки множинного доступу з розпізнаванням несучої та виявленням конфліктів CSMA/CD, який використовується і в 10BaseT. Крім цього, Fast Ethernet може працювати на кабелях декількох типів, зокрема й на кручений парі.

У мережах Ethernet застосовується метод доступу до середовища передавання інформації, так званий методом колективного доступу з розпізнаванням несучої та виявленням колізій (Carrier-Sense-Multiply-Access With Collision Detection, CSMA/CD). Цей метод застосовується тільки в мережах із загальною шиною (до яких належать і радіомережі, що породили цей метод). Усі комп'ютери цієї мережі мають прямий доступ до спільної шини, тому вона може використовуватися для передачі інформації між будь-якими двома вузлами мережі. Простота схеми підключення - це один із чинників, що визначили успіх стандарту Ethernet.

УДК 004.056:658.382 (043.2)

Р.В. Жадько, В.Є. Курушкін
Національний авіаційний університет, м. Київ

СИСТЕМА IP-ВІДЕОСПОСТЕРЕЖЕННЯ ПІДПРИЄМСТВА

Система IP-відеоспостереження підприємства базується на використанні інтернет-протоколу (IP) для передачі відеоданих через комп'ютерні мережі. Вона забезпечує не лише високу якість зображення, але й гнучкість налаштувань та широкі можливості аналізу відеоданих.

Однією з головних переваг систем IP-відеоспостереження є їх висока ефективність у забезпеченні безпеки. Вони дозволяють підприємствам контролювати доступ до приміщень, виявляти незаконні дії та запобігати крадіжкам. Важливим аспектом є також можливість віддаленого спостереження, що дозволяє оперативно реагувати на події та вживати заходів безпеки у реальному часі.

Застосування систем IP-відеоспостереження на підприємствах розширюється на різні сфери діяльності. Вони застосовуються у виробничих комплексах для контролю якості та безпеки працівників, у торгових центрах для запобігання крадіжок та втрати товарів, а також в офісних приміщеннях для забезпечення загальної безпеки та моніторингу робочих процесів.

Важливим аспектом впровадження системи IP-відеоспостереження є процес встановлення та налаштування. Це вимагає професійного підходу та досвіду для забезпечення оптимального функціонування системи. При цьому, система може бути легко розширена та інтегрована з іншими системами безпеки, такими як контроль доступу або система пожежної сигналізації.

Надзвичайно важливою складовою системи IP-відеоспостереження є можливість аналізу відеоданих за допомогою штучного інтелекту. Це дозволяє автоматично виявляти підозрілу або небезпечну активність, використовуючи алгоритми комп'ютерного зору. Такий аналіз може значно полегшити процес виявлення випадків порушення безпеки та допомогти вчасно реагувати на них.

Однак, впровадження системи IP-відеоспостереження на підприємстві також вносить свої виклики. Наприклад, забезпечення конфіденційності та захисту персональних даних є важливим завданням, яке потребує дотримання відповідних правил та нормативних актів.

У світлі вищевказаного, розуміння системи IP-відеоспостереження та її потенціалу для розвитку сучасних підприємств є надзвичайно важливим. Її

впровадження може поліпшити безпеку, оптимізувати бізнес-процеси та забезпечити ефективне управління.

Моделювання на основі програми IP Video System Design Tool 8. IP Video System Design Tool містить калькулятор поля зору, фокусну відстань об'єктива, камери відеоспостереження та калькулятори пропускної здатності, калькулятор щільності пікселів і роздільної здатності, а також багато інших інструментів CCTV, щоб ви могли швидко та легко створювати систему відеоспостереження.

Реалістичні 3D-моделі допомагають створювати візуально привабливі проєкти та проєкти відеоспостереження, які виділяються. Функція імпорту користувацьких 3D-моделей (версія Pro) дає змогу імпортувати безоплатні 3D-моделі з Google 3D Warehouse та з іншого програмного забезпечення 3D, що підтримує відкритий формат Collada.

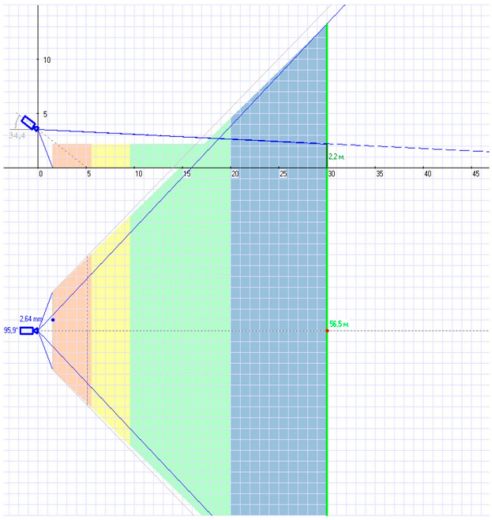


Рис. 1. Вікно креслення встановлення камери відеокамери

Вибір місць розташування відеокамер здійснюється на двовимірній поверхні плану об'єкта. Програма одночасно виконує побудову зони видимості для камери і колірну градацію зі ступенем виявлення. Це дасть змогу точно розрахувати параметри, необхідні для правильної побудови системи охорони. Покаже мінуси і помилки, які могли бути не враховані.

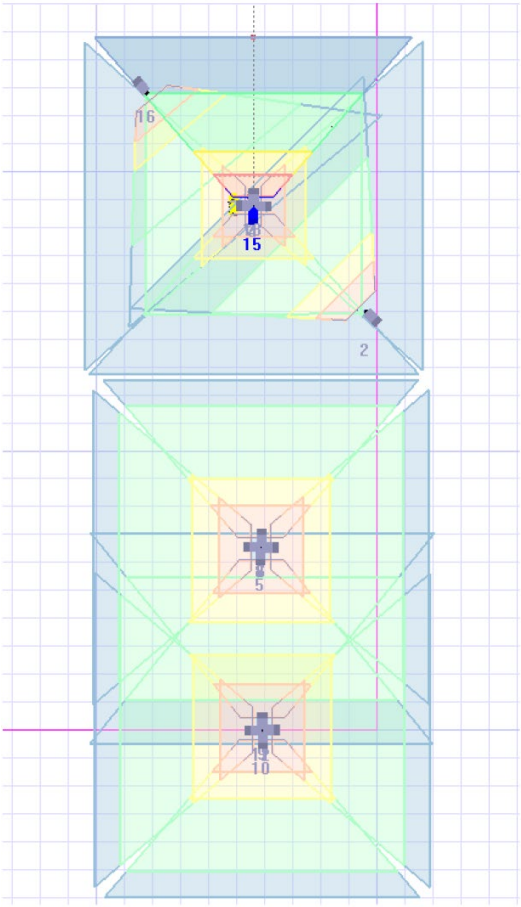


Рис. 2. Місця розташування камер моніторингу території та зони їхнього огляду

З рис. 2 видно, що за такого розташування відеокамер досягається повний огляд території та можливість розпізнавання об'єктів.

Так само програма дає змогу переглянути попередній огляд із відеокамер, для ефективнішого і зручнішого розташування камер, що, зі свого боку, впливає на моніторинг зони огляду.

Розрахунок умовно мертвої зони. Умовно мертва зона - це та частина місця огляду за горизонталлю, яку відеокамера не фіксує, і яка є невидимою для деяких об'єктів, що перебувають у русі (рис. 3).

Відрізок BE, позначений *p*, є граничною лінією, коли починається огляд камери. Відрізок *p* паралельний площині спостереження камери і знаходиться на відстані *l* від місця встановлення камери. Із трикутника EAB на рисунку 3:

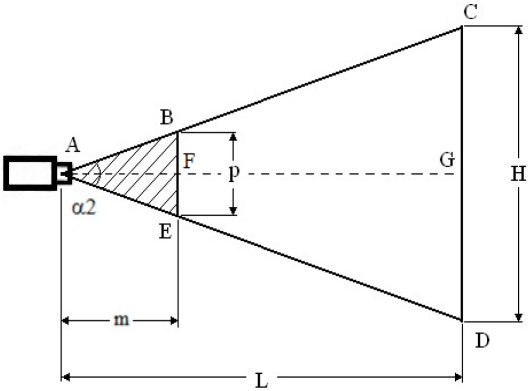


Рис. 3. Розташування камери вище за об'єкт спостереження

$$AF = BF / tg(\alpha_2/2) = BE / arctg(\alpha_2/2), \quad (1)$$

Остаточно для довжини умовно мертвої зони отримуємо:

$$l = p/2\ tg(\alpha_2/2), \quad (2)$$

Як відомо, чим ширше об'єктив відеокамери, тим довшим стає відрізок *p*, що дає змогу пристрою захоплювати більше об'єктів і реєструвати їх. Але при цьому збільшується мертва зона відеокамери. Довжина відрізка *p*, переступаючи яку, об'єкт починає потрапляти на екран монітора, дорівнює добутку швидкості руху даного об'єкта v на час перетину *t*, тобто:

$$p = v \cdot t, \quad (3)$$

Значення p дорівнюватиме часу t_p. Це час, коли охоронець встигне помітити об'єкт, що становить приблизно 2 с. Авто на паркінг території може мати максимальну швидкість лише 5 км/год, а ймовірна швидкохідність людини 10 км/год. Звідси середня швидкість дорівнює 7,5 км/год або 2,08 м/с і знаходимо:

$$p = 2{,}08 \cdot 2 = 4{,}16 \text{ м}$$

Підставляємо у формулу (3):

$$l = 4{,}16/2 \operatorname{tg}(90°/2) = 2{,}08 \text{ м}$$

Особливо важливим елементом системи відеоспостереження є розрахунок параметрів сліпої зони камери. Сліпа зона - територія, яка не входить в огляд елемента стеження. Щоб знайти значення мертвої зони камери, розглянемо трикутник ADG, у якому *n* - це позначення середньої висоти людини, а точка Q - це точка початку сліпої зони. Інакше кажучи, якщо об'єкт перебуває лівіше від цієї точки, то він потрапить у мертву зону, інакше він буде входити в кадр зйомки (рис. 4).

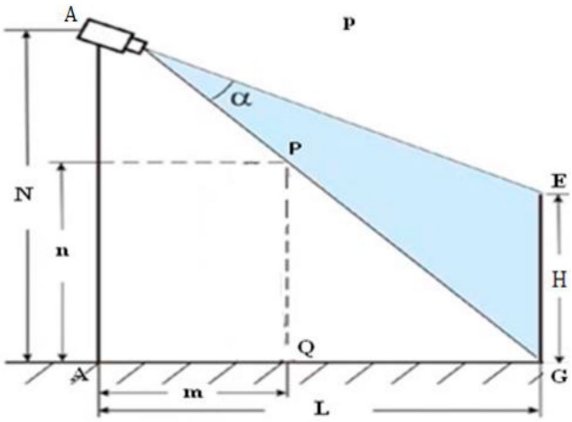


Рис. 4. Визначення мертвої зони під відеокамерою

Висновки

Добре продумана охоронна система є запорукою безпеки та збереження особливо важливих об'єктів. У кваліфікаційній роботі було розглянуто принцип функціонування мережевої системи безпеки, її особливості та якість роботи порівняно з іншими системами. Також було вивчено проблеми, які могли б виникнути під час розроблення або під час роботи системи, та їхні рішення. Проведено короткий огляд по обладнанню, необхідного для створення даної системи вдеоспостереження. При створенні системи відеоспостереження було враховано безліч чинників, що впливають на правильну роботу системи, і умови, які впливали на вибране обладнання.

У результаті для роботи системи використовується 10 камер, з них 6 купольних і 4 вуличних. Для купольних камер кути огляду по вертикалі і горизонталі дорівнювали 43 і 46 градусів відповідно, а до-

вжина мертвої зони становила 1,2 метра. Для вуличних камер кути огляду становили 28 і 48 градусів відповідно, а сліпа зона становила 2,3 метра.

Загальний потік від усіх камер дорівнював 897,84 Мбіт/с. Цього вистачає для роботи системи, оскільки мережа була побудована на кабелі витої пари UTP CAT 6, верхня гранична швидкість, яку може забезпечити кабель, дорівнює 1000 Мбіт/с.

Загальний обсяг архівованих даних склав приблизно 200 Тб, що дало змогу заздалегідь визначитися з пристроєм збереження даних.

Список літератури

1. H. Turtiainen, A. Costin, T. Hämäläinen, T. Lahtinen and L. Sintonen, "CCTV-FullyAware: toward end-to-end feasible privacy-enhancing and CCTV forensics applications," 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 2022, pp. 1227-1234.

2. S. F. Ifedola et al., "Design And Installation Of Wired Closed-Circuit Television (CCTV)," 2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS), Nagpur, India, 2022, pp. 216-219.

3. M. R. Bintang, K. Rossa Sungkono and R. Sarno, "Time and Cost Optimization in Feasibility Test of CCTV Project using CPM and PERT," 2019 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 2019, pp. 678-683.

УДК 621.3

Є.Л. Желуденко
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ DOCSIS

Тема телекомунікаційної мережі з використанням технології DOCSIS дуже актуальна в сучасну цифрову епоху. DOCSIS (специфікація інтерфейсу служби передачі даних через кабель) — це стандарт, який забезпечує високошвидкісну передачу даних через мережі кабельного телебачення. Він використовується для надання послуг Інтернету та кабельного телебачення приватним і комерційним клієнтам. Розроблений компанією CableLabs, він забезпечує високошвидкісний доступ до Інтернету через гібридні оптоволоконні коаксіальні мережі. DOCSIS забезпечує двосторонній зв'язок між кабельною головною станцією та обладнанням на місці клієнта, полегшуючи інтерактивні послуги.

DOCSIS 1.0: DOCSIS 1.0 був представлений у 1997 році та був першою версією специфікації. Він забезпечив швидкість передачі даних до 40 Мбіт/с і швидкість передачі даних до 10 Мбіт/с. DOCSIS 1.0 дозволив надавати перші широкосмугові Інтернет-послуги через дротові мережі, забезпечуючи значне підвищення швидкості в порівнянні з комутованим підключенням.

DOCSIS 2.0: DOCSIS 2.0 був випущений у 2001 році та ще більше покращив можливості дротових мереж. Він запровадив зв'язування каналів, що дозволяло об'єднувати декілька каналів для отримання вищих швидкостей. DOCSIS 2.0 підвищив швидкість вихідного потоку до 38 Мбіт/с, а швидкість вхідного потоку – до 30 Мбіт/с, створивши більш надійні інтернет-додатки та служби.

DOCSIS 3.0: DOCSIS 3.0 був представлений у 2006 році та приніс значні успіхи дротовим мережам. Він запровадив зв'язування каналів із підтримкою до 8 каналів вихідного потоку та 4 каналів висхідного потоку, що призвело до вищої швидкості передачі даних та кращої ефективності мережі. DOCSIS 3.0 запропонував швидкість вихідного потоку до 1 Гбіт/с і швидкість висхідного потоку до 100 Мбіт/с, забезпечуючи надшвидке підключення до Інтернету та передачу високоякісного потокового відео та інших послуг, що потребують великої пропускної здатності.

DOCSIS 3.1: DOCSIS 3.1 був випущений у 2013 році та ознаменував великий прогрес у можливостях дротової мережі. Він представив передові методи модуляції, такі як OFDM (мультиплексування з ортогональним частотним поділом), і збільшив кількість доступних каналів. DOCSIS 3.1 підтримує мультигігабітні швидкості зі швидкістю вхідного потоку до 10 Гбіт/с і швидкістю вихідного потоку до 1 Гбіт/с. Крім того, було покращено ефективність мережі та затримку, що робить її придатною для таких програм, як віртуальна реальність і хмарні служби.

DOCSIS 4.0: DOCSIS 4.0 наразі знаходиться в розробці та розроблений, щоб ще більше розширити межі можливостей кабельної мережі. Мета полягає в тому, щоб забезпечити мультигігабітні швидкості та підвищити ефективність мережі за допомогою передових технологій, таких як Full Duplex DOCSIS, яка забезпечує симетричні швидкості вхідного та вихідного каналів. DOCSIS 4.0 розроблено для підтримки нових технологій, таких як інтеграція 5G і додатки з низькою затримкою, що дозволяє кабельним операторам відповідати вимогам майбутніх широкосмугових послуг.

Підводячи підсумок, DOCSIS здійснив революцію в наданні широкосмугового зв'язку, використовуючи існуючу інфраструктуру та пристосовуючись до нових технологій, таких як 5G і FTTH. Він став невід'ємною частиною сучасних широкосмугових мереж, надаючи мільйонам користувачів у всьому світі доступ до високошвидкісного з'єднання. Зі швидким розвитком Інтернету та зростанням попиту на високошвидкісну передачу даних використання технології DOCSIS стало важливим для телекомунікаційних компаній. Це дає змогу кабельним компаніям надавати своїм клієнтам послуги високошвидкісного Інтернету без необхідності масштабної модернізації інфраструктури. Використання технології DOCSIS також дозволило кабельним компаніям пропонувати низку розширених послуг, таких як відео за запитом, онлайн-ігри та телеконференції.

Кожна версія DOCSIS принесла значні поліпшення в швидкості передачі даних, підтримці нових послуг та покращенні якості обслуговування. Дослідження цих версій дозволило оцінити переваги і обмеження технології DOCSIS в цілому. Впровадження наступного покоління DOCSIS 4.0 відкриває нові можливості для ще більш швидкої та надійної передачі даних в мережах, побудованих на цій технології.

УДК 004.738.7:004.5 (043.2)

О.О. Зелінський, В.Є. Курушкін, Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

ЗАБЕЗПЕЧЕННЯ QOS В МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ ЗАСОБАМИ ОС LINUX

QoS, або якість обслуговування, є критичним аспектом для забезпечення ефективної передачі даних у мережевому середовищі. Ми провели це дослідження з метою вивчення можливостей та функціональності засобів QoS, які надає ОС Linux, і їх впливу на якість обслуговування.

Наш аналіз розпочався з літературного огляду, де ми вивчили різні джерела, що стосуються забезпечення QoS в Linux. Він допоміг нам отримати глибше розуміння концепцій, принципів та практик, пов'язаних з QoS в цій операційній системі.

Наступним кроком були експериментальні дослідження. Ми налаштували різні параметри QoS і виміряли показники якості обслуговування, такі як затримки, пропускна здатність та втрати пакетів. Ці експерименти допомогли нам зрозуміти, які налаштування є оптимальними для досягнення потрібної якості обслуговування.

Крім того, ми дослідили взаємодію засобів QoS в Linux з іншими компонентами мережевої інфраструктури, такими як маршрутизатори, комутатори та мережеві контролери. Це дало нам можливість вивчити можливості співпраці та синхронізації для забезпечення QoS на різних рівнях мережі.

Одним з наших головних результатів було підтвердження ефективності та продуктивності засобів QoS в Linux. Ми провели вимірювання та оцінку різних сценаріїв мережевої передачі даних, включаючи потокове відео, відеоконференції та хмарні додатки. Наші результати показали, що засоби QoS в Linux дозволяють досягнути заданих рівнів обслуговування для цих видів трафіку.

Отримані результати мають практичне значення в кількох аспектах. Вони допомагають покращити якість обслуговування в мережах, забезпечуючи стабільну передачу даних з правильним рівнем пріоритету та мінімізацією затримок і втрат пакетів. Крім того, вони допомагають оптимізувати використання мережевих ресурсів, розподіляючи їх ефективно між різними типами трафіку.

Отримані результати також служать рекомендаціями для системних адміністраторів, мережевих інженерів та розробників програмного забез-

печення. Вони допомагають приймати обґрунтовані рішення щодо налаштування мережі та засобів QoS в Linux, що сприяє досягненню кращої продуктивності, ефективності та задоволення потреб користувачів.

На основі наших досліджень, ми рекомендуємо використовувати засоби QoS в ОС Linux для досягнення заданих рівнів якості обслуговування у мережевих середовищах. Продовжуючи дослідження в цій області, ми можемо вдосконалити і розширити функціональність засобів QoS в Linux, що приведе до подальшого покращення якості передачі даних.

Архітектура операційної системи. Відкритий процес розробки є найбільшою перевагою Linux. Будь-хто може вносити зміни, які стануть доступними всім, оскільки вихідний код ядра вільно доступний для кожного.

«Ядро Linux написано мовою С і асемблером. Між цими двома мовами існує звичайний компроміс: код на С більш переносимий і простий у підтримці, тоді як код на асемблері сприяє великій швидкості виконання. У загальному випадку асемблер у ядрі використовується тільки в тих місцях, де найбільш критичним показником є швидкість, або там, де потрібна реалізація коду, специфічного для конкретної платформи.

Хоч і в своїй основі ядро Linux монолітне, воно не є чистим монолітним ядром. Внесення змін і доповнень не викликає особливих труднощів, оскільки монолітний проєкт ядра досить модульний всередині.

Спрощена архітектура Linux-подібної ОС, з усіма низькорівневими деталями, які тільки можуть знадобитися для платформонезалежної ОС. Варто вказати дві характерні особливості ядра:

- ядро відокремлює прикладні програми від апаратних засобів;
- одна частина ядра враховує специфіку архітектури та апаратури, тоді як інша частина ядра є переносною» [1].

Архітектура ядра ОС Linux представлена на Рис. 1.

Ядро досягає переносимості, частково за рахунок того, що воно застосовує по відношенню до себе ті ж самі трюки, що і по відношенню до призначених для користувача додатків. Це означає, що певна частина ядра забезпечує відокремлення частини ядра, що залишилася, від апаратних засобів так само, як ядро відокремлює призначені для користувача додатки від тієї самої апаратури. І додатки, і частина ядра, стають переносними завдяки такому поділу.

Інтерфейс низькорівневої, залежної від архітектури частини в загальному випадку визначається незалежною від архітектури частиною коду.

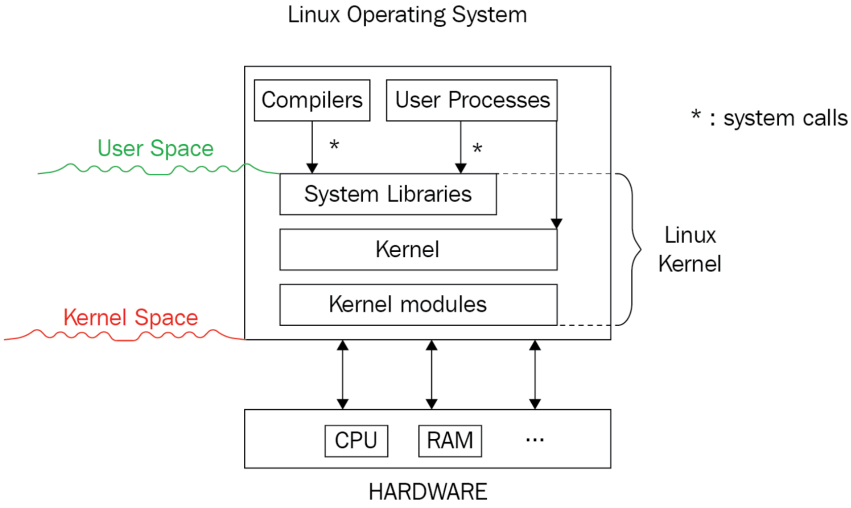


Рис. 1. Архітектура ОС Linux

Таким чином, перенесення ядра на нову платформу зводиться до ідентифікації можливостей, на зразок розглянутих вище, і реалізації їх, як того вимагає нова платформа.

Перенесення користувацьких додатків далі підтримується за допомогою шару між додатками і ядром - стандартною бібліотекою C (libc). Додатки взаємодіють з ядром тільки через libc, але ніяк не безпосередньо.

Спосіб взаємодії з ядром через libc не залежить від архітектури, причому libc оберігає користувацький код від зайвої деталізації. Унаслідок того, що існує вищезгаданий механізм, усі користувацькі додатки, і навіть більша частина бібліотеки C, взаємодіють із ядром за допомогою способу, який не залежить від архітектури.

Операційна система, яка складається з ядра Linux, майже повністю ізольована від усіх прикладних програм. Ядро функціонує в режимі ядра - захищеному режимі процесора. Web-оглядачі, поштові клієнти, ігри та інші користувацькі програми запускаються поза режимом ядра в користувацькому режимі. Ядро має прямий, неконтрольований доступ до системних ресурсів, таких як пам'ять, процесор, периферія. За допомогою системних викликів інтерфейсу syscall запити користувацьких додатків перехоплюються ядром. Цей інтерфейс перевіряє

дані, що надходять від користувацьких програм, перш ніж передати їх у ядро. Таким чином здійснюється захист від краху ядра від некоректно написаних програм [2].

Крім відмінностей між режимами, ядро і користувацькі програми займають різні області пам'яті. Кожен процес має власний віртуальний адресний простір чотири гігабайти, здебільшого ядро займає тільки один гігабайт пам'яті, тоді як програма отримує три гігабайти. Програми користувацького режиму не мають прав доступу до пам'яті ядра напряму.

До підтримуваних апаратних платформ належать:

- x86 основна 32-бітна архітектура Intel, до цієї категорії відносяться процесори AMD та інших виробників, однак на комп'ютери з процесорами Intel 386 або 486 Red Hat Enterprise Linux не може бути встановлений. Залежно від версії WS, AS або ES, підтримується від 2 і вище процесорів, і оперативну пам'ять від 256 мегабайт;
- 64-бітні процесори фірми Intel. AMD64. Це 64-бітна архітектура від фірми AMD. Підтримується від 1 процесора і більше та від 512 мегабайт оперативної пам'яті.

IBM архітектура. Red Hat Enterprise Linux підтримує сервери S/390 і сервери eServer серій zSeries, iSeries, pSeries від компанії IBM.

У системах із симетричним мультипроцесорним опрацюванням процесори повинні розподілити роботу таким чином, щоб не заважати один одному, і при цьому вони не повинні витрачати на цю координацію дуже багато часу, що веде до того, що додаткова продуктивність процесора буде майже повністю витрачена.

Ядро Linux від версії 2.4 підтримує модель NUMA, для якої час доступу до різних ділянок пам'яті може варіюватися залежно від різновидів процесора [3].

Підсумовуючи сказане, слід зазначити, що ізоляція ядра від призначених для користувача додатків значно сприяє збільшенню надійності роботи системи і розширюваності.

Операційні системи Linux - це системи з відкритим кодом, однак для того, щоб адміністратори могли самостійно виправити дірки в безпеці або поліпшити продуктивність системи, вони повинні володіти знаннями, принаймні, не меншими, ніж розробники корпорації Red Hat. З огляду на те, що під час подальшого встановлення на систему нових патчів або сервіспаків, зміни затираються, або призводять до порушення працездатності, ві-

дкритість кодів ядра або основних сервісів не є перевагою. Крім цього, можливі проломи в безпеці та стабільності роботи системи можуть бути спричинені зміною коду системних програм.

Є ймовірність інтегрування Linux у будь-яку локальну мережу. Фактично будь-який дистрибутив Linux застосовують, як серверну операційну систему або звичайну робочу станцію. Web-сервер (Apache), сервер електронної пошти (Sendmail), ftp-сервер, файловий сервер Samba або сервер IP телефонії мають усі шанси бути легко встановленими в операційній системі Linux. Усі служби Unix, включно з Networked File System (NFS), віддаленим доступом (Telnet, Rlogin), роботою в TCP/IP мережах (рис. 2), dial-up-доступом за протоколами SLIP, L2TP і PPP підтримуються в цій ОС. Використання ОС у вигляді Інтернет-шлюзу вважається однією з найпоширеніших версій експлуатації ОС Лінукс, оскільки дає змогу містити всередині себе проксі-сервер, міжмережевий екран, поштовий сервер, DHCP і DNS сервери та інші мережеві утиліти. Інтернет-шлюз має можливість працювати як на одному з комп'ютерів мережі, так і на окремому сервері [4].

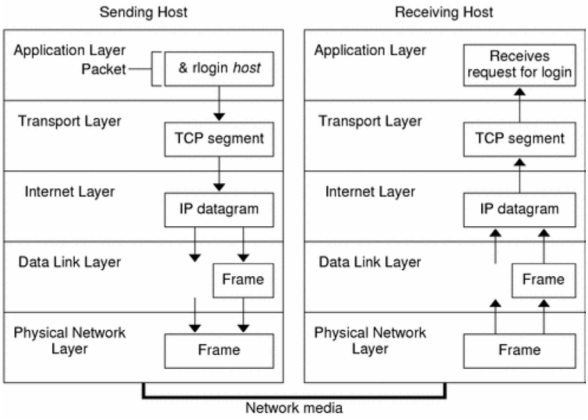


Рис. 1.2. Архітектура стека протоколів TCP/IP ОС Linux

«TCP/IP стек у Linux відповідає всім стандартам, а також перевершує реалізацію TCP/IP в інших ОС за багатьма своїми можливостями. Підтримка TCP/IP охоплює просунуту маршрутизацію (policy routing, QoS and Fair Quering), traffic shaping, пакетну фільтрацію (firewalling), multicasting, підтримку "прозорого" проксі, masquerading, тунелінг, aliasing та ін. Крім IPv4, у ядро Linux входить підтримка

IPv6. Стандартно в поставку Linux входять: Apache - http-сервер, який користується найбільшою популярністю в Internet, Sendmail - програмка передавання електронної пошти (Mail Transfer Agent), FTP, POP3/IMAP, сервер доменних імен DNS, проксі-сервер Squid, який кешує http проксі-сервер Squid, засоби, що забезпечують пакетну фільтрацію, файрвол Iptables. Крім того підтримується підключення Linux-машини як сервера або відвідувача для іншої мережі, а саме, діє єдине впровадження (sharing) файлів і віддалений друк у Macintosh, NetWare і Windows. У Linux вірусів немає! Бо самі основи побудови операційної системи ліквідують імовірність роботи вірусів. Linux вважається багатокористувацькою операційною системою. Усіх користувачів поділяють на 2 види: звичайні користувачі та адміни. Таким чином, поділ прав призводить до того, власне звичайний користувач не має доступу до системних файлів, а перебудову операційної системи йому не класифікують як можливу.

Висновки

У цій роботі мною спроєктовано шлюз для використання в ЛОМ компаній, розташованих у містах-супутниках м. Києва, і тих, що мають низькошвидкісне підключення до мережі Інтреннет. Передбачається використання цього сервера як шлюзу IP телефонії (Asterisk) і шлюзу виходу в Інтернет.

Список літератури

1. R. K. Boggavarapu and S. Jiang, "Deduplication-aware I/O Buffer Management in the Linux Kernel for Improved I/O Performance and Memory Utilization," 2020 12th International Conference on Knowledge and Smart Technology (KST), Pattaya, Thailand, 2020, pp. 70-74.

2. R. Karayat, M. Jadhav, L. S. Kondaka and A. Nambiar, "Web Application Penetration Testing & Patch Development Using Kali Linux," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1392-1397.

3. R. Karayat, M. Jadhav, L. S. Kondaka and A. Nambiar, "Web Application Penetration Testing & Patch Development Using Kali Linux," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1392-1397.

УДК 004.056.004

Ю.Є. Яремчук, В.В. Карпінець, І.С. Зоря
Вінницький національний технічний університет, м. Вінниця

ВДОСКОНАЛЕННЯ СТЕГАНОГРАФІЧНОГО МЕТОДУ PVD ЗАХИСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Вступ. Для вирішення проблем спотворень зображення пропонуються різні методи. Результати аналізу цих методів показують, що оборотні методи приховування даних активно досліджуються не лише для відновлення вихідного зображення, але й для отримання секретних даних. LSB (Найменший значущий біт) і PVD (Піксельна різниця) – типові приклади методів приховування даних. У схемі PVD зображення розділено на блоки, де використовуються два послідовних пікселі у кожному блоці. Багато дослідників використовують стеганографічний підхід на основі PVD, щоб розробити деякі ефективні стеганографічні схеми кольорових зображень.

У ході дослідження методу PVD та різних варіантів його модифікацій було зроблено висновок щодо доцільності його вдосконалення шляхом використання різноспрямованості на кольорових зображеннях для вбудовування ЦВЗ, а також використання модифікованої таблиці діапазонів квантування. Тобто мінімальна різниця між пікселями буде братись не послідовно, так як у стандартному методі [1], а у двох або у трьох напрямках. Це дасть можливість знайти найбільш відповідні пікселі для вбудовування ЦВЗ, що, у свою чергу, збереже високу якість зображення. А модифікована таблиця діапазонів квантування надасть можливість уникнення помилок при вилученні ЦВЗ.

Основна частина. У запропонованому вдосконаленому методі пропонується розбиття кольорового зображення на блоки, що не перекриваються, і значення пікселів у кожному блоці розкладаються на R, G та B. У процесі вбудовування значення пікселів R, G та B кожного блоку перегрупуються для застосування PVD схема у двох або трьох напрямках. Для того, щоб вбудувати ЦВЗ необхідно знайти мінімальне значення у перегрупованих блоках. Секретні дані вкладаються у двох або трьох напрямках на основі мінімального значення. Два пікселі кожної пари розподіляються на два зображення для ідеального вилучення ЦВЗ. У процесі вилучення отримуються секретні дані на основі алгоритме вилучення схеми PVD з модифікованою таблицею діапазонів квантування у двох стегозображеннях. Модифікована таблиця

діапазонів квантування дасть можливість зменшення кількості виникнення помилок при витягуванні вбудованого ЦВЗ.

У модифікованому методі пропонується в якості таблиці діапазонів квантування (ТДК) використати декілька варіантів таблиць, що відрізняються розмірністю регіонів і, відповідно, кількістю вбудованих бітів. Для вибору ТДК, що забезпечує найменші візуальні спотворення контейнера в процесі стегоперетворення, був проведений обчислювальний експеримент на основі 200 цифрових знаків у градаціях сірого, в які ЦВЗ занурювався класичним PVD при використанні різних ТДК. За результатами проведених експериментів спостерігалось збільшення значень PSNR для цифрового знаку зі збільшенням кількості регіонів, тобто гірші результати досягалися при використанні 6 регіонів (R) – для цифрового знаку у градаціях сірого значення PSNR складало 40,5364дБ; для 13 регіонів – 45,8762дБ. Так як розширена таблиця викликає ще більшу кількість помилок, то пропонується модифікована ТДК. Значення t приймається мінімальним при значеннях upper - lower ≤ 13 і максимальним при upper - lower > 13. Модифікована ТДК наведена у табл. 1.

Таблиця 1 – Модифікована таблиця діапазонів квантування

	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8
[lower, upper]	[0,1]	[2,5]	[6, 11]	[12, 19]	[20, 29]	[30, 41]	[42, 55]	[56, 71]
t	1	2	2	3	3	3	3	4
	R_9	R_{10}	R_{11}	R_{12}	R_{13}	R_{14}	R_{15}	R_{16}
[lower, upper]	[72, 89]	[90, 109]	[110, 131]	[132, 155]	[156, 181]	[182, 209]	[210, 239]	[240, 255]
t	4	4	4	5	5	5	5	4

Вдосконалений метод PVD для захисту цифрових зображень опишемо такими кроками:

Крок 1: Розподіл кольорового зображення C на блоки розміром 2x2. Якщо і-тий блок C^i, то пікселі в C^i дорівнюють: $C^i_{j,k}$ $(0 \le j, k \le 1)$.

Крок 2: Розподіл кольорових пікселів у кожному блоці на R, G та B. $C^i_{j,k}$ розкладається на $R^i_{j,k}$, $G^i_{j,k}$ та $B^i_{j,k}$ $(0 \le j, k \le 1)$.

Крок 3: Перегрупування $R^i_{j,k}$, $G^i_{j,k}$ та $B^i_{j,k}$ значень пікселів у блоці C^i для генерації $NR^i_{j,k}$, $NG^i_{j,k}$ та $NB^i_{j,k}$ $(0 \le j, k \le 1)$.

Крок 4: Знаходження мінімального значення пікселя $NR^i_{j,k}$, $NG^i_{j,k}$ та $NB^i_{j,k}$ відповідно. Функція повертає мінімальне значення.

Крок 5: Створення пар у двох або трьох напрямках.

Крок 6: Застосування методу PVD у двох або трьох напрямках.

Крок 6-1: Використання методу PVD до двох пар для вбудовування секретних даних. Дві пари після виконання схеми PVD, які визначаються як ($S_1NR^i_{0,1}$, $SNR^i_{0,0}$) і ($S_2NR^i_{0,1}$, $SNR^i_{0,0}$).

Крок 6-2: Використання методу PVD до трьох пар для вбудовування секретних даних. Три пари після використання алгоритму PVD, які визначаються як ($S_1NR^i_{0,1}$, $SNR^i_{0,0}$), ($S_2NR^i_{0,1}$, $SNR^i_{0,0}$) і ($S_3NR^i_{0,1}$, $SNR^i_{0,0}$).

Крок 7: Поділ пікселів двома парами або трьома парами до двох зображень.

Крок 8: Створення двох кольорових стегозображеннь S_1C і S_2C. Функція поєднує R, G та B для створення кольорового зображення.

Крок 9: Повторення наведених вище дій для усіх блоків.

Для визначення практичної цінності запропонованого удосконалення проведено аналіз показника PSNR та досліджено експериментальним шляхом кількісні показники модифікованого методу за рахунок реалізованої програмної розробки.

Висновок. Запропоновано вдосконалення стеганографічного методу PVD та розроблено відповідний алгоритм. Запропоновано використати модифіковану таблицю діапазонів квантування для вбудовування інформації у цифрове зображення, щоб зменшити кількість помилок під час витягування ЦВЗ. Також запропоновано алгоритм приховування даних із використанням різноспрямованої різниці значень пікселів на основі кольорового зображення, що надає можливість зберегти кращу якість зображення після вбудовування в нього ЦВЗ в порівнянні із попередніми методами.

Для аналізу модифікованого методу були порівняні такі основні показники зображення як PSNR, ємність та індекс якості для зображень із вбудованим ЦВЗ вдосконаленим методом та його попередніми модифікаціями. Експериментальні результати продемонстрували, що запропонована схема має високу здатність до вбудовування та прийнятну непомітність у якості візуального зображення.

Список літератури. 1. Wu H.C. Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods / H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang // IEEE Transactions on Image and Signal Processing. – 2005. – № 5. – P. 611 − 615. – ISBN 0-8247-2777-0

УДК 654.1

В.І. Іванцов, А.Г. Тараненко
Національний авіаційний університет, м. Київ

ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ МОБІЛЬНОГО АБОНЕНТА

Визначення місцезнаходження є дуже важливою функцією в мережі стільникового мобільного зв'язку. Стільникові мережі постійно розвиваються і зазнають все більше оновлень. Саме завдяки цьому, ми можемо дуже точно визначати де перебуває конкретний абонент. Перелік того, де функція визначення місцезнаходження потрібна, достатньо великий. Вона вирішує деякі важливі питання безпеки і реалізована у різноманітних додатках, що використовують цю функцію, щоб покращити свій сервіс та зробити більш комфортне життя людей. Наприклад, якщо у власника було викрадено злодієм мобільний телефон, то можливо встановити де перебуває даний пристрій, знайти та повернути його власнику, або ж для змоги персонально пропонувати рекламні акції та послуги на мобільний телефон користувача, коли він перебуває поряд. Це все можливо за допомогою послуги LCS (LoCation Services).

Послуга визначення місцезнаходження LCS в мережах UMTS та GSM розподіляється певним чином між існуючими елементами мережі. Для роботи та підтримки LCS до всієї системної архітектури доданий важливий новий мережний елемент, а саме шлюзовий мобільний центр визначення місцезнаходження GMLC (Gateway Mobile Location Centre).

В наземній мережі доступу UTRAN (Universal Terrestrial Radio Access Network), так і в базовій мережі CN (Core Network) присутні обладнання та функції LCS. Компоненти, що містяться в UTRAN, здійснюють збір та обробку даних про позиціонування для визначення місцезнаходження мобільного пристрою. Центр GMLC забезпечує в базовій мережі CN зв’язок між компонентами для передачі даних позиціонування іншим сервісам або додаткам клієнтів. За допомогою контролера SRNC (Serving Radio Network Controller) контролюються та завершаються вимірювання параметрів радіоканалу, а також вимірювання параметрів режиму м’якого хендоверу.

Важливо зазначити, щоб визначати місцерозташування для позиціонування за допомогою GPS (Global Positioning System), створений окремий мережний центр SMLC (Serving Mobile Location

Centre). В мережі GSM він може бути вбудованим до контролеру базової станції BSC (Base Station Controller), або бути окремим елементом фізичної мережі.

Також варто сказати, що послуга LCS є важливою тоді, коли абонент перебуваєте в незнайомому місці і не знаєте наскільки далеко він знаходиться від свого будинку і в якому напрямку йому далі рухатись. Вона визначить поточне місце абонента та прокладе найкоротший маршрут до потрібного йому місця. Використовуючи географічні координати, що для зручності підв'язані до певних квадратів на сітці карти, а також номери будинків і назви вулиць, точна інформація про місцерозташування відобразиться на екрані гаджету абонента. Інформація може бути виведена у вигляді текстових повідомлень, голосових повідомлень або певного зображення карти. Важливим є те, що всю потрібну інформацію можна подивитися в будь-який момент, коли вона потрібна абоненту.

Сервіси LCS мають декілька шляхів розвитку. Це використання точної інформації про місцезнаходження, яка отримується за допомогою GPS-приймача, або можна використовувати інформацію про приблизне місцезнаходження користувача взявши за основу радіопокриття мережі зв'язку. Ще одним із шляхів є обчислення часу за допомогою сучасних методів та інших даних, що є в радіомережі, які надсилаються до мобільного пристрою користувача. На основі цієї інформації розробляється та є доступними велика кількість комерційних додатків, що допомагають користувачам у різних сферах життя. До прикладу, такими комерційними додатками, що для своєї роботи використовують інформацію про місцезнаходження, є додатки "Airbnb", "Google Maps", "Uklon", "Eway", гра "Pokemon Go" та багато інших.

В підсумку, з'ясувавши структуру роботи послуги LSC та користь її застосування, можна сказати, що використання її дозволяє вирішити багато питань в різних сферах життя. Важливо підкреслити, що послуга визначення місцезнаходження постійно вдосконалюється, оновлюється та розвивається. З'являються нові набори функцій, які все більше допомагають користувачам, розширюють своє коло застосування. Вона стала невід'ємною частиною сучасних стільникових мереж, щоб до центрів обробки передавати дані про позиціонування із мобільних пристроїв. Багато комерційних додатків беруть її в свій склад, щоб функціональність цих додатків була більш вищою.

УДК 621.315.212

А. Коваленко, В. Антонов
Національний авіаційний університет, м. Київ

СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА ПІДПРИЄМСТВА

У сучасному інформаційному суспільстві передача даних має ключове значення для ефективного функціонування організацій. Зростаючі обсяги інформації, швидкість передачі даних та висока надійність стали невід'ємною частиною успішного бізнесу. Саме тут важливу роль відіграє структурована кабельна система. Структурована кабельна система є комплексом обладнання, кабелів та аксесуарів, які використовуються для передачі даних, голосу та відео в приміщеннях. Вона забезпечує інфраструктуру для мережі передачі даних, що дозволяє ефективно забезпечувати комунікацію між комп'ютерами, пристроями зв'язку та іншими пристроями.

Приклад підключення кабелів доступу до житлових приміщень та мережі

Екрановані з’єднувальні розетки в окремих приміщеннях повинні бути технічно узгоджені з прокладеними кабелями, що може бути досягнуто, наприклад, тим фактом, що з’єднувальні розетки, розподільна панель і кабель походять з одного асортименту продукції одного виробника. Це єдиний спосіб уникнути можливих збоїв, спричинених невідповідностями або збоями. Розетки доступні з одним або двома підключеннями (наприклад, для ПК і телефону).

Незалежно від застосування (телефон, Інтернет або, в майбутньому, IP-телебачення), тип роз’єму RJ45, який зарекомендував себе як універсальний роз’єм, слід використовувати для всіх з’єднань. Щоб бути готовими до поточних і майбутніх послуг і додатків, роз’єми підключення повинні відповідати 10 Gigabit Ethernet (так звана категорія 6A).

Місце встановлення розподільних коробок значною мірою залежить від запланованого використання приміщень та їх розмірів. Якщо остаточне призначення кімнати ще не визначено під час монтажу, одне з’єднання на 3,75 м окружності кімнати виявилося хорошим орієнтиром. Наприклад, для кімнати площею 12 квадратних метрів і довжиною стін 3 і 4 метри це означає:

Периметр кімнати: 3м + 4м + 3м + 4м = 14м

1 з'єднання на 3,75 м: 14 м : 3,75 м = 3,73

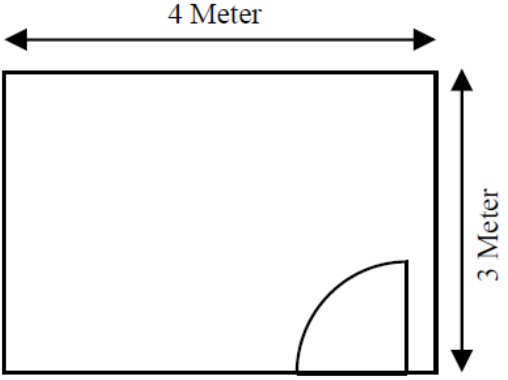


Рис. 1 - Кімната

Для цього простору необхідно передбачити 3,73, тобто 4 заокруглені з'єднання.

Практично використовувати дві подвійні розетки, адже там, де є ПК, часто потрібен і телефон.

Порада: на практиці виявилося корисним надавати занадто багато з'єднань, а не занадто мало. Відсутня розподільна коробка, яку неможливо модернізувати пізніше або можна модернізувати лише з великими зусиллями, дратує набагато більше, ніж занадто багато розподільних коробок, які вам не знадобляться пізніше.

Порада: Крім з'єднувальних розеток, необхідно також встановити розетки для живлення приладів.

Що включає:

- точка підключення пасивного будинку

=> HÜP = пункт вводу в будинок - електронні компоненти

=> ENS = Технологія електричних систем для будинку та будівництва (Это у них модемы свичи роутеры)

Лінія, яка веде в будівлю ззовні, закінчується в пункті передачі будинку. Технологія електронної системи забезпечує передачу даних (наприклад, DSL) і телефонний зв'язок. Вони підключаються до патч-панелі гнучкими кабелями (патч-кабелі з роз'ємами 6 категорії RJ45 для Інтернету та передачі даних та/або роз'єми 3 категорії RJ11/12 для телефону). Ці гнучкі кабелі закуповуються замовником. Кабельне/супутникове телебачення передається через окремі коаксіальні кабелі та компоненти. Електропроводка, описана в цій брошурі, не має

нічого спільного з класичним кабельним телебаченням. Однак він підходить для майбутнього відео через IP та IP-телебачення, оскільки ці послуги розглядаються як дані DSL. Порада: Рекомендується використовувати розподільники RJ45 і розетки із захистом від перегину для контактів 1/2 і 7/8 або можливість підключення штекерів RJ11/12, щоб запобігти пошкодженню контактів під час використання телефонних штекерів (RJ11/12). уникати.

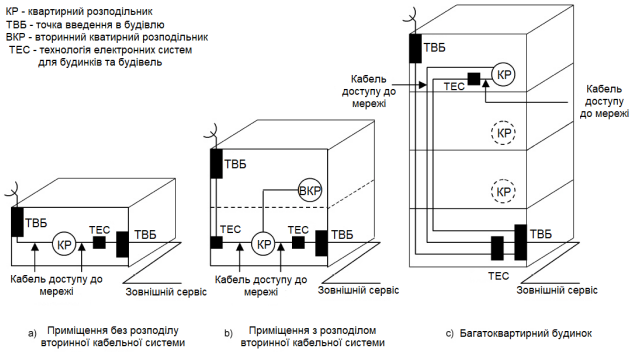


Рис 2. - Підключення квартирної електропроводки

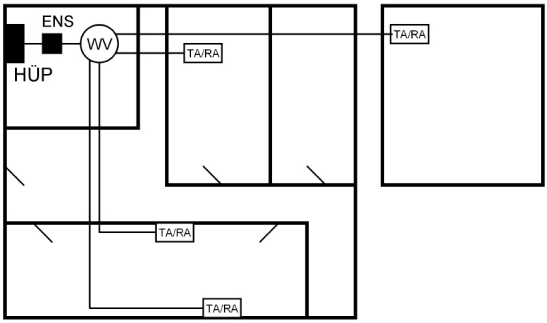


Рис 3. - квартира DIN EN50173-4:2007

Абревіатура: HÜP = точка передачі будинку ENS = технологія електричних систем для будинків і будівель

WV = квартирний розподільник TARA = підключення до інформаційних технологій.

Структурована кабельна система (СКС) виникла з метою створення надійного та ефективного середовища для передачі даних, забезпечення гнучкості та масштабованості мережі, а також спрощення управління та підтримки. Побудова СКС включає етапи проектування, розгортання та експлуатації, які потребують розуміння принципів та використання міжнародних стандартів. Компоненти СКС включають зовнішні та внутрішні магістралі, горизонтальну підсистему та функціональні елементи, які сприяють правильній роботі та ефективності кабельної системи.При виборі оптоволоконних кабелів потрібно враховувати різні параметри, такі як пропускна здатність, довжина магістралей та горизонтальних з'єднань, витримка від загублення сигналу та шуми, для забезпечення правильної роботи мережі. Вибір кабелю для СКС підприємства у багатоповерховій будівлі залежить від таких факторів, як передавальна спроможність, тип передачі даних (мідний або оптичний), відстань передачі, електромагнітна сумісність та вартість.Розрахунки горизонтальної та магістральної підсистем, схеми розміщення елементів СКС на поверхах, апертури оптичного кабелю, загасання та взаємні впливи в оптичному кабелі є важливими етапами проектування СКС. Перелік обладнання для СКС підприємства має бути складений з урахуванням вимог та потреб організації. Загальні висновки підсумовують, що структурована кабельна система є необхідним компонентом сучасних мереж для забезпечення ефективної передачі даних та оптимального функціонування підприємства. Розуміння основних принципів та застосування стандартів у побудові СКС є важливим для досягнення надійності, ефективності та масштабованості мережі.

УДК 654.000:621.305

С.С. Корєнєва
В.В. Антонов
Національний авіаційний університет, м. Київ

КОНВЕРГЕНТНА МЕРЕЖА ЗВ'ЯЗКУ

На сучасному етапі розвитку галузі зв'язку велике значення має організація технічної експлуатації систем і мереж зв'язку. Значну увагу приділено перспективним засобам і технологіям телеко-мунікацій, проблемам впровадження новітніх інформаційно-комуніка-ційних технологій, стану та розвитку телекомунікацій, моделям при-скореного розвитку телекомунікацій.

Конвергенція в телекомунікаціях означає надання мережами з різними технологічними можливостями практично однакового набору послуг або об'єднання кінцевих пристроїв, таких як телефон, персональний комп'ютер та телеприймач, в єдиний термінал.

Конвергенція передбачає створення конвергентних систем зв'язку на основі об'єднання мереж, що відрізняються рядом ознак. Це насамперед мережі, що використовують різноманітні телекомуніка-ційні технології, локальні та територіальні мережі, дротові та бездро-тові мережі, фіксовані та мобільні мережі, мережі доступу та транспортні мережі.

Конвергенція обумовлена бажанням мати єдину інфраструктуру для певних послуг, навіть якщо ці служби підтримуються різними технічними рішеннями. Ці рішення можуть базуватися на телекомунікаційних або інформаційних технологіях. Важливо відзначити, що конвергенція сервісів також призводить до значного збільшення можливостей єдиного сервісу, як це відбувається, наприклад, у мультимедійних комунікаціях. Природно, що конвергенція послуг завжди передбачає певний рівень конвергенції в технічних системах, які надають ці послуги.

У сфері мережевої конвергенції найбільший інтерес представляє той факт, що послуги Інтернету можна надавати через лінії доступу до телефонної мережі. Тому конвергенцію можна розглядати як взаємодію між телефонною мережею та Інтернетом на межі телефонної мережі. Надання послуг телефонії між користувачами Інтернету та користувачами телефонної мережі є одним із основних напрямків конвергенції мереж.

Ще одним важливим напрямком конвергенції є стирання кордонів між фіксованими та мобільними мережами. Йдеться про інтеграцію комутаторів для проводових і мобільних радіомереж (так званий комбінований комутатор, CombiSwitch) і конвергенцію послуг, тобто абоненти можуть отримувати послуги за будь-якого доступу до мережі.

Комп'ютерна та мережева інтеграція є природним результатом процесів загальної конвергенції. Можна з упевненістю стверджувати, що розвиток комп'ютерної техніки та її архітектури став основою для розробки принципів і системних рішень, реалізованих у сучасних мережах.

Багаторівневе представлення концепції конвергенції: основу такої піраміди становлять фізичні мережеві компоненти як фіксованих, так і мобільних мереж (базові станції, багатосистемні мобільні користувацькі термінали, точки доступу, контролери базових станцій). Наступний рівень складається з самих мереж як набору компонентів із чітко визначеними топологічними рівнями та зонами покриття. Наступний рівень — це набір програм, які забезпечують підтримку різноманітних служб, таких як голос, дані та мультимедіа. Для доступу до всіх існуючих систем потрібен інтерфейс користувача (телефон, смартфон).

Отже, конвергенція породжує нову парадигму завдяки можливості доступу до інформації «в будь-який час, у будь-якому місці, з будь-якого пристрою». Рушійною силою конвергенції в інформаційно-телекомуніка-ційних системах є розробка нових і вдосконалення існуючих послуг. Конвергенція фіксованих і мобільних інформаційно-телекомуніка-ційних платформ і мереж служить технологією спільного використан-ня ресурсів мереж мобільного і фіксованого зв'язку для надання користувачу єдиної безперебійної послуги незалежно від його місце-знаходження, а також для організації єдиної послуги та єдиний тариф на послуги.

УДК 004.7:004.62 (043.2)

В.М. Костяненко, Ю.В. Петрова

Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА ЖИТЛОВОГО КОМПЛЕКСУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ QUADRO PLAY

Ключові слова: Телекомунікаційна мережа, телефонія, телебачення, мережа «Інтернет», мобільний зв’язок, конвергенція, базова станція, UMTS. В сучасному світі телекомунікації займають все більше й більше місця у повсякденному житті людей, що створює потребу в розвитку технологій і систем комунікацій. Швидкий і надійний доступ до інформації та зв'язку є ключовим фактором розвитку суспільства та його економіки. Quadro Play - інноваційна технологія, яка об'єднує можливості телефонної мережі, телебачення, доступу до інтернету та інших сервісів. Використання цієї технології дозволяє забезпечити належний рівень якості телекомунікаційних та інтернет-послуг для мешканців житлового комплексу. Це комплексне рішення, яке дозволяє користувачам отримувати всі ці послуги від одного провайдера, що забезпечує зручність управління послугами та потенційну економію на їх вартості. Технологія Quadro Play є важливою частиною стратегії "конвергенції" в сфері телекомунікацій. Конвергенція означає злиття різних технологій та послуг на одній платформі. Вона дозволяє забезпечити більшу гнучкість та зручність для користувачів, оскільки вони можуть отримати різні послуги через одне з'єднання [1]. Quadro Play може використовувати різні технології передачі даних, включаючи DSL, кабельний модем, оптоволокно, бездротові технології та інші. Вибір технології може впливати на швидкість і надійність послуг, а також на вартість і складність встановлення та управління мережею. Телефонія є ключовим компонентом будь-якої телекомунікаційної мережі, включаючи мережу Quadro Play. З технологічної точки зору, вона може бути реалізована як традиційна PSTN (Public Switched Telephone Network) телефонія або як IP-телефонія Використання технології Quadro Play може вимагати спеціалізованого обладнання, яке підтримує різні типи послуг. Це може включати в себе спеціалізовані модеми, маршрутизатори, комутатори та інше обладнання, що може підвищити вартість встановлення та управління мережею [2]. Детальний аналіз технічних параметрів і розрахунків, пов'язаних з побудо-

вою мережі Quadro Play, дозволяє оптимізувати процеси проектування та впровадження, а також забезпечити стабільну роботу мережі.

Використання сучасного обладнання і передових технологій в рамках побудови мережі Quadro Play відкриває можливості для подальшого розвитку та модернізації мережі, а також забезпечує можливість інтеграції з новими технологіями.

Проектування мережі Quadro Play для житлового комплексу передбачає врахування конкретних потреб та вимог жителів, включаючи швидкість доступу до інтернету, якість зв'язку, доступ до цифрового телебачення тощо [3]. Комплексний підхід до розрахунку параметрів мережі, включаючи коефіцієнта навантаження у радіоканалі системи UMTS, зони покриття БС, параметрів одномодового оптичного волокна, ділянки регенерації, є ключовим для побудови ефективної та надійної мережі Quadro Play. Результати дослідження показали, що Quadro Play - це ефективна та гнучка технологія, яка забезпечує одночасне надання послуг телефонії, широкосмугового доступу до Інтернету, цифрового телебачення та мобільного зв'язку. Використання Quadro Play дозволяє забезпечити високу якість обслуговування, широкий спектр послуг та високий рівень задоволеності користувачів.

В ході роботи було проведено підбір необхідного обладнання для побудови мережі Quadro Play, розраховано приблизну вартість побудови мережі, а також оцінено об'єм трафіку та коефіцієнт навантаження в радіоканалі системи UMTS. Результати підтверджують важливість правильного проектування та планування при побудові телекомунікаційних мереж на основі технології Quadro Play і вказують на перспективність її використання для майбутнього розвитку телекомунікаційних мереж, зокрема в житлових комплексах.

Список використаних джерел:

1. OpenWorldLearning. Exploring Triple Play In Telecommunications: What It Is And How It Works (2023) [https://www.openworldlearning.org/exploring-triple-play-in-telecommunications-what-it-is-and-how-it-works/]

2. M. Katz, Creating Quad and Triple Play Solutions for Operators [https://www.researchgate.net/publication/228784636_Quad_play_a_new_telecom_service_trend]

3. Francisco J. Hens; José M. Caballero, "Quadruple Play," in Triple Play: Building the converged network for IP, VoIP and IPTV [http://surl.li/hegyj]

УДК 621.396.4

О.Ю. Юдін, Д.М. Бондаренко, Н.В. Лисенко,
О.А. Липський, Я.І. Стефанишин,
ДержНДІ технологій кібербезпеки та захисту інформації, м. Київ

ПЕРСПЕКТИВИ СТВОРЕННЯ ТА ВИКОРИСТАННЯ СТАНЦІЙ ТРОПОСФЕРНОГО СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ

Вступ. Специфіка тропосферного розповсюдження радіохвиль обумовлює значні додаткові апаратурні витрати (і, відповідно, громіздкість станцій тропосферного зв'язку, ТРС), наслідком чого, наразі, є втрата комерційної привабливості порівняно з супутниковими технологіями. Разом з тим, підвищена оперативність і зручність розгортання, зменшення експлуатаційних витрат (зокрема, на оренду супутникових каналів), незалежність від непередбачуваних дій орендодавця, а також практична відсутність ризиків цілеспрямованого придушення, наразі, актуалізують використання ТРС. Робота містить основні характеристики та результати випробувань експериментальних зразків ТРС "Гермес".

Основна частина. Тропосферне розповсюдження радіохвиль, загалом, пов'язано із значно більшими затуханнями на трасі (до 80 дБ), порівняно з трасами прямої видимості, а також багатопроменевістю. Зважаючи на це, тропосферний сигнал має низку особливостей, зокрема, повільні та швидкі завмирання, залежність від часу доби та року, відстані і частоти, метеорологічних та кліматичних факторів, висоти встановлення антен та кутів їх закриття, а також втрат підсилення антен. Наслідком цього є специфічні спотворення інформаційного сигналу (селек-тивні завмирання та міжсимвольна інтерференція).

На світовому ринку тропосферних станцій домінують компанії США (Comtech Systems та Cubic GATR Technologies), забезпечуючи створення сучасних станцій та постачання їх силовим структурам.

Основу конструкції вітчизняної ТРС "Гермес", розміщеної на автомобільному причепі (Рис. 1), становить використання широкосмугових сигналів на тропосферному відрізку траси, активної фазованої приймально–передавальної антени, турбокодування для корегування помилок, комп'ютерного управління та термостатування обладнання.

До складу ТРС включено приймально-передавальну антену (ППА), модеми цифровий та ШПС, модуль управління, опорно-

поворотний пристрій та блок безперебійного живлення. ППА включає 64 приймально-передавальні модулі, які випромінюють сигнали потужністю, орієнтовно, 5 Вт кожний. На тропосферному відрізку траси модемом ШПС формується широкосмуговий сигнал, який детектується за допомогою узгодженого фільтра на поверхневих акустичних хвилях.

Рис. 1. Загальний вигляд експериментальних зразків ТРС “Гермес”

Основні технічні характеристики ТРС “Гермес”: режими роботи “ШПС” та, на інтервалі дифракційного розповсюдження радіохвиль, “ВСС” (в яких забезпечуються, відповідно, інтервали зв’язку ≥120 км та <60 км, швидкість передавання інформації 2,048 Мбіт/с та 4,096 Мбіт/с, а також модуляція BPSK та QPSK), робоча частота 4,435–4,75 ГГц, потужність випромінювання ≥250 Вт, коефіцієнт підсилення фазованої антени ≥34 дБі), ймовірність помилки передавання інформації (при Eb/No=3 дБ), не гірше 10^{-4}, потужність споживання <2 кВА.

Висновки. Тропосферні станції спеціального зв’язку мають перспективи розвитку, як певна альтернатива станціям супутникового зв’язку. Випробування створених експериментальних зразків ТРС “Гермес” з активною фазованою антенною решіткою підтвердили необхідність максимального спрощення конструкції, зокрема, створення легкої (переносної) малопотужної ТРС для дифракційного відрізку траси (60 км) з пасивною фазованою антенною решіткою і традиційним локалізованим приймально-передавальним пристроєм та більш потужної ТРС для тропосферного відрізку траси, яка має підвищені відстані (більше 120 км) та швидкості передавання інформаційного потоку, а також роз-поділений приймально-передавальний пристрій.

УДК 621.396.4

О.Ю. Юдін[1], О.А. Липський[1], Я.І. Стефанишин[1], А.М. Алесин[2], А.А. Алесин[2]

[1]ДержНДІ технологій кібербезпеки та захисту інформації, м. Київ
[2]Приватне акціонерне товариство "МІРРАД", м. Київ

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ V- ТА E-ДІАПАЗОНІВ

Вступ. Наразі можливості традиційних діапазонів частот (до 40 ГГц) практично вичерпані. Поточним світовим трендом удосконалення широкосмугових засобів зв'язку є освоєння діапазону міліметрових (ММ) хвиль, перспективність якого визначається можливістю значного збільшення швидкостей передавання інформації. Суттєвим недоліком ММ- діапазону є значне затухання радіохвиль в атмосфері, що обумовлює, порівняно, невеликі інтервали зв'язку. Разом з тим, цей недолік відіграє і позитивну роль, обмежуючи можливості впливу засобів радіоелектронної боротьби (РЕБ). Крім того, перспективність ММ-діапазону, наразі, визначається нерозвиненістю засобів РЕБ цього діапазону. Робота містить результати випробувань макету радіолінії V-діапазону.

Основна частина. Загалом, послаблення радіохвиль в атмосфері зрос-тає з підвищенням частоти. Атмосферні гази і водяна пара обумовлюють в радіодіапазоні частоти резонансного затухання, зокрема, 22,2 (H_2O), 60 (O_2), 118,8 (O_2) та 180 (H_2O) ГГц. Наразі, в ММ-діапазоні для радіоліній зв'язку використовуються два відрізки, зокрема, V–діапазон (59–64) ГГц (в якому знаходиться частота резонансного затухання, обумовлена атомарним O_2) та E–діапазон (71–76 і 81–86) ГГц. Зважаючи на це, V-діапазону притаманне значне погонне затухання радіохвиль в атмосфері (до 14 дБ/км), внаслідок чого інтервали зв'язку складають 2–5 км. Величина погонного затухання E-діапазону – біля 0,5 дБ/км, що дозволяє збільшити інтервал зв'язку до 10–12 км.

Радіолінії V- та E-діапазону забезпечують недосяжні раніше швид-кості передавання даних (до 2 та 10 Гбіт/с відповідно), типово при їх створенні використовується адаптивна модуляція та ретрансляція. Коло світових виробників радіорелейних станцій (РРС) цих діапазонів включає компанії США (BrigeWave Communications; Fastback Networks; E-band Communications), Норвегії (Ericsson), Греції (Intra-

com-Telecom) та інших країн.

Особливістю побудови макетного зразка РРС V-діапазону "Кассіопея" (Рис. 1) є використання спільного гетеродину та окремих антен з коефіцієнтами підсилення (що відрізняються на 25–30 дБі) для літерних передавача та приймача.

Рис. 1. Загальний вигляд макетного зразка РРС "Кассіопея"

Основні технічні характеристики РРС "Кассіопея": робочі частоти 58,75 та 61,25 ГГц; потужність випромінювання – 10 дБм, модуляція – BPSK, дуплексне рознесенням робочих частот – 2,5 ГГц, сумарний коефіцієнт підсилення передавальної та приймальної антен – 60 дБі, температура шумів вхідного підсилювача – 500 К, цифровий модем з турбокодуванням Q–Flex фірми Teledyne Paradise Datacom Ltd, USA.

У результаті випробувань радіолінії V-діапазону забезпечено передавання на відстань 1,75 км цифрової інформації зі швидкістю 10 Мбіт/с з бітовим відношенням сигнал/шум E_b/N_0=7 дБ (досягнуті показники, в основному, визначалися характеристиками вибраної траси та цифрового модема Q–Flex.

Висновки. ММ-діапазон видається перспективним для оперативної організації захищеного локального зв'язку, в основному, тактичного рів-ня, зокрема, V–діапазон для створення локальних мереж спеціального зв'язку (локальні спеціальні об'єкти, рій дронів тощо) та дистанційного керування спеціальними об'єктами (наприклад, дистанційне управління радіолокатором), а E–діапазон, переважно, для створення радіоліній "першої та останньої милі".

УДК 004.056.5 (043.2)

Є.Ю. Лиштва, В.П. Климчук
Національний авіаційний університет, м. Київ

ЗАХИСТ МУЛЬТИМЕДІЙНИХ МЕРЕЖ ВІД АТАК DDOS НА ОСНОВІ ТЕХНОЛОГІЇ DPI

DDoS-атаки стають все поширенішими і серйознішими загрозами для мультимедійних мереж. У таких атаках велика кількість шкідливого трафіку спрямовується на цільовий сервер з метою перевантаження та призведення до відмови у його роботі.

Одним з ефективних засобів захисту є використання технології Deep Packet Inspection (DPI). DPI дозволяє аналізувати заголовки та вміст пакетів даних, що пересилаються через мережу, та виявляти аномалії та підозрілу активність.

Застосування DPI для захисту мультимедійних мереж від атак DDoS має кілька переваг. По-перше, воно дозволяє відокремити легітимний трафік від шкідливого, ідентифікувати зловмисники та їх методи атаки. По-друге, DPI може виявити характерні ознаки DDoS-атак, такі як надмірний обсяг запитів чи неправильно сформовані пакети, і прийняти відповідні захисні заходи. Нарешті, DPI дозволяє швидко реагувати на нові типи DDoS-атак та надавати актуальний захист.

Однак, варто зазначити, що застосування DPI вимагає значних ресурсів, які можуть впливати на продуктивність мережі. Додатково, зловмисники постійно вдосконалюють свої методи атаки, що може ускладнити роботу системи DPI. Тому, ефективне застосування DPI для захисту мультимедійних мереж від атак DDoS потребує постійного моніторингу, аналізу та оновлення системи захисту.

У підсумку, технологія DPI є потужним інструментом у захисті мультимедійних мереж від атак DDoS. Її використання дозволяє виявляти та блокувати шкідливий трафік, забезпечуючи стабільну роботу мережі та захищаючи її від негативного впливу атак. Однак, необхідно забезпечувати постійний моніторинг та оновлення системи захисту, щоб протистояти постійному розвитку методів атаки.

Системи виявлення та запобігання вторгненням. Впровадження подібних систем для захисту інформації є необхідністю для всіх серйозних мережевих інфраструктур, оскільки існують програми, які постійно вишукують уразливості в будь-якому обладнанні, підключеному до глобальної мережі. Наприклад, пошуковий движок Shodan в автоматичному режимі

збирає інформацію про під'єднані пристрої, які не мають жодної частини системи безпеки. Користувачі Shodan знаходять системи управління крематорієм, газовою станцією тощо, які не мають реквізитів доступу, або вони налаштовані за замовчуванням. Отже, до них можна легко проникнути та зменшити працездатність.

Проти такого впливу і спрямовані системи виявлення та запобігання вторгненням, тому вони є часто використовуваним інструментом у політиці безпеки.

Система виявлення вторгнень (СВВ) (англ. Intrusion Detection System (IDS)) - програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу.

Система запобігання вторгненням (СЗВ) (англ. Intrusion Prevention System (IPS)) - програмний або апаратний засіб, що здійснює моніторинг мережі або системи в реальному часі з метою виявлення, запобігання або блокування шкідливої активності.

Системи запобігання вторгненням можна вважати розширенням систем виявлення вторгнень, оскільки завдання відстеження атак залишається однаковим. Але СЗВ повинна відстежувати вторгнення в реальному часі й одразу здійснювати дії щодо запобігання атакам. Для цього вони використовують: скидання з'єднань, блокування потоків трафіку в мережі, видачу сигналів оператору. Крім цього, такі системи можуть дефрагментувати пакети, змінювати порядок TCP пакетів для захисту від пакетів зі зміненими SEQ і ACK номерами тощо.

Ці системи використовуються для автоматизації процесу контролю над подіями, які протікають у комп'ютерній системі або мережі, та аналізу цих подій з метою пошуку ознак проблем безпеки. Через те, що кількість різних способів і видів організації несанкціонованих вторгнень у мережі за останній час значно збільшилась, то системи виявлення вторгнень стали обов'язковою частиною інфраструктури безпеки для більшості організацій. Цьому сприяють як велика кількість літератури з цього питання, яку потенційні зловмисники уважно вивчають, так і все більш витончені підходи до виявлення спроб проникнення в інформаційні системи.

Сучасні системи виявлення вторгнень мають різну архітектуру, основними з яких є: мережева та локальна. Мережеві системи встановлюють на виділених для цих цілей комп'ютерах так, щоб вони могли аналізувати трафік, що протікає локальною обчислювальною мережею. Локальні ж си-

стеми розміщуються на тих комп'ютерах, які потребують захисту, і вивчають певні події (програмні виклики або дії користувача).

Крім архітектури СВВ також можуть розрізняти за методикою виявлення: частина систем шукає аномальну поведінку, інша - зловмисну.

Методики виявлення аномальної та зловмисної поведінки користувачів. Системи виявлення аномальної поведінки (від англ. Anomaly Detection) засновані на тому, що СВВ відомі ознаки, що характеризують правильну або допустиму поведінку об'єкта спостереження. Під "нормальною" або "правильною" поведінкою розуміють дії, які виконуються об'єктом і не суперечать політиці безпеки.

Системи виявлення зловмисної поведінки (Misuse Detection) засновані на тому, що заздалегідь відомі ознаки, що характеризують поведінку зловмисника. Найпоширенішою реалізацією технології виявлення зловмисної поведінки є експертні системи (наприклад, системи Snort, RealSecure IDS, Enterasys Advanced Dragon IDS). Технології, що використовуються в цих системах (рис. 1).

Рис. 1. Існуючі технології СВВ

Висновки

Застосування технології DPI для захисту від DDoS-атак є важливим етапом у забезпеченні безпеки хмарних сервісів та мереж. Використання DPI дозволяє аналізувати та фільтрувати мережевий трафік, ідентифікувати та блокувати шкідливі пакети, що дозволяє знизити вплив DDoS-атак на інфраструктуру та забезпечити нормальну роботу мережі та сервісів.

Загалом, результати цієї роботи підтверджують важливість Cloud-технологій та застосування технології DPI для забезпечення безпеки мереж та інформаційних систем. Cloud-технології дозволяють покращити доступність, ефективність та масштабованість інфраструктури, забезпечуючи гнучкість та зниження витрат. Водночас, застосування DPI стає необхідним для виявлення та мінімізації впливу DDoS-атак на системи, дозволяючи аналізувати та фільтрувати мережевий трафік.

Проте, важливо враховувати обмеження технології DPI, такі як великі обчислювальні витрати та можливість помилок аналізу пакетів. Це вимагає ретельної настройки та постійного підтримання системи DPI з урахуванням особливостей мережі та типів атак.

Список літератури

1. Dmitry S. Vorunichev, Mihail S. Kostin and Sergey N. Zamuruev, "Classification of Methods of Reverse Engineering inthe Configuration Management of OriginalHigh-Tech Radio Electronic Products", 2018 IEEE International Conference “Quality Management Transport and Information Security Information Technologies” (IT &QM&IS), 24–28 Sept. 2018.

2. Jia-Hui HUANG, Dong-Qin FENG and Hong-Jian WANG, "A Method for Quantifying Vulnerability of Industrial Control System Based on Attack Graph[J]", ACTA AUTOMATICA SINICA, vol. 42, no. 5, pp. 792-798, 2017.

3. Chi-qian JIA and Dong-qin FENG, "Security assessment for industrial control systems based on fuzzy analytic hierarchy process[J]", Journal of Zhejiang University(Engineering Science), vol. 50, no. 4, pp. 759-765, 2016.

4. YL Zheng and S Zheng, "Cyber Security Risk Assessment for Industrial Automation Platform[C]", 2017 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 341-344.

5. Y Chen, J Hong and CC Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations[J]", IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 2541-2552, 2018.

УДК 621.341

Л.А. Лісовський, В.В. Антонов
Національний авіаційний університет, м. Київ

HFC МЕРЕЖА

Інтернет розвивається з шаленою швидкістю з моменту свого заснування. І разом із цим ми спостерігаємо відповідне зростання пропускної здатності виділеної мережі. У той час як закон Мура є сумно відомим у кремнієвих сферах, закон Нільсена про пропускну здатність Інтернету став відомим у світі мереж. В основному йдеться про те, що швидкість підключення до мережі для домашніх користувачів високого класу буде зростати на 50% на рік.

Цей закон спричинив велику частину розробки трафіку та планування пропускної здатності мережі у світі постачальників послуг. Це також призвело до багатьох досліджень на ці теми.

Дослідження закону Нільсена і кривих Клунана було розширено, включивши також використання трафіку на додаток до швидкості з'єднання з мережею. У його діаграмі нижче, відомому як Криві Клунана, закон Нільсена представлені синьою лінією посередині. Оскільки це логарифмічна шкала, 50% зведений річний темп зростання (CAGR) відображається як пряма лінія. Цікавим фактом є те, що графік починається з 1982 року з телефонного модему на 300 бод. Зараз ми перебуваємо в четвертому десятилітті та уважно слідкуємо за цією тенденцією.

Клунан зазначив, що середнє споживання абонентів у прайм-тайм (він же Tavg) також слідує цій же базовій тенденції, як показано на рисунку 1.1. Для постачальників послуг важливим показником є використання трафіку в групі послуг (SG). Використання трафіку SG є функцією кількості абонентів (Nsub) помноженої на середню пропускну здатність на підряд (Tavg) і показано серією рядків над лінією Нільсена.

Коли оператори підходять до планування потужності, вони намагаються зрозуміти, як довго може тривати архітектура HFC, перш ніж їм доведеться перейти до мережі Fiber to Premise (FTTP). Щоб зрозуміти це, наведена нижче діаграма збільшує криву Клунана та закон Нільсена протягом наступних двох десятиліть.

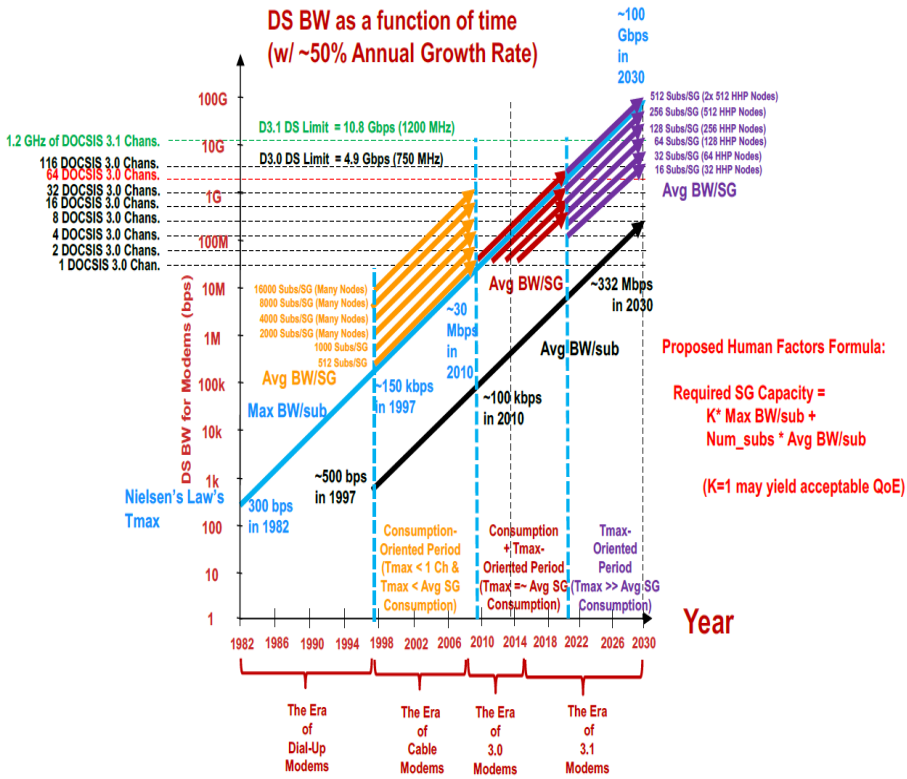


Рис. 1.1. Криві Клунана

Він передбачає, що максимальна швидкість мережі досягне 10 Гбіт/с до ~2024 року і перевищить 100 Гбіт/с на початку 2030-х років. Початкова ціль DOCSIS 3.1 (D3.1) становила 10 Гбіт/с, тож це означає, що HFC може досягти своєї стелі приблизно до 2024 року!

На перший погляд, це страшна пропозиція, оскільки мережі HFC можуть бути застарілими через 5-7 років, а для створення інфраструктури FTTP можуть знадобитися десятиліття. Таким чином, ключовим питанням стає: «Що відбувається з переважною більшістю передплатників HFC, які не належать до найвищих рівнів швидкості (так званих рівнів білборд), і коли?».

УДК 621.396 (043.2)

Б.В. Ломаєв
Національний авіаційний університет, м. Київ

БЕЗПРОВОДОВА МЕРЕЖА WLAN WI-FI – ВИД СУЧАСНОЇ ТА ЗРУЧНОЇ МЕРЕЖІ

Вступ. В теперішній час в області телекомунікаційних систем широкого застосування набуває використання безпроводових мереж WLAN Wi-Fi, що в свою чергу приводить до необхідності її правильної організації. Дане питання є досить важливим, бо розширення безпроводових мереж Wi-Fi в сучасному світі сприяє покращенню доступу до інформації та забезпечує зручність підключення для користувачів. В умовах сьогодення, даний тип мережі має стрімкий технологічний розвиток, що зацікавлює і привертає увагу більшості користувачів збільшуючи попит. Частішими стають випадки надання переваги в користуванні саме цьому типу мережі. Саме тому оптимальне проектування та ефективне використання безпроводових мереж є важливими завданнями для забезпечення надійного та швидкого доступу до мережі.

Організація безпроводової мережі WLAN Wi-Fi. Організація безпроводової мережі WLAN Wi-Fi є досить складним та особливим процесом який потребує детального аналізу та вивчення певних задач, з урахуванням багатьох факторів та принципів роботи безпроводових мереж Wi-Fi. Тому, в дослідженні розглядається та детально описується процес ефективної організації безпроводової мережі WLAN Wi-Fi в офісному приміщенні з використанням для цього всіх можливих та необхідних засобів.

На першому етапі було детально розглянуто теоретичні основи організації безпроводової мережі Wi-Fi, а саме класифіковані різні типи безпроводових мереж, описані використовувані протоколи безпроводових мереж Wi-Fi, аналізовано характеристики Wi-Fi мережі та її компонентів з виділенням основних переваг та недоліків, оглянуто стандарти Wi-Fi та їх різновиди.

В основній частині приділялася значна увага етапам проектування мережі та їх аспектам. Було запропоновано певний підхід щодо вибору місця розташування точок доступу (APs) з урахуванням низки факторів та принципів, які здатні впливати на загальну ефективність та продуктивність мережі. Було запропоновано підхід щодо розрахунку

кількості необхідних точок доступу та їх розміщення в офісному приміщенні при відповідному врахуванні різних умов. Окрема увага приділялася питанню забезпечення безпеки мережі та захисту від несанкціонованого доступу з наведенням ряду заходів та методів щодо належного захисту. Був наведений приклад розробленої структурної схеми організації мережі, що заснована на стандарті IEEE 802.11ac, та в якій передбачається визначення компонентів, необхідних для створення мережі та їх взаємозв'язків.

Наприкінці було розглянуто необхідні кроки для можливості успішної практичної реалізації безпроводової локальної мережі WLAN Wi-Fi офісного приміщення.

По-перше було проведено вибір мережевого обладнання, детальне обґрунтування, підстави обрання тих чи інших елементів з описом їх повного функціоналу. Важливим також було розглянути процес авторизації і доступу користувачів всередині мережі, саме тому було докладно описано принцип влаштування даного процесу.

Аналіз результатів організації мережі проводився шляхом проведення комплексної візуалізації покриття мережі з отриманням за допомогою спеціалізованого програмного забезпечення таких результатів, як рівень сигналу та очікувана фізична швидкість. Кожна отримана в ході дослідження теплова карта дала змогу наочно проілюструвати дані показники.

Результати та висновки. У підсумку можна зазначити що в ході виконання прикладного дослідження були виконані всі необхідні кроки та дії стосовно організації безпроводової мережі WLAN Wi-Fi в офісному приміщенні. Таким чином була розроблена та організована безпроводова локальна мережа WLAN Wi-Fi офісного приміщення на основі стандарту 802.11ac, розглянуті основні принципи та рішення її побудови.

Задачею, яка була вирішена, є забезпечення належного покриття та швидкості передачі даних безпроводової мережі. В результаті були отримані очікувані показники рівня сигналу та фізичної швидкості що досягаються у всьому приміщенні.

УДК 004.75

Майборода Д.В., Малоєд М.М.

Національний авіаційний університет, м. Київ

ЕНЕРГОЕФЕКТИВНА ОБРОБКА НАВАНТАЖЕНЬ В ІНФОРМАЦІЙНІЙ МЕРЕЖІ

Актуальність досліджуваної теми обумовлена тим, що розподілені центри обробки даних (ЦОД) мають велике споживання енергії. Вирішення проблем енергоефективності у розподілених ЦОД є особливо актуальним. Згідно з дослідженнями, у 2020 році частка електроенергії, споживаної такими системами, становила приблизно 1% загального світового виробництва електроенергії.

Аналіз показує, що ця частка продовжує зростати, оскільки обсяги обчислювального обладнання у розподілених центрах швидко збільшуються. У такому контексті важливо, щоб система обслуговування навантаження у складі цих центрів забезпечувала високу обчислювальну продуктивність і доступність для задоволення вимог щодо якості надання послуг для різних типів навантажень. Таких як SDN, NFV, Edge Computing, Network Slicing та bDDN.

На сьогоднішній день існує багато наукових та практичних підходів до підвищення енергоефективності обслуговування навантажень у розподілених ЦОД.

1. Підходи на рівні апаратного забезпечення
2. Горизонтальне масштабування та консолідація
3. Енергоефективний розподіл навантаження

Більшість цих підходів спрямовані на зниження енергоспоживання системи, зберігаючи при цьому рівень продуктивності. Проте, вони не враховують специфіку навантаження і суворі вимоги до доступності системи при його обробці.

Ці вимоги пояснюються необхідністю забезпечення якості послуг "з кінця в кінець" у динамічно змінюваному навантаженні. Наприклад, підвищення енергоефективності шляхом зменшення активних обчислювальних вузлів розподіленої системи може негативно вплинути на якість телекомунікаційних послуг у динамічних умовах. Крім того, існуючі підходи не використовують індивідуальні характеристики енергоспоживання обчислювальних вузлів, що є

особливо важливим у гетерогенних системах, де споживання енергії окремих вузлів може суттєво відрізнятись.

Таким чином тема енергоефективної обробки навантажень в інформаційній мережі є актуальною, існує багато підходів до її вдосконалення. Більшість з них спрямовані на зниження енергоспоживання системи, але не враховують специфіку навантаження та вимоги до доступності. Необхідні подальші розробки, що враховуватимуть ці фактори для досягнення ефективної обробки навантажень в ІКМ.

Література

1. Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating

global data center energy-use estimates. Science, 367(6481), pp. 984-986. DOI:

https://doi.org/10.1126/science.aba3758.

2. Data Center Market and Technology Trends Power Electronics presentation. (2016). [Електронний ресурс] Yole Développement, APEC, available at: https://www.slideshare.net/Yole_Developpement/data-center-market-and technologytrends-power-electronics-presentation-held-at-apec-2016-from-yole-dveloppement. (lastaccessed 18.10.2021).

3. Barroso, L. A., & Hölzle, U. (2007). The case for energy-proportional computing.

Computer, 40(12), pp. 33-37. DOI: https://doi.org/10.1109/mc.2007.443.

УДК 621.329

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

РОЗРАХУНОК НАДІЙНОСТІ НАДЗЕМНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

На сьогоднішній день, базові станції стали більш потужними та можуть обслуговувати більше користувачів одночасно, що дозволяє забезпечувати якісний мобільний зв'язок навіть в густонаселених місцях. Також, вони мають покращену функціональність та більш широкі можливості зв'язку, що дозволяє їм працювати з різноманітними технологіями мобільного зв'язку. Проте, наразі є кілька проблем, пов'язаних з надійністю базових станцій. Одна з них - це проблема енергоспоживання. БС вимагають значної кількості електроенергії для своєї роботи, що може призвести до високих витрат та забруднення довкілля. Крім того, існують проблеми, пов'язані з технічними несправностями та невідповідністю до встановлених стандартів.

RBS 2000 забезпечує просту структуру та швидке розгортання мережі. DBS3900 має тільки два типи основних функціональних модулів, таким чином значно скорочуючи витрати на запасні частини та обслуговування.

Базова система Flexi Multiradio BTS GSM/EDGE від Nokia Siemens Networks заснована на технології активних антени, яка об'єднує антену та радіообладнання в єдиний функціональний блок, що має окремі підсилювачі потужності для кожного елемента антени. Активна антена дозволяє здійснювати формування променів – фокусування окремого радіо підключення та його направлення на конкретного користувача – а також використовувати різні технології в одному блоці.

БС WiMAX/LTE: Airspan Air4G (MacroMAXe), призначена для розгортання у три секторній конфігурації, що є оптимальним для розгортання мереж мобільного WiMAX та LTE. Система повністю підтримує протокол R6 для роботи зі шлюзом мережі доступу (ASN Gateway) як розподіленим, так і централізованим.

Базова станція Huawei DBS3900 забезпечує просту структуру та швидке розгортання мережі. DBS3900 має тільки два типи основних функціональних модулів, таким чином значно скорочуючи витрати на запасні частини та обслуговування. Віддалений радіо модуль має наступні переваги:

- може монтуватися на вежі, довжина лінії живлення значно скорочується і витрати на підводні лінії також скорочуються;

- скорочення втрат на живильних лініях що призводить до збільшення коефіцієнта посилення потужності від 3 до 5 дБ та підвищення радіусу покриття більш як на 20%. Тобто, може бути досягнуто покриття традиційної макро-BTS за меншої потужності шафи.

- підтримка розподільного встановлення радіо модулів, що значно підвищує гнучкість при проектуванні покриття вздовж залізничних колій.

Розрахунок за надійністю за статистичними даними базується на наступних припущеннях:

1. Всі вироби, за якими аналізується статистичний матеріал, рівно надійні..

2. Відмова будь-якого виробу є випадковою подією. Для цього вироби повинні пропрацювати час, достатній для припрацювання елементів, але не достатній для настання періоду їхнього старіння. У цьому випадку інтенсивності відмов елементів виробу в період експлуатації (випробувань) можна вважати величинами постійними.

3. Експлуатація (випробування) виробів проходила за однакових умов, тому вихідні дані не потребують коригування за рахунок впливу кліматичних, механічних та інших факторів.

Всі методи розрахунку надійності можна поділити на дві групи за видами відмов: за раптовими відмовами та за поступовими відмовами. За джерелом отримання інформації розрізняють аналітичні методи розрахунку надійності (розрахункові) та методи за даними експлуатації (статистичний розрахунок). За повнотою розрахунку та інформації, яка в результаті цього розрахунку отримана методи поділяються на повні та наближені

Теоретичні відомості розрахунку надійності варіантів резервування, під час виконання розрахунків без урахування умов експлуатації РЕА використовують методику орієнтовного методу розрахунку надійності, при виконанні розрахунків з урахуванням умов експлуатації РЕА використовують методику повного розрахунку надійності, виконуючи розрахунки, роблять ряд припущень: РК елементів РЕА як надійність з’єднані послідовно, інтенсивності відмов РК є постійними величинами, відмови РК є незалежними подіями, наробітки до відмови РК підкоряються експоненціальному розподілу.

УДК 05.12.02 (043.2)

А.А. Молдован
Національний авіаційний університет, м. Київ
Науковий керівник, к.т.н.,доцент Зуєв О.В.

СИСТЕМА МОБІЛЬНОГО ЗВ'ЯЗКУ

Галузь мобільного зв'язку відноситься до числа високотехнологічних областей економіки, для неї характерний відносно короткий життєвий цикл використання технології і виробництва послуг, а також високий рівень конкуренції. Розвиток мобільного оператора тісним чином пов'язаний з результатами його інноваційної діяльності. Результати інноваційної діяльності конкретного підприємства відповідають обраній ним інноваційній стратегії. Мобільний зв'язок в наш час є однією з найважливіших частин інфраструктури держави, а також невід'ємним елементом повсякденного життя окремої людини. Тому велика увага приділяється саме розробці та удосконаленні мереж мобільного радіозв'язку.

Одним із видів таких мереж являються стільникові мережі рухомого радіозв'язку (СМРЗ), які забезпечують двосторонні бездротові з'єднання з рухомими станціями, які можуть переміщуватися з високою швидкістю на великій території, покритій мережею базових станцій. Глобальною стратегією в галузі мобільного радіозв'язку стали розробка та впровадження єдиних міжнародних стандартів та створення на їх основі міжнародних та глобальних мереж загального використання.

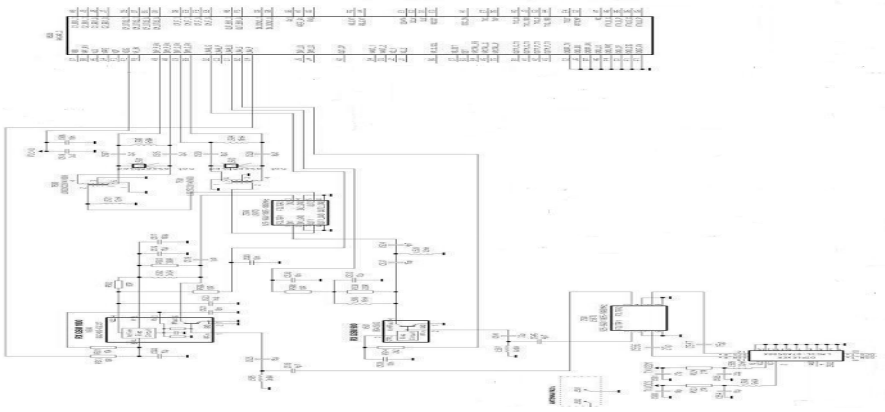
В сучасних умовах активно розробляються концепції універсального персонального зв'язку, мережам рухомого зв'язку (МРЗ), здійснюється інтенсивне впровадження стільникових МРЗ: мереж персонального радіовиклику та систем супутникового зв'язку. Такі мережі призначені для передачі даних (ПД) і забезпечення рухомих і стаціонарних об'єктів телефонним зв'язком . Передача даних рухомому абонентові різко розширює його можливості, оскільки, крім телефонних, він може приймати телексні і факсимільні повідомлення, різного роду графічну інформацію та завжди бути в онлайн доступі до всесвітньо мережі інтернет. Збільшення обсягу інформації вимагатимуть скорочення часу її передачі та одержання. Тому на сьогодні спостерігається стійке зростання виробництва мобільних засобів радіозв'язку (стільникових радіотелефонів, супутникових користувальницьких терміналів).

Дослідження мережі транкінгового зв'язку направлені на визначення класифікації по методу передачі мовної інформації: аналогові і цифрові; залежно від кількості БС і загальної архітектури: однозонові або багатозонові системи; за методом об'єднання БС у багатозонові системи. БС можуть поєднуватися за допомогою єдиного комутатора (системи із централізованою

комутацією), або з'єднуватися один з одним безпосередньо, або через системи з розподіленою комутацією (СРК); за типом багатостанційнного доступу: FDMA, FDMA+TDMA; за способом пошуку і призначення каналу: системи з децентралізованим (СДК) і централізованим (СЦК) керуванням. Пристрій обєднання радіосигналів дозволяє використати те саме антенне устаткування для одночасної роботи приймачів і передавачів на декількох частотних каналах. РТ працюють тільки в дуплексному режимі. Рознос частот прийому і передачі становить від 3 МГц до 45 МГц.

Детальний аналіз основних функцій, принципу роботи, будови та загальної комплектації базової станції стільникового зв'язку GSM , розгляд стільникових телефонних мереж (СТМ), які на відміну від стаціонарних варто враховувати те, що абонентська лінія включається не в конкретний вузол комутації, а безпосередньо в мережу, що може поєднувати не тільки кілька стільникових мереж у межах однієї країни, але мережі різних країн. Тому необхідно чітко визначити зони обслуговування кожної зі структурно-функціональних одиниць.

Загальні характеристики стандарту GSM, структурна схема стільникової системи стандарту GSM, мережеві і радіо інтерфейси, структура служб, та обслуговування виклику в мережах стандарту GSM дає можливість наблизитись до обґрунтування та вибору функціональної та принципової схеми виймального пристрою БС. Забезпечення прийому сигналів БС від МС є основним і найбільш відповідальним завданням всіх засобів стільникового зв'язку . У принциповій схемі тракту прийому БС стандарту GSM розглядається функціональний елемент такий як електронний антенний перемикач Diplexer.



Висновки

1. Обґрунтована функціональна схема приймача БС GSM.
2. Обґрунтована принципова схема тракту прийому БС GSM.

УДК 621.39 (043.2)

В.А. Несват
Національний авіаційний університет, м. Київ

МОДЕРНІЗАЦІЯ КОМУНІКАЦІЙНОЇ ЛІНІЇ СЕГМЕНТУ СУПУТНИКОВОЇ СИСТЕМИ НАВІГАЦІЇ GPS

Системи глобального супутникового позиціонування являють собою невід'ємну частину технологічного прогресу, на базі яких створюються нові технології та виводять на новий рівень вже наявні. Досліджуваний комплекс глобального супутникового позиціонування (GPS Global Positioning System) – це високотехнологічна інформаційна система що складається з п'яти основних сегментів:

1. Космічний;
2. Наземний-керуючий;
3. Космічних доповнень;
4. Наземних доповнень;
5. Користувачів.

Всі з данних п'ти являють собою об'єкти дослідження, для подальшого вдосконалення всієї системи.

Метою роботи є дослідження можливостей модернізації комунікаційної лінії. В результаті проведеної роботи були надані загальні дані про систему, її роль та задачі, проаналізовано та досліджено матеріали пов'язані з тематикою, базуючись на матеріалах яких було проведено подальше прикладне дослідження.

Об'єктом дослідження даної роботи стала комунікаційна лінія яка являє собою сукупність різних рівнів, складових та сегментів. Перша частина дослідження передбачала собою окреслення загальних відомостей та особливостей будови, складу даної системи, були виділені певні складові системи такі як космічна складова та наземна, які беруть безпосередню участь в комунікації та обміном специфічною інформацією. Метою другої частини дослідження був аналіз всіх сукупних даних, які беруть участь у процесі обміну інформацією, вивчення їх можливостей та особливостей, наведено функціональні та графічні типи, які належать до різних підсистем та доповнень. Третя частина дослідження – це фактична реалізація пропонованого методу модернізації, ціллю якого є покращення характеристик швидкості передачі даних в комунікаційній лінії.

Було досліджено роботу та особливості системи глобальної супутникової навігації (GPS), функціональних типів даних, які приймають участь у обміні інформацією, на основі інших матеріалів та досліджень був запропонований власний метод модернізації який передбачає собою заміну методу передавання даних, а саме зміну модуляції сигналів на більш вигідну та ефективну BPSK → QPSK. Ця модифікація дозволить передавати навігаційні дані з швидкістю більшою в два рази (100 біт/с), на відміну від попередньої (50 біт/с) в тій же смузі частот. Це досягається за рахунок ключової відмінності між ними: пропускної можливості 2 біти на символ проти 1 біту на символ. Приклад моделювання даного методу наведено на рис. 1.

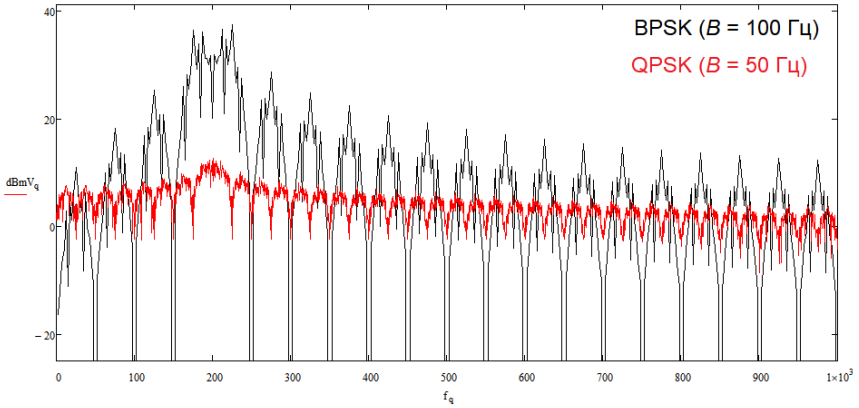


Рис. 1. Спектральні характеристики змодельованих сигналів

З рис. 1 видно, що ширина основної пелюстки модуляції QPSK вдвічі вужча порівняно з BPSK, що й забезпечує підвищення ефективності функціонування системи при її можливій розглянутій модернізації.

УДК 654.1

А.В. Новіченко, А.Г. Тараненко
Національний авіаційний університет, м. Київ

ЕЛЕКТРОННІ ТАБЛО З ТЕХНОЛОГІЄЮ ПАКЕТНОЇ РАДІОПЕРЕДАЧІ

Дана робота присвячена дослідженню ефективності електронних табло з використанням технології GPRS в громадському транспорті. Розвиток інформаційних технологій та підвищення вимог до обслуговування пасажирів призвели до необхідності створення сучасних систем передачі інформації на зупинках та в транспорті. Технологія GPRS має ряд переваг, таких як достатньо висока швидкість передачі даних, глобальне охоплення мобільним зв'язком, надійність та стабільність зв'язку, можливість дистанційного управління та гнучкість налаштування. Метою даного дослідження є вивчення принципів роботи інформаційного табло з біжучою стрічкою, його функціональних можливостей та ефективності у забезпеченні інформаційного обслуговування пасажирів та управління громадським транспортом. Отримані результати можуть сприяти вдосконаленню системи громадського транспорту та підвищенню зручності для користувачів.

Основна частина роботи присвячена дослідженню ефективності електронних табло з технологією GPRS в громадському транспорті. Під час дослідження було проведено огляд сучасного використання електронних табло та визначено їх переваги. Окрема увага була приділена технічним аспектам впровадження GPRS в електронні табло, зокрема аналізу параметрів передачі даних та стабільності зв'язку. Був проведений порівняльний аналіз інших технологій передачі інформації та їх ефективності. Результати дослідження вказують на позитивний вплив електронних табло з GPRS на роботу громадського транспорту, зокрема зменшення часу очікування пасажирів, покращення зручності та зниження запізнень. Ці дані є важливими для розроблення рекомендацій щодо використання даної технології для покращення якості пасажирських перевезень у громадському транспорті.

На основі проведених досліджень та аналізу результатів можна зробити висновок, що впровадження електронних табло з технологією GPRS в громадський транспорт є ефективним та корисним рішенням. Вони значно поліпшують інформаційне середовище для пасажирів, забезпечуючи актуальну та зручну інформацію про рух транспорту,

розклади, маршрути та інші корисні дані. Крім того, таке впровадження сприяє підвищенню рівня комфорту та задоволеності пасажирів, а також зменшенню часу очікування та невпевненості у відправленні. Узагалі, впровадження електронних табло з технологією GPRS є важливим кроком до модернізації громадського транспорту та покращення якості його обслуговування.

Електронні табло з біжучім рядком, підтримувані технологією GPRS, зазвичай мають наявність SIM-карти, яка встановлюється в табло і забезпечує його зв'язок з мережею оператора зв'язку. Це дозволяє оновлювати вміст табла в режимі реального часу та змінювати відображену інформацію.

За допомогою технології GPRS, центральний сервер може відправляти команди та оновлення на електронні табла. Це дозволяє операторам системи масового обслуговування керувати та оновлювати інформацію на таблах з центрального пункту керування. Наприклад, сервер може надсилати розклади руху, зміни у маршрутах або інші важливі повідомлення на табло.

Це достатньо дешевий спосіб бездротової передачі даних і більш гнучкий у порівнянні з іншими методами. Він забезпечує передачу даних в радіоінтерфейсі зі швидкістю 171,2 кбіт/с, яка підвищується до 473,6 кбіт/с у підсистемі EDGE. У даному випадку пристрій працює в частотному діапазоні системи GSM, це (880,2 … 959,8) МГц або (1710,2 … 1879,8) МГц.

УДК 621.311.13

П.С. Павленко, М.М. Малоєд

Національний авіаційний університет, м. Київ

ПРИСТРІЙ БЕЗПРЕБІЙНОГО ЖИВЛЕННЯ

На сьогоднішній момент система електропостачання вузла зв'язку повинна задовольняти такі вимоги як: економічність, надійність, безпека, безперебійність. А якість електроенергії, що поставляється до обладнання вузла зв'язку, повинна відповідати певним нормам: стабільність частоти мережі живлення, рівень напруги, а також час перемикання на джерело резервного живлення.

Як правило, вузли зв'язку розміщуються в житлових будинках, електропостачання в яких здійснюється лише від одного джерела живлення. При виникненні будь-якої аварії, яка пов'язана з електропостачанням у житловому будинку, виходячи з договорів на електропостачання споживачів 3 категорії електропостачання, саме до них належать житлові будинки, щоб відновити електроживлення дається 24 години. У випадку коли аварія з електроживленням відбувається в житловому будинку, в якому розташовується вузол зв'язку, а з нього, наприклад, підключені послуги телебачення, телефонії, доступу в інтернет для якогось району міста, то організація, яка надає ці послуги (провайдер) та її абоненти зазнають збитків. У договорі між абонентом та провайдером є пункт, згідно з яким послуги зв'язку повинні надаватися безперервно.

Пропонуючи самому провайдеру забезпечити собі першу безперебійну категорію. Використовуючи при цьому такі засоби як: установка автономної системи безперебійного живлення, яка включає випрямляч, інвертор, розрядний пристрій, зарядний пристрій, блок управління, що підвищує трансформатор, акумулятори, а також дизельгенератор і бензогенератор.

Насамперед проводиться аналіз устаткування вузла зв'язку, з урахуванням цього аналізу виконується розрахунок електричних навантажень вузла зв'язку. З розглянутих дослідницьких завдань розраховується джерело безперебійного харчування. Вибирається ємність та тип акумуляторних батарей. Виконується розрахунок повної електричної потужності, що споживається типовим вузлом зв'язку, на підс-

таві цього розрахунку підбираються кабельні лінії та комутаційна апаратура. Для того, щоб знизити втрати електроенергії та підвищити ефективність електроустановок, проводиться розрахунок компенсуючих конденсаторів.

Проводиться розрахунок та вибір схеми заземлення. Проводиться розрахунок необхідної потужності та вибір дизель-генератора для резервування електроживлення вузла зв'язку.

Основний параметр системи електроживлення – це здатність забезпечувати безперебійну та безперервну роботу всього обладнання у вузлі зв'язку. За допомогою комплексних показників надійності можна характеризувати цю здатність.

Розрахункові показники надійності таких пристроїв як: випрямляч, інвертор, зарядний пристрій є близькими за своїми значеннями, що ускладнює вибір кращого за надійністю ДБЖ. Вибір здійснюється за такими показниками надійності як коефіцієнт готовності, середній час напрацювання на відмову, ймовірність безвідмовної роботи.

На сьогоднішній момент не існує жодних норм, протягом якого часу система безперебійного електроживлення повинна забезпечувати електроенергією вузол зв'язку, а саме доступ в інтернет. Як наслідок, це призводить до великих збитків організацій, робота яких заснована на постійному підключенні до мережі інтернет. Загалом, вся система електропостачання має бути побудована так, щоб в умовах аварійного режиму вона мала можливість забезпечити безперебійне живлення всього обладнання вузла зв'язку протягом 24 годин (10 годин від акумуляторів та 14 годин від резервного генератора).

У ході виконання роботи було досліджено та спроектовано джерело безперебійного живлення для вузла зв'язку, що має цифрове управління та призначене для захисту електронної апаратури зв'язку від проблем, що виникають у мережі електроживлення.

Було обрано структурну схему побудови з постійно включеної акумуляторної батареї, що дозволило виконати вимоги, що висуваються до електроживлення у вузлах зв'язку. Були розраховані та обрані основні елементи функціональної схеми мостового інвертора. Було досягнуто технічних показників, які необхідні для живлення вузла зв'язку під час аварійної роботи зовнішньої електромережі. Забезпечено належний рівень якості виробу, що відповідає прийнятим стандартам.

УДК 004.7(043.2)

С.В. Печерний
В.Є. Курушкін
Національний авіаційний університет, м. Київ

МОДЕЛЮВАННЯ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ IPV6 З ВИКОРИСТАННЯМ ПРОГРАМНОГО ПАКЕТУ PACKET TRACER

Сьогодні політики виділення IPv4-адрес регіональних реєстрів Internet відлякують усіх бажаючих отримати відкритий адресний простір. Адресний простір IPv4 став дефіцитним ресурсом, отримання блоку відкритих адрес потребує багато паперів та бюрократичної тяганини.

Іншим підходом до вирішення проблеми дефіциту адресного простору є збільшення тривалості IP-адреси. Якщо IP-адреси стануть довшими, їх можна буде вільно роздавати та використовувати, і вони не будуть дефіцитним ресурсом. IPv6 надає можливість розгорнути нові типи програм, які засновані на використанні відкритого адресного простору або шифрують інформацію в самій IP-адресі, наприклад, множинна адресація та організація мереж з контрольованою безпекою.

IPv6 стала надзвичайно стабільною і надійною технологією з моменту її впровадження. Розгортання IPv6 було успішно проведено протягом багатьох років, тому використання її наразі не потребує додаткового програмного забезпечення чи патчів. Значна кількість операційних систем підтримує IPv6, і вона активована за замовчуванням у деяких постачальників послуг. Враховуючи ці факти, IPv6 вже зараз доступна для широкого кола користувачів.

Інтернет-протокол - це набір правил маршрутизації та адресації, які дозволяють пакетам даних подорожувати мережею і досягати місця призначення. Дані, що надсилаються через Інтернет, розбиваються на менші компоненти, які називаються пакетами. До кожного пакета додається IP-інформація, щоб підготувати маршрутизатор до відправлення пакета в потрібне місце. Кожному пристрою або домену, підключеному до Інтернету, присвоюється IP-адреса, і пакет надсилається туди, де йому присвоєно IP-адресу, щоб дані були відправлені туди, куди їм потрібно.

Інтернет-протокол версії 4 (IPv4) - це протокол для використання в мережах з комутацією пакетів на канальному рівні (наприклад, Ethernet). IPv4 забезпечує можливість обробки приблизно 4,3 мільярда адрес.

Інтернет-протокол версії 6 (IPv6) є більш досконалим і кращим, ніж IPv4. IPv6 має можливість надавати необмежену кількість адрес. IPv6 прийшов на зміну IPv4, щоб обслуговувати зростаючу кількість мереж по всьому світу і вирішити проблему вичерпання IP-адрес.

Однією з відмінностей між IPv4 і IPv6 є зовнішній вигляд IP-адрес: в той час як IPv4 використовує чотири однобайтових десяткових числа, розділених крапками (наприклад, 192.168.1.1), IPv6 використовує шістнадцяткові числа, розділені двокрапкою (наприклад, fe80::d4a8:6435:d2d8:d9f3b11).

Згідно з дослідженнями, IPv6 є швидшим і досконалішим протоколом ніж IPv4. Протокол IPv6 має достатню кількість IP адрес на майбутнє, який в свою чергу спрощує роботу маршрутизаторів і мережі в цілому. З наукової точки зору протокол IPv6 став в рази продуктівнішим стала швидша маршрутизація, яка спрощує процеси розгортання, також була збільшена ємність і конфігурація мережі, більша мобільність. Створення мереж з протоколом IPv6 стало простішим, також зявилось більше можливостей для розроблення мережі.

IPv4 має суттєвий істотний недолік під час підключення до Інтернету , однак IPv6 згодом замінить IPv4 як кращий протокол . під час підключення до Інтернету , однак IPv6 згодом замінить IPv4 як протокол , якому надається перевага .

Звичайно, у нього є і переваги, і недоліки. Важливість впровадження відбувається в тому, що його Інтернет розвивається і розвиватиметься ще довгий час. Завдяки IPv6 у наступних кількох століть, інші не шукають ідей для створення нових технологій розширення мережі.

УДК 043.2

Д.П. Присяжний, П.В. Павловський, І.В. Абрамчук
Вінницький національний технічний університет, м. Вінниця

ЗАХИСТ ПОТОКОВОГО ВІДЕО ВІД НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ З ВИКОРИСТАННЯМ КРИХКИХ ЦВЗ

У роботі розглянуто метод вбудовування крихких ЦВЗ, в якому при створенні водяного знаку для збільшення безпеки алгоритму замість хеш-функції MD5 використано функцію з ключем HMAC-SHA-256, а також використано псевдовипадкова послідовність для знаходження позиції для вбудовування блоків згенерованого ЦВЗ, поріг значень якої генерується динамічно. Біти згенерованого ЦВЗ вбудовуються у два останні найменш значущі біти векторів руху для розширення корисного навантаження вбудовування до 256 бітів завдяки алгоритму HMAC-SHA256. Особливості кожного кадру, такі як кольорова насиченість та яскравість елементів можуть бути використані при генерації водяних знаків для виявлення просторових змін та маніпуляцій над кольоровими характеристиками. Сильні візуальні особливості, які використовуються для генерації крихкого цифрового знаку складаються з набору коефіцієнтів, отриманих з передбачуваних INTRA та INTER блоків, що використовуються при стисненні відеопотоку. Різниця складається у тому, що INTRA-метод використовує для стиснення дані лише поточного кадру, в той час як INTER-метод дозволяє проаналізувати наступні кадри та на основі отриманої інформації про мінімальні зміни у кадрі збільшити компресію статичних областей. Дані характеристики, що використовується для генерації водяного знаку, складаються з квантованих постійних коефіцієнтів (DC) і перших двох змінних коефіцієнтів (AC), що входять до низькочастотних коефіцієнтів у порядку сканування зиґзаґом кожного блоку в межах INTRA 4×4 і INTER 4×4. Обирається DC-коефіцієнт, який є показником середньої енергії по усіх 4×4 пікселях та коефіцієнти з найбільшою енергією у межах перших декількох низькочастотних коефіцієнтів. Високочастотні коефіцієнти майже близькі до нуля та ігноруються під час квантування коефіцієнтів ДКП. Також коефіцієнт DC і два перших коефіцієнта AC є більш стабільними, ніж інші коефіцієнти, при маніпуляції зображенням. Усі отримані дані та коефіцієнти зберігаються в буфері для кожного кодованого блоку в кожному кадрі до моменту миттєвого оновлення декодера (IDR), який свідчить

про відсутність зображення у потоці бітів, що вимагають посилання в порядку декодування до кадрів безпосередньо перед I-кадром. Кадри IDR є I-кадрами, які не посилаються на будь-які кадри поза поточної групи кадрів (GOP). GOP складається з I-кадру та усіх інших P-кадрів, які розташовані між кадрами IDR. Тому кодована підпослідовність відео починається з кадру IDR і закінчується, коли з'являється новий кадр IDR, сигналізуючи про наявність нової підпослідовності, що підлягає кодуванню або закінченню передавання. У кінці кожної групи кадрів ознаки присутні в буфері проходять через захищену функцію хешування HMAC-SHA256.

Процес створення ЦВЗ. Змішування характеристик, що зберігаються у буфері, з секретним ключем K. Створення хешу з отриманої послідовності за допомогою SHA-256. Змішування хешу з секретним ключем K. Застосування обробки SHA-256. Отримана хеш-послідовність довжиною 256 біт використовується в якості крихкого водяного знаку, який вбудовується у вектори руху (MV) в H.264/AVC. Вбудовування крихкого водяного знаку виконується над векторами руху в межах P-кадрів, які мають високі показники руху (зміни) та належать до вибраних блоків вбудовування. Секретний ключ K використовується для генерування псевдовипадкової послідовності для вибору позиції блоків вбудовування. Для ретельного вибору блоків вбудовування необхідно розглянути два обмежувальні параметри. Сусідні блоки пропущених блоків відкидаються. Інше обмеження – необхідність уникнення вбудовування інформації у блоки з відсутністю руху та блоки з незначними рухами.

Процес вилучення цифрового водяного знаку виконується на рівні декодеру H.264/AVC та без потреби у оригінальному відеопотоці. Цей процес схожий на процес вбудовування, адже включає в себе обчислення кадрів з найбільшою руховою активністю, вибір позиції вбудовування на основі ключа K, ентропійне декодування векторів руху і застосування двох умов, які виконуються у процесі вбудовування. Біти водяного знаку потім вилучаються з двох останніх найменш значущих бітів компонентів MV_x і MV_y для кожного блоку вбудовування.

На етапі автентифікації необхідно визначити візуальні особливості, які були використані при вбудовуванні. Ці особливості видобуваються перед оберненим квантуванням і операціями перетворення усередині алгоритму H.264/AVC-декодера. Наприкінці кожної неза-

лежної групи кадрів, визначеної декодером, ці дані шифруються з використанням функції HMAC-SHA-256 для перевірки цілісності, використовуючи той самий ключ K, щоб отримати хеш-значення, які будуть порівнюються з вилученими бітами водяного знаку. Будь-які зміни особливостей або хеш-значень будуть означати зміни у контейнері. Таким чином, вміст автентифікується лише, якщо оригінальні та обчислені значення хешу однакові. У разі невдалої автентифікації виявлення фальшивих кадрів виконується окремо. Щоб визначити розташування фальсифікованих кадрів у межах пошкодженої групи кадрів отримувач обчислює хеш-значення усіх кадрів у GOP на рівні декодера, та обчислюються хеш-значення оригінальної групи кадрів.

Для аналізу ефективності крихкого цифрового водяного знаку необхідно провести перевірку на можливість втручання у просторову, часову та область кольору. Втручання можливе шляхом зміни порядку кадрів, їх заміну, зміна розмірів, повертання та зміна кольору області чи окремих областей. У запропонованому алгоритмі ємність водяного знаку залежить від рухової активності та спотворенням, що спричиняються вбудовуванням. Для потоку відео зі значною руховою активністю ($\sigma \geq 3{,}870$) кількість підходящих блоків для вбудовування звичайно більша, ніж у відео з незначною руховою активністю, отже і об'єм даних для вбудовування може бути збільшений. Під час аналізу отримані значення оцінки якості відео (VQM) у діапазоні від 0,292 до 0,398, що призводить до незначного розходження між оригіналом та відеопослідовності з водяним знаком. Отримано індекс SSIM, який зазвичай використовується при оцінюванні відео з водяними знаками щодо оригіналу з точки зору подібності або розбіжностей яскравості, контрасту і структурних подібностей. Значення SSIM, близьке до 1, вказує на високу подібність двох відео і 0 – на повну невідповідність. З отриманих результатів аналізу відео можна зробити висновок, що на відео немає якихось видимих змін після процесу вбудовування, оскільки усі значення SSIM дуже близькі до 1.

Висновки. Запропоновано метод вбудовування крихких ЦВЗ та проведено оцінювання його ефективності. У результаті оцінювання виявлено, що запропонований метод є дієвим, забезпечує можливість виявлення несанкціонованої модифікації та дозволяє вбудувати в середньому у 2,03 рази більше інформації зі збільшенням пікового співвідношення сигналу до шуму на 0.05, що є непомітним для неозброєного ока.

УДК 621.3

О.Г. Редько
Національний авіаційний університет, м. Київ

ВІДЕОКОНФЕРЕНЦЗВ'ЯЗОК ПІДПРИЄМСТВА

Відеоконференція - це інтерактивний інструмент, який включає аудіо, відео, комп'ютерні та комунікаційні технології для здійснення зв'язку віддалених територіально співрозмовників «віч-на-віч» у реальному часі, а також поділу всіх типів інформації, включаючи дані, звук, зображення, документи тощо подібне.

По суті, відеоконференція дозволяє повноекранне відео, можливість оперативного обміну даними та доку-ментами роблять відеоконференції подолати бар'єр відстані, який нас поділяє. Висока якість звуку та потужним інструментом з найширшим спектром практичного застосування. Історія відеоконференцій починається з 1964 року, коли дослідницький підрозділ компанії AT&T представив Videophone - Першу аудіовізуальну систему електронної взаємодії двох осіб у режимі реального часу. На сьогодні досягнення в галузі комп'ютерної техніки дозволяють нам говорити про таку унікальну комунікаційну систему, як відеоконференція.

Відеоконференція (videoconference) - область інформаційної технології, що забезпечує одночасно двосторонню передачу, обробку, перетворення та подання інтерактивної інформації на відстань у режимі реального часу за допомогою апаратно-програмних засобів обчислювальної техніки.

Взаємодія в режимі відеоконференцій також називають сеансом відеоконференцзв'язку.

Відеоконференцзв'язок (скорочена назва ВКЗ) - це телекомунікаційна технологія інтерактивної взаємодії двох і більше віддалених абонентів, при якій між ними можливий обмін аудіо- та відеоінформацією в реальному масштабі часу з урахуванням передачі керуючих даних.

Відеоконференція застосовується як засіб оперативного прийняття рішення у тій чи іншій ситуації; при надзвичайних ситуаціях; для скорочення витрат на відрядження в територіально розподілених організаціях; підвищення ефективності; проведення судових процесів з дистанційною участю засуджених, а також як один із елементів технологій телемедицини та дистанційного навчання.

У більшості державних та комерційних організаціях відеоконференція приносить великі результати та максимальну ефективність, а саме:

- знижує час на переїзди та пов'язані з ними витрати;
- прискорює процеси прийняття рішень у надзвичайних ситуаціях;
- скорочує час розгляду справ у судах загальної юрисдикції;
- збільшує продуктивність праці;
- вирішує кадрові питання та соціально-економічні ситуації;
- дає можливість приймати більш обґрунтовані рішення за рахунок залучення за потреби додаткових експертів;
- швидко та ефективно розподіляє ресурси, і так далі.

Для спілкування в режимі відеоконференції користувач повинен мати кінцевий пристрій (кодек) відеоконференцзв'язку, відеотелефон або інший засіб обчислювальної техніки. Як правило, комплекс пристроїв для відеоконференцзв'язку складається:

- центральний пристрій - кодек з відеокамерою та мікрофоном, що забезпечує кодування/декодування аудіо- та відео-інформації, захоплення та відображення контенту;
- пристрій відображення інформації та відтворення звуку.

Як кодек може використовуватися персональний комп'ютер із програмним забезпеченням для відеоконференцій.

Велику роль відеоконференції грають канали зв'язку, тобто транспортна мережу передачі. Для підключення до каналів зв'язку використовуються мережеві протоколи IP або ISDN.

Існує два режими роботи ВКС, які дозволяють проводити двосторонні (режим «точка-точка») та багатосторонні (режим «многоточка») відеоконференції.

Як правило, відеоконференцзв'язок у режимі «точка-точка» задовольняє потреби тільки на початковому етапі впровадження технології, і незабаром виникає необхідність одночасної взаємодії між кількома абонентами. Такий режим роботи називається багатоточковим або багатоточковим відеоконференцзв'язком. Для реалізації цього режиму потрібна наявність активації багатоточкової ліцензії в кодеку за умови, якщо пристрій підтримує цю функцію або спеціального відеосервера MCU (англ. Multipoint Control Unit), або програмно-апаратної системи управління.

Для впровадження відеоконференцзв'язку керівнику (особі, яка приймає рішення) організації необхідно визначити головну мету застосування: проведення на-рад, підбір персоналу, оперативність під час прийняття рішень, здійснення контролю, дистанційне навчання, консультація лікарів, проведення судових засідань, допит свідків тощо. При цьому необхідно враховувати основні правила відеоконференцзв'язку:

- гарантована високошвидкісна послуга зв'язку або виділені канали зв'язку лише для сеансів відеоконференцій;
- стабільне та надійне електроживлення телекомунікаційного обладнання та відеоконференцзв'язку;
- оптимальні шумо- та ехо-поглинаючі особливості приміщення, в якому буде встановлено обладнання відеоконференцзв'язку;
- правильне розташування обладнання відеоконференцзв'язку по відношенню до світлового фону приміщення;
- коректне налаштування телекомунікаційного обладнання та відеоконференцзв'язку з обслуговування якості послуги зв'язку з пріоритезацією передачі даних;
- компетентний обслуговуючий технічний персонал;
- технічний супровід та передплата оновлення обладнання через сертифікованого виробником постачальника;

Враховуючи функції та цілі застосування, обладнання відеоконференцзв'язку систематизується на категорії та класи.

УДК 654.21

Т.І. Ружинський
Національний авіаційний університет, м. Київ

VOIP-ТЕХНОЛОГІЯ В ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ

VoIP-технологія, що дає змогу використовувати будь-яку мережу з пакетною комутацією на базі протоколу IP як засіб організації та ведення міжнародних, міжміських і місцевих телефонних розмов, а також передавання факсів у режимі реального часу.

Практична значущість розвитку корпоративної мережі підприємства на основі IP-телефонії обумовлена не тільки можливістю зниження витрат на телефонні переговори і технічне обслуговування.

Нині в галузі телекомунікацій спостерігається процес конвергенції мереж. Це означає, що наявні мережі (мережі передавання даних, мережі телефонії, мережі широкомовлення) використовують єдину інфраструктуру для передавання трафіку. Конвергенція дасть змогу значно розширити спектр послуг, що надаються мережами зв'язку, підвищити їхню якість, знизити вартість обслуговування обладнання і значно скоротити його обсяги, уніфікувати мережі зв'язку і підвести їх під єдині стандарти. Конвергенція мереж стане можливою після реалізації мереж наступного покоління NGN Next Generation Network.

NGN є мультисервісною мережею на базі мереж із комутацією пакетів. NGN здатна обслуговувати трафік мови, даних і відео. Це породило термін "Triple-Play Services", що вказує на здатність NGN підтримувати послуги, пов'язані з передачею цих трьох форм подання інформації.

За результатами дослідження Info-tech Research складається рейтинг пропозицій виробників. Виробник потрапляє в ту чи іншу групу після інтегрованої оцінки за критеріями виробник/продукт. У кожного з цих критеріїв є складові, за якими складається загальний бал окремо за оцінкою виробника, окремо за оцінкою продукту.

Було проведено огляд провідних пропозицій ринку корпоративної телефонії та уніфікованих комунікацій.

Alcatel-Lucent. Продукт OpenTouch.

Avaya. Продукт Aura, IP Office.

Cisco. Продукт Unified Communications.

Digium. Продукт Switchvox.

Interactive Intelligence.продукт Customer Interaction Center.

Mitel. Продукт Communications Director.
NEC. Продукт UNIVERGE Series.
Shore Tel. Продукт UC Platform, IP Phones.
Siemens. Продукт Open Scape.
Toshiba. Продукт Strata CIX Series.
Чемпіони:

- Cisco, за його точно орієнтований продукт і конкурентоспроможні ціни.
- Avaya, за його пакет IPT і основних можливостей уніфікованих комунікацій (UC).
- Mitel, за його дуже гнучкий варіант розгортання, сильну платформу уніфікованих комунікацій і зосередження на бізнес-комунікаціях.

Премія цінності:

- Digium, за пропозицію рівню підприємств малого та середнього бізнесу комунікаційних можливостей за дуже конкурентоспроможною ціною.

Премія цінності - одна з окремих нагород Infornetics Research. Представник, який отримує цю премію має найбільш розумний продукт за співвідношенням ціна/якість. Тобто, це оцінка того, на скільки пропозиція дійсно варта своїх грошей. У кожного виробника в цій оцінці є свої плюси і мінуси. Необхідно проаналізувати кожен продукт більш детально, щоб підібрати найбільш відповідне рішення до конкретних вимог.

Можливо, для деяких компаній цей функціонал - усе, що необхідно. Тоді єдиною різницею стає ціна, адже всі ці функції реалізовані у кожного представника. Якщо ж ні, то необхідно розглядати просунуті характеристики. Переваги, тобто просунуті характеристики - диференціатори ринку, доленосні для продукту.

На основі проведеного огляду робимо вибір на користь Mitel за такими критеріями: виробник є чемпіоном на ринку IPT. Рішення підтримує всі базові функціональні можливості уніфікованих комунікацій і більший, порівняно з іншими постачальниками, набір просунутих функціональних можливостей. За трьома основними актуальними вимогами ринку рішення Mitel посідає лідируючі позиції.

УДК 621.396.2

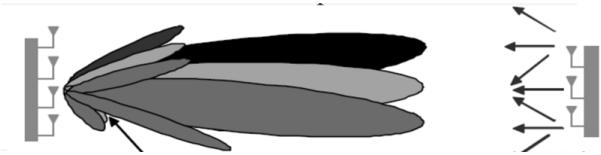
Д.О. Рябченко, М.М. Малоєд
Національний авіаційний університет, м. Київ

ПРОСТОРОВО-ЧАСОВА ОБРОБКА СИГНАЛІВ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

Просторово-часова обробка STP (Space-time processing) є однією з найбільш досліджуваних технологій бездротового зв'язку, оскільки вона пропонує вирішення таких проблем, як перешкоди, смуги пропускання та дальності дії [1]. Метод STP застосовується як для приймальної, так й передаючих частин або обох одночасно.

У теперішній час головний акцент зроблено на застосуванні MIMO-систем. Незважаючи на дедалі ширше використання антенних решіток, можна сміливо стверджувати, що тільки їх сумісне використання на базовій станції та терміналах користувача може забезпечити переваги використання багатовимірних сигнальних просторів та, у кінцевому підсумку, неймовірне зростання пропускної здатності і швидкості передачі даних.

На рисунку показана MIMO-система, в якій базова станція та мобільний термінал оснащені декількома антенами, що забезпечують одночасну бездротову передачу декількох потоків даних. Кожна антена мобільного терміналу забезпечує передачу окремого потоку даних, що випромінюються всеспрямовано. Антена базової станції здатна формувати кілька променів, що забезпечують вибір та прийом потокових даних. Вочевидь, що в порівнянні з традиційною системою, пропускна здатність, внаслідок багатоканальності, суттєво збільшується, чим й зумовлений підвищений інтерес до MIMO-систем.



За наявності релеївського завмирання при розповсюджені радіохвиль та однаковій кількості передавальних і приймальних антен пропускна здатність багатоантенного каналу зв'язку зростає, приблизно, лінійним чином зі збільшенням числа антен.

При когерентному складанні сигналів у приймальній частині з використанням таких методів, як технологія додавання при максимальних відносинах MRC (maximal ratio combining), середнє значення відношення сигнал-шум прийнятого сигналу зростає на $10 \cdot \log10(N)$, де N – кількість антен.

Застосування просторово-часових блокових і гратчастих кодів дає якісний стрибок у підвищенні швидкості та надійності передачі в умовах завмирань. Причому, для блокових існують максимально правдоподібні алгоритми декодування, які використовують лише лінійні операції в приймачі.

Щоб ефективно скористатися структурою радіоканалу з просторово-часовим поділом для систем з кількома антенними елементами, застосовується також адаптивна просторово-часова обробка сигналів.

У зв'язку з тим, що алгоритми просторової обробки вимагають великих обсягів обчислень, а також із тим, що кишенькові пристрої характеризуються обмеженою ємністю акумулятора та можливостями обробки, майже всі розробки STP-технології раніше були прив'язані до обладнання базових станцій та точок доступу. Але з поступовим розвитком технологій носимих пристроїв зі зниженим енергоспоживанням та появою новітніх методів просторово-часової обробки ця технологія також стає застосовною до мобільних пристроїв.

Однак для отримання переваг, що надають MIMO-системи, необхідно подолати низку проблем. Насамперед успіх нових концепцій до їхнього широкого впровадження повинен гарантуватися правильним вибором антенних конструкцій та геометричних характеристик. Наприклад, поточна тенденція мініатюризації розміру стільникових телефонів ускладнює розміщення кількох близько розташованих антен.

Загалом, сучасні методи просторово-часової обробки сигналів в системах мобільного зв'язку надають величезне поліпшення пропускної спроможності, швидкості, дальності та надійності передачі цифрових даних, що є необхідним для задоволення потреб сучасних систем мобільного зв'язку та майбутніх версій.

СПИСОК ЛІТЕРАТУРИ

1. Семенова О.О. Системи рухомого зв'язку /О.О. Семенова, А.О. Семенов, В.С. Бєлов. Навч.посіб. – Вінниця: ВНТУ, 2017. – 185с.

УДК 004.056.5

Д.Д. Савченко, І.Є. Терентьєва
Національний авіаційний університет, м. Київ

ОГЛЯД МЕТОДІВ ОБРОБКИ СИГНАЛІВ У СЕРЕДОВИЩІ МУЛЬТИМЕДІА

Основна концепція проектування системи зв'язку полягає в тому, щоб передавати інформацію за мінімально можливих витрат, одночасно забезпечуючи достатньо високу якість і максимальну користь для користувача. У мультимедійній комунікації типи інформації, які потребують високої швидкості передачі та високої швидкості обробки через їх великий обсяг, тобто аудіо, зображення, відео та графічні джерела, є найбільш критичними; комунікаційні системи (мережі та пристрої) часто досягають своїх можливостей для цих типів даних. Тому обробка, зберігання та передача аудіовізуальних сигналів стала одним із найважливіших рушійних факторів у розробці пристроїв із постійно зростаючою обчислювальною потужністю та пам'яттю, а також мереж ізбільшою ємністю.

Мультимедійні джерела або генеруються за допомогою сенсорного захоплення (камера, мікрофон, з аналого-цифровим перетворенням), або генеруються синтетично, наприклад графіка, синтезована мова чи звуки. Для відтворення та споживання людьми часто необхідне інше перетворення у відповідне фізичне середовище (наприклад, генеруваннязвукової хвилі через гучномовець).

Завдяки стисненню мультимедійного сигналу має бути досягнуто найбільш компактне представлення, що забезпечує найвищу можливу якість сприйняття. Після захоплення сигнал перетворюється в цифрове представлення з кінцевою кількістю вибірок і рівнями амплітуди. Цей крок вже впливає на кінцеву якість. Якщо діапазон швидкості, який може передати канал-кандидат, або роздільна здатність, необхідна програмі, невідомі на момент отримання даних, доцільно захопити сигнал із найвищою можливою якістю та, якщо необхідно, зменшити його до нижчої якості пізніше.

Під час перебоїв з електроенергією, через війну в країні, можуть виникатизатримки у передачі даних.

Для зменшення затримки обслуговування у службах потокового передавання в прямому ефір пропонується використовувати проксі-

сервер DASH, що розташовується поблизу базової станції.

У службах потокового передавання в прямому ефірі важливим параметром якості обслуговування є затримка обслуговування, яка визначається як різниця між часом, коли відбувається подія в прямому ефірі, і часом, коли подія в прямому ефірі відтворюється на приймальному терміналі. Зменшивши затримки буферизації, затримку служби можна мінімізувати. Однак у типовій службі мультимедійного мовлення Long-Term Evolution (LTE) необхідна буферизація, щоб уникнути перебоїв у роботі служби.

Запропонований механізм дозволяє вибирати альтернативні представлення у випадку сегментів які потрібно відновити за допомогою HTTP. Механізм заснований на проксі-сервері DASH, розташованому поблизу базової станції, тому представлення можна вибрати з урахуванням пропускної здатності, яка виділяється для терміналу, що відновлює втрачений сегмент, це адаптивне відновлення помилок дає змогу уникнути голодування буфера без збільшення затримкиобслуговування.

Проксі-сервер може дізнатися доступну пропускну здатність одноадресного каналу від базової станції та вибрати найбільш відповідне представлення для кожного сегмента. В результаті оцінки продуктивності проксі-сервера DASH у контексті мультимедійної трансляційної служби LTE, можна зробити висновок, що проксі-сервер із підтримкою буфера можна використовувати для покращення нестабільності та середньої якості сегмента. Однак проксі-сервер, який не підтримує буфер, менш складний і може забезпечити мінімальну затримку для служби.

Альтернативні підходи для проксі-серверів, що використовують різні алгоритми адаптації в контексті послуг мультимедійного мовлення LTE, підлягають подальшому вивченню. Впровадження проксі-сервера для перевірки пропозиції в реальному середовищі є ще одним майбутнім кроком.

Список літератури

1. 3GPP TS 26.234: "Transparent end-to-end packet switched streaming service (PSS); Protocols and codecs".

2. 3GPP TS 26.244: "Transparent end-to-end packet switched streaming service (PSS); 3GPP file format (3GP)

УДК-004.7.056

Р.П. Салей, В.Є. Курушкін
Національний авіаційний університет, м. Київ

СИСТЕМА ЗАХИСТУ ПЕРИМЕТРУ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ D-LINK

Ключові слова: комп'ютерна мережа, кібербезпека, D-Link, NetDefendOS.

Забезпечення безпеки вимагає багатопрофільної та багаторівневої структури. Подібно до моделей OSI або TCP/IP, які складають основу мережевих технологій, безпека повинна забезпечуватися на кожному рівні, який створює кіберпростір. Рівні можна розібрати на такі компоненти: безпека периметра, безпека мережі, безпека кінцевих точок, безпека даних, управління політикою та операції.

"Процес побудови системи захисту відповідає наступним універсальним принципам:

- Проектування системи захисту має йти зверху донизу;
- Захист повинен бути безперервним, циклічним, проактивним процесом;
- Ефективний захист забезпечується шляхом резервування засобів безпеки;
- Ступінь захищеності системи вимірюється захищеністю її найслабшої ланки;
- При створенні системи безпеки необхідний компроміс між витратами та ризиками."

"Брандмауери, які використовуються для простих цілей, таких як фільтрація пакетів, сьогодні майже втратили своє використання. Безпека не може бути забезпечена лише інформацією про порт та IP, також з'явилося багато потреб, таких як виявлення вторгнень та обізнаність про програми". Для задоволення цих потреб були розроблені системи Уніфікованого управління загрозами (UTM). За допомогою цієї системи фільтрація пакетів і потреби безпеки можуть бути задоволені з однієї системи. Однак ця система втратила свою продуктивність, оскільки для задоволення потреб безпеки працюють різні служби. У відповідь на проблеми та потреби, згадані вище, використовуються брандмауери наступного покоління (NGFW).

Порівнюючи операційні системи захисту мереж, що створені на основі стандартних операційних систем, таких як Unix або Microsoft Windows, NetDefendOS пропонує повну інтеграцію всіх своїх підсистем, поглиблений адміністративний контроль усіх функціональних можливостей, а також Проблеми експлуатації та захисту інформаційно-комунікаційних систем, 7-8 червня 2022 мінімальну поверхню для атак, що допомагає звести нанівець ризик від атаки безпеки. Традиційні IP-маршрутизатори або комутатори зазвичай перевіряють усі пакети, а потім приймають рішення про переадресацію на основі інформації, знайденої в заголовках пакетів. Завдяки цьому підходу пакети пересилаються без будь-якого відчуття контексту, що усуває будь-яку можливість виявлення й аналізу складних протоколів і застосування відповідних політик безпеки.

NetDefendOS використовує техніку перевірки стану, що перевіряє та пересилає трафік на основі кожного з'єднання. Виявляє, коли встановлюється нове з'єднання, і зберігає невелику інформацію або стан у своїй таблиці стану протягом усього часу цього з'єднання. Завдяки цьому дана операційна система захисту мережі може розуміти контекст мережевого трафіку, що дозволяє виконувати поглиблене сканування трафіку, застосовувати керування смугою пропускання та ряд інших функцій. Підхід до перевірки стану додатково забезпечує високу пропускну здатність із додатковою перевагою конструкції, яка має високу масштабованість. "Щоб доповнити низькорівневу фільтрацію пакетів, яка перевіряє лише заголовки пакетів у таких протоколах, як IP, TCP, UDP і ICMP, брандмауери NetDefend забезпечують шлюзи прикладного рівня (ALG), які забезпечують фільтрацію на вищому рівні OSI програми."

Висновок

Сьогодні обладнання компанії D-Link використовують все більше світових компаній в різних сферах для реалізації своїх амбіцій у повній мірі, необхідний високий рівень захисту конфіденційної інформації, підтверджує затребуваність не тільки обладнання, а й фахівців, що налаштовують дану систему. Актуальність даної роботи для компаній важко переоцінити, оскільки фінансові витрати, що необхідні для побудови системи захисту, окупаються менш ніж за рік, і, в той же час компанії отримують високий рівень інформаційної безпеки.

УДК 004.056.52

А.С. Страх, Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

ЕФЕКТИВНІСТЬ СИСТЕМИ ЗАХИСТУ AMAZON WEB SERVICES: РЕЗУЛЬТАТИ ТА ПЕРЕВАГИ

Забезпечення безпеки та захисту даних в системі хмарних серверів Amazon Web Services (AWS) є вирішальним фактором для ефективного використання цього сервісу. Як користувач AWS, я розумію важливість міцної системи захисту для збереження конфіденційності, цілісності та доступності моїх даних. У цьому тексті ми розглянемо систему захисту AWS та її значення для забезпечення надійного захисту даних і інфраструктури.

Для забезпечення безпеки і захисту в хмарному середовищі Amazon Web Services (AWS) використовуються різноманітні методи, включаючи ідентифікацію та автентифікацію, контроль доступу, шифрування і моніторинг. AWS надає комплексні інструменти, такі як управління доступом на основі ролей (IAM), політики безпеки, сервіси шифрування та моніторингові рішення, що дозволяють користувачам забезпечувати безпеку своїх хмарних серверів.

Додатково, в рамках матеріалів і методів для захисту хмарних серверів AWS використовуються інтелектуальні сервіси безпеки, які автоматизують виявлення та реагування на потенційні загрози. Наприклад, AWS CloudTrail забезпечує контроль та аудит дій в хмарному середовищі, а Amazon GuardDuty аналізує логи подій для виявлення підозрілих активностей і вторгнень. Крім того, AWS пропонує рішення для резервного копіювання даних, реплікації і відновлення систем, які допомагають забезпечити високу доступність і надійність хмарних серверів.

Результати використання системи захисту Amazon Web Services (AWS) є вражаючими. Завдяки комплексному підходу до безпеки, AWS забезпечує надійний захист інфраструктури та даних клієнтів. Основні результати, які можна виділити, включають:

Висока доступність: AWS забезпечує високий рівень доступності, що гарантує безперебійну роботу інфраструктури. Ре-

зервування даних, розподіл навантаження та автоматичне масштабування дозволяють забезпечити неперервну роботу сервісів.

Захист від фізичних загроз: AWS здійснює контроль доступу до своїх датацентрів, включаючи фізичні периметри, системи моніторингу та фізичну безпеку обладнання. Це забезпечує захист від фізичних загроз, таких як вторгнення, крадіжка обладнання або незаконний доступ до серверів.

В цій роботі була проведена детальна аналітика системи захисту хмарних серверів Amazon Web Services.

Результати дослідження вказують на високу ефективність цієї системи у забезпеченні безпеки та захисту даних. Отримані результати мають велику наукову новизну та практичну цінність, їх можна використати для розвитку та вдосконалення систем захисту в хмарних середовищах, забезпечуючи надійну захисту важливих інформаційних ресурсів та протидіючи сучасним загрозам в сфері кібербезпеки.

Список використаних джерел:

Amazon Web Services Security - https://aws.amazon.com/security/
AWS Security Best Practices - https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
AWS Identity and Access Management (IAM) Documentation - https://docs.aws.amazon.com/iam/

УДК 004.056 (043.2)

С.В. Татаринцев, Д.І. Бахтіяров, В.М. Чуприн
Національний авіаційний університет, м. Київ

ІНФОРМАЦІЙНА СИСТЕМА МОНІТОРИНГУ ТА АНАЛІЗУ ІНТЕРНЕТ ТРАФІКУ НА БАЗІ ПРОТОКОЛУ NETFLOW

Протокол NetFlow є досить актуальним для моніторингу мережі в сучасному середовищі, де високосегментовані топології та велика кількість точка-точка з'єднань ускладнюють завдання моніторингу трафіку. Використання NetFlow дозволяє отримати повну картину розподілу трафіку в мережі та забезпечити аналіз його характеристик, таких як джерело трафіку, цільовий адрес, протокол, порти, використані ресурси мережі та інші параметри.

Завдяки протоколу NetFlow можна виявляти та усувати проблеми з мережевим трафіком, такі як затори, збої в роботі мережі, атаки та інші проблеми, що можуть негативно впливати на продуктивність мережі та безпеку інформації. Крім того, аналіз даних NetFlow може допомогти забезпечити оптимальну робо-ту мережі, налаштувати правила мережевої безпеки та вирішувати інші проблеми, що стосуються мережі.

Протокол NetFlow є досить актуальним в контексті моніторингу трафіку в мережах. З його допомогою можна збирати детальну інформацію про трафік, яка дозволяє аналізувати його характеристики та використовувати для вирішення різноманітних завдань.

Було поставлено завдання написати зручний графічний інтерфейс для виве-дення даних з бази даних MySQL. Системному адміністратору має бути зручно шукати необхідну мережеву інформацію, відображати за фільтрами. Зрештою було написано 2 форми: Форма з авторизацією; Форма програми.

Форма авторизації складається з двох елементів TextBox, трьох елементів Label та однієї кнопки Button. Після натискання кнопки відбувається звіряння введених аутентифікаційних даних з тими, що прописані у файлі en-ter.cs. Під час введення неправильних облікових даних виходить повідомлення «Неправильний логін або пароль».

При введенні пароля включена функція приховування пароля від сторонніх очей, тому у стані, що працює, дана форма виглядає так, як на рис. 1.

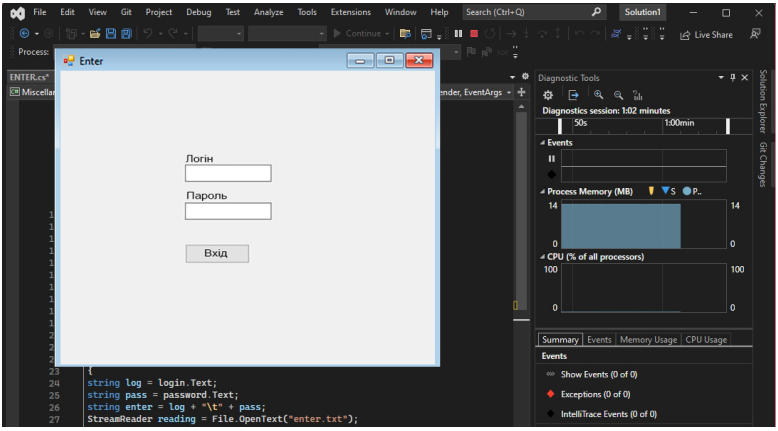


Рис.1. Реалізація форми ENTER.cs у програмному середовищі Visual Studio 2022

Крім форми з авторизацією є основна частина програми під назвою FOR-MULA.cs, код якої представлено на рис. 2.

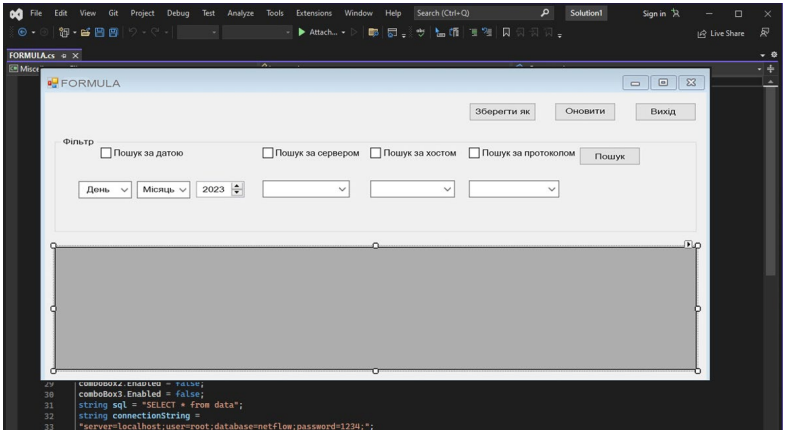


Рис. 2. Вікно програми FORMULA.cs

DataGridView призначений для виведення таблиці з бази даних MySQL. Цей елемент управління має безліч налаштувань.

Після успішного входу в програму друга форма автоматично відкриється. Пошук із зазначенням фільтрів допомагає швидше знайти потрібну інформацію. Можна вказати як дату, і сервер, якщо він відомий, і протокол передачі.

Кнопка «Оновити» оновлює інформацію та підвантажує нову базу даних. Якщо натиснути кнопку «Зберегти як», можна отримати вивантаження поточного звіту до excel-файл (рис. 3). Кнопка «Вихід» повертає до попередньої форми з авторизацією.

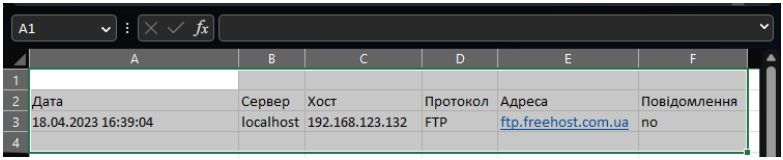


Рис. 3. Вигляд вивантаженого поточного звіту в програмному пакеті Microsoft Excel 2021

Висновки

Використання протоколу NetFlow в локальній мережі підприємства може бути корисним з багатьох причин. Спочатку, протокол NetFlow дозволяє збирати детальну статистику щодо трафіку в мережі. Це може допомогти адміністраторам мережі отримати більш глибоке розуміння того, як використовується їхня мере-жа. Наприклад, вони можуть виявити надмірні обсяги трафіку в певні години дня або трафік, що генерується певними додатками або пристроями.

Крім того, використання NetFlow може допомогти виявити можливі загрози безпеці мережі, такі як атаки або шкідливе програмне забезпе-чення. Аналіз NetFlow може допомогти виявити незвичайні мережеві ак-тивності, які можуть бути зумовлені зловмисниками, що намагаються зламати мережу.

Загалом, використання протоколу NetFlow може допомогти покращити продуктивність та безпеку локальної мережі підприємства, забезпечуючи адмініс-траторам мережі засоби для отримання детальної інформації про трафік та мож-ливі загрози.

Список літератури

1. D. González-Sánchez et al., "Model-Driven Network Monitoring Using NetFlow Applied to Threat Detection," 2022 IEEE 8th International Conference on Network Softwarization (NetSoft), Milan, Italy, 2022, pp. 450-455.

2. M. H. Haghighat, Z. A. Foroushani and J. Li, "SAWANT: Smart Window Based Anomaly Detection Using Netflow Traffic," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1396-1402.

УДК 621.3

Є.І. Шевченко
Національний авіаційний університет, м. Київ

АДАПТИВНИЙ АЛГОРИТМ МАРШРУТИЗАЦІЇ ДЛЯ МЕРЕЖ УПРАВЛІННЯ БПЛА

Після віроломного нападу на Україну російською федерацією держава бореться не тільки з ворогами, а й з наслідками цієї страшної війни. Виходячи з аналізу стану навколишнього середовища сьогодні в Україні, набуває все більшої актуальності питання визначення та контролю негативних факторів, які впливають на стан водяних, лісових ресурсів держави.

А особливо актуальні зараз є великі ударні БПЛА, на борт таких дронів можна розмістити до 500 кілограмів вибухівки. Завдяки таких БПЛА є можливість знищувати ворожі склади з боєприпасами за тисячі кілометрів від оператора, такі безпілотникі програмуються за координатам за допомогою маршрутизатора. Найголовнішою перевагою БПЛА – це берегти життя наших солдатів які боронять Україну, завдяки розвідувальним БПЛА вони можуть дізнатися де знаходить ворог, і вже за допомогою цього приняти найвигідніше для них рішення.

Метою роботи є дослідження та розгляд всіх можливих методи маршрутизації, недоліки та переваги кожного з них. Вибрати та дослідити найкращий із маршрутизаторів для БПЛА. Довести чому саме він найкращий у теперішній час.

Об’єктом дослідження є маршрутизатор для БПЛА. Маршрутизатор - це електричний пристрій за допомогою якого можна запрограмувати БПЛА на координати, і в подальшому цей безпілотник зможе літати без втручання оператора.

Моїм вибором та моєю рекомендацією буде протокол маршрутизації централізованого збору даних (ПЦЗД) можливий для FANET, де дані запитуються та збираються з посиланням на характеристики даних замість ідентифікаторів відправника або приймача. Через бездротовий характер моделі зв'язку БПЛА можна віддавати перевагу багатоадресному обміну даними замість одноадресного.

Цей алгоритм маршрутизації може бути використаний, коли запит даних генерується декількома БПЛА, а розподіл даних здійснюється алгоритмами за запитами. ПЦЗД може бути використаний у FANET, щоб

забезпечити різноманітні типи програм у однорідній системі БПЛА для накопичення точних даних із конкретної області місії.

Як правило, для такого типу архітектури справедлива модель публікації-підписки. Вона з'єднується автоматично з джерелами даних, які називаються видавцями, і з споживачами даних, які називаються підписниками. Вузол джерела приймає інформацію, яку потрібно опублікувати, а потім починає розповсюдження даних. Після того як опубліковані дані досягнули БПЛА у мережі він намагається знайти повідомлення про підписку, а потім пересилає ці дані до БПЛА-адресата.

Основна перевага цього алгоритму маршрутизації полягає в тому, що він може надсилати підписникам лише зареєстрований вміст.Протоколи маршрутизації централізованого збору розділені у трьох вимірах:

– просторове розділення: БПЛА можуть спілкуватися де завгодно, і дізнатися ідентифікатор чи місцезнаходження один одного не є обов'язковим;

– часове розділення: для спілкування поміж БПЛА, вони не повинні бути одночасно в Інтернеті, і дані можуть передаватися абонентам миттєво або пізніше;

– розділення потоку: доставка даних може бути надійно виконана за допомогою асинхронної структури зв'язку.

Було виконано аналіз протоколів для бездротового обміну даними, які зазвичай використовуються в БПЛА, а саме IEEE 802.11n та IEEE 802.15.4 Було досліджено вплив застосування протоколу маршрутизації спеціального дистанційного вектора за запитом, в залежності від таких факторів як топології мережі (типу зірка чи сітчата) та кількості БПЛА.

Факторами порівняння були обрані: кількість успішно переданих пакетів, швидкість руху БПЛА та час затримки доставки пакетів «кінець в кінець».

УДК 004.77

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

ЗАХИЩЕНА МЕРЕЖА НА БАЗІ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ТЕХНОЛОГІЇ VPN

Для забезпечення технології безпечної передачі даних по загальнодоступній (незахищеній) мережі використовують узагальнену назву – захищений канал (secure channel). В даному випадку термін «канал» підкреслює той факт, що захист даних забезпечується між двома вузлами мережі (хостами чи шлюзами) впродовж деякого віртуального шляху, якій був прокладений в мережі з комутацією пакетів.

Захищений канал можна побудувати за допомогою технології VPN. VPN (англ. Virtual Private Network, Віртуальна приватна мережа) — це логічна мережа, створена поверх інших мереж, яка використовує загальнодоступні чи віртуальні канали інших мереж. Забезпечення безпеки передавання пакетів, використовуючи загальнодоступні мережі, може реалізуватися з використанням шифрування, внаслідок чого створюється закритий для доступу сторонніх канал обміну інформацією. Використання технології VPN дозволяє об'єднати декілька територіально віддалених мереж в єдину мережу із застосування непідконтрольних каналів.

У залежності від протоколів та призначень, VPN надає можливість застосувати три види з’єднань: вузол-вузол, вузол-мережу та мережу-мережу.

При передачі інформації через VPN-канали, вона потрапляє на вхід VPN-каналу, і після повного проходження через канал, з’являється на іншій стороні, в точці призначення. Такий процес вважається «тунелюванням» – створення логічного тунелю у мережі Інтернет, якій повинен поєднати дві точки. При застосуванні «тунелю» особиста інформація стає невидимою для інших користувачів Інтернету. Перед тим як інформація потрапляє до інтернет-тунелю, дані зашифровуються, і це дає інформації додатковий захист.

Захищений тунель створюється компонентами віртуальної мережі, такі компоненти мають назву ініціатор та термінатор тунелю. Ініціатор створення тунелю інкапсулює початковий пакет в новий пакет, який повинен містити заголовок з інформацією щодо відправника та отримувача. Пакети, які повинні бути інкапсульовані, можуть відно-

ситися до протоколу будь-якого типу, включаючи пакети протоколів, які не можуть бути маршрутизовані. Всі пакети, які передаються до тунелю, належать до пакетів IP.

Термінатор тунелю здійснює зворотній процес до інкапсуляції. Саме термінатор видаляє нові заголовки та направляє кожен пакет саме тому отримувачу в локальній мережі.

Класифікують VPN за типом середовища в якому воно використовується:

- захищене, це найпоширеніший варіант віртуальних мереж. За допомогою цього варіанту можливо створити надійну і захищену підмережу на базі ненадійної мережі, Інтернету. Як приклад використання захищених протоколів VPN: IPSec, SSL та PPTP;

- довірче, воно використовується у випадках, коли середовище, в якому передаються дані, можна вважати надійним і необхідно вирішити задачу створення віртуальної підмережі в межах більшої мережі. Питання забезпечення безпеки, в такому разі, стають неактуальними. Прикладами подібних VPN рішень є: Multi-protocol label switching (MPLS) та L2TP (Layer 2 Tunnelling Protocol).

Для захисту інформації в технології VPN використовується шифрування (encryption), підтвердження справжності (authentication) та контроль доступу (access control). Зазвичай мережа VPN утворюється на рівнях не вище мережевого, також використання криптографії на цих рівнях дозволяє працювати на транспортних протоколах (такі як TCP, UDP) в незмінному вигляді.

Дотримуючись належного рівня реалізації та при використанні спеціального програмного забезпечення, мережа VPN може забезпечити досить високий рівень шифрування переданої інформації. Якщо правильно підібрати всі компоненти для створення захищеної мережі з використанням технології VPN, це забезпечить анонімність в перебування мережі.

Список літератури

1. VPN протоколи [Електронний ресурс] – Режим доступу до ресурсу: https://www.cactusvpn.com/ua/beginners-guide-to-vpn/vpn-protocol/

2. A Framework for IP Based Virtual Private Networks [Електронний ресурс] – Режим доступу до ресурсу: http://www.ietf.org/rfc/rfc2764.txt

3. *Virtual private network (VPN) [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Virtual_private_network*

УДК 004.056.5

О.В. Яремчук, В.Є. Курушкін
Національний авіаційний університет, м. Київ

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO PIX FIREWALL

Будь-яка організація, яка бажає надавати послуги, зобов'язана забезпечити захист своєї мережі. Захищена мережа допоможе вам убезпечити конфіденційну інформацію від атак та, зрештою, збереже репутацію вашої компанії. Брандмауер - це пристрій захисту мережі, котрий моніторить вхідний і вихідний мережевий трафік та вирішує, дозволити чи заблокувати певний трафік на базі заданого переліку правил безпеки. Компанія Cisco пропонує як міжмережеві екрани, спрямовані на боротьбу із загрозами, так і пристрої Unified Grows Management (UTM).[1]

Міжмережевий екран PIX (Private Internet Exchange), будучи правильно налаштованим, перешкоджає несанкціонованим з'єднанням з однієї мережі з іншою. Мережу, захищену брандмауером PIX Firewall, називають внутрішньою мережею або "Internal", а мережу, з якої контролюються з'єднання, - зовнішньою мережею чи "External".[2] PIX Firewall має опцію підтримки додаткових зовнішніх мереж, котрі можуть використовуватися як мережі периметру або демілітаризованих зон (DMZs). Підключеннями між периметром, зовнішньою та внутрішньою мережами можна контролювати завдяки брандмауеру PIX Firewall. При безпечному з'єднанні весь трафік між внутрішньою та зовнішньою мережами повинен проходити через брандмауер. Зовнішня мережа, переважно, має доступ до Інтернету і містить системи, які підтримують зовнішню мережу. Такі сервіси містять веб-сервер, FTP-сервер або SMTP-сервер (електронної пошти).[2] Підключення до цих серверів додатків можна контролювати за допомогою списків доступу на підключеному до Інтернету маршрутизаторі. В схемі проєкту використовується Cisco PIX 515 для захисту внутрішньої корпоративної мережі від зовнішніх зловмисників, одночасно дозволяючи внутрішнім хостам доступ до Інтернету. PIX створює три інтерфейси безпеки: зовнішній, внутрішній і DMZ. Він забезпечує зовнішнім користувачам обмежений доступ до DMZ і відсутність доступу до внутрішніх

ресурсів. Внутрішні користувачі можуть отримати доступ до DMZ і зовнішніх ресурсів.

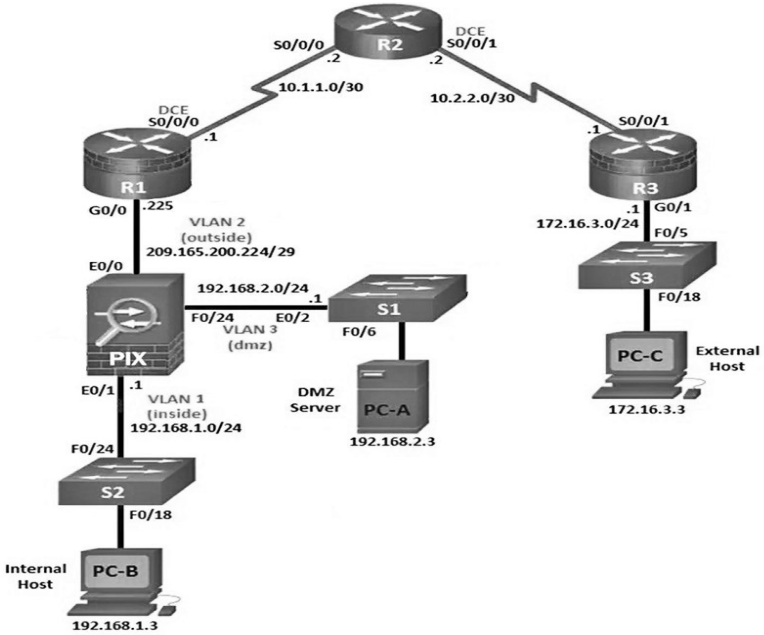


Рис.1 Структурна схема проєкту мережі

В проєкті мережі Cisco PIX Firewall налаштовано для керування адміністратором внутрішньої мережі та віддаленим адміністратором. Інтерфейси VLAN рівня 3 забезпечують доступ до трьох областей: внутрішньої, зовнішньої та DMZ. Cisco PIX Firewall показав себе як оптимальний варіант для забезпечення безпеки малих та середніх мереж, поєднуючи такі функції як рівні безпеки інтерфейсу, вбудовані списки керування доступом і стандартні політики перевірки.

Список літератури:

1. What Is Network Security?. Cisco. URL: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html (дата звернення: 01.06.2023).
2. Introduction [Cisco PIX Firewall Software]. Cisco. URL: https://www.cisco.com/en/US/docs/security/pix/pix41/configuration/guide/pix41int.html (дата звернення: 01.06.2023).

УДК 654.1

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

МЕРЕЖА РАДІОДОСТУПУ СИСТЕМИ СТІЛЬНИКОВОГО ЗВЯ'ЗКУ

Нинішній час можна назвати епохою телекомунікацій. Кожна сучасна людина використовує засоби телекомунікацій у повсякденному житті. За останні роки телекомунікаційні технології набули надзвичайного поширення, причому водночас із комп'ютерною технікою та технологіями комп'ютерних мереж з'явилися комп'ютерна телефонія, телеконференцзв'язок, електронна пошта та ін. Сучасний розвиток мобільних технологій дозволяє обробляти все більші об'єми інформації, тим самим відкриваючи для користувача мобільного пристрою (смартфона, планшета, нетбука) нові можливості навчання, ведення бізнесу або маніпуляції з різними видами мультимедійних даних.

Системи зв'язку стандарту GSM розраховані на використання у різних сферах. Вони надають широкий діапазон послуг з передачі мовних повідомлень і даних, аварійних сигналів, забезпечують підключення до телефонних мереж загального користування (PSTN), мереж передачі даних (PDN) і цифрових мереж з інтеграцією служб (ISDN).

У стандарті UMTS пропонується набір послуг, який включає до себе як високошвидкісний мобільний доступ до мережі Інтернет, так і технологію радіозв'язку. Цю технологію також ще називають технологією 3G.

Мережі третього покоління 3G працюють на частотах дециметрового діапазону (близько 2 ГГц), швидкість передачі даних становить понад 2 Мбіт/с. Завдяки цій швидкості, можна комфортно дивитися на мобільному пристрої фільми, телепрограми, завантажувати дані, а також організувати відеотелефонний зв'язок. Технологія 3G використовує кілька мобільних стандартів.

Найбільш поширеними є три з них:

• CDMA2000 — є подальшим розвитком стандарту 2 покоління CDMA One;

• WCDMA (UMTS) (англ. Wideband Code Division Multiple Access — широкосмуговий CDMA) — технологія радіоінтерфейсу, обрана більшістю операторів стільникового зв'язку для забезпечення широкосмугового радіодоступу з метою підтримки послуг 3G.

• TD-SCDMA (англ. Time Division — Synchronous Code Division Multiple Access) — китайський стандарт мобільних мереж третього покоління.

Архітектура мереж 3G використовує ту ж відому архітектуру, яка застосовується у всіх основних системах другого покоління і подібна вже до розглянутої архітектури системи GSM.

Мережа 3G будується на базі тих же компонентів. В основу архітектури входить: мобільна телефонна станція, в системі UMTS вона називається UE (User Equipment); базова телефонна станція, по використовуваної термінології — вузол B (Node B); контролер базової станції (BSC) і центр комутації мобільного зв'язку (MSC).

Long Term Evolution (LTE, англ. Long Term Evolution — «довготерміновий розвиток»), маркетингова назва 4G — назва мобільного протоколу передачі даних; проект 3GPP, стандарт з удосконалення UMTS для задоволення майбутніх потреб у швидкості.

Мережі 4G на основі стандарту LTE працюють у всіх існуючих діапазонах частот, що виділені для стільникового зв'язку по всьому світу.

Швидкість закачування за стандартом 3GPP LTE в теорії досягає 326,4 Мбіт/с (download), і 172,8 Мбіт/с (upload). Практично забезпечується швидкість передачі даних від базової станції до пристрою абонента до 100 Мбіт/с і швидкість від абонента до базової станції до 50 Мбіт/с.

Мережа LTE складається з двох компонентів: мережі радіодоступу E-UTRAN і базової мережі SAE (System Architecture Evolution) або EPC (Evolved Packet Core Network).

Технології мобільного голосового зв'язку та високошвидкісної бездротової передачі даних наразі стрімко розвиваються, що змушує замислитися про перспективи використання нових стандартів і систем зв'язку вже в найближчому майбутньому. Сьогодні експертам і технічним фахівцям телекомунікаційних компаній, операторам зв'язку й провайдерам послуг доводиться виконувати складні завдання переходу на нові технології. При цьому слід дотримуватися поєднання нових технологій зі старими, їх раціонального застосування в інтересах як операторів, так і користувачів.

УДК 621.391

В.М. Яценко, О.Ю. Лавриненко
Національний авіаційний університет, м. Київ

СИСТЕМА ГОЛОСОВОЇ АУНТЕНТИФІКАЦІЇ В ДИСТАНЦІЙНОМУ БАНКІВСЬКОМУ ОБСЛУГОВУВАННІ

У зв'язку з бурхливим розвитком біометричних технологій у світі, особливе місце в дослідженнях «Центру мовленнєвих технологій» займає розробка інноваційних рішень щодо голосовій біометрії. Отримані рішення для створення та ведення фонообліків, проведення автоматичної ідентифікації особистості за голосом засновані на таких методах автоматичного використання голосу та мови, для яких не має значення мова, акцент диктора та діалект, а також зміст тексту мови, що вимовляється.

Унікальність голосової біометрії полягає в тому, що це єдина біометрична модальність, яка дозволяє ідентифікувати людину по телефону. Це важливо, наприклад, при віддаленому доступі до різних послуг, при криміналістичній ідентифікації, де єдиним доказом є запис телефонної розмови підозрюваного.

Крім того, голосова ідентифікація не потребує спеціалізованого дорогого обладнання. Все, що потрібно – звичайний мікрофон. При цьому рівні надійності голосова біометрії не поступається, а по деяким характеристикам перевищує характеристики інших систем біометричної ідентифікації.

Унікальність голосу людини обумовлена безліччю фізіологічих особливостей (будовою голосових зв'язок, трахеї, носових порожнин, манерою вимови звуків, розташуванням зубів). Комбінація цих особливостей індивідуальна, як і відбитки пальців. Однак на практиці жодна з унімодальних систем біометричної ідентифікації, у тому числі й голосова, не може гарантувати 100% ідентифікації особистості.

В даний час для збільшення обсягів інформації, що передається, застосовуються різні методи, наприклад частотне і тимчасове ущільнення сигналів. Для виконання завдання розпізнавання мови в першу чергу необхідно визначити моменти початку та закінчення вхідного слова та пауз усередині нього.

Постановка задачі. Визначення моментів початку та закінчення фрази за наявності шуму є важливим завданням розпізнавання мови.

Зокрема, при автоматичному розпізнаванні мови важливо точно визначити моменти початку та закінчення слова.

Процедура виявлення моментів початку та закінчення фрази істотно зменшує число арифметичних операцій, якщо обробляти лише ті сегменти, в яких є мовний сигнал. Внаслідок цього швидкість обробки збільшуватиметься. Найбільш поширеним способом стиснення мовних даних є видалення пауз між фразами, словами, окремими звуками. Як показали численні дослідження, в мові може бути до 50% пауз, а в діалозі їх обсяг може досягати 70%. Тому було створено різні алгоритми, які усувають надмірність мови, виділяючи лише значущі її параметри.

Ідентифікація особи за голосом, що проводиться в реальних умовах, зустрічається з низкою серйозних труднощів.

По-перше, можливі спотворення, пов'язані безпосередньо з диктором та зумовлені особливостями його психофізичного стану, захворюванням тощо. Ці спотворення за допомогою будь-якої автоматизованої системи обробки та класифікації виключити неможливо, можна лише зменшити їхній вплив.

По-друге, виникають апаратні спотворення на різних ділянках проходження мовного сигналу при його запису, обробці та зберіганні.

По-третє, на голосовий сигнал неминуче накладаються зовнішні механічні шуми, які можуть суттєво спотворювати його. Найважливішим завданням систем голосової ідентифікації є зменшення негативного впливу другого та третього чинників.

Зазвичай виділяють: спотворення сигналу, пов'язані з самим диктором, з шумом навколишнього середовища, зі спотворенням мікрофонної системи (у тому числі електромагнітні перешкоди), спотворення, що виникають у каналі запису при передачі сигналу, та спотворення при програмній обробці сигналу в комп'ютері.

В кінцевому підсумку перешкоди, що виникають у апаратній частині системи ідентифікації, зводяться до частотних та амплітудних спотворень вихідного спектру та сигналу.

УДК 004.7:005.72 (043.2)

І.П. Холод
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА МЕТОДИКИ СПРОЩЕННЯ ІНТЕГРАЦІЇ З МІКРОСЕРВІСАМИ ТА СТОРОННІМИ API У NODE.JS ДОДАТКАХ

Мікросервіси – це архітектура, в якій створюються і розміщуються різні компоненти програмного забезпечення як окремі ізольовані служби. Кожен з них розгортається окремо, і вони спілкуються через чітко визначені мережеві інтерфейси. Мікросервіси призначені як «маленькі» (нечітко визначені) і зберігаються в єдиному обмеженому контексті. Мікросервіси мають багато переваг. Через свою ізольованість і сувору вимогу до спілкування через чітко визначені інтерфейси мікросервіси запобігають швидким і брудним рішенням, які часто зустрічаються в монолітах. Ці хаки всередині моноліту призводять до втрати зчеплення та збільшення зв'язку — двох основних причин складності [1].

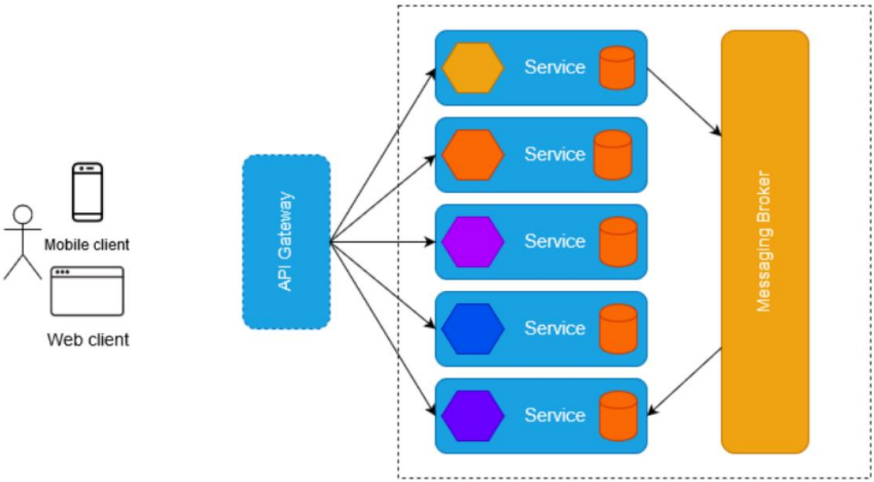


Рис. 1. Модель архітектури мікросервісів

Багато хто стверджує, що ви можете зберегти цю поведінку в моноліті. Насправді, оскільки це легко і тому що надто мало архітекторів, які працюють у наших базах коду, моноліти зазвичай падають через цю саму невдачу. Складність виникає через низьку когезію та високу зчеплення. Мік-

росервіси надають структуру, щоб уникнути цього. Цю перевагу неможливо переоцінити. Оскільки ми тримаємо монстра складності в страху, розробка систем десятирічної давності може продовжувати розвиватися зі швидкістю розробки, коли система була абсолютно новою. Знову й знову складність, викликана слабкою згуртованістю та тісним зв'язком, була причиною повільного розвитку старих проектів. Згуртованість і зв'язок – це традиційно технічний борг, який бере на нас ноги, сповільнюючи нас. Назбирайте його з роками, і ви будете боротися з цим. Якщо послуги написані з урахуванням них, а інфраструктура надає це, інші переваги можуть включати горизонтальну масштабованість, можливість тестування, надійність, спостережливість, замінюваність і незалежність від мови. Недоліком мікросервісів є те, що для досягнення цих переваг ви повинні забезпечити базову інфраструктуру, яка їх підтримує. Без цієї підтримки ви можете легко опинитися з ненадійною та непрозорою системою — або ви зможете заново винаходити колесо надійності в кожній окремій службі.

Express.js — це безкоштовна платформа веб-додатків з відкритим вихідним кодом для Node.js. Він використовується для швидкого та легкого проектування та створення веб-додатків. Веб-програми — це веб-програми, які можна запускати у веб-браузері. Оскільки для Express.js потрібен лише javascript, програмістам і розробникам стає легше створювати веб-додатки та API без будь-яких зусиль. Express.js — це фреймворк Node.js, що означає, що більшість коду вже написана для роботи програмістами. Ви можете створювати односторінкові, багатосторінкові або гібридні веб-програми за допомогою Express.js. Express.js є легким і допомагає організувати веб-додатки на стороні сервера в більш організовану архітектуру MVC. Важливо вивчити javascript і HTML, щоб мати можливість використовувати Express.js. Express.js полегшує керування веб-додатками. Це частина технології на основі javascript, яка називається програмним стеком MEAN, що означає MongoDB, ExpressJS, AngularJS і Node.js. Express.js є внутрішньою частиною MEAN і керує маршрутизацією, сеансами, HTTP-запитами, обробкою помилок тощо. Бібліотека JavaScript Express.js допомагає програмістам створювати ефективні та швидкі веб-програми. Express.js покращує функціональність node.js. Насправді, якщо ви не використовуєте Express.js, вам доведеться виконати багато складного програмування, щоб створити ефективний API. Це полегшило програмування на node.js і надало багато додаткових функцій.

Express.js підтримує JavaScript, який є широко використовуваною мовою, яку дуже легко вивчити і яка також підтримується всюди. Тому, якщо

ви вже знаєте JavaScript, то вам буде дуже легко програмувати за допомогою Express.js. За допомогою Express.js ви можете легко створювати різні види веб-додатків за короткий проміжок часу. Express.js забезпечує просту маршрутизацію для запитів, зроблених клієнтами [2]. Він також забезпечує проміжне програмне забезпечення, яке відповідає за прийняття рішень щодо надання правильних відповідей на запити, зроблені клієнтом. Без Express.js вам доведеться написати свій власний код для створення компонента маршрутизації, що займає багато часу та виснажливе завдання. Express.js пропонує програмістам простоту, гнучкість, ефективність, мінімалізм і масштабованість. Він також має перевагу потужної продуктивності, оскільки є основою Node.js. Node.js виконує всі виконання дуже швидко за допомогою циклу подій, що дозволяє уникнути будь-якої неефективності [3]. Потужна продуктивність Node.js і простота кодування за допомогою Express.js є найпопулярнішими функціями, які люблять розробники веб-додатків. Оскільки Express.js написаний на Javascript, ви можете створювати веб-сайти, веб-додатки або навіть мобільні програми, використовуючи його.

Інтеграція з мікросервісами та сторонніми API у Node.js додатках може бути спрощена кількома способами.

Використання бібліотек для HTTP запитів, axios або node-fetch:

- ці бібліотеки дозволяють виконувати HTTP запити до інших сервісів, обробляти відповіді та передавати дані між мікросервісами та сторонніми API.

Використання SDK або бібліотек, наданих постачальником сервісу:

- деякі компанії надають власні SDK або бібліотеки для взаємодії зі своїми сервісами. Наприклад, для роботи з Twitter (*X*) або Facebook API є власні бібліотеки, які спрощують процес інтеграції.

Використання фреймворків для мікросервісної архітектури:

- Express, NestJS, або Fastify: Ці фреймворки для Node.js дозволяють легко створювати мікросервіси та обробляти HTTP запити між ними.

Використання патернів проектування:

- REST або GraphQL: Розроблення API з використанням стандартів архітектури REST або GraphQL спрощує інтеграцію мікросервісів.

Обробка помилок та забезпечення безпеки:

- обробка помилок. Важливо мати систему обробки помилок для забезпечення стабільності системи.

Аутентифікація та авторизація:

- Забезпечення безпеки API шляхом використання токенів, JWT або інших методів аутентифікації.

Тестування:

- юніт-тести та інтеграційні тести. Важливо перевіряти, як ваші мікросервіси взаємодіють один з одним, а також тестувати сторонні API.

Незалежно від того, який підхід буде обрано, важливо дотримуватися чистого коду, документування та моніторингу, щоб забезпечити ефективну роботу системи.

Спрощення інтеграції. Деякі практики можуть допомогти подальшому оптимізуванню процесу:

Кешування та попереднє завантаження даних:

- Redis або Memcached. Використання інструментів кешування може допомогти зберігати попередньо завантажені дані для покращення швидкодії та зниження навантаження на сервери.

Резервне копіювання та відновлення:

- резервне копіювання. Забезпечення системи резервного копіювання для ваших мікросервісів та зовнішніх API допоможе у відновленні даних у разі втрати.

Моніторинг та журналювання:

- Використання інструментів моніторингу, таких як Prometheus, Grafana або ELK stack: Ці інструменти дозволяють вам відстежувати стан мікросервісів та сторонніх API, а також виявляти проблеми.

Автоматизація та контейнеризація:

- Docker або Kubernetes: Використання контейнерів спрощує розгортання, масштабування та управління мікросервісами. Контейнеризація також дозволяє автоматизувати процеси розгортання та керування сервісами.

Розроблення API Gateway:

- API Gateway: Створення шару абстракції між вашими мікросервісами та зовнішніми API допоможе управляти доступом, контролем версій та розподілом навантаження.

Структуроване логування:

- використання структурованих журналів. Додає чіткість у журналах, що спрощує відлагодження та вирішення проблем.

Ці практики можуть значно спростити процес інтеграції та управління мікросервісами та сторонніми API в додатках на Node.js.

Приклад 1. Використання Axios для HTTP запитів.

Припустимо, у вас є мікросервіс для каталогування книг, і ви хочете витягти дані про книги зовнішнього сервісу.

```
const axios = require('axios');

// URL зовнішнього API для книг
const externalAPI = 'https://example.com/api/books';

// Виконання GET-запиту до зовнішнього API
axios.get(externalAPI)
  .then(response => {
    // Обробка отриманих даних
    const books = response.data;
    // Робота зі списком книг
    console.log(books);
  })
  .catch(error => {
    // Обробка помилок
    console.error('Помилка отримання даних про книги', error);
  });
```

Рис. 2. Інтеграція з сервісом каталогування книг

Приклад 2. Узагальнення логіки запитів. Зроблення функції, яка обробляє HTTP-запити і повертає оброблені дані, може спростити код та узагальнити логіку.

```
const axios = require('axios');

// Функція для виконання HTTP-запитів
async function fetchBooks(url) {
  try {
    const response = await axios.get(url);
    return response.data;
  } catch (error) {
    throw new Error('Помилка отримання даних про книги');
  }
}

// Виклик функції для отримання книг
const externalAPI = 'https://example.com/api/books';
fetchBooks(externalAPI)
  .then(books => {
    console.log(books); // Обробка списку книг
  })
  .catch(error => {
    console.error(error);
  });
```

Рис. 3. Узагальнення логіки запитів

Цей підхід дозволяє узагальнити процес виконання HTTP-запитів, зменшуючи повторення коду та спрощуючи обробку помилок. Такий код може бути легко використаний для інтеграції з будь-якими сторонніми API.

Висновки

Узагальнюючи, спрощення інтеграції мікросервісів та сторонніх API у Node.js додатках може бути досягнуте шляхом використання відповідних бібліотек для HTTP-запитів, створення універсальних функцій для обробки запитів та ретельного використання патернів проектування API. Застосування таких практик спрощує розробку, зменшує дублювання коду та полегшує підтримку системи.

Використання бібліотек, таких як Axios, у поєднанні з узагальненими функціями для виконання запитів, дозволяє ефективно інтегрувати мікросервіси та сторонні API. Це спрощує процес отримання даних та обробки відповідей, зменшуючи кількість коду та сприяючи стабільності системи. Такий підхід дозволяє розробникам швидше та ефективніше реалізовувати та підтримувати взаємодію з різноманітними сервісами та API.

Список літератури

1. O. Chaplia and H. Klym, "An Approach for Automated Code Deployment Between Multiple Node.js Microservices," 2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT), Lviv, Ukraine, 2023, pp. 202-205, doi: 10.1109/ELIT61488.2023.10310996.

2. M. Kang et al., "Scaling JavaScript Abstract Interpretation to Detect and Exploit Node.js Taint-style Vulnerability," 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 1059-1076, doi: 10.1109/SP46215.2023.10179352.

3. S. Kumar, S. Umrao, H. Gupta and K. Saxena, "Project Management and Evaluation system Using Node JS," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 567-571, doi: 10.1109/ICACITE57410.2023.10183175.

НАУКОВЕ ВИДАННЯ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

7 – 9 ЧЕРВНЯ 2023 Р.

М. КИЇВ

ГОЛОВНИЙ РЕДАКТОР ОДАРЧЕНКО Р.С.

КОМП'ЮТЕРНА ВЕРСТКА ЛАВРИНЕНКО О.Ю.

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

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

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