МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

V ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«TELECOMMUNICATION: PROBLEMS AND INNOVATION»

20 грудня 2023 року

Збірник тез

м. Київ

V Всеукраїнська науково-технічна конференція «Telecommunication: problems and innovation». Збірник тез. – К.: ДУІКТ, 2023. – 56 с.

Збірник містить тези доповідей учасників конференції, представлених на V Всеукраїнській науково-технічній конференції «Telecommunication: problems and innovation», яка проводилась 20 грудня 2023 р. на кафедрі Телекомунікаційних систем та мереж Навчально-наукового інституту телекомунікацій Державного університету інформаційно-комунікаційних технологій, м. Київ.

Робочі мови – українська та англійська.

На конференції розглянуті проблеми, інновації та перспективи у сфері телекомунікацій.

СЕКЦІЯ 1

Телекомунікаційні системи та мережі

ВИКОРИСТАННЯ ДРОНІВ В ЯКОСТІ БАЗОВИХ СТАНЦІЙ СТІЛЬНИКОВОЇ НАЗЕМНОЇ СИСТЕМИ РАДІОДОСТУПУ

Заїка Віктор Федорович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто основні переваги та виклики використання дронів у стільниковій наземній системі радіодоступу. З розвитком технологій та поширення безпілотних апаратів (дронів), нові можливості відкриваються для покращення стільникового зв'язку. Використання дронів в якості базових станцій стільникової наземної системи радіодоступу (RAN) стає перспективним рішенням для покращення покриття, забезпечення швидкого реагування на потреби та підтримку ефективного використання радіочастотного ресурсу.

Дрони, як базові станції, використовуються для забезпечення мережевого покриття та забезпечення доступу до мережі в труднодоступних чи аварійних областях. Вони можуть бути оперативно задіяні для надання додаткового покриття в зоні лихварних обставин або в подіях масового скупчення користувачів.

Переваги використання дронів у RAN:

1. Розширення покриття:

Дрони можуть оперативно піднятися на велику висоту, що дозволяє їм забезпечити покриття великої території, включаючи віддалені та важкодоступні райони.

2. Забезпечення екстреного зв'язку:

В разі природних катастроф, аварій чи інших надзвичайних ситуацій, дрони можуть швидко встановити мобільний зв'язок, допомагаючи забезпечити ефективний екстрений зв'язок.

3. Мобільність та гнучкість:

Дрони мають високий рівень мобільності, що дозволяє їм швидко пересуватися для покриття різних областей або для забезпечення додаткового покриття під час масових заходів.

4. Використання в масових подіях:

У масових заходах, таких як концерти, фестивалі чи спортивні події, дрони можуть забезпечити додатковий потік пропускності для забезпечення стабільного підключення для великої кількості користувачів.

Дрони, як базові станції, потребують енергетичного живлення, що може бути викликом у довгостроковому вимірі, особливо в умовах тривалого покриття.

Необхідно розробити ефективні алгоритми управління рухом дронів для максимізації покриття та оптимізації використання ресурсів.

Використання дронів для стільникового зв'язку потребує ретельного управління щодо безпеки та приватності даних, що передаються через цю мережу.

Необхідно розробити стандартизовані протоколи та інтерфейси для забезпечення сумісності та інтеграції дронів у стільникову наземну систему.

Використання дронів в якості базових станцій стільникової наземної системи радіодоступу відкриває нові перспективи для розвитку та вдосконалення мобільних мереж. Поступовий розвиток та вирішення технічних викликів може призвести до покращення якості

обслуговування та розширення можливостей мобільного зв'язку у важкодоступних чи екстрених ситуаціях.

ЛІТЕРАТУРА

1. Покоління мереж стільникового зв'язку [Електронний ресурс] – Режим доступу до ресурсу: https://all-spares.ua/ru/articles-and-video/what-are-1g2g-3g-etc.-mobile-networks.html.
2. Гнатушенко, В.В. Системи супутникового та стільникового зв’язку [Текст]: навч. посіб. / В.В. Гнатушенко, О.О. Дробахін, В.М. Корчинський. – Д.: РВВ ДНУ, 2012. – 80 с.

МОЖЛИВОСТІ НОВОГО ПОКОЛІННЯ БЕЗПРОВІДНОГО ЗВ’ЯЗКУ WI-FI 7

Табор Денис Іванович
Державний університет інформаційно-комунікаційних технологій, м.Київ

Нові технології та послуги, пов'язані з передачею відеосигналів високої роздільної здатності, віртуальною та доповненою реальністю, іграми, хмарними обчисленнями, а також необхідністю підтримки великої кількості користувачів з інтенсивним трафіком у бездротових мережах вимагають високої продуктивності технології Wi-Fi, яка стала невід’ємною частиною повсякденного життя.

В данний час використовуется технологія Wi-Fi 5 на заміну і в доповнення якій приходить Wi-Fi 6 та 6E. І хоча останні мають доволі багато покращень, все ж не забезпечують швидкозростаючих вимог до бездротової мережі.

Тому у 2019 році було розпочато розробку розширення до існуючих стандрату IEEE 802.11be, який не тільки стане модернізацією існучих стандартів, та зазнає багато змін.

Заявлено такі зміни і покращення майбутнього стандарту 802.11be:

Передача на частоті 320 МГц і ефективніше використання фрагментованих каналів;

Агрегація каналів;

Використання до 16 антен, а також удосконалення протоколів під час використання MIMO;

Координовані прийом та передача з використанням кількох точок доступу;

Поліпшені адаптація до каналу та протокол ретрансляції;

Можлива адаптація до нормативних правил, специфічних для спектру 6 ГГц;

Передача з використанням модуляції 4096 КАМ (4K-QAM);

Передача в безперервних та фрагментованих каналах 320/160+160 МГц та 240/160+80 МГц;

Змінений формат кадру для покращеної прямої сумісності;

Більш ефективний розподіл ресурсів під час використання OFDMA;

Прискорена процедура прослуховування каналу;

Можливе неявне прослуховування каналу;

Гнучкіший метод пропуску смуг;

Інтеграція розширень Time-Sensitive Networking (TSN) для трафіку реального часу з низькою затримкою;

Підтримка з'єднань точка-точка за допомогою точки доступу.

Важливим напрямком розробки Wi-Fi 7 є підтримка програм реального часу (ігри, віртуальна та доповнена реальність, управління роботами). Примітно, що хоча WiFi по-особливому обслуговує аудіо- та відеотрафік, довгий час вважалося, що забезпечення на рівні стандарту гарантовано малих затримок (одиниць мілісекунд), також відоме як Time-Sensitive Networking, у мережах Wi-Fi принципово неможливе.

Важливим питанням, пов'язаним з Wi-Fi 7, є його взаємодія зі стільниковими мережами 4G, 5G) і 3GPP (LTE-LAA/NR-U), що працюють у тих же діапазонах частот, що не ліцензуються. Для вивчення проблем, пов'язаних із співіснуванням Wi-Fi та стільникових мереж, IEEE 802.11 створив комітет Coexisting Standing Committee (Coex SC – постійний комітет із співіснування).

Удосконалення протоколу фізичного рівня (PHY – Physical Layer) для технології EHT (Extremely High Throughput Full Duplex – надзвичайно висока пропускна спроможність у повнодуплексному режимі). Одночасне використання діапазонів 2.4, 5 та 6 ГГц є однією з особливостей технології EHT, яка дозволяє підвищити ефективність використання ресурсів спектру. Число потоків зросте від 8 до 16. Що дозволить подвоїти швидкість передачі даних.

Щоб забезпечити пропускну здатність не менше 30 Гбіт/с, вводяться безперервні смуги пропускання 240 МГц, несуміжні смуги 160+80 МГц, суміжні 320 МГц та несуміжні 160+160 МГц.

Використовуючи метод доступу до каналу OFDMA – з поділом за часом та частотою (аналогічний тому, що використовується у мережах 4G та 5G) – надає нові можливості для оптимального розподілу ресурсів. Для підвищення ефективності використання спектра одному користувачеві дозволено призначення 3-х RU (Resource Unit – ресурсні блоки) – Multi-RU, що дозволяє підвищити продуктивність в мережах з великою кількістю користувачів та підтримує пряму передачу між кліентськими пристроями.

Нововведенням є скоординована робота точок доступу. Хоча у багатьох постачальників є власні реалізації контролерів точок доступу, для забезпечення безшовного покриття, та як правило налаштування в них обмежені. Нововведення включає скоординовані планування передачі даних, спрямовану передачу сигналу і розподілені системи MIMO. Координація кількох точок доступу спрямована на оптимізацію вибору каналу та регулювання навантаження між точками доступу для досягнення ефективного використання та збалансованого розподілу радіоресурсів. Стандарт 802.11be дозволить точкам доступу різних виробників координувати між собою розклад передач, щоб зменшити взаємну інтерференцію.

Існуючі системи IEEE 802.11 використовують повторну передачу даних (MPDU – MAC protocol data unit), щоб гарантувати надійність передачі в бездротових каналах зв'язку, схильних до різних перешкод. В автоматичному повторному запиті (ARQ) одержувач просто відмовляється від помилкового MPDU, перш ніж отримати повторно переданий MPDU. Для виконання вимог вищої надійності та зменшенням затримки в IEEE 802.11be вводиться гібридний автоматичний контроль за повторною передачею (HARQ – Hybrid Automatic Retransmission Control) для збільшення ймовірності правильного розшифрування пакетів даних. На відміну від ARQ, HARQ, приймач зберігає неправильно розшифровані пакети і поєднує їх з повторно переданим перед розшифровкою.

Наочно основні відмінності між стандартами Wi-Fi 5, 6, 6E та 7 наведені у таблиці.

	802.11n	802.11ac	802.11ax	802.11be
Частоти, GHz	2.4, 5	5	2.4, 5, 6	2.4, 5, 6
Канали зв’язку, Mhz	20, 40	20,40,80,80+80,160	20,40,80,80+80,160	20,40,80,160,320
Модуляція	OFDM	OFDM	OFDM, OFDMA	OFDM, OFDMA
Канали MU-MIMO, шт	1x1, 2x2	8x8	8x8	16x16
Протоколи безпеки	WPA2	WPA2	WPA3	WPA3
Швидкість, Гбіт/с	0,6	6,77	9,6	30

Wi-Fi Alliance було заявлено що специфікація нових стандартів Wi-Fi 7 буде завершено до кінця першого кварталу 2024. Після цього буде можливе розгортання повноцінних мереж на данній технології.

Вже у 2022 компанія Intel спільно зі своїм партнером Broadcom провела успішну демонстрацію технології Wi-Fi 7, при випробуваннях дослідних пристроїв було отримано стабільну швидкість передачі інформації 5 Гбіт/с.

На сьогодні вже доступні у продажу пристрої з заявленою підпримою Wi-Fi 7. Це точки доступу та маршрутизатори таких виробників: Ubiquiti, TP-Link, ZTE та інші. Також підтримка Wi-Fi 7 анонсована у топових моделях смартфонів та ноубків.

Висновки. Враховуючи наведені переваги, впровадження Wi-Fi 7 може більш якісно вирішити задачі при використанні бездротової мережі:

- Перегляду потокового відео максимальної роздільної здатності;
- Використання пристроїв віртуальної реальності;
- Одночасної роботи великої кількості клієнтів, включаючи IoT;

Список використаних джерел

1. IEEE 802.11be Wi-Fi 7: New Challenges and Opportunities [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/document/9152055
2. IEEE P802.11be IEEE Draft Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: Enhancements for Extremely High Throughput (EHT) [Електронний ресурс] Режим доступу: https://standards.ieee.org/ieee/802.11be/7516/
3. Wi-Fi 7 to get the final seal of approval early next year, new standard is up to 4.8 times faster than Wi-Fi 6 [Електронний ресурс] Режим доступу: https://www.tomshardware.com/networking/wi-fi-7-to-get-the-final-seal-of-approval-early-next-year-delivers-48-times-faster-performance-than-wi-fi-6

ВАРІАНТ АЛГОРИТМУ ОПТИМАЛЬНОГО РОЗПОДІЛУ ТРАФІКУ

Брезіцький Сергій Миколайович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут Телекомунікацій

Оптимальний розподіл трафіку телекомунікаційної мережі за критерієм мінімальної кількості обслуговуваних пакетів по всій мережі. Оптимізація трафіку відбувається в два етапи: на першому етапі здійснюється пошук глобального оптимального рішення; на другому етапі здійснюється пошук маршрутів між кожною парою джерело-приймач в рамках оптимального рішення першого етапу оптимізації [1]. Двоетапна оптимізація дозволяє скоротити кількість незалежних змінних у цільовій функції, знайденій на першому етапі оптимізації. Для отримання математичної моделі мережі використовується тензорний аналіз складних систем, що дозволяє одночасно знаходити лінійно незалежні змінні, що мінімізують розмірність і складність розв'язуваної задачі.

Математична модель телекомунікаційної мережі дозволяє знайти оптимальний розподіл інформаційних потоків по каналах зв'язку. Особливістю цього методу є те, що замість незалежних змінних у цільовій функції між кожною парою джерело-приймач існують не всі види маршрутів трафіку, а фазові змінні, які в загальному випадку будуть менше маршрутів. Це зменшує розмірність цільової функції і, отже, прискорює пошук оптимального рішення. Початковими даними для вирішення задачі оптимізації трафіку мережі є топологія мережі провайдера з кількістю каналів N, матриця запитів між окремими мережами, потоки між мережами, зазвичай задаються у вигляді матриці запитів, що представляє собою матрицю розмірністю DxD, де елемент dij - показує інтенсивність потоку від i-ї мережі до j-ї мережі.

Аналізованими характеристиками є потоки трафіку та завантаження каналів зв'язку при обмеженнях на параметри якості обслуговування. Усі подальші обчислення виконуються в

середовищі MathCAD. Після побудови матриці шляхів (A) з кожної мережі в кожну формується S можливих шляхів з кожної мережі в кожну за всіма можливими шляхами. Для знаходження цільової функції необхідно знайти інтенсивності навантажень (L1) на кожному з каналів шляхом перемноження матриці шляхів (A) на матрицю всіх змінних (L), перед тим як обидві транспонувати. Матриця пропускних швидкостей (C) є аналогом інтенсивності обслуговування трафіку по каналах зв'язку. Тоді цільова функція набуде вигляду:

$$F = \sum_{n=0}^{N} \frac{\frac{L1_n}{C_n}}{1 - \frac{L1_n}{C_n}}$$

Початкові значення всіх S-змінних приймемо рівними нулю. За допомогою блоку Given-Find необхідно знайти початкові значення змінних для знаходження мінімуму цільової функції. Необхідно застосувати наступну систему обмежень:

- всі змінні повинні бути числами не від'ємними;
- інтенсивності навантажень на кожному каналі повинні бути строго менше їх пропускних здатностей;
- загальна кількість трафіку запитів з однієї мережі в іншу не повинна перевищувати значень матриці запитів.

Значення цільової функції F показує середню кількість пакетів, які перебувають на обслуговуванні. Після знаходження початкових точок для пошуку оптимізаційної задачі необхідно провести знову операцію пошуку, тільки замість блоку Given-Find використовувати Given-Minimize, в якості обмежень використовуємо ту ж саму систему. При порівнянні отриманих значень двох цільових функцій видно, що оптимізація пройшла успішно, оскільки значення цільової функції зменшилося, тобто зменшилася середня кількість пакетів в секунду на обслуговуванні [2].

Список використаних джерел

1. Andrew Tanenbaum, David Wetherall, Computer networks, global edition, Pearson; 6th edition, 2021
2. Su, Zicheng & Chow, Andy & Zhong, Renxin. (2021). Adaptive network traffic control with an integrated model-based and data-driven approach and a decentralised solution method. Transportation Research Part C Emerging Technologies. 128. 103154. 10.1016/j.trc.2021.103154.https://www.researchgate.net/publication/351770604_Adaptive_network_traffic_control_with_an_integrated_model-based_and_data-driven_approach_and_a_decentralised_solution_method

МЕТОДИКА МОНІТОРИНГУ МЕРЕЖ TCP/IP

Акуленко Оксана Олександрівна,
Довбенко Антон Володимирович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто мережі TCP/IP, які є основою сучасного Інтернету та корпоративних інформаційних систем. Для забезпечення надійності, ефективності та безпеки мережі, необхідно впроваджувати систему моніторингу, яка надає детальні відомості про стан та використання ресурсів. У цій статті розглянемо методику моніторингу мереж TCP/IP, спрямовану на виявлення проблем, вдосконалення продуктивності та забезпечення безпеки.

1. Використання систем моніторингу ресурсів

Одним із ключових елементів методики моніторингу є використання систем, які надають інформацію про ресурси мережі. Це може включати в себе моніторинг пропускної здатності, використання CPU та пам'яті, аналіз трафіку та інші характеристики.

2. Моніторинг Протоколів та Портів

Важливо відстежувати роботу протоколів та портів у мережі. Моніторинг дозволяє виявляти аномалії та неправильне використання ресурсів, а також слідкувати за діяльністю на конкретних портах для виявлення можливих загроз безпеці.

3. Виявлення аномалій та вторгнень

Використання систем виявлення аномалій і вторгнень (IDS/IPS) є важливою складовою моніторингу мереж. Це дозволяє вчасно виявляти незвичайну активність та потенційні загрози безпеці.

4. Моніторинг безпеки з'єднань

Враховуючи важливість безпеки в мережі TCP/IP, методика моніторингу повинна включати аналіз безпеки з'єднань. Це може включати виявлення незахищених з'єднань, моніторинг шифрування та перевірку легітимності комунікацій.

5. Логування та аналіз подій

Ведення журналів та аналіз подій допомагає відстежувати дії користувачів та події в мережі. Це не тільки допомагає виявляти проблеми, але й є важливим інструментом для дослідження подій у випадку інцидентів безпеки.

6. Моніторинг відмовостійкості

Важливо визначити рівень відмовостійкості мережі. Моніторинг може включати в себе тестування на відновлення після збоїв, аналіз роботи пристроїв в умовах високого трафіку та інші параметри, які впливають на доступність мережі.

7. Автоматизація та повідомлення

Ефективна методика моніторингу включає автоматизацію процесів та систему повідомлень. Автоматичні оповіщення про можливі проблеми або загрози дозволяють оперативно реагувати та усувати проблеми.

Методика моніторингу мереж TCP/IP визначається високою складністю та потребує системного підходу. Інтеграція систем моніторингу, аналізу та безпеки дозволяє ефективно управляти мережею, забезпечуючи надійність та безпеку її функціонування. Регулярне вдосконалення методики забезпечить адаптацію до змін у мережевому середовищі та вчасну реакцію на нові загрози та виклики.

ЛІТЕРАТУРА

1. Олифер В.Г., Олифер Н.А. Компьютерние сети. Принципи, технологии, протоколи. 2-е издание. – СПб.:Питер, 2005. – 864с.
2. Гольдштейн Б.С. Протоколи сети доступа.Том 2. - М.: Радио и связь, 1999. 314с.

БАГАТОШАРОВІ ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ

Захаржевська Аліна Анатоліївна,
Кравченко Олеся Сергіївна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто багатошарові телекомунікаційні мережі (БТМ), які стали важливою основою для забезпечення ефективного та надійного зв'язку в сучасному світі. Ці мережі використовують різні рівні та протоколи для передачі голосу, даних і відео, забезпечуючи високу пропускну здатність та низьку затримку. У цій статті ми розглянемо

ключові аспекти багатошарових телекомунікаційних мереж та їхній вплив на сучасне суспільство.

Структура багатошарових телекомунікаційних мереж

Багатошарові телекомунікаційні мережі складаються з різних рівнів (шарів), кожен з яких відповідає за певні функції. Основні шари включають:

- Фізичний шар: Відповідає за передачу бітів по фізичному середовищу, такому як мідь, оптоволокно чи радіохвилі.
- Канальний шар: Забезпечує надійний передачу даних між пристроями на одному фізичному каналі та виявлення та виправлення помилок.
- Мережевий шар: Відповідає за визначення маршрутів та керування потоками даних між різними мережевими вузлами.
- Транспортний шар: Забезпечує ефективну та надійну передачу даних від кінцевого пункту до кінцевого пункту, розбиваючи великі обсяги даних на менші пакети.
- Сеансовий шар: Управляє сесіями між пристроями та забезпечує надійний обмін даними.
- Представлення: Відповідає за перетворення даних так, щоб їх можна було правильно інтерпретувати і обробляти на кінцевому пристрої.
- Застосування: Визначає специфікації взаємодії між програмами та забезпечує обмін даними між пристроями в мережі.

Переваги багатошарових телекомунікаційних мереж

Ефективність та пропускна здатність: Розділення функцій на шари дозволяє ефективно використовувати ресурси мережі та підтримувати високу пропускну здатність.

Масштабованість: БТМ легко масштабується для включення нових пристроїв та розширення обсягу трафіку.

Надійність: розділення функцій допомагає уникнути однієї точки витоку та забезпечити надійну роботу мережі.

Гнучкість та адаптивність: шарова архітектура дозволяє впроваджувати нові технології та стандарти без необхідності зміни всієї мережевої інфраструктури.

Багатошарові телекомунікаційні мережі є важливим елементом інфраструктури для сучасного суспільства. Їхній успіх полягає у здатності забезпечувати ефективний зв'язок, надійність та безпеку в умовах постійної зміни технологій та вимог користувачів. БТМ продовжують розвиватися, впроваджуючи нові технології та стандарти, щоб відповідати викликам сучасності.

ЛІТЕРАТУРА

1. Електронні системи: навчальний посібник / Й. Й. Білинський, К. В. Огороднік, М. Й. Юкиш. — Вінниця: ВНТУ, 2011. — 208 с.

2. Математичні моделі та методи дослідження телекомунікаційних каналів: [монографія] / І. В. Горбатий. — Л. : Сполом, 2006. — 156 с. : іл. — Бібліогр.: с. 150—154 (53 назви). — ISBN 966-665-374-5

МЕТОДИКА СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ МІЖМІСЬКОЇ ТЕЛЕФОННОЇ МЕРЕЖІ

Личманюк Юлія Сергіївна,
Панченко Лілія Євгеніївна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто міжміські телефонні мережі, які в сучасному світі відіграють ключову роль у забезпеченні надійного та ефективного зв'язку між різними містами та регіонами. Створення та впровадження таких мереж вимагає досконалої методики, яка охоплює різні аспекти, починаючи від проектування та закінчуючи ефективним впровадженням та підтримкою. У цій статті розглянемо основні етапи та важливі аспекти методики створення та впровадження міжміської телефонної мережі.

Етап 1: аналіз та планування

1.1 Визначення потреб

Першим кроком є визначення потреб користувачів та бізнес-вимог, що визначатиме обсяг та характеристики міжміської телефонної мережі.

1.2. Аналіз існуючої інфраструктури

Оцінка існуючої телефонної та інформаційно-комунікаційної інфраструктури для визначення можливостей і обмежень.

1.3. Розробка технічного завдання

Створення технічного завдання, яке визначатиме технічні вимоги, обладнання та програмне забезпечення для міжміської телефонної мережі.

Етап 2: Проектування та архітектура

2.1. Вибір технологій

Вибір технологій, які найкраще відповідають вимогам та потребам міжміської телефонної мережі, таких як IP-телефонія, комутація чи використання волоконно-оптичного зв'язку.

2.2. Проектування мережевої топології

Розробка мережевої топології, яка включає в себе розташування обладнання, вибір маршрутів та забезпечення резервування для забезпечення високої доступності.

2.3. Вибір інфраструктурних постачальників

Вибір постачальників обладнання, програмного забезпечення та інших інфраструктурних компонентів.

Етап 3: Реалізація та впровадження

3.1. Розгортання обладнання та інфраструктури

Установка та конфігурування обладнання відповідно до проекту та технічного завдання.

3.2. Проведення тестувань

Виконання різних рівнів тестувань для перевірки працездатності та відповідності вимогам.

3.3. Навчання персоналу та підтримка

Навчання персоналу для роботи з новою системою та надання підтримки після впровадження.

Етап 4: Моніторинг та оптимізація

4.1. Моніторинг роботи мережі

Впровадження систем моніторингу для постійного відстеження працездатності та виявлення можливих проблем.

4.2. Оптимізація та розширення

Постійна оптимізація та розширення мережі відповідно до нових потреб та технологічних рішень.

Створення та впровадження міжміської телефонної мережі - це складний та відповідальний процес, який вимагає інтегрованого підходу. З ретельним плануванням, правильним вибором технологій та ефективним впровадженням, міжміська телефонна мережа може стати надійною та високоефективною інфраструктурою для сприяння зв'язку та розвитку бізнесу.

ЛІТЕРАТУРА

1. Єгунов М. М., Бежаєва Є. Б., Шерстнева О. Г. Проектування МТМ на базі SDH. Навчальний посібник. - Н .: СібГУТІ, 2002.

2.Бакланов І.Г., Технології виміру первинних мереж. Частина 1. Системи Е1, PDH, SDH .-2000.- 142 с.

СИСТЕМА АВТОМАТИЗОВАНОГО ПРОЕКТУВАННЯ LINKSIM

Солонець Нелля Андріївна,
Стеблянко Ілля Сергійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто системи автоматизованого проектування, які стають важливим інструментом для розробників та інженерів у сфері телекомунікацій. Однією з передових систем у цій області є LinkSim, що відзначається своєю здатністю до автоматизованого проектування та оптимізації мережевих з'єднань. У цій статті ми розглянемо основні аспекти та переваги системи автоматизованого проектування LinkSim..

LinkSim - це інноваційна система, яка надає інженерам та розробникам телекомунікаційних мереж зручний та ефективний інструмент для автоматизованого проектування та моделювання різних аспектів мережевого з'єднання. Заснована на передових технологіях, LinkSim пропонує високий рівень точності та гнучкість для вирішення різноманітних завдань.

Основні функції LinkSim:

1. Проектування та оптимізація мереж

LinkSim дозволяє інженерам автоматизовано проектувати та оптимізувати розгалужені телекомунікаційні мережі, забезпечуючи найкращу ефективність та використання ресурсів.

2. Моделювання параметрів каналів зв'язку

Система дозволяє встановлювати та моделювати різні параметри каналів зв'язку, включаючи пропускну здатність, затримку, шум та інші характеристики.

3. Аналіз пропускної здатності та джерел закупівлі

LinkSim надає засоби для ефективного аналізу пропускної здатності мережі та оптимізації джерел закупівлі, спрощуючи вибір обладнання та розміщення резервних джерел.

4. Симуляція різних сценаріїв

Інженери можуть проводити симуляції різних сценаріїв роботи мережі, досліджуючи її стійкість та продуктивність в різних умовах.

5. Автоматизація процесу впровадження змін

LinkSim пропонує автоматизований процес впровадження змін у мережі, що значно економить час та зменшує ймовірність помилок.

Переваги використання LinkSim:

1. Ефективність та точність

LinkSim дозволяє інженерам працювати швидше та точніше, спрощуючи та автоматизуючи ряд завдань, які раніше вимагали значних зусиль.

2. Гнучкість та адаптованість

Система адаптована до різних потреб і може використовуватися для розробки мереж різних масштабів та конфігурацій.

3. Економія часу та ресурсів

Автоматизовані функції LinkSim дозволяють значно зменшити час на планування та впровадження мережі, ефективно використовуючи ресурси.

4. Підтримка інновацій

LinkSim підтримує інновації у галузі телекомунікацій, дозволяючи інженерам швидко впроваджувати нові технології та покращення.

LinkSim представляє собою потужний інструмент для інженерів та розробників у сфері телекомунікацій, дозволяючи автоматизувати та оптимізувати процеси проектування та моделювання мереж. З врахуванням його ефективності, гнучкості та здатності підтримувати інновації, LinkSim стає невід'ємною частиною сучасного телекомунікаційного галузі, сприяючи розвитку швидких, ефективних та надійних мереж для сучасного світу.

ЛІТЕРАТУРА

1. Проектирование и техническая эксплуатация систем передачи: Учеб.пособие для вузов, под ред. В.Н. Гордиенко и В.В. Крухмалева. - М.: Радио и связь. - 2006. [64- 344с.]

ВПРОВАДЖЕННЯ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ WIMAX

Пелепей Максим Михайлович,
Топорков Євгеній Олександрович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто технологію WiMAX (Worldwide Interoperability for Microwave Access), яка представляє собою стандарт бездротового передавання даних, який відкриває нові перспективи для створення високошвидкісних та надійних мереж зв'язку. У цій статті ми розглянемо основні переваги та впровадження мереж на основі технології WiMAX.

1. Огляд технології WiMAX

WiMAX - це технологія бездротового зв'язку, яка дозволяє передавати дані на великі відстані з високою швидкістю та надійністю. Вона використовує радіохвилі у діапазоні мікрохвиль для створення бездротового з'єднання, що надає можливості аналогічні традиційним мережам DSL та кабельного з'єднання.

2. Переваги впровадження мереж WiMAX:

2.1. Висока швидкість передачі даних

Однією з ключових переваг технології WiMAX є висока швидкість передачі даних. Мережі на основі WiMAX можуть забезпечити швидкості, схожі з кабельним і DSL-з'єднаннями, що робить їх ідеальними для високопропускних застосувань, таких як стрімінг відео та онлайн-ігри.

2.2. Широкий діапазон покриття

Технологія WiMAX може забезпечувати широкий діапазон покриття, що робить її ефективною для впровадження в міських та сільських областях. Це дозволяє забезпечити доступ до високошвидкісного Інтернету там, де провідні мережі можуть бути неефективними чи недоступними.

2.3. Гнучкість та легкість впровадження

Мережі WiMAX відзначаються гнучкістю та легкістю впровадження. Вони можуть бути розгорнуті швидко, а апаратне забезпечення може бути встановлено з мінімальними труднощами, що дозволяє швидко забезпечити доступ до бездротового зв'язку в нових областях.

2.4. Надійність та стабільність

WiMAX володіє високою надійністю та стабільністю з'єднання, що робить його ідеальним вибором для підприємств та житлових комплексів. Можливість обслуговування багатьох користувачів одночасно без втрати якості з'єднання є важливим фактором.

2.5. Можливість використання в рухомих об'єктах

WiMAX може бути використаний для побудови мереж для рухомих об'єктів, таких як транспортні засоби або поїзди, забезпечуючи швидкий та стабільний доступ до Інтернету для пасажирів.

3. Використання технології WiMAX у різних галузях:

3.1. Телекомунікації

WiMAX використовується в телекомунікаційних мережах для забезпечення високошвидкісного доступу до Інтернету та передачі даних.

3.2. Підприємства та офіси

Мережі WiMAX можуть бути впроваджені в підприємства та офіси, забезпечуючи надійний та швидкий Інтернет для робочих потреб.

3.3. Розважальна промисловість

WiMAX може слугувати основою для бездротового доступу до розважальних послуг, таких як стрімінг відео, музика та ігри.

Впровадження мереж на основі технології WiMAX відкриває нові можливості для ефективного та високошвидкісного бездротового зв'язку. Її переваги включають високу швидкість передачі даних, широкий діапазон покриття, гнучкість впровадження та надійність. Технологія WiMAX може бути використана в різних галузях, що дозволяє забезпечити ефективний та доступний зв'язок для користувачів у будь-якому місці та часі.

ЛІТЕРАТУРА

1. Sassan Ahmadi An overview of nextgeneration mobile WiMAX technology // IEEE Commun. Mag, vol. 47, no. 6, pages 84-98, June 2009. 11. WiMAX Forum, WiMAX Forum Mobile System Profile. V1.2.0, Sept. 2006.

2.So-In C., Jain R., Tamimi A.-K. Capacity Evaluation for IEEE 802.16e Mobile WiMAX // Journal of Computer Systems, Networks, and Communications. – 2010. – P. 1-12.

МЕТОДИКА ПОБУДОВИ ТА ВПРОВАДЖЕННЯ БАГАТОКАНАЛЬНОЇ СИСТЕМИ ПЕРЕДАЧІ НА ПІДСТАВІ PDH ТА SDH

Аварі Алісіно Залмайович,
Антіпін Андрій Олексійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто багатоканальні системи передачі даних на основі PDH (Plesiochronous Digital Hierarchy) та SDH (Synchronous Digital Hierarchy), які є ключовими компонентами сучасних телекомунікаційних інфраструктур. Ці технології дозволяють ефективно передавати великі обсяги даних на великі відстані з високою швидкістю та

надійністю. У цій статті розглянемо методику побудови та впровадження багатоканальної системи передачі на підставі PDH та SDH.

1. Огляд PDH та SDH

PDH та SDH є ієрархічними структурами для організації та передачі цифрових сигналів. PDH використовує плесіохронічний підхід, де різні канали мають невеликі різниці в часі, тоді як SDH працює на синхронних циклах, забезпечуючи точний та синхронізований обмін даними.

2. Етапи побудови та впровадження багатоканальної системи передачі:

2.1. Проектування Системи

Перший етап - це ретельне проектування системи. Визначення обсягу передачі даних, вибір типу системи (PDH або SDH), визначення вимог до пропускної здатності та надійності є ключовими аспектами.

2.2. Вибір обладнання та технологій

Вибір відповідного обладнання та технологій визначається вимогами проекту. Враховуючи розмір системи, може бути обрано обладнання PDH або SDH, а також вибрані відповідні канали передачі.

2.3. Розгортання інфраструктури

Після вибору технологій і обладнання розпочинається розгортання інфраструктури. Це включає встановлення кабельних систем, встановлення обладнання на станціях та облаштування вузлів з'єднання.

2.4. Конфігурація та тестування

Після розгортання системи проводиться конфігурація обладнання та проводяться тестування для перевірки правильності підключення, надійності та швидкості передачі даних.

2.5. Налаштування та оптимізація

Останнім етапом є налаштування та оптимізація системи. В цьому процесі може використовуватися моніторинг для пошуку і усунення можливих проблем, а також для оптимізації пропускної здатності та ефективності.

3. Переваги використання PDH та SDH для багатоканальних систем:

3.1. Висока Пропускна Здатність

PDH та SDH дозволяють передавати великі обсяги даних з високою швидкістю, що робить їх ідеальними для багатоканальних систем.

3.2. Надійність та стабільність

Системи на основі PDH та SDH володіють високою надійністю та стабільністю з'єднання, що забезпечує безперебійну передачу даних.

3.3. Гнучкість та розширюваність

PDH та SDH є гнучкими системами, які легко розширюються та адаптуються до зростання обсягів передачі даних.

3.4. Легкість управління та обслуговування

Ці технології дозволяють легко керувати та обслуговувати багатоканальні системи, використовуючи моніторинг та діагностичні засоби.

Багатоканальні системи передачі на підставі PDH та SDH стали невід'ємною частиною сучасних телекомунікаційних мереж. Впровадження цих технологій вимагає ретельного планування, вибору обладнання та правильної конфігурації. Завдяки їхнім перевагам у високій пропускній здатності, надійності та гнучкості, системи PDH та SDH є ефективними рішеннями для багатоканальної передачі даних у великих телекомунікаційних мережах.

ЛІТЕРАТУРА

1. Букрина Е. В. Сети связи и системы коммутации: Учебное пособие. - Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2007. - 186 с

2.Б.Ю. Жураковський, І.О. Зенів КОМП'ЮТЕРНІ МЕРЕЖІ ЧАСТИНА 2 НАВЧАЛЬНИЙ ПОСІБНИК. Електронний ресурс. Режим доступу: https://ela.kpi.ua/bitstream/123456789/36641/1/Zhurakovskyi_Zeniv_Kompiuterni_merezhi_Ch2.pdf

МЕТОДИКА ПОБУДОВИ МЕРЕЖ IP-ТЕЛЕФОНІЇ НА ОСНОВІ ПРОТОКОЛУ SIGTRAN

Журович Олександр Олександрович,
Зевєлєв Марк Андрійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто протокол SIGTRAN (Signaling Transport), який є ключовим компонентом для забезпечення ефективного обміну сигналізаційними даними в мережах IP-телефонії. У цій статті ми розглянемо методику побудови мереж IP-телефонії, використовуючи протокол SIGTRAN.

1. Огляд протоколу SIGTRAN:

SIGTRAN - це сімейство протоколів, призначених для транспортування сигналізаційних повідомлень у IP-мережах. Він використовує TCP/IP-протоколи для ефективного та надійного обміну сигналізаційними даними, такими як SS7 (Signaling System 7) у традиційних телефонних мережах.

2. Етапи побудови мережі IP-телефонії з використанням SIGTRAN:

2.1. Аналіз вимог та вибір архітектури:

Перший етап - це ретельний аналіз вимог до мережі IP-телефонії. Визначення кількості користувачів, обсягу трафіку та потреб у безпеці є важливими кроками. Вибір архітектури мережі визначить, як буде організовано обробку сигналізаційних даних.

2.2. Вибір компонентів та протоколів:

На основі визначених вимог обираються компоненти та протоколи. У випадку IP-телефонії з використанням SIGTRAN, вибирається необхідне обладнання та програмне забезпечення, підтримуюче протокол SIGTRAN.

2.3. Налаштування серверів та інфраструктури:

Після вибору компонентів проводиться налаштування серверів та інфраструктури мережі. Це включає встановлення та налаштування сигналізаційних серверів, IP-шлюзів та іншого обладнання.

2.4. Конфігурація SIGTRAN:

SIGTRAN визначає стек протоколів для транспортування сигналізаційних даних. На цьому етапі проводиться конфігурація SIGTRAN для забезпечення правильного обміну даними між серверами.

2.5. Забезпечення безпеки:

Безпека є важливим аспектом будь-якої мережі, тим більше у випадку IP-телефонії. Встановлення заходів безпеки, таких як шифрування трафіку та захист від атак, є обов'язковим.

3. Переваги використання SIGTRAN для IP-телефонії:

3.1. Ефективний Транспорт Сигналізаційних Даних:

SIGTRAN забезпечує ефективний транспорт сигналізаційних даних, використовуючи TCP/IP, що робить його ідеальним для мереж IP-телефонії.

3.2. Масштабованість та гнучкість:

Мережі IP-телефонії на основі SIGTRAN легко масштабовані та гнучкі, що дозволяє їм адаптуватися до зростання обсягу трафіку та кількості користувачів.

3.3. Сумісність із сучасними технологіями:

SIGTRAN ідеально поєднується з іншими сучасними технологіями, такими як VoIP (Voice over IP), що дозволяє створювати комплексні та ефективні рішення.

3.4. Надійність та висока пропускна здатність:

Цей протокол гарантує надійність та високу пропускну здатність для передачі сигналізаційних повідомлень, важливих для встановлення та управління дзвінками.

Методика побудови мереж IP-телефонії на основі протоколу SIGTRAN вимагає комплексного підходу та виважених вирішень. З використанням цього протоколу можна створити ефективну та надійну інфраструктуру для передачі сигналізаційних даних у мережах IP-телефонії, що відповідає вимогам сучасного світу зв'язку.

ЛІТЕРАТУРА

1. Гольдштейн Б . С. , Пінчук О.В., Суховицький О.Л. IP-телефонія. - М: Радіо і зв'язок, 2001. - 336с.

2.Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи. 2-ге видання. - СПб.: Пітер, 2005. - 864с.

МЕТОДИКА ПОБУДОВИ ТА ВПРОВАДЖЕННЯ ВОСП З ХВИЛЬОВИМ МУЛЬТИПЛЕКСУВАННЯМ

Павлов Владислав Анатолійович,
Оніщук Ольга Петрівна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто віртуальні оптичні системи передачі (ВОСП) з хвильовим мультиплексуванням, які відіграють важливу роль у сучасних телекомунікаційних мережах, забезпечуючи велику пропускну здатність та ефективний обмін даними. У цій статті розглянемо методику побудови та впровадження ВОСП з хвильовим мультиплексуванням.

1. Огляд віртуальних оптичних систем передачі (ВОСП):

ВОСП є передовою технологією в області оптичних мереж, де використовується віртуалізація та хвильове мультиплексування для передачі великої кількості каналів даних по одному оптичному волокну. Ця технологія дозволяє підвищити пропускну здатність та зменшити витрати на інфраструктуру.

2. Етапи побудови та впровадження ВОСП:

2.1. Аналіз вимог та потреб:

Перший етап - це ретельний аналіз вимог та потреб мережі. Визначення потрібної пропускної здатності, покриття та інших параметрів.

2.2. Вибір технологічних рішень:

Вибір технологічних рішень включає в себе вибір обладнання, що підтримує ВОСП, а також визначення конфігурації мережі та параметрів мультиплексування.

2.3. Проектування хвильового мультиплексування:

Для ефективного використання оптичного волокна проводиться проектування хвильового мультиплексування, визначаючи частотні діапазони для кожного каналу та встановлюючи параметри передачі.

2.4. Встановлення та налаштування обладнання:

На цьому етапі встановлюється та налаштовується спеціалізоване обладнання для ВОСП, таке як оптичні хаби, трансмітери та приймачі, а також управління віртуалізацією.

2.5. Розгортання мережі:

Після встановлення обладнання проводиться розгортання ВОСП-мережі. Важливо врахувати фізичні аспекти, такі як розташування волокон та точок з'єднання.

2.6. Налаштування безпеки та моніторингу:

Забезпечення безпеки мережі включає в себе налаштування заходів шифрування та доступу, а також систем моніторингу для виявлення та вирішення можливих проблем.

2.7. Тестування та оптимізація:

Перед введенням в експлуатацію мережу слід протестувати для перевірки працездатності та надійності. Після введення в експлуатацію проводиться оптимізація параметрів для максимізації ефективності.

3. Переваги ВОСП з хвильовим мультиплексуванням:

3.1. Велика пропускна здатність:

Використання хвильового мультиплексування дозволяє передавати велику кількість каналів даних одночасно, забезпечуючи високу пропускну здатність.

3.2. Ефективне використання ресурсів:

ВОСП дозволяє ефективно використовувати оптичне волокно, розділяючи його на різні хвилі та канали для оптимізації пропускної здатності.

3.3. Гнучкість та швидкість розгортання:

ВОСП дозволяє швидко розгортати нові канали та мережі, забезпечуючи гнучкість у відповіді на зростання обсягу даних.

3.4. Енергоефективність:

Зменшення фізичного обладнання завдяки віртуалізації призводить до енергоефективності мережі.

Методика побудови та впровадження ВОСП з хвильовим мультиплексуванням є ключовою для створення сучасних телекомунікаційних інфраструктур. З використанням цієї технології можна досягти високої продуктивності та ефективності передачі даних в оптичних мережах, що є особливо важливим у сучасному світі постійного зростання обсягу інформації.

ЛІТЕРАТУРА

1. Каток В. Б., Руденко І.Е., Ранський Є. Г., Однорог П.М. Волоконно оптичний зв’язок / Під ред. Катка В.Б. – К.: Логос, 2015. – 383 с.
2. Хмелёв К. Ф. Основы фотонного транспорта. Київ, Техніка, 2008. - 680 с.

РОЗРОБКА МЕТОДИКИ ПОЄДНАННЯ ДВОХ РІЗНИХ ПІДМЕРЕЖ В ОДНУ КОРПОРАТИВНУ МЕРЕЖУ

Паршина Оксана Іванівна,
Паршин Микола Володимирович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто корпоративні мережі, які стають все більш складними, особливо коли компанія росте або має розсіяні офіси. Поєднання двох різних підмереж в єдину корпоративну мережу вимагає ретельного планування та розробки методики для забезпечення ефективності, безпеки та доступності. У цій статті ми розглянемо ключові етапи розробки методики поєднання двох різних підмереж в одну корпоративну мережу.

1. Аналіз типів підмереж:

Першим кроком є аналіз типів підмереж, які слід поєднати. Це може бути з'єднання офісів різних локацій, підключення віддалених філій чи інші сценарії. Важливо визначити вимоги до пропускної здатності, безпеки та сервісів для кожної підмережі.

2. Вибір технологій поєднання:

На основі аналізу визначаються технології, які будуть використані для поєднання підмереж. Це може бути використання VPN (віртуальних приватних мереж), MPLS (многорівневого протоколу комутації пакетів), апаратного з'єднання чи інших методів.

3. Налаштування маршрутизації та перекриття IP-Адрес:

Важливим етапом є налаштування маршрутизації між підмережами та вирішення конфліктів IP-адрес. Використання технологій, таких як Network Address Translation (NAT), може допомогти уникнути конфліктів.

4. Забезпечення безпеки:

Безпека є ключовим аспектом при поєднанні різних підмереж. Використання шифрування та встановлення брандмауерів для захисту від несанкціонованого доступу є необхідними заходами.

5. Впровадження QoS (Quality of Service):

Для забезпечення якісного обслуговування різних типів трафіку важливо впровадити QoS. Це дозволяє пріоритезувати та керувати пропускною здатністю для важливих додатків та послуг.

6. Резервне забезпечення та відновлення:

Враховуючи важливість неперервної роботи корпоративної мережі, слід розглядати можливості резервного забезпечення та відновлення після збоїв для забезпечення високої доступності.

7. Моніторинг та логування:

Наставництво та логування мережевої діяльності є важливим етапом для виявлення проблем, моніторингу пропускної здатності та відслідковування подій в корпоративній мережі.

8. Тестування та оцінка продуктивності:

Перед впровадженням методики важливо провести тестування, щоб переконатися у її ефективності та безпекові. Оцінка продуктивності допомагає виявити можливі недоліки та вдосконалити методику.

9. Документація та навчання персоналу:

Після успішного впровадження важливо створити документацію, яка описує методику, конфігурації та правила експлуатації. Крім того, персонал повинен отримати навчання щодо нових можливостей та відповідальностей.

Поєднання двох різних підмереж в одну корпоративну мережу — це важливий етап для оптимізації інфраструктури компанії та забезпечення її ефективної роботи. Розробка та впровадження методики дозволить забезпечити стабільність, безпеку та високу доступність корпоративної мережі в умовах зростання бізнесу.

ЛІТЕРАТУРА

1. Пайпер Б. «Адміністрування мереж Cisco: освоєння за місяць» / пер. з анг. М. А. Райтмана. – М.: ДМК Пресс, 2018. – 316 с.

2.Азаров О. Д. Комп’ютерні мережі: навчальний посібник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук. – Вінниця : Вінницький Національний Технічний Університет, 2013. – 371 с.

РОЗРОБКА МЕТОДИКИ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ ДЛЯ ПІДПРИЄМСТВА “ЕДЕДЖЕНСІ

Полтко Денис Романович,
Старченко Ігор Володимирович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто створення ефективної корпоративної мережі, що є ключовим завданням для сучасних підприємств, оскільки вона визначає стабільність комунікації та обміну даними в організації. У цій статті розглянемо методику розробки корпоративної мережі для підприємства "ЕДЕДЖЕНСІ".

1. Аналіз вимог та потреб бізнесу:

Перший етап розробки методики - це ретельний аналіз вимог та потреб бізнесу "ЕДЕДЖЕНСІ". Визначення обсягу даних, кількості працівників, вимог до безпеки та доступності є важливим для подальшого планування мережі.

2. Проектування інфраструктури мережі:

На основі аналізу визначається архітектура мережі. Це включає в себе розташування серверів, комутаторів, маршрутизаторів, систем безпеки та інших пристроїв.

3. Вибір технологій та обладнання:

Важливим етапом є вибір технологій та обладнання для мережі. Враховуючи потреби "ЕДЕДЖЕНСІ", може бути використане сучасне обладнання, таке як швидкі комутатори, високопродуктивні сервери та системи безпеки.

4. Розгортання інфраструктури:

На цьому етапі здійснюється фізичне та логічне розгортання інфраструктури мережі. Кабелювання, підключення пристроїв, налаштування комутаторів та розгортання серверів здійснюються відповідно до попередньої архітектури.

5. Налаштування систем безпеки:

Забезпечення безпеки мережі - це пріоритет. Встановлення брандмауерів, систем виявлення вторгнень та шифрування даних допомагає захистити корпоративну інформацію "ЕДЕДЖЕНСІ" від несанкціонованого доступу.

6. Налаштування систем моніторингу та адміністрування:

Створення системи моніторингу для відстеження стану мережі та налагодження систем адміністрування для керування конфігурацією та підтримки мережі.

7. Впровадження систем запуску та резервного забезпечення:

Запуск систем та резервне забезпечення є критичним для підтримки стійкої роботи бізнес-процесів "ЕДЕДЖЕНСІ". Розгортання резервних серверів, створення регулярних резервних копій та відновлення в разі відмов - важливі завдання.

8. Тестування та оцінка продуктивності:

Проведення тестування для перевірки пропускної здатності, стійкості та безпеки мережі. Оцінка продуктивності допомагає виявити можливі покращення та оптимізації.

9. Документація та навчання персоналу:

Створення докладної документації про конфігурацію та управління мережею, а також навчання персоналу для ефективного використання нової інфраструктури.

Розробка методики побудови корпоративної мережі для підприємства "ЕДЕДЖЕНСІ" вимагає цілеспрямованості, експертності та залучення висококваліфікованих спеціалістів. З дотриманням вищезазначених етапів можна створити мережу, що відповідає усім вимогам та гарантує ефективність бізнес-процесів підприємства.

ЛІТЕРАТУРА

1. Абрамов В.О. Клименко С.Ю. Базові технології комп’ютерних мереж.2014. -49с

2. Берлин А. Н. Абонентские сети доступа и технологии высокоскоростных сетей, 2016. – 277 с.

МЕТОДИКА ДОСЛІДЖЕННЯ ЕНЕРГЕТИЧНИХ ПАРАМЕТРІВ СИСТЕМИ СУПУТНИКОВОГО ЗВ'ЯЗКУ ТА МЕТОДІВ ЇХ ПОКРАЩЕННЯ

Якимчук Юрій Олексійович,
Казенко Георгій Олексійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

Супутникові системи зв'язку відіграють ключову роль у сучасному світі, забезпечуючи глобальну комунікацію та низьку латентність для різних сфер життя. Однак забезпечення ефективної роботи супутникових систем вимагає уваги до енергетичних параметрів. У цій статті розглянемо методику дослідження енергетичних параметрів системи супутникового зв'язку та шляхи їх покращення.

1. Аналіз вихідних даних та енергетичних витрат:

Перший етап методики - це збір та аналіз вихідних даних щодо енергетичних витрат супутникової системи. Це включає в себе споживання енергії при передачі та отриманні сигналів, роботу обладнання та енергозберігаючі методи.

2. Оцінка робочих характеристик супутникового обладнання:

Оцінка робочих характеристик обладнання, такого як приймально-передавальні апарати, антени та комутаційні системи, дозволяє визначити їхній внесок у загальні енергетичні витрати системи.

3. Впровадження енергоефективних технологій:

Використання енергоефективних технологій є важливим аспектом покращення енергетичних параметрів. Розробка та впровадження енергозберігаючого обладнання, оптимізація роботи алгоритмів та використання сучасних енергозберігаючих чіпів - ключові аспекти цього етапу.

4. Вдосконалення процесів керування енергією:

Розробка ефективних систем керування енергією дозволяє адаптувати споживання енергії відповідно до активності системи. Це може включати в себе динамічне вимкнення частин обладнання під час періодів неактивності або використання систем автоматичного регулювання.

5. Використання сонячних елементів та акумуляторів:

Ще одним способом покращення енергетичних параметрів є використання сонячних елементів та акумуляторів. Застосування сонячних панелей для зарядки акумуляторів може забезпечити додатковий джерело енергії та зменшити залежність від інших джерел.

6. Розробка програмного забезпечення для моніторингу енергоспоживання:

Створення програмного забезпечення для моніторингу енергоспоживання дозволяє системі автоматично адаптуватися до змін у робочих умовах, оптимізувати енергозбереження та виявляти можливі несправності.

7. Проведення симуляцій та тестувань:

Перед впровадженням розроблених методів покращення, важливо провести симуляції та тестування в контрольованих умовах. Це дозволяє визначити ефективність нових рішень та виявити можливі недоліки.

8. Оптимізація архітектури системи:

Архітектурна оптимізація системи може сприяти покращенню енергетичних параметрів. Розробка оптимальних конфігурацій та зменшення кількості перетоків даних може значно скоротити енергетичні витрати.

9. Постійне вдосконалення та моніторинг:

Постійне вдосконалення є ключем до успіху в покращенні енергетичних параметрів. Використання знань, отриманих під час експлуатації, для постійного вдосконалення методів та технологій.

10. Співпраця з виробниками та НДДС:

Співпраця з виробниками обладнання та науково-дослідними установами може прискорити процес впровадження нових технологій та методів покращення енергетичних параметрів.

Методика дослідження та покращення енергетичних параметрів систем супутникового зв'язку вимагає комплексного підходу та використання різноманітних технологій. З регулярним вдосконаленням та співпрацею з індустрією можна досягти значного покращення продуктивності та стійкості супутникових систем при зменшенні енергетичних витрат.

ЛІТЕРАТУРА

1. Гнатушенко, В.В. Системи супутникового та стільникового зв’язку [Текст]: навч. посіб. / В.В. Гнатушенко, О.О. Дробахін, В.М. Корчинський. – Д.: РВВ ДНУ, 2012. – 80 с.

2.ОНАЗ-ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ’ЯЗКУ, «Розрахунок та аналіз супутникового каналу зв'язку», М.Б. Проценко, І.Ю. Рожновська.

МЕТОДИКА ПОБУДОВИ ТА ВПРОВАДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ ОФІСНИХ ПРИМІЩЕНЬ ПРАТ “ДАТА ГРУП”

Гоначарова Юлія Петрівна,
Іваніченко Світлана Іванівна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

В сучасному бізнес-середовищі ефективна телекомунікаційна мережа є важливою складовою для успішного функціонування підприємства. У цій статті розглянемо методику побудови та впровадження телекомунікаційної мережі для офісних приміщень ПрАТ “Дата груп”.

1. Аналіз Вимог та Потреб Підприємства

Перший крок - це ретельний аналіз вимог і потреб підприємства. Визначення кількості працівників, їхніх потреб у швидкості та стабільності з'єднання, а також видів послуг, які будуть використовуватися в телекомунікаційній мережі.

2. Розробка Технічного Проекту

На основі отриманих вимог розробляється технічний проект мережі. Це включає в себе вибір обладнання, планування інфраструктури, розташування точок доступу, створення плану нумерації IP-адрес та інші технічні аспекти.

3. Вибір Технологій та Обладнання

Вибір технологій, які відповідають потребам підприємства, грає важливу роль. Включення сучасних технологій, таких як Wi-Fi 6, VoIP, безпровідні точки доступу, сприяє створенню ефективної та масштабованої інфраструктури.

4. Прокладання Кабельної Інфраструктури

Етап прокладання кабельної інфраструктури включає в себе правильний вибір типу кабелю (волокно, мідь), його прокладання та забезпечення необхідних зон для подальшого розширення.

5. Конфігурація та Тестування Мережі

Після встановлення обладнання важливо правильно сконфігурувати мережу та провести тестування для визначення швидкості передачі даних, якості зв'язку та виявлення можливих неполадок.

6. Впровадження та Навчання Персоналу

Після успішного тестування мережу вводять в експлуатацію, а персонал навчається використовувати нову інфраструктуру.

7. Підтримка та Моніторинг

Останнім етапом є налагодження системи моніторингу для постійного відстеження стану мережі та підтримка для вирішення будь-яких потенційних проблем.

Методика побудови та впровадження телекомунікаційної мережі для офісних приміщень ПрАТ "Дата груп" - це комплексний підхід, що враховує технічні, організаційні та експлуатаційні аспекти. Справно побудована та належно налаштована мережа дозволяє підприємству ефективно використовувати сучасні технології та забезпечити надійну та швидку комунікацію.

ЛІТЕРАТУРА

1.Царьов Р.Ю. Структуровані кабельні системи: навч. посіб. для студентів вищих навчальних закладів. / Царьов Р.Ю., Нікітюк Л. А., Резніченко П. І. – Одеса: ОНАЗ ім. О.С. Попова, 2012. – 260 с.: іл.

2.Крилов В.М. Структуровані кабельні системи:навч. посіб.по вивч.дисц. / Крилов В.М. – Київ:ДУТ, 2015. - 112 с.

РОЗРОБКА МЕТОДИКИ СТВОРЕННЯ МЕРЕЖ П'ЯТОГО ПОКОЛІННЯ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

Ковальов Олександр Євгенович,
Римар Дмитрій Борисович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

Запровадження технологій п'ятого покоління (5G) вимагає не лише розширення пропускної здатності та зменшення латентності, але і використання нових підходів до архітектури мережі. У цій статті ми розглянемо методику розробки мереж п'ятого покоління з використанням програмно-конфігурованих мереж (SDN).

1. Розуміння Вимог 5G:

Перший етап - ретельне розуміння вимог 5G, таких як висока пропускна здатність, зменшення латентності, підтримка масового підключення пристроїв та енергоефективність.

2. Вибір Архітектури SDN:

Обираючи SDN, важливо визначити тип архітектури, що найкраще відповідає вимогам 5G. Це може бути централізована архітектура, де логіка прийняття рішень знаходиться в центральному контролері, або розподілена, коли контроль здійснюється на кожному вузлі.

3. Визначення Мережевих Служб та Функцій:

Визначення служб та функцій, які мережа має надавати, є ключовим етапом. Це включає в себе розподілене введення/виведення, віртуалізацію функцій та інші аспекти, що підтримують основні вимоги 5G.

4. Створення Віртуальних Мережевих Функцій (VNF):

Використання технологій віртуалізації для створення VNF дозволяє динамічно розгортати та управляти функціями мережі в реальному часі.

5. Забезпечення Безпеки:

Врахування аспектів безпеки на всіх рівнях мережі є важливим завданням. Використання шифрування, ідентифікації та аутентифікації допомагає забезпечити конфіденційність та доступність мережевих служб.

6. Впровадження Технологій Network Slicing:

Network slicing дозволяє створювати віртуальні мережі для конкретних вимог, забезпечуючи ізольовані ресурси та функціональність для кожного типу послуг.

7. Розгортання Fog Computing та Edge Computing:

Використання Fog та Edge Computing допомагає зменшити латентність та забезпечити обробку даних ближче до кінцевих користувачів, що є важливим для реалізації послуг інтернету речей (IoT) та інших високопродуктивних додатків.

8. Управління Трафіком та Ресурсами:

Розробка ефективних алгоритмів управління трафіком та ресурсами дозволяє оптимізувати використання мережевих ресурсів та забезпечити стабільну роботу системи при змінних умовах.

9. Автоматизація та Оркестрація:

Використання автоматизації та оркестрації допомагає управляти та масштабувати великі мережеві сервіси, забезпечуючи швидкість та ефективність.

10. Тестування та Оптимізація:

Перед впровадженням важливо провести тестування системи в реальних умовах та оптимізувати параметри для досягнення оптимальної продуктивності.

Розробка мереж п'ятого покоління з використанням програмно-конфігурованих мереж є складним завданням, що вимагає глибокого розуміння технологій 5G та ефективного використання SDN. Із застосуванням цих методів можна створити високоефективні та гнучкі мережі, які відповідають високим стандартам швидкодії та якості обслуговування.

ЛІТЕРАТУРА

1. Берлин А.Н. Телекоммуникационные сети и устройства: Учебное пособие / А.Н. Берлин — М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. — 319 с.

2.Гимадинов, Р.Ф. Кластеризация в мобильных сетях 5G. Случай частичной мобильности / Гимадинов, Р.Ф., Мутханна, А.С., Кучерявый, А.Е. // Информационные технологии и телекоммуникации. 2015. Т. 3. № 2. С. 44-52.

МЕТОДИКА ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМ РАДІОЗВ'ЯЗКУ, ЩО ВИКОРИСТОВУЮТЬ ТЕХНОЛОГІЮ MIMO

Марчук Ольга Миколаївна,
Треньова Катерина Олександрівна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянута методика підвищення завадостійкості систем радіозв'язку, які використовують технологію MIMO. MIMO (Multiple Input, Multiple Output), технологія стала ключовим елементом розвитку бездротових комунікацій. Використання MIMO дозволяє передавати та отримувати більше одного сигналу через різні антени, що призводить до підвищення пропускної здатності та ефективності систем радіозв'язку. Однак, для максимізації ефективності, необхідно також приділити увагу завадостійкості системи.

Аналіз імпульсного шуму та завад в каналі:

Перед розгортанням системи MIMO важливо ретельно проаналізувати характеристики імпульсного шуму та потенційних завад в каналі. Це визначає параметри системи, такі як кількість антен, розташування та напрямок їхньої дії.

Використання алгоритмів спільного виявлення та декодування:

Алгоритми спільного виявлення та декодування дозволяють ефективно впоратися із завадами та інтерференцією в системах MIMO. Їхнє використання може покращити точність розпізнавання сигналів та знизити ймовірність помилок.

Просторова фільтрація для мінімізації міжантенної завади:

Використання просторової фільтрації дозволяє мінімізувати вплив міжантенної завади. Розташування та налаштування антен враховується для зменшення перехрещування та інтерференції між антенами.

Адаптивне управління антенами:

Адаптивне управління антенами - це ключовий компонент для максимізації завадостійкості. Система повинна бути здатною динамічно змінювати параметри антен відповідно до умов каналу для мінімізації впливу завад.

Використання технології Beamforming:

Beamforming є технікою, яка спрямовує сигнал у конкретному напрямку, підсилюючи його та зменшуючи вплив завад. Застосування beamforming може значно поліпшити якість зв'язку в умовах завад.

Апаратне впровадження методів скасування міжантенної завади:

Апаратне впровадження методів скасування міжантенної завади дозволяє видалити або значно зменшити вплив небажаних сигналів, що дістаються до антени.

Використання технологій Space-Time Coding:

Space-Time Coding є методом, що дозволяє передавати інформацію через різні антени та часові інтервали. Це допомагає забезпечити стійкість до завад та помилок.

Тестування та моделювання завад в реальних умовах:

Перед реальним розгортанням системи важливо виконати тестування та моделювання в реальних умовах, що дозволить оцінити реальну завадостійкість системи.

Системи автоматичного виявлення та корекції помилок:

Використання систем автоматичного виявлення та корекції помилок дозволяє системі ефективно виявляти та виправляти помилки, що виникають внаслідок завад чи інтерференції.

Співпраця з іншими технологіями:

Забезпечення завадостійкості системи MIMO може бути покращено співпрацею з іншими технологіями, такими як канал зв'язку, впровадження технологій управління ресурсами, та інші.

Методика підвищення завадостійкості систем радіозв'язку з використанням технології MIMO є складним завданням, що вимагає глибокого розуміння характеристик каналу та ефективного використання передових методів обробки сигналів. З правильним підходом та використанням відповідних методів, можливо досягти високої завадостійкості та ефективності систем MIMO в різноманітних умовах роботи.

ЛІТЕРАТУРА

1. Огляд технології MIMO і порівняння швидкості [Електронний документ] - Режим доступу: https://usb-modem.com.ua/ua/blog/ua-testiruem-antenny-mimo-2x2-pri-slabom-signale/

2. MIMO-технологія (Multiple Input Multiple Output) — метод просторового кодування сигналу [Електронний документ] - Режим доступу: http://hi-news.pp.ua/kompyuteri/8996-mimo-tehnologya-multiple-input-multiple-output-metod-prostorovogo-koduvannya-signalu.html

СЕКЦІЯ 2

Інформаційні системи та технології

ЗАСТОСУВАННЯ IoT У ВИРОБНИЦТВІ ДЛЯ ЕФЕКТИВНОГО УПРАВЛІННЯ ЛАНЦЮГОМ ПОСТАЧАННЯ

Бурик Ігор Сергійович
Державний університет інформаційно-комунікаційних технологій
Науковий керівник: Срібна І.М.,
професор кафедри Інженерії програмного забезпечення автоматизованих систем Державного університету інформаційно-комунікаційних технологій,
м. Київ

Дослідження зосереджую на аналізі та вдосконаленні методів захисту інформації в мережах Інтернету речей (IoT). Особливу увагу приділяю застосуванню TLS/SSL у MQTT та використанню OpenSSL

Постановка задачі

Розглядається стрімкий розвиток IoT та виклики, пов'язані з забезпеченням безпеки. Автори вказують на значення захисту даних у сучасних IoT системах, звертаючи увагу на потенційні загрози.

Мета дослідження

Визначається мета аналізу ефективних методів захисту даних в IoT. Завдання охоплює ідентифікацію ключових проблем у безпеці IoT та розробку рішень для їх подолання.

Результати дослідження

Проводився детальний аналіз різних методів захисту, включаючи шифрування та аутентифікацію. Розглядався протоколи безпеки та їх роль у захисті інформації в IoT, а також важливість TLS/SSL і OpenSSL.

Висновки та перспективи

Підсумовую необхідність комплексного підходу до забезпечення безпеки в IoT. Наголошую на важливості реалізації ефективних захисних механізмів та надаються конкретні рекомендації для поліпшення безпеки в мережах IoT.

Список використаних джерел

1. Осипчук С.О., Мошинська А.В., Кіращук В.В. (2019), “Прикладні аспекти реалізації рішень передавання інформації в технологіях інтернету речей”. Матеріали XIII Міжнародної науково-технічної конференції ПТ-19 Перспективи телекомунікацій, с.17–21.

2. Пристрої IoT, що використовуються в логістиці. [Електронний ресурс]. Режим доступу: https://www.mokosmart.com/uk/iot-in-logistics/

3. Weyrich, M. and Ebert, C. (2016). Reference architectures for the internet of things. IEEE Software 33 (1): 112-116.

4. Zarghami, Shirin, Middleware for Internet of Things, Faculty of Electrical Engineering, Mathematics and Computer Science Software Engineering, University of Twente, nov 2013.

5. Архітектура і технології IoT. [Електронний ресурс]. – Режим доступу: https://learn.ztu.edu.ua/pluginfile.php/68838/mod_resource/content/2/%D0% B-1.pdf – Назва з екрану. – Дата звернення: 22. 04.2023.

ОСОБЛИВОСТІ ОПТИМІЗАЦІЇ ВИРОБНИЧИХ ПРОЦЕСІВ З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Панасюк Володимир Володимирович
Державний університет інформаційно-комунікаційних технологій
Науковий керівник: Калинюк А.М.,
кандидат математичних наук, доцент кафедри Математичного аналізу
Державного університету інформаційно-комунікаційних технологій, м. Київ

Дослідження розглядає розвиток систем міського планування на основі даних з IoT-сенсорів, підкреслюючи їх важливість для комфорту та безпеки мешканців. Акцент робиться на ролі IoT в оптимізації міської інфраструктури, включаючи паркування та моніторинг.

Постановка задачі

Розглядається важливість ефективного міського планування в контексті сучасних викликів урбанізації. Акцентується на значущості IoT у зборі та аналізі даних для поліпшення міського середовища.

Мета дослідження

Визначається мета дослідження - аналіз можливостей використання IoT для розвитку міського планування, з особливим фокусом на підвищенні комфорту та безпеки.

Результати дослідження

Проводився детальний аналіз використання IoT-сенсорів у міському плануванні, розглядаючи їх роль у оптимізації транспортної інфраструктури та моніторингу екологічних показників.

Висновки та перспективи

Підсумовується внесок IoT у розвиток міських систем, з акцентом на їх ефективність та інноваційність у підвищенні комфорту та безпеки мешканців.

Список використаних джерел

1. Виділені комунікації короткого радіусу дії [Електронний ресурс] – Режим доступу до ресурсу: ttps://en.wikipedia.org/wiki/Dedicated_shortrange_communications (дата звернення: 23.11.2023).
2. Датчики руху [Електронний ресурс] – Режим доступу: // https://en.wikipedia.org/ (дата звернення: 23.11.2023).
3. Єршова, О. Л. Бажан, Л. І. // Розумне місто – концепція, моделі, технології, стандартизація// електрон. текст. дані [Електронний ресурс] – Режим доступу: http://194.44.12.92:8080/jspui/handle/123456789/5372 (дата звернення: 23.11.2023).

IOT В МЕДИЦИНІ: ВІДНОВЛЕННЯ ЗДОРОВ'Я ЧЕРЕЗ ІННОВАЦІЇ ТА ТЕХНОЛОГІЧНИЙ ПРОГРЕС

Ратушняк Роман Миколайович
Державний університет інформаційно-комунікаційних технологій
Науковий керівник: Ткаленко Оксана Миколаївна,
доцент кафедри
Інженерії програмного забезпечення автоматизованих систем
Державного університету інформаційно-комунікаційних технологій, м. Київ

Протягом останнього десятиліття в системі охорони здоров'я відбулися кардинальні зміни, спричинені перебудовою соціально-економічних засад суспільства. Дослідження аналізує використання Інтернету Речей (IoT) в охороні здоров'я, зосереджуючись на попередженні захворювань та вдосконаленні медичної діагностики.

Постановка задачі

Дослідження ставить за мету визначити можливості та виклики використання IoT в системах медичного моніторингу та діагностики, враховуючи переваги носимих пристроїв, інноваційних технологій та управління медичними установами.

Мета дослідження

Мета - проаналізувати вплив Інтернету Речей на покращення сучасної медицини через попередження захворювань та вдосконалення медичної діагностики. Дослідження спрямоване на ідентифікацію ключових переваг і можливих викликів в процесі впровадження IoT в охороні здоров'я.

Результати дослідження

Моніторинг Пацієнтів: IoT надає можливість неперервного моніторингу через смарт-годинники та інші носимі пристрої, що дозволяє вчасно виявляти аномалії та попереджувати захворювання.

Інноваційні Технології: Використання датчиків зображень та звуку забезпечує точнішу та швидшу медичну діагностику, покращуючи методи визначення захворювань.

Висновки та перспективи

Висновки: Впровадження IoT в охороні здоров'я має значний потенціал для поліпшення медичних послуг, але вимагає уваги до аспектів безпеки та конфіденційності.

Перспективи: Є перспективи для подальших досліджень в області вдосконалення систем IoT для забезпечення точності та ефективності медичної діагностики, а також розвитку стандартів безпеки.

Список використаних джерел

1. Kotevski A., Koceska N., Koceski S. E-health monitoring system. International Conference on Applied Internet and Information Technologies. 2016. P. 259-263.
2. Internet of Things (IOT) security: imperva. URL: https://www.imperva.com/learn/applicationsecurity/iot-internet-of-things-security/
3. Cybersecurity and the Internet of Things: security. URL https://www.securitymagazine.com/articles/90793-cybersecurity-and-the-internet-of-things

КЛАСИФІКАЦІЇ ЗАШИФРОВАНОГО ТРАФІКУ В МЕРЕЖАХ TLS: ПОГЛЯД НА СУЧАСНІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Брезіцький Сергій Миколайович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут Телекомунікацій

У останні роки різко зросла частка мережевого трафіку, який шифрується протоколом TLS. У зашифрованому трафіку відсутня інформація щодо типу даних, наприклад, відеотрафіку, аудіотрафіку чи веб-трафіку. Різні типи трафіку мають різні вимоги до якості обслуговування. Таким чином, інформація про типи трафіку необхідна маршрутизатору мережі для ефективного розподілу ресурсів під них. Тому класифікація зашифрованого трафіку в реальному часі за типом передаваних даних є важливим інструментом забезпечення якості обслуговування.

Класифікацію зашифрованого трафіку можна реалізувати різними методами. Для класифікації в реальному часі часто використовується підхід, заснований на аналізі незашифрованої інформації, яка міститься в TLS "рукостисканні" (Рис. 1), що використовується для узгодження криптографічних функцій між сторонами обміну. Широкого поширення набули нейромережеві алгоритми [1], які реалізують цей підхід, оскільки вони здатні виявляти залежності в даних без попередньої обробки, наприклад, в корисному навантаженні незашифрованого TLS " рукостисканні ".

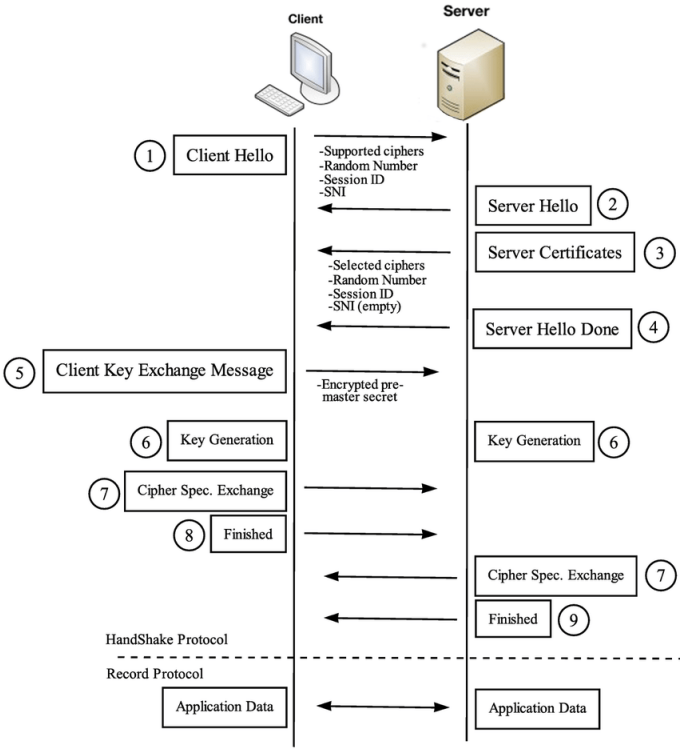

Рис. 1. Схема TLS "рукостисканні"

В данний момент розглядається можливість додатку до протоколу TLS, який дозволить приховати розширення Server Name Indicator (SNI), що передається у TLS "рукостисканні" і часто використовується як важлива ознака для визначення типу трафіку.

Список використаних джерел

1. Wang W. [et al.] Malware traffic classification using convolutional neural network for representation learning // 2017 International Conference on Information Networking (ICOIN) / IEEE. 33 2017. P. 712–71.7.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ КЕРУВАННЯ БЕЗДРОТОВИМИ ПРИЛАДАМИ ПО ЗАХИЩЕНОМУ КАНАЛУ ЗВ'ЯЗКУ

Акуленко Оксана Олександрівна,
Довбенко Антон Володимирович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто бездротові технології, які використовуються повсюди, від побутових пристроїв до великих корпоративних систем. Однак разом зі зростанням популярності бездротових засобів зв'язку виникають нові виклики щодо безпеки. Розробка програмного забезпечення для керування бездротовими приладами через захищений канал зв'язку стає критичною задачею для забезпечення конфіденційності та цілісності передаваних даних.

Основні аспекти розробки

1. Шифрування та аутентифікація

Розробка програмного забезпечення повинна включати ефективні методи шифрування для захисту від несанкціонованого доступу та перехоплення інформації. Також важливо впроваджувати механізми аутентифікації, щоб переконатися, що лише вповноважені користувачі можуть отримувати доступ до бездротових приладів.

2. Захист від атак

Розробники повинні удосконалювати програмне забезпечення для захисту від різних видів атак, таких як атаки типу "man-in-the-middle" та атаки з використанням фальшивих базових станцій. Захист від вразливостей, таких як атаки "replay" та "packet injection," також є важливою частиною безпеки бездротових комунікацій.

3. Забезпечення цілісності даних

Програмне забезпечення повинно включати механізми для перевірки цілісності переданих даних. Введення контрольних сум та цифрових підписів дозволяє виявляти будь-які спроби зміни чи порушення цілісності інформації під час передачі.

4. Управління ключами та сертифікатами

Безпека бездротового каналу в значній мірі залежить від ефективного управління ключами та сертифікатами. Розробка програмного забезпечення повинна передбачати безпечне зберігання та обмін ключами для забезпечення конфіденційності і безпеки.

Розробка програмного забезпечення для керування бездротовими приладами через захищений канал зв'язку вимагає комплексного підходу до безпеки та захисту даних. Застосування сучасних криптографічних методів, механізмів аутентифікації та ефективних стратегій захисту дозволяє забезпечити надійність та безпеку використання бездротових технологій у різних галузях.

ЛІТЕРАТУРА

1.Безпека вашої системи керування. [Електроний ресурс]// - Режим доступу: https://www.controlglobal.com/assets/knowledge_centers/abb/assets/abb_secure_control_sys.pdf
2.Конфіденційність. [Електроний ресурс]// - Режим доступу: https://searchsecurity.techtarget.com/definition/Wired-Equivalent-Privacy

ЗАСТОСУВАННЯ GPS-ТРЕКЕРІВ

Захаржевська Аліна Анатоліївна,
Кравченко Олеся Сергіївна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто GPS-технології, які вже давно стали не просто розкішшю, але і необхідністю в сучасному світі. GPS-трекери, здатні визначати місцезнаходження та вести запис про рух об'єктів, мають широкий спектр застосувань - від особистого використання до оптимізації бізнес-процесів.

1. Особисте використання GPS-трекерів

1.1. Захоплення моменту

GPS-трекери дозволяють фіксувати маршрути подорожей та захоплювати моменти. Вони стають надійними компаньйонами для туристів, подорожуючи як пішки, так і на транспорті.

1.2. Безпека та спостереження

Батьки використовують GPS-трекери для відстеження місцезнаходження своїх дітей. Це забезпечує безпеку та спокій, забезпечуючи можливість вчасно реагувати на небезпеку чи втрату.

2. Трекінг транспортних засобів

2.1. Автомобільний сектор

В автомобільній індустрії GPS-трекери дозволяють власникам та менеджерам відстежувати рух автомобілів, зменшувати споживання пального, оптимізувати маршрути і виявляти несправності в роботі автотранспорту.

2.2. Логістика та доставка

Компанії у сфері логістики використовують GPS-технології для відстеження вантажів, планування оптимальних маршрутів та підвищення ефективності доставки.

3. Бізнес та фліт-менеджмент

3.1. Управління флотом

Компанії, які мають великі автопарки, використовують GPS-трекери для контролю роботи транспорту, визначення оптимальних маршрутів та зменшення витрат.

3.2. Відстеження робочого часу

GPS-технології також використовуються для відстеження робочого часу співробітників, що дозволяє ефективно керувати робочим процесом та оптимізувати робочі потоки.

GPS-технології та GPS-трекери вже давно вийшли за межі використання в автомобілях та стали важливим інструментом в різних сферах життя. Від особистого використання до підтримки бізнес-процесів, вони дозволяють власникам та менеджерам отримувати точну інформацію та приймати обгрунтовані рішення для оптимізації діяльності та покращення ефективності.

ЛІТЕРАТУРА

1. Навігація. Основи визначення місцеположення та скеровування / Б. Гофманн-Велленгоф, К. Легат, М. Візер ; пер. з англ. за ред. : Я. С. Яцківа ; літ. ред. : О. Є. Смолінська. — Л.: ЛНУ ім. І. Франка, 2017. — 449 с.

2.Серапинас Б.Б. Глобальные системы позиционирования. — М. : ИКФ "Каталог", 2012. — 106 с.

УМОВИ ЕКСПЛУАТАЦІЇ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Личманюк Юлія Сергіївна,
Панченко Лілія Євгеніївна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто міжміські телефонні мережі, які в сучасному світі відіграють ключову роль у забезпеченні надійного та ефективного зв'язку між різними містами та регіонами. Створення та впровадження таких мереж вимагає досконалої методики, яка охоплює різні аспекти, починаючи від проектування та закінчуючи ефективним впровадженням та підтримкою. У цій статті розглянемо основні етапи та важливі аспекти методики створення та впровадження міжміської телефонної мережі.

1. Середовище та температурні умови

Одним із важливих аспектів експлуатації телекомунікаційного обладнання є створення оптимальних умов середовища. Температура та вологість повинні залишатися в межах визначених стандартів, оскільки висока температура може призвести до перегріву, а низька - до конденсації та утворення конденсату, що може спричинити корозію та інші дефекти.

2. Електропостачання та джерела живлення

Стабільне електропостачання є критичним для роботи телекомунікаційного обладнання. Забезпечення ефективного джерела живлення та застосування систем резервування може уникнути втрати даних та забезпечити безперебійну роботу в умовах перебоїв електропостачання.

3. Вентиляція та охолодження

Ефективна система вентиляції та охолодження є ключовою для уникнення перегріву обладнання. Забезпечення достатнього об'єму повітря та використання систем охолодження, таких як кондиціонери або вентилятори, може запобігти надмірному нагріванню та забезпечити стабільну роботу.

4. Захист від зовнішніх факторів

Телекомунікаційне обладнання повинно бути захищене від зовнішніх факторів, таких як вода, пил, вібрації та інші небажані впливи. Використання водонепроникних корпусів, фільтрів та інших захисних засобів допомагає зберегти цілісність обладнання.

5. Віддалене моніторинг та управління

Використання систем віддаленого моніторингу та управління дозволяє операторам слідкувати за станом обладнання, виявляти проблеми та вчасно реагувати на них навіть без присутності фахівців на місці.

6. Регулярне технічне обслуговування

Проведення регулярного технічного обслуговування та періодична перевірка обладнання допомагає виявляти можливі несправності та запобігати виникненню проблем. Це включає перевірку заземлення, обстеження кабелів, апаратної діагностики тощо.

7. Безпека та контроль доступу

Забезпечення високого рівня безпеки для телекомунікаційного обладнання включає контроль доступу до приміщень, шифрування даних, використання паролів та інших методів захисту від несанкціонованого доступу.

Умови експлуатації телекомунікаційного обладнання мають визначальний вплив на його надійність та тривалість служби. Забезпечення оптимального середовища, стабільного живлення та ефективного управління є критичним для забезпечення безперебійної та продуктивної роботи телекомунікаційної інфраструктури. Всі ці аспекти має бути уважно розглянуті та враховані під час планування, будівництва та експлуатації телекомунікаційних мереж.

ЛІТЕРАТУРА
1.Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П.Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013ю — 256 с. ISBN 978-617-574-087-3
2.Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. — Львів: «Магнолія 2006», 2010. — 262 с. ISBN 966-8340-69-8

ВПРОВАДЖЕННЯ ПРИСТРОЮ ШЛЮЗА ДЛЯ З'ЄДНАННЯ МЕРЕЖ ZIGBEE ТА GPRS

Солонець Нелля Андріївна,
Стеблянко Ілля Сергійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто впровадження пристрою шлюза, який може об'єднувати мережі ZigBee і GPRS, стає ключовим етапом у створенні зручних та універсальних IoT-систем. У цій статті ми розглянемо важливість та переваги використання пристрою шлюза для з'єднання мереж ZigBee та GPRS.

1. Значення з'єднання мереж ZigBee та GPRS

Мережі ZigBee і GPRS використовуються в різних сценаріях IoT, проте вони можуть виникати у великих труднощах у випадках, коли потрібно об'єднати дані з різних джерел. Застосування пристрою шлюза дозволяє вирішити цю проблему, створюючи єдину точку з'єднання для обміну інформацією між мережами.

2. Основні функції пристрою шлюза zigbee та GPRS:

2.1. Конвертація протоколів

Пристрій шлюза використовується для конвертації протоколів мережі ZigBee та GPRS. Це дозволяє пристрою "розуміти" дані, отримані від пристроїв в мережі ZigBee, та передавати їх у форматі, зрозумілому для мережі GPRS і навпаки.

2.2. Забезпечення безпеки

Пристрій шлюза відіграє ключову роль у забезпеченні безпеки передачі даних між мережами. Він може використовувати різні методи шифрування та аутентифікації для захисту від несанкціонованого доступу та витоку інформації.

2.3. Управління трафіком

Пристрій шлюза використовується для ефективного управління трафіком між мережами, що дозволяє оптимізувати передачу даних та зменшити можливі затримки.

2.4. Моніторинг та діагностика

Пристрій шлюза може надавати можливості для моніторингу та діагностики стану мереж, що допомагає вчасно виявляти проблеми та здійснювати їх розв'язання.

3. Переваги впровадження пристрою шлюза:

3.1. Єдина точка керування

Використання пристрою шлюза дозволяє створити єдину точку керування для обох мереж, що спрощує процес адміністрування та моніторингу.

3.2. Зменшення затрат на інфраструктуру

Об'єднання мереж за допомогою шлюза може призвести до зменшення витрат на інфраструктуру, оскільки дозволяє використовувати одні канали передачі даних та обладнання.

3.3. Розширення можливостей IoT

З'єднання мереж ZigBee та GPRS за допомогою пристрою шлюза розширює можливості IoT, дозволяючи використовувати різноманітні типи пристроїв та сценарії в одній системі.

Впровадження пристрою шлюза для з'єднання мереж ZigBee та GPRS є стратегічно важливим кроком у створенні сучасних та ефективних IoT-систем. Це дозволяє не тільки оптимізувати обмін даними між різними пристроями, але й забезпечує безпеку, ефективне управління та розширює можливості використання різних типів пристроїв. Пристрій шлюза - це ключовий компонент для розвитку та вдосконалення сучасних телекомунікаційних систем.

ЛІТЕРАТУРА

1.Academic Journals [Електронний ресурс] – Електроні дані – "A new gateway node for wireless sensor network applications" - Режим доступу: https://academicjournals.org/journal/SRE/article-full-text-pdf/1E8BDF161051

2.International Journal of Future Generation Communication and Network-ing [Електронний ресурс] – Електроні дані – "The Design of Wireless Sensor Network Gateway based on ZigBee and GPRS" – Режим доступу: http://article.nadiapub.com/IJFGCN/vol7_no2/5.pdf

МЕТОДИКА ПОБУДОВИ ТА ВПРОВАДЖЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ IOT НА ОСНОВІ СУЧАСНИХ ПРОТОКОЛІВ

Аварі Алісіно Залмайович,
Антіпін Андрій Олексійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто і*нтернет речей (IoT), який є ключовим елементом сучасного технологічного ландшафту, і побудова ефективних бездротових мереж для IoT є завданням важливим для забезпечення надійного та ефективного обміну даними. У цій статті ми розглянемо методику побудови та впровадження бездротової мережі IoT на основі сучасних протоколів.*

1. Огляд сучасних протоколів для IoT:

1.1. MQTT (Message Queuing Telemetry Transport):

MQTT є легким та ефективним протоколом, розробленим спеціально для обміну повідомленнями між пристроями IoT. Він визначає простий та масштабований механізм публікації-підписки, що робить його ідеальним для масштабованих IoT-мереж.

1.2. CoAP (Constrained Application Protocol):

CoAP є протоколом, спеціально розробленим для обміну даними в обмежених умовах, таких як обмежені ресурси пристроїв IoT. Він використовує архітектуру REST, спрощуючи взаємодію між пристроями.

1.3. LoRaWAN (Long Range Wide Area Network):

LoRaWAN - це протокол для низькошвидкісних, довгодіючих бездротових мереж, ідеально підходить для пристроїв IoT, які вимагають далекого зв'язку та довгого терміну служби.

1.4. NB-IoT (Narrowband IoT):

NB-IoT - це стандарт мобільного зв'язку, розроблений для підключення пристроїв IoT. Він використовує низькочастотний спектр для забезпечення широкого покриття та зниження витрат енергії.

2. Етапи побудови та впровадження бездротової мережі IoT:

2.1. Визначення Вимог:

Перший етап - визначення вимог до мережі IoT. Це включає визначення обсягу передачі даних, швидкості, кількості пристроїв та їхніх характеристик.

2.2. Вибір протоколів:

Вибір сучасних протоколів залежить від конкретних потреб системи. MQTT часто використовується для великих мереж, CoAP - для обмежених пристроїв, LoRaWAN та NB-IoT - для забезпечення далекого зв'язку.

2.3. Проектування інфраструктури:

На цьому етапі створюється детальний план інфраструктури мережі IoT, включаючи розташування вузлів з'єднання, маршрутизацію та забезпечення безпеки.

2.4. Розгортання програмного та апаратного забезпечення:

Розгортання включає в себе встановлення та налаштування необхідного програмного та апаратного забезпечення, такого як базові станції, пристрої IoT та сервери збору даних.

2.5. Тестування та оптимізація:

Після розгортання важливо провести тестування для перевірки працездатності мережі та оптимізації її параметрів для досягнення максимальної ефективності.

Побудова та впровадження бездротової мережі IoT на основі сучасних протоколів - це важливий етап в розвитку сучасних телекомунікаційних технологій. Вибір відповідних протоколів та правильна методика реалізації грають ключову роль у забезпеченні ефективної та надійної бездротової комунікації для пристроїв IoT.

ЛІТЕРАТУРА

1. Нежуренко А. Телекоммуникационные решения – взгляд изнутри. – Режим доступу: http://www.seti-ua.com/, 2005.

2.Traffic Engineering in Software-Defined Networking: Measurement and Management http://onrc.stanford.edu/research_sdn_ approach_ to_ mpls_ traffic _engineering.html.

РОЗРОБКА МЕТОДИКИ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ ДЛЯ ОФІСНОГО ПРИМІЩЕННЯ

Журович Олександр Олександрович,
Зевєлєв Марк Андрійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто корпоративні мережі, які стали ключовим елементом сучасного бізнесу, забезпечуючи швидкий та надійний обмін даними в офісних приміщеннях. Розробка ефективної методики побудови корпоративної мережі є критично важливою для забезпечення високоякісного зв'язку та безпеки в офісному середовищі. У цій статті ми розглянемо ключові етапи та принципи розробки такої методики.

1. Аналіз вимог та потреб користувачів:

Перший крок - це ретельний аналіз вимог та потреб користувачів. Це включає визначення обсягу трафіку, кількості користувачів, типів підключених пристроїв, а також потреб в безпеці та надійності.

2. Проектування топології та архітектури мережі:

На основі визначених вимог розробляється топологія та архітектура мережі. Важливо визначити, чи буде використовуватися провідна чи бездротова технологія, яка буде структура мережі (зірка, лінійна, комбінована) та де будуть розташовані мережеві вузли.

3. Вибір обладнання та компонентів:

На цьому етапі обирається мережеве обладнання та компоненти, що відповідають потребам мережі. Це включає в себе комутатори, маршрутизатори, файрволи, точки доступу, а також необхідне програмне забезпечення.

4. Розгортання інфраструктури:

Після вибору обладнання проводиться розгортання інфраструктури мережі. Це включає встановлення та налаштування обладнання, розкладання кабельної інфраструктури, а також встановлення необхідного програмного забезпечення.

5. Налаштування системи безпеки:

Безпека є пріоритетним аспектом корпоративних мереж. Проводиться налаштування системи безпеки, включаючи налаштування файрволів, VPN (віртуальних приватних мереж), антивірусного захисту та систем виявлення вторгнень.

6. Конфігурація сервісів та додаткових функцій:

Крім базового налаштування, конфігуруються додаткові сервіси та функції, такі як гостьовий доступ до мережі, керування політикою доступу, мережевий моніторинг та резервне копіювання.

7. Тестування та оптимізація:

Після завершення налаштувань проводиться тестування мережі для перевірки її працездатності та надійності. В разі виявлення проблем проводиться оптимізація параметрів мережі.

8. Документація та підготовка персоналу:

Важливо створити документацію, що включає схеми мережі, конфігураційні файли та інструкції з експлуатації. Крім того, персонал повинен бути навчений роботі з новою мережевою інфраструктурою.

9. Підтримка та моніторинг:

Після введення в експлуатацію мережа потребує постійної підтримки та моніторингу. Важливо вчасно виявляти та виправляти проблеми, а також вдосконалювати мережу з урахуванням зростання бізнесу та технологічних змін.

Розробка методики побудови корпоративної мережі для офісного приміщення є складним та відповідальним завданням. Всі етапи, від аналізу вимог до підтримки та моніторингу, мають бути виконані з увагою до деталей. Ефективна корпоративна мережа забезпечить стабільну та безпечну роботу всіх інформаційних систем підприємства.

ЛІТЕРАТУРА

1 Абрамов В.О. Клименко С.Ю. Базові технології комп’ютерних мереж.2014. -49с

2. Берлин А. Н. Абонентские сети доступа и технологии высокоскоростных сетей, 2016. – 277 с.

МЕТОДИКА РОЗРОБКИ ПРОГРАМНОГО ЗАСОБУ РОБОТИ АПАРАТНОГО КОДЕКА НА БАЗІ ПРОТОКОЛУ ПЕРЕДАЧІ ДАНИХ WS2812B

Павлов Владислав Анатолійович,
Оніщук Ольга Петрівна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто апаратні кодеки, що використовують протокол передачі даних WS2812B, і здобули популярність у світі електроніки та освітлення за їхню здатність керувати кольоровими світлодіодами із великою точністю та гнучкістю. Розробка програмного забезпечення для таких апаратних кодеків є ключовою для досягнення бажаних ефектів та функціональності. У цій статті розглянемо методику розробки програмного засобу для апаратного кодека на базі протоколу WS2812B.

1. Зрозуміння протоколу WS2812B:

Першим етапом є ретельне вивчення протоколу передачі даних WS2812B. Це включає в себе розуміння структури бітових даних, необхідних для керування кожним світлодіодом, а також особливостей сигналу передачі.

2. Вибір мови програмування та інструментів розробки:

На основі вивченого протоколу вибирається мова програмування та інструменти розробки. Зазвичай використовуються мови високого рівня, такі як C++ або Python, а також популярні інтегровані середовища розробки, наприклад, Arduino IDE або PlatformIO.

3. Розробка драйвера для апаратного кодеку:

Створюється драйвер, який забезпечує взаємодію програмного забезпечення з апаратним кодеком. Драйвер повинен коректно інтерпретувати команди від програми та відправляти їх до світлодіодів через протокол WS2812B.

4. Створення алгоритмів керування кольорами:

Важливим етапом є розробка алгоритмів керування кольорами світлодіодів. Це може включати в себе зміну яскравості, зміну кольору, плавні переходи між кольорами та інші ефекти відповідно до бажань користувача.

5. Оптимізація та управління ресурсами:

Під час розробки слід звертати увагу на оптимізацію програмного забезпечення для ефективного використання ресурсів мікроконтролера чи мікропроцесора, на якому виконується програма.

6. Вивчення та виправлення помилок:

Розробка програмного забезпечення — це ітеративний процес, тому важливо вивчати та виправляти помилки, щоб забезпечити стабільну та надійну роботу кодеку.

7. Реалізація додаткових функцій:

Залежно від конкретних вимог можуть бути реалізовані додаткові функції, такі як синхронізація з музикою, використання сенсорів або інших елементів введення для керування світлодіодами.

8. Тестування та валідація:

Після завершення розробки проводяться тестування та валідація програмного забезпечення. Це включає в себе перевірку роботи всіх функцій, стабільності та правильності передачі даних.

9. Документація та підтримка:

Важливо створити документацію, яка пояснює принципи роботи програмного забезпечення, інструкції щодо використання та можливості розширення. Також слід забезпечити можливість підтримки та оновлень програмного забезпечення.

Розробка програмного забезпечення для апаратного кодеку на базі протоколу WS2812B — це завдання, яке вимагає глибокого розуміння протоколу та вправності у програмуванні. З дотриманням вищезазначених етапів можна створити програмне забезпечення, яке дозволить максимально використовувати потенціал кольорових світлодіодів та створювати захоплюючі світлові ефекти.

ЛІТЕРАТУРА

1. B. Kernighan The C Programming Language / Brian W. Kernighan, Dennis M. Ritchie - 2-е вид. - New Jersey AT&T Bell Laboratories 1988 - 288с

2. Elecia White / Making Embedded Systems: Design Patterns for Great Software - Reilly Media, Inc., Sebastopol, CA - 2012 - 311с

МЕТОДИКА ПОБУДОВИ МЕРЕЖ IP-ТЕЛЕФОНІЇ НА ОСНОВІ НА ОСНОВІ ПРОТОКОЛУ MGCP

Паршина Оксана Іванівна,
Паршин Микола Володимирович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто IP-телефонію, яка стала важливою складовою сучасних телекомунікацій, забезпечуючи гнучкість та ефективність в комунікаціях бізнесу. Протокол MGCP (Media Gateway Control Protocol) використовується для управління мультимедійними потоками у мережах IP-телефонії. У цій статті розглянемо методику побудови мережі IP-телефонії на основі протоколу MGCP.

1. Розуміння протоколу MGCP:

Першим етапом є докладне вивчення протоколу MGCP. Розуміння структури повідомлень, команд та відповідей є ключовим для ефективної роботи з цим протоколом.

2. Проектування архітектури мережі:

На основі вивчення протоколу MGCP розробляється архітектура мережі. Визначаються компоненти, такі як мультимедійні шлюзи (Media Gateways), контролери ресурсів та сервери управління.

3. Вибір обладнання та софтуеру:

Важливим етапом є вибір обладнання та софтуеру, яке підтримує протокол MGCP. Мультимедійні шлюзи та контролери ресурсів повинні бути сумісними з обраною архітектурою.

4. Налаштування мультимедійних шлюзів:

Мультимедійні шлюзи використовуються для перетворення мультимедійних потоків між аналоговими та цифровими форматами. Налаштування цих шлюзів включає в себе параметри кодеків, обробки сигналів та маршрутизації.

5. Конфігурація контролерів ресурсів:

Контролери ресурсів відповідають за взаємодію з мультимедійними шлюзами та управління ресурсами. Конфігурація включає в себе налаштування каналів, визначення груп та взаємодію з серверами управління.

6. Розгортання серверів управління:

Сервери управління відповідають за виконання команд, отриманих від контролерів ресурсів. Це включає в себе управління з'єднаннями, маршрутизацію та відстеження стану обладнання.

7. Налаштування безпеки:

Забезпечення безпеки мережі IP-телефонії є критичним завданням. Встановлення заходів шифрування, аутентифікації та контролю доступу допомагає уникнути несанкціонованого доступу та збереження конфіденційності даних.

8. Тестування та валідація:

Перед введенням в експлуатацію важливо провести тестування всіх компонентів мережі. Валідація включає перевірку правильності конфігурації, роботи мультимедійних потоків та реагування системи на різні сценарії.

9. Документація та навчання персоналу:

Створення документації, яка описує архітектуру мережі, конфігурації та правила експлуатації, є важливим етапом. Навчання персоналу допомагає забезпечити ефективне використання нової мережі.

Методика побудови мережі IP-телефонії на основі протоколу MGCP вимагає глибокого розуміння протоколу та інтеграції різних компонентів. З використанням цієї методики можна

досягти ефективного та безпечного функціонування IP-телефонії в корпоративному середовищі.

ЛІТЕРАТУРА

1. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-Телефония. - М.: Радио и связь, 2001. — 336с.
2.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 2-е издание. – СПб.:Питер, 2005. – 864с.

МЕТОДИКА ПОБУДОВИ МЕРЕЖ IP-ТЕЛЕФОНІЇ НА ОСНОВІ ПРОТОКОЛУ H.323

Полтко Денис Романович,
Старченко Ігор Володимирович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто створення ефективної корпоративної мережі, що є ключовим завданням для сучасних підприємств, оскільки вона визначає стабільність комунікації та обміну даними в організації. У цій статті розглянемо методику розробки корпоративної мережі для підприємства "ЕДЕДЖЕНСІ".

1. Розуміння протоколу H.323:

Першим етапом є докладне вивчення протоколу H.323. Розуміння структури повідомлень, сесій та управління ресурсами є важливим для успішної реалізації мережі IP-телефонії.

2. Аналіз вимог та потреб користувачів:

Аналіз потреб користувачів та бізнес-вимог є ключовим для визначення обсягу мережі. Це включає в себе кількість користувачів, типи дзвінків (внутрішні чи зовнішні), потреби у багатоканальності тощо.

3. Вибір обладнання:

Вибір обладнання, яке підтримує протокол H.323, є ключовим кроком. Це може бути відеоконференц-обладнання, IP-телефони, маршрутизатори та інше обладнання для реалізації сесій та передачі голосу та відео.

4. Налаштування мережевої інфраструктури:

На основі обраного обладнання розробляється архітектура мережі. Це включає в себе комутатори, маршрутизатори, сервери взаємодії та інші компоненти.

5. Налаштування відомостей про домен:

H.323 використовує термін "домен" для групування обладнання та користувачів. Налаштування параметрів домена, таких як ім'я домена, адреса відеоголовки та інші, є необхідним для успішної роботи протоколу.

6. Конфігурація медіа-кодеків:

H.323 підтримує різні кодеки для стискання аудіо та відео. Конфігурація цих параметрів важлива для забезпечення оптимальної якості звуку та відео в мережі.

7. Забезпечення безпеки:

Забезпечення безпеки мережі IP-телефонії має високий пріоритет. Встановлення VPN, шифрування даних та захист від несанкціонованого доступу є важливими елементами.

8. Реалізація системи адміністрування:

Створення системи адміністрування для відстеження стану мережі, моніторингу використання ресурсів та вирішення можливих проблем.

9. Тестування та оцінка продуктивності:

Перед введенням в експлуатацію важливо провести тестування для визначення пропускної здатності, стійкості та ефективності мережі. Оцінка продуктивності допомагає виявити можливі удосконалення.

10. Документація та навчання персоналу:

Створення детальної документації щодо конфігурації мережі та процедур адміністрування. Навчання персоналу для ефективного використання нової інфраструктури.

Методика побудови мережі IP-телефонії на основі протоколу H.323 вимагає комплексного підходу та врахування великої кількості факторів. З дотриманням вищезазначених етапів можна успішно реалізувати стабільну та продуктивну систему IP-телефонії на підприємстві.

ЛІТЕРАТУРА

1.Packet based multimedia communication systems. ITU-T Recommendation H.323. - Geneva, 1998, April.

2.Using the Flow Label Field in IPv6. IETF RFC 1809. - June, 1995.

МЕТОДИКА ПОБУДОВИ МЕРЕЖІ IP-ТЕЛЕФОНІЇ ДЛЯ ПІДПРИЄМСТВ

Збіняков Павло Васильович,
Полосенко Анна Олегівна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

У даній статті розглянуто методику побудови мережі IP-телефонії для підприємств. В сучасному бізнес-середовищі важливо мати надійну і ефективну систему зв'язку, і IP-телефонія стає все більш популярним вибором для підприємств будь-якого розміру.

1. Аналіз потреб і розробка стратегії

Перед розпочатком будівництва IP-телефонної мережі важливо провести аналіз потреб підприємства. Визначте кількість працівників, обсяг телефонного трафіку, потреби в додаткових функціях (відеоконференції, переадресації, групового дзвінка тощо). Розробіть стратегію, що враховує поточні і майбутні потреби.

2. Вибір обладнання та платформи

Вибір обладнання є ключовим етапом. Обрати потрібно IP-телефонію обладнання, яке відповідає розміру підприємства та його вимогам. Розгляньте можливості серверів, шлюзів, телефонів, а також програмного забезпечення для управління системою.

3. Встановлення основної інфраструктури

Перевірте і підготуйте мережеву інфраструктуру для впровадження IP-телефонії. Важливо мати стійку та безпечну мережу, здатну передавати телефонний трафік з необхідною пропускною здатністю та якістю обслуговування.

4. Розробка плану нумерації та інтеграція з існуючими системами

Розробіть систему нумерації, яка враховує потреби підприємства та дозволяє ефективне управління внутрішньою та зовнішньою комунікацією. Інтегруйте IP-телефонію з існуючими системами, такими як електронна пошта, календарі, CRM системи тощо.

5. Забезпечення безпеки та резервування

Безпека є важливим аспектом будь-якої телефонної мережі. Застосовуйте заходи безпеки для захисту від несанкціонованого доступу та атак. Також важливо реалізувати систему резервування для забезпечення неперервності роботи в разі відмови обладнання чи мережі.

6. Навчання персоналу та підтримка

Проведіть навчання персоналу з використання нової IP-телефонної системи. Забезпечте регулярну технічну підтримку та моніторинг для вирішення можливих проблем та оптимізації роботи системи.

Побудова мережі IP-телефонії для підприємства є комплексним завданням, яке вимагає ретельного планування та інтеграції. З дотриманням вищезазначених етапів та використанням сучасних технологій можна створити ефективну та надійну телефонну систему, що відповідає потребам підприємства та сприяє підвищенню продуктивності комунікацій.підприємстві.

ЛІТЕРАТУРА

1 Мак-Квери С., Мак-Грю К. Фой С. Передача голосовых данных по сетям Cisco Frame Relay, ATM и IP.: Пер. с англ. – М: Издательский дом «Вильямс», 2002. - 512с.: ил. – Парал. тит. англ.
2. Рослякова А. Самсонов М. Шибаева И. IP-телефония. – М.: Эко-Трендз, 2003.-252 с.: ил.

МЕТОДИКА ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ БЕЗПРОВОДОВОЇ МЕРЕЖІ НА ОСНОВІ СУЧАСНИХ ТЕХНОЛОГІЙ

Якимчук Юрій Олексійович,
Казенко Георгій Олексійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

З великим зростанням використання безпроводових мереж в сучасному світі, питання підвищення пропускної здатності стає ключовим для забезпечення високоякісного та стабільного з'єднання. У даній статті розглянемо методику, яка базується на сучасних технологіях для підвищення пропускної здатності безпроводової мережі.

1. Використання технології Wi-Fi 6

Wi-Fi 6 (802.11ax) є новим стандартом безпровідного з'єднання, призначеним для підвищення ефективності мережі в умовах великої кількості підключених пристроїв. Впровадження Wi-Fi 6 дозволяє збільшити пропускну здатність, поліпшити роботу в умовах великої концентрації користувачів та забезпечити більш швидку передачу даних.

2. Використання технології MU-MIMO

Множинний вхід та вихід (MU-MIMO) дозволяє передавати дані одночасно до кількох пристроїв, замість послідовного передавання. Ця технологія допомагає підвищити пропускну здатність мережі та покращити роботу в умовах високого трафіку.

3. Використання технології Beamforming

Beamforming дозволяє підсилювати сигнал в напрямку конкретного пристрою, замість відправлення сигналу в усі боки. Це зменшує перешкоди та покращує якість сигналу, що в свою чергу позитивно впливає на пропускну здатність.

4. Використання частотного спектру 5ГГц

Перехід на використання частотного спектру 5ГГц замість 2.4ГГц дозволяє уникнути перенасичення та забезпечити більше доступного простору для передачі даних. Це особливо важливо в областях з великою густотою безпроводових мереж.

5. Впровадження технології SDN (Software-Defined Networking)

SDN дозволяє централізовано управляти трафіком та ресурсами мережі. Завдяки SDN можливе швидке реагування на зміни в навантаженні, оптимізація шляхів передачі даних та ефективне використання ресурсів.

Підвищення пропускної здатності безпроводової мережі є ключовим завданням для задоволення ростучих потреб у з'єднанні в сучасному світі. Використання сучасних технологій, таких як Wi-Fi 6, MU-MIMO, Beamforming та SDN, дозволяє покращити якість з'єднання,

забезпечити стабільність та підвищити загальну продуктивність безпроводових мереж. Реалізація цих технологій повинна проводитися відповідно до індивідуальних потреб і умов конкретного підприємства чи мережі.

ЛІТЕРАТУРА

1.“A Survey on Device-To-Device Communication In Cellular Networks,” IEEE Commun. Surveys and Tutorials, vol. 16, no. 4, 2014, pp. 1801–19. // A. Asadi, Q. Wang, and V. Mancuso
2.“Cognitive Cellular Systems within the TV Spectrum,” Proc. IEEE DySPAN, 2010, pp. 1–12. // J. Sachs, I. Mari, and A. Goldsmith

РОЗРОБКА АДАПТИВНОГО КОРЕКТОРА ПРИЙМАЛЬНОГО КАНАЛУ МОДЕМУ ПЕРЕДАЧІ ДАНИХ

Гоначарова Юлія Петрівна,
Іваніченко Світлана Іванівна
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

З удосконаленням технологій передачі даних у сучасному світі, розробка адаптивних коректорів для приймального каналу модемів стає ключовою завданням. Адаптивні коректори дозволяють покращити якість прийому даних в умовах шумів та інтерференції, забезпечуючи стабільне та ефективне з'єднання. У цій статті ми розглянемо процес розробки адаптивного коректора для приймального каналу модему передачі даних.

1. Аналіз Середовища Передачі Даних

Першим етапом є аналіз середовища передачі даних, де планується використовувати модем. Це включає в себе вивчення різних видів шумів, інтерференції та інших зовнішніх факторів, які можуть впливати на якість прийому сигналу.

2. Вибір Адаптивних Алгоритмів Корекції

На основі отриманих даних обираються адаптивні алгоритми корекції, які можуть ефективно працювати в конкретних умовах. Серед таких алгоритмів можуть бути алгоритми на основі лінійної алгебри, алгоритми зворотного зв'язку та інші.

3. Моделювання та Тестування

Після вибору алгоритмів проводиться моделювання роботи адаптивного коректора. Важливо врахувати різні умови передачі даних та визначити, як ефективно коректор працює в кожному з них. Тестування включає аналіз швидкості реакції коректора та його точності в умовах спотворень сигналу.

4. Оптимізація та Підготовка до Впровадження

На основі результатів тестування проводиться оптимізація адаптивного коректора. Це може включати в себе підбір оптимальних параметрів алгоритмів, удосконалення обчислювальної швидкості та зменшення витрат пам'яті. Після цього коректор готується до впровадження в реальні умови.

5. Впровадження та Підтримка

Останнім етапом є впровадження адаптивного коректора в робочі умови модему передачі даних. Забезпечення стабільної роботи, підтримка та вдосконалення коректора з часом стають важливим завданням для забезпечення найвищої ефективності.

Розробка адаптивного коректора приймального каналу модему передачі даних є складним процесом, який вимагає глибокого аналізу та тестування в різних умовах. Проте, з правильним підходом, такий коректор може значно поліпшити якість передачі даних, забезпечуючи стабільне та ефективне з'єднання в різних умовах експлуатації.

ЛІТЕРАТУРА

1.Тяжев А.И. Адаптивный цифровой корректор амплитудно-частотных характеристик каналів 2016

9. Джиган В. И. Библиотека алгоритмов адаптивной фильтрации // Доклады 6-й Международной конференции «Цифровая обработка сигналов и ее применения (DSPA-2004)» (Российская академия наук: Институт проблем управления им. В. А. Трапезникова, 31 марта — 2 апреля 2004 г.). — Москва, 2004. - Том 1. - С. 89-94

МЕТОДИКА СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ПРОЕКТУ СХОВИЩА ДЛЯ ТЕЛЕКОМУНІКАЦІЙНОГО ПІДПРИЄМСТВА НА БАЗІ ХМАРНИХ ТЕХНОЛОГІЙ

Ходаківський Дмитро Олександрович,
Глущенко Олексій Володимирович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

В сучасному світі телекомунікаційні підприємства постійно стикаються з великим обсягом даних, високою швидкістю зростання обсягів і потребою в ефективному управлінні і зберіганні цих даних. Впровадження хмарних технологій для створення та управління сховищем є важливим кроком у покращенні ефективності роботи телекомунікаційних компаній.

1. Аналіз потреб та обрання стратегії

Першим кроком у впровадженні хмарного сховища є ретельний аналіз потреб телекомунікаційного підприємства. Визначення обсягів даних, різновидів і їх важливості допоможе обрати відповідні хмарні сервіси та стратегію зберігання.

2. Вибір хмарного постачальника та платформи

Під час вибору хмарного постачальника необхідно врахувати ряд факторів, таких як надійність, безпека даних, масштабованість та вартість. Важливо також визначити оптимальну хмарну платформу, яка відповідає потребам та інфраструктурі підприємства.

3. Розробка архітектури сховища

Створення ефективної архітектури сховища включає в себе визначення структури даних, забезпечення їхньої інтеграції та розробку механізмів забезпечення безпеки. Розробка також повинна враховувати можливості масштабування для відповіді на зростаючі потреби.

4. Реалізація та інтеграція

На цьому етапі здійснюється реалізація архітектури, встановлення необхідних програмних та апаратних засобів. Важливо також врахувати процес інтеграції з існуючими системами підприємства та навчання персоналу використовувати новий інструментарій.

5. Моніторинг та оптимізація

Завершальним етапом є постійний моніторинг роботи сховища та вдосконалення його ефективності. Впровадження автоматизованих систем моніторингу та аналітики дозволяє оперативно виявляти та усувати можливі проблеми.

Впровадження хмарних технологій для створення та управління сховищем є стратегічним рішенням для телекомунікаційних підприємств. Це не лише дозволяє збільшити масштаби та надійність сховища, але й сприяє оптимізації витрат та підвищенню загальної ефективності бізнес-процесів. Правильна методика впровадження гарантує успішну реалізацію проекту та створення стійкої та інноваційної інфраструктури для телекомунікаційного підприємства.

ЛІТЕРАТУРА
1. Aaron Hurst “How to build a cloud data warehouse for the first time” https:// www.information-age.com/build-cloud-data-warehouse-first-time-123486854/
2.Countants “How a Cloud-Hosted Data Warehouse For an Enterprises Works” https://www.countants.com/blogs/how-a-cloud-hosted-data-warehouse-for-an- enterprises-works/

ПЕРСПЕКТИВИ РОЗВИТКУ ТА ВПРОВАДЖЕННЯ НОВІТНІХ ТЕХНОЛОГІЙ ОПТОВОЛОКОННОГО ЗВ'ЯЗКУ

Герасимчук Владислав Сергійович,
Федчук Володимир Сергійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

Оптоволоконний зв'язок визначається як ключовий елемент інфраструктури для передачі даних у сучасному світі. Новітні технології оптоволоконного зв'язку постійно еволюціонують, забезпечуючи швидше, надійніше та більш ефективне з'єднання для компаній, домогосподарств і мобільних платформ. Погляд на перспективи розвитку цих технологій стає ключовим для розуміння та планування майбутнього інформаційного суспільства

1. Швидкість передачі даних.

Нові технології дозволяють значно збільшити пропускну здатність оптоволоконних ліній, забезпечуючи велику швидкість передачі даних. Це стає актуальним у зв'язку з постійним зростанням обсягів цифрового вмісту і вимог до передачі великих обсягів даних.

2. 5G і Інтернет речей (IoT).

Оптоволоконний зв'язок є ключовим компонентом для ефективного функціонування мереж 5G та розвитку Інтернету речей. Впровадження 5G та розширення IoT вимагають надійних і швидких мереж, які можуть бути забезпечені тільки за участю оптоволоконного зв'язку.

3. Інновації в області обладнання.

Високоефективні матеріали та конструкції оптоволоконних кабелів дозволяють збільшити дальність передачі сигналу і зменшити втрати. Це робить оптоволоконний зв'язок більш витратним, але ефективним з точки зору енергоефективності.

4. Використання в інших сферах.

Оптоволоконний зв'язок широко використовується в сферах медицини для високоточного передавання даних у реальному часі. Також ці технології знаходять своє застосування у наукових дослідженнях, де необхідна надійна і швидка передача великих обсягів інформації.

5. Безпека та захист інформації.

- Кібербезпека.

Забезпечення захищеної передачі даних стає особливо важливим в умовах зростаючих загроз кібербезпеки. Оптоволоконний зв'язок дозволяє зменшити ризики перехоплення сигналів і втручання в передачу інформації.

6. Зелена технологія.

У порівнянні з іншими технологіями передачі даних, оптоволоконний зв'язок відзначається високою енергоефективністю. Це стає актуальним у контексті зростання питань стосовно сталості та захисту навколишнього середовища.

Висновок:

Перспективи розвитку та впровадження новітніх технологій оптоволоконного зв'язку безперечно обіцяють багато нових можливостей у сфері комунікацій та інформаційних технологій. Зростаючі вимоги до швидкості передачі даних, розвиток мереж 5G, ефективне використання в інших галузях та зелена технологія стають джерелами натхнення для постійного вдосконалення оптоволоконного зв'язку, що визначатиме курс майбутнього.

ЛІТЕРАТУРА

1. ШИРОКОСМУГОВИЙ ДОСТУП ДО МЕРЕЖІ ІНТЕРНЕТ ЯК ВАЖЛИВА ПЕРЕДУМОВА ІННОВАЦІЙНОГО РОЗВИТКУ УКРАЇНИ [Електронний документ] - Режим доступу: http://old2.niss.gov.ua/content/articles/files/Dubov_dostup-02ccf.pdf .

3. ПРОЕКТУВАННЯ МЕРЕЖІ НА ОСНОВІ ВОЛЗ [Електронний документ] - Режим доступу: https://openarchive.nure.ua/bitstream/document/8500/1/3_zhulenko.pdf .

TAP3 AND NRTRDE CDR TRANSFER FORMATS

Sahaidak Viktor
Educational-scientific Institute of Telecommunications and Information
State University of Information and Communication Technologies
Kyiv, Ukraine

To make possibility for mobile user to perform call to another country, telecommunication operators have developed roaming agreements. In order to exchange billing information TAP3 and NRTRDE were developed.

TAP3 (Transferred Account Procedures) is a CDR interchange format between operators, for use in roaming scenarios, developed by GSMA in 1991. It is strictly formatted and rigidly specified file, which uses ASN1 to encode data. There are two types of TAP3 records - Notification Records and transferBatch.

Notification records are used by visited network to inform home network, that it is available, but roaming users are not using services. Following types of record are containing file available/creation time, file sequence number (it is monotonically increasing number, which allows the receiver to know if any files have been missed between the file that's being currently parsed, and the previous file) and TAGID code of receiver and sender.

TransferBatch contains 2 parts – file level and CDR level. File level also contain following parts:

Batch Control Information which contains TADIG code of sender and receiver, file sequence (it is monotonically increasing number, which allows the receiver to know if any files have been missed between the file that's being currently parsed, and the previous file), Transfer Cut Off Timestamp, File Available Timestamp, TAP3 identification fields - Specification Version Number and Release Version Number;

Accounting Information which provides information about taxes and local currencies in CDRs;

Audit Control Information – provides total charge of roaming users consumed on visited network with timestamps of first and last sessions.

TAP3 CDR level supports MO (mobile origination) and MT (mobile terminating) calls, Supplementary Service, VoLTE MO and MT calls, GPRS, SMS events.

Usually, TAP3 records are delivered to home network within 30 days from end call time, otherwise home operator won't be charged for services consumed by roamer on visited network. If there are problems on visitor network to provide TAP records (operational problems, validation, re-rating, transfer via a MVNO, etc) than timescale is increased to 40 days.

NRTRDE (Near Real Time Roaming Data Exchange) is CDR format exchange between operators for revenue assurance and fraud protection. It is also use ASN1 for data encoding. NRTRDE file consists of following parts:

File Level contain information about NRTRDE identification fields - Specification Version Number and Release Version Number, TADIG codes of sender and receiver, sequence number, File Available Timestamp, Call Events Count.

Call Detail Level supports MO and MT calls, GPRS

According to TD.106, NRTRDE records are delivered to home network within 4 hours from end call time. If there are problems on visitor network to provide NRTRDE records (operational problems, validation, re-rating, transfer via a MVNO, etc) than timescale is increased to 8 hours.

References:

1. Nick vs Networking [online]// An intro to GSMA TAP3 Files – Available - https://nickvsnetworking.com/an-intro-to-gsma-tap3-files/
2. GSMA [online]// Use of TAP for the Single IMSI Wholesale Billing Interface – Available - https://www.gsma.com/get-involved/working-groups/interoperability-data-specifications-and-settlement-group/standardised-b2b-interfaces-specified-by-ids/open-standards-specifications/tap3-open-standard-download-form
3. The MACH Blog [online]// Introducing TAP-NRTRDE Reconciliation– Available - https://machinsights.wordpress.com/2013/04/09/introducing-tap-nrtrde-reconciliation/
4. GSMA [online]// Use of NRTRDE for the Single IMSI Fraud Interface – Available - https://www.gsma.com/get-involved/working-groups/interoperability-data-specifications-and-settlement-group/standardised-b2b-interfaces-specified-by-ids/open-standards-specifications/tap3-open-standard-download-form

СЕКЦІЯ 3

Інформаційна безпека телекомунікаційних систем і мереж

ОГЛЯД СТАНДАРТІВ ЗАХИСТУ І ПРОТИДІЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО WI-FI МЕРЕЖ

Табор Денис Іванович
Державний університет інформаційно-комунікаційних технологій, м.Київ

Радіоканал передачі даних, який використовується у Wi-Fi мережах, потенційно схильний до втручання з метою порушення конфіденційності, цілісності й доступності інформації. Під час під'єднання до мережі передбачено аутентифікацію та шифрування, але ці елементи захисту мають свої вади.

Розгляньмо актуальні загрози інформації, яка циркулює в бездротовій мережі:

перехоплення й порушення цілісності конфіденційної інформації, яка передається бездротовими мережами. Зловмисник, який перебуває в зоні дії точок доступу, може перехоплювати радіосигнал, розшифровувати й ретранслювати дані, водночас залишаючись майже непоміченим. Використання антен і підсилювачів дає змогу зловмисникові перебувати на значному віддаленні від цілі в процесі перехоплення;

порушення доступності інформації, яка циркулює в бездротових мережах. Інформація може бути обмежена як перешкодами в каналі зв'язку, так і атаками зловмисників, які спрямовані на вузли бездротової мережі.

Є також і загрози інформації, яка зберігається на вузлах абонентів бездротової мережі:

ідентифікаційні дані абонентів бездротової мережі можуть бути як перехоплені під час пересилання по бездротовій мережі, так і отримані зловмисником під час отримання доступу до мобільного станції. Ці дані можуть бути використані для під'єднання до бездротової мережі від імені легального користувача;

несанкціонований доступ до інформації, що зберігається локально на вузлах мережі, може бути отримано завдяки неправильним налаштуванням безпеки абонента бездротової мережі.

Початковий стандарт шифрування WEP (Wired Equivalent Privacy) був дискредитований через вразливості в алгоритмі розподілу ключів RC4 (Rivest Cipher 4). У 2003 році створено стандарт WPA (Wi-Fi Protected Access). Стандарт WPA використовує протокол цілісності тимчасових ключів TKIP (Temporal Key Integrity Protocol). Також у ньому використовується метод контрольної суми MIC (Message Integrity Code), який дає змогу перевіряти цілісність пакетів. У 2004 році створено стандарт WPA2, який являє собою поліпшений WPA. Основна відмінність між WPA і WPA2 полягає в технології шифрування, який поєднує симетричний алгоритм блочного шифрування AES (Advanced Encryption Standart) та TKIP. WPA2 забезпечує більш високий рівень захисту мережі, оскільки TKIP дає змогу створювати ключі завдовжки до 128 біт, а AES – до 256 бітів. Нині алгоритм WPA2 є найбільш поширеним алгоритмом захисту бездротових мереж.

У 2017 році було розкрито інформацію про критичні проблеми програми сертифікації бездротового зав'язку WPA2, які дають можливість обійти захист і, як наслідок, прослуховувати трафік Wi-Fi, який курсує між точкою доступу і користувачем. Комплекс вразливостей у WPA2, який отримав назву KRACK (Key Reinstallation Attacks), було виявлено зведеною групою дослідників із різних університетів і компаній.

У 2018 році створено новий стандарт безпеки – WPA3. Творці WPA3 спробували усунути концептуальні недоробки, які випливли з появою атаки KRACK. Оскільки ключова вразливість ховалася в чотирьохелементному рукостисканні, у стандарт WPA3 додалася

обов'язкова підтримка більш надійного методу з'єднання – SEA (Simultaneous Authentication of Equals), також відомого як Dragonfly. Технологія SEA основана на протоколі обміну ключами Діффі–Геллмана з використанням кінцевих циклічних груп. SEA надає інтерактивний метод, відповідно до якого дві й більше сторін встановлюють криптографічні ключі, що засновані на знанні пароля однією або декількома сторонами. Результуючий ключ сесії, який отримує кожна зі сторін для аутентифікації з'єднання, вибирається на основі інформації з пароля, ключів і MAC-адрес обох сторін. Якщо ключ однієї зі сторін виявиться скомпрометованим, це не спричинить компрометації ключа сесії. І навіть дізнавшись пароль, атакуючий не зможе розшифрувати пакети.

Стандарт WPA3 передбачає два режими роботи: WPA3-Personal і WPA3-Enterprise. WPA3- Personal забезпечує надійний захист, особливо якщо користувач задав стійкий пароль, який не можна отримати словниковим перебором. Але якщо пароль не зовсім тривіальний, то має допомогти нове обмеження на кількість спроб аутентифікації в межах одного рукостискання. WPA3- Enterprise забезпечує шифрування на основі 192-розрядних ключів.

Нині стандарт IEEE 802.11 також дає можливість під'єднання до мережі Wi-Fi за допомогою протоколу захисту OWE (Opportunistic Wireless Encryption). Протокол OWE забезпечує безпеку даних, які передаються по незахищеній мережі, шляхом їх шифрування. Водночас від користувачів не потрібно будь-яких додаткових дій і введення паролів для під'єднання до мережі. Атаки, які відбуваються у відкритій мережі, належать до пасивних. Коли до мережі під'єднується багато клієнтів, зловмисник може зібрати дуже багато даних, просто фільтруючи інформацію, яка проходить через нього. Протокол OWE використовує опортуністичне шифрування, щоб захищатися від пасивного підслуховування. Воно також запобігає атаці з внесенням пакетів, коли зловмисник намагається порушити роботу мережі, створюючи й передаючи особливі пакети даних, що видаються частиною нормальної роботи мережі.

Проте, незважаючи на переваги та усунуті вади, протокол WPA3 має і два типи вад, яких припустилися під час проєктування. Перший призводить до атак зі зниженням рейтингу, а другий – до витоків бічного кеша. Алгоритм кодування пароля в Dragonfly містить умовні гілки. Якщо зловмисник може визначити, яку гілку ланцюга «if-thenelse» було вилучено, він може дізнатися, чи було знайдено елемент пароля в конкретній ітерації цього алгоритму. В основі атаки по бічному каналу на основі синхронізації лежить атака на метод рукостискання Dragonfly. Цей метод використовує певні мультиплікативні групи, алгоритм кодування пароля використовує змінну кількість ітерацій для кодування пароля. Точна кількість ітерацій залежить від пароля, який використовується, і MAC-адреси точки доступу і клієнта. Зловмисник може виконати віддалену тимчасову атаку на алгоритм кодування пароля, щоби визначити, скільки ітерацій знадобилося для кодування пароля. Відновлена інформація може бути використана для виконання парольної атаки, яка схожа на автономну атаку за словником.

Насамперед атакам піддаються некоректно сконфігуровані пристрої, пристрої зі слабкими й не досить довгими ключами шифрування, а також пристрої, які використовують вразливі методи аутентифікації. Велика частина успішних зламів відбувається завдяки неправильним налаштуванням точок доступу та програмного забезпечення. Найбільш поширеними є два технічних сценарії атак на мережі Wi-Fi – це перехоплення пакетів, які пов'язані з аутентифікацією клієнта (рукостискання – handshake) з подальшим перебором пароля за словником, і створення підробленої точки доступу з паралельним проведенням атаки «відмови в обслуговуванні» на справжню точку доступу.

Найбільш поширена атака на мережу Wi-Fi, захищену протоколами WPA-PSK або WPA2- PSK, – це атака за словником. Протокол захисту WPA-PSK або WPA2-PSK використовує ключ попередньої сесії (PTK – Pairwise Transient Key), який, відповідно, складається з попереднього загального ключа (PSK – Pre-Shared Key) та п'яти інших параметрів, таких як SSID (символьна назва бездротової точки доступу Wi-Fi), Authenticator

Nounce (ANounce), Supplicant Nounce (SNounce), Authenticator MAC-address (MAC-адреса точки доступу) та Suppliant MAC-address (MAC-адреса wifi-клієнта). Цей ключ надалі використовує шифрування між точкою доступу та клієнтом. Зловмисник, який прослуховує ефір, може перехопити всі п'ять параметрів, окрім PSK. PSK отримується завдяки використанню парольної фрази WPA-PSK, яку відправляє користувач разом із SSID. Комбінація цих двох параметрів пересилається за стандартом формування ключа на основі пароля PBKDF2 (Password Based Key Derivation Function), який генерує 256-бітовий загальний ключ. У звичайній WPA-PSK/WPA2- PSK атаці за словником зловмисник може використовувати програмне забезпечення, яке виводить 256-бітний PSK для кожної парольної фрази й використовувати її з іншими параметрами, які було описано під час створення PTK. PTK буде використовуватися для перевірки контрольної суми (MIC – Message Integrity Check) в одному з пакетів handshake. Якщо вони збігатимуться, то парольна фраза в словнику буде правильною. Водночас використовуються вразливості протоколу аутентифікації користувачів – відкрито передачу ANounce, SNounce, MAC-адреси точки доступу і MAC-адреси WiFi-клієнта. Якщо під час відтворення алгоритму аутентифікації відбудеться успішна авторизація користувача, значить обраний зі словника пароль є істинним й атака призвела до успішного злому мережі.

Захист мережі за допомогою від'єднання відповіді на широкомовний запит ідентифікатора бездротової мережі ESSID (Extended Service Set Identification) і приховування назви мережі в службових пакетах Beacon frame є недостатнім, оскільки мережу все одно видно на певному радіоканалі та зловмисник чекає авторизованого під'єднання до мережі, адже водночас у незашифрованому вигляді передається ESSID. На цьому захисний захід втрачає сенс. Деякі системи безперервно розсилають ім'я мережі в ефір, намагаючись під'єднатися. Це також є цікавою атакою, оскільки в такому випадку можна «пересадити» користувача на свою точку доступу й отримувати всю інформацію, яку він передає по мережі.

Висновки

Отже, можна виділити основні рекомендації із забезпечення безпеки бездротових Wi-Fi мереж:

для забезпечення безпеки даних, які передаються по бездротовій мережі, необхідно використовувати шифрування WPA2/WPA3 зі стійким паролем;

не під'єднуватися до відкритих Wi-Fi мереж. Ці мережі можуть прослуховуватися або навіть повністю контролюватися зловмисниками. За нагальної потреби під'єднання до такої мережі необхідно використовувати VPN-з'єднання.

З огляду на вищевикладене для захисту Wi-Fi мереж потрібно впроваджувати комплексний підхід до забезпечення інформаційної безпеки.

Необхідно приділяти увагу підвищенню обізнаності співробітників у питаннях інформаційної безпеки та перекривати потенційні вектори атак на мережу. Впроваджувати безпечні методи аутентифікації з перевіркою сертифікатів, обмежувати доступ клієнтів гостьової мережі до локальної обчислювальної мережі, проводити регулярний аналіз захищеності бездротових мереж, виявляти й від'єднувати несанкціоновані точки доступу.

Список використаних джерел

Mathy Vanhoef, Key Reinstallion Attacks. Breaking WPA2 by forcing nonce reuse. URL: http:// www.krackattacks.com.

Mathy Vanhoef, Eyal Ronen, Dragonblood. Analysing WPA3's Dragonfly Handshake. URL: http:// wpa3.mathyvanhoef.com.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ (IOT) ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ: СУЧАСНІ ВИКЛИКИ ТА РІШЕННЯ

Кондратенко Данило Володимирович
Державний університет інформаційно-комунікаційних технологій
Науковий керівник: Полоневич О.В.,
кандидат економічних наук, доцент кафедри
Інженерії програмного забезпечення автоматизованих систем
Державного університету інформаційно-комунікаційних технологій,
м. Київ

Дослідження фокусується на методиках захисту інформації в мережах Інтернету речей (IoT) від несанкціонованого доступу. Підкреслюється зростання IoT-пристроїв і відповідна потреба в ефективних захисних стратегіях.

Постановка задачі

Розглядається швидкий розвиток IoT та його вплив на підвищення ризиків у сфері безпеки даних. Обговорюється зручність "розумних" пристроїв та їх взаємодія.

Мета дослідження

Визначено мету аналізу ефективності існуючих та потенційних методик захисту в IoT, з акцентом на протидію несанкціонованому доступу.

Результати дослідження

Було розглянуто фізичне та логічне проектування IoT мереж, роль протоколів на різних рівнях OSI, а також важливість TLS/SSL аутентифікації поверх MQTT.

Висновки та перспективи

Підкреслюється необхідність індивідуального та комплексного підходу до забезпечення безпеки в IoT. Обговорюються потенційні ризики та стратегії їх мінімізації.

Список використаних джерел

1. “How the internet of things can help create a better new normal” – Режим доступу до ресурсу: https://www.wired.co.uk/article/bc/vodafone-iot
2. “IoT Architecture: the Pathway from Physical Signals to Business Decisions” – Режим доступу до ресурсу: https://www.altexsoft.com/blog/iotarchitecture-layers-components/
3. “Internet of Things: security and privacy implications” – Режим доступу до ресурсу: https://www.researchgate.net/publication/275228804_Internet_of_Things_security _and_privacy_implications
4. “Privacy” – Режим доступу до ресурсу: https://www.gsma.com/aboutus/legal/privacy

РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ БЕЗПЕКИ НА ОСНОВІ МЕРЕЖ СТІЛЬНИКОВОГО ЗВ’ЯЗКУ

Титарчук Назар Олегович,
Федчук Володимир Сергійович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

З ростом використання мобільних телефонів та розвитком технологій стільникового зв'язку, питання безпеки стає все важливішим. Розробка ефективної методики для підвищення безпеки в мережах стільникового зв'язку є критичним завданням. У цій статті розглянемо ключові кроки для створення такої методики

1. Аналіз загроз та вразливостей:

Перший етап - це ретельний аналіз можливих загроз та вразливостей у мережах стільникового зв'язку. Це включає в себе аналіз можливих атак, перехоплення зв'язку, аутентифікаційні проблеми та інші ризики.

2. Розробка системи аутентифікації та авторизації:

Створення ефективної системи аутентифікації та авторизації є ключовим елементом безпеки. Використання сучасних методів, таких як біометричні дані та двофакторна аутентифікація, може значно підвищити рівень захисту.

3. Захист зв'язку та данних:

Забезпечення шифрування зв'язку та захисту особистих даних є важливим аспектом. Використання протоколів шифрування та застосування технологій VPN може допомогти уникнути перехоплення та несанкціонованого доступу до інформації.

4. Моніторинг та виявлення аномалій:

Розробка системи моніторингу, яка виявляє аномалії та потенційні загрози, є необхідною. Використання алгоритмів машинного навчання для аналізу поведінки користувачів та виявлення невідомих загроз може значно покращити ефективність моніторингу.

5. Захист від атак типу DDoS:

Атаки типу DDoS можуть стати серйозною загрозою для мереж стільникового зв'язку. Розробка захисних механізмів та системи виявлення DDoS-атак є важливою для забезпечення доступності мережі.

6. Забезпечення фізичної безпеки обладнання:

Фізична безпека обладнання та інфраструктури грає важливу роль. Захисні заходи, такі як контроль доступу до серверних приміщень та застосування технологій відеоспостереження, можуть допомогти уникнути фізичних атак.

7. Навчання та свідомість користувачів:

Важливою частиною методики є навчання та підвищення свідомості користувачів. Інструкції з безпеки, навчання виявлення підозрілих ситуацій та коректного використання безпечних методів взаємодії з мережею.

8. Розробка плану відновлення після інциденту:

Необхідно розробити план відновлення, який включає в себе процедури відновлення після інциденту. Це дозволить ефективно відреагувати на можливі загрози та відновити нормальну роботу системи.

9. Співпраця з безпековими організаціями:

Залучення до співпраці з безпековими організаціями та використання їхніх ресурсів та знань може допомогти у забезпеченні найвищого рівня безпеки.

10. Регулярні аудити та оновлення:

Проведення регулярних аудитів безпеки та оновлення заходів захисту є важливим етапом. Технології швидко розвиваються, і важливо відстежувати нові загрози та застосовувати відповідні вдосконалення.

Методика підвищення безпеки мереж стільникового зв'язку вимагає комплексного підходу та постійного вдосконалення. Із залученням нових технологій та експертних знань можна створити надійну та стійку систему, яка відповідає найвищим стандартам безпеки в сфері стільникового зв'язку.

ЛІТЕРАТУРА

1.Лазоренко Л.В. Аналіз ринку мобільного зв’язку України та напрямки його розвитку – 2017.
2.Усик С. П. Аналіз послуг мобільного зв’язку на ринку України. – 2013.

МЕТОДИ ДОСЛІДЖЕННЯ ЗАХИСТУ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

Ковальов Олександр Євгенович,
Римар Дмитрій Борисович
Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут телекомунікацій
м. Київ

З розвитком сучасних телекомунікаційних та мережевих технологій виникає необхідність в дослідженні та захисті мультисервісних мереж, що об'єднують різні види послуг у єдиному середовищі. У цій статті ми розглянемо методи дослідження захисту мультисервісних мереж для забезпечення конфіденційності, цілісності та доступності послуг.

1. Аналіз Загроз та Визначення Вразливостей:

Перший крок у дослідженні захисту мультисервісних мереж - аналіз потенційних загроз та визначення вразливостей. Це може включати в себе аналіз можливостей атак, перехоплення даних, введення даних та інші ризики.

2. Використання Шифрування для Захисту Даних:

Важливим аспектом захисту є використання шифрування для конфіденційності даних. Введення шифрування на різних рівнях мережі, включаючи рівень транспортного та рівень даних, допомагає уникнути неправомірного доступу.

3. Розробка Політик Аутентифікації та Авторизації:

Створення ефективних політик аутентифікації та авторизації є важливим етапом в захисті мультисервісних мереж. Використання двофакторної аутентифікації та строгих політик керування доступом допомагає зменшити ризик несанкціонованого доступу.

4. Захист Від Атак Типу DDoS:

Атаки типу DDoS можуть спричинити серйозні перебої у роботі мультисервісних мереж. Розробка та впровадження механізмів виявлення та захисту від DDoS-атак є критичним елементом.

5. Використання Вогневих Стін та Інтранет-Гейтвеїв:

Застосування вогневих стін та інтранет-гейтвеїв допомагає контролювати та фільтрувати трафік, що проходить через мережу. Це дозволяє виявляти та блокувати неправомірний трафік.

6. Вдосконалення Процесів Виявлення Інцидентів:

Розробка ефективних систем виявлення інцидентів дозволяє оперативно реагувати на потенційні загрози та забезпечує реальний час в разі атаки.

7. Впровадження Технологій Blockchain для Забезпечення Цілісності Даних:

Використання технології блокчейн може бути корисним для забезпечення цілісності даних у мультисервісних мережах. Це особливо важливо для послуг, де важлива конфіденційність та точність інформації.

8. Використання Технологій SDN та NFV для Гнучкості та Захисту:

Впровадження Software-Defined Networking (SDN) та Network Functions Virtualization (NFV) дозволяє створювати гнучкі та легко налаштовувані мережі, а також забезпечує можливості швидкого реагування на нові загрози та атаки.

9. Тестування Відновлення Після Інциденту:

Проведення тестів відновлення після інциденту допомагає переконатися в ефективності заходів захисту та забезпечити швидке відновлення роботи мережі після атаки чи неполадок.

10. Навчання та Підвищення Кваліфікації Персоналу:

Організація регулярних тренінгів та підвищення кваліфікації персоналу є важливим елементом захисту мультисервісних мереж. Інформований та навчений персонал може більш ефективно реагувати на потенційні загрози.

Методи дослідження захисту мультисервісних мереж є важливими для забезпечення безпеки та стійкості сучасних телекомунікаційних систем. Комбінування технологій та розуміння внутрішніх та зовнішніх загроз допомагає створювати ефективні та надійні мережі, які відповідають вимогам сучасного інформаційного суспільства.

ЛІТЕРАТУРА

1. Заїка В.Ф., Варфоломеєва О.Г., Домрачева К.О., Гринкевич Г.О. “ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ НАСТУПНОГО ПОКОЛІННЯ” Київ – 2019 – 315с.

2.Олифер В.Г., Олифер Н.А. Компьютерние сети. Принципи, технологии, протоколи. 2-е издание. – СПб.:Питер, 2005. – 864с.

ЗМІСТ

СЕКЦІЯ 1
ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ