Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
кафедра радіотехнічних систем
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Математична модель ключів шифрування в мережах TETRA для телекомунікаційних систем

Виконав(ла): студент(ка) II курсу, групи РРм - 61
спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

_____ Трухан О.П.
(підпис) (прізвище та ініціали)

Керівник _____ Паляниця Ю.Б.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Хвостівська Л.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Дунець В.Л.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра радіотехнічних систем
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дунець В. Л.
(підпис) (прізвище та ініціали)
« » 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 172 Телекомунікація та радіотехніка
(шифр і назва спеціальності)

студенту Трухану Олександру Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Математична модель ключів шифрування в мережах TETRA для телекомунікаційних систем

Керівник роботи Паляниця Юрій Богданович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*29*» листопада 2024 року № 4/7-1145.

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Об'єкт дослідження: процес управління ключами я шифрування в телекомунікаційних мережах. Предмет дослідження: теоретичний аналіз, алгоритми генерації, розподілу та оновлення ключів шифрування у мережах TETRA.

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналітична частина
Основна частина
Науково - дослідна частина
Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Представлення
Актуальність теми
Розвиток та аналіз технологій методів управління ключами шифрування у мережах TETRA
Принцип роботи та аналіз запропонованого підходу
Наукова новизна
Загальні висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Зелінський І.М., доц. каф. ПВ		
Безпека танадзвичайних	Окіпний І.Б., зав. каф. МТ		
ситуаціях			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
	Отримання завдання		виконано
	Аналіз завдання		виконано
	Виконання розділу 1		виконано
	Виконання розділу 2		виконано
	Виконання розділу 3		виконано
	Виконання розділу 4		виконано
	Оформлення пояснювальної записки		виконано
	Оформлення графічного та презентаційного матеріалу		виконано
	Перевірка роботи на антиплагіат		виконано
	Попередній захист кваліфікаційної роботи		виконано
	Захист кваліфікаційної роботи		

Студент _____ Трухан О. П.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Паляниця Ю. Б.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Математична модель ключів шифрування в мережах TETRA для телекомунікаційних систем» // Кваліфікаційна робота // Трухан Олександр Петрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет прикладних інформаційних технологій та електроінженерії, група РАм - 61 // Тернопіль, 2024 // с. – , Рисунок – , табл. – , додат. – , бібліогр. – .

Ключові слова: МЕРЕЖІ TETRA, E2EE, УПРАВЛІННЯ КЛЮЧАМИ, ГЕНЕРАЦІЯ КЛЮЧІВ, РОЗПОДІЛ КЛЮЧІВ.

У кваліфікаційній роботі мережі TETRA розглядаються як критично важлива технологія для забезпечення надійного та безпечного зв’язку. Проаналізовано управління ключами шифрування, їх генерацію, розподіл та зберігання. Вивчено існуючі підходи до шифрування, такі як алгоритм AES-256 (Розширений стандарт шифрування), із визначенням переваг і недоліків. Запропоновано перспективні рішення для розподілених систем управління ключами та адаптивних алгоритмів шифрування, спрямованих на підвищення ефективності та безпеки мереж TETRA.

ANNOTATION

Title of the qualification thesis: "Mathematical Model of Encryption Keys in TETRA Networks for Telecommunications Systems" // Qualification thesis // Trukhan Oleksandr Petrovych // Ternopil Ivan Puluj National Technical University, Faculty of Applied Information Technologies and Electrical Engineering, group RAm - 61 // Ternopil, 2024 // p. – , fig. – , table – , append. – , bibliogr. – .

Keywords: TETRA NETWORKS, END-TO-END ENCRYPTION (E2EE), KEY MANAGEMENT, KEY GENERATION, KEY DESTRIBITION.

The qualification work considers TETRA networks as a critical technology for ensuring reliable and secure communication. Encryption key management, including their generation, distribution, and storage, is analyzed. Existing encryption approaches, such as the AES-256 algorithm (Advanced Encryption Standard), are examined with an identification of their advantages and disadvantages. Prospective solutions for distributed key management systems and adaptive encryption algorithms are proposed to enhance the efficiency and security of TETRA networks.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасні телекомунікаційні мережі, такі як TETRA (Terrestrial Trunked Radio), відіграють ключову роль у забезпеченні надійного та безпечного зв’язку в критично важливих галузях, таких як громадська безпека, транспорт та енергетика. Постійне зростання загроз кібербезпеки вимагає нових підходів до захисту інформації, зокрема через удосконалення механізмів шифрування та управління ключами. Мережі TETRA, які широко використовуються у службових комунікаціях, повинні забезпечувати не лише високу швидкість та якість зв’язку, але й надійний захист переданих даних.

Розробка математичних моделей, які дозволяють оптимізувати управління ключами шифрування в таких мережах, є важливим кроком до підвищення їх ефективності та безпеки. Це дослідження спрямоване на вирішення цих завдань, враховуючи актуальність захисту інформації у світі зростаючого обсягу даних і ризиків.

Метою роботи є розробка математичної моделі управління ключами шифрування для мереж TETRA, яка забезпечує високий рівень безпеки, ефективність обробки даних та стійкість до сучасних кіберзагроз.

Завдання дослідження:

1. Дослідити сучасні методи управління ключами шифрування у мережах TETRA, включаючи генерацію, розподіл і зберігання ключів
2. Розробити та проаналізувати модель управління ключами шифрування для забезпечення адаптивності та стійкості до кіберзагроз.
3. Розрахувати оптимальні параметри системи розподілу ключів з урахуванням реальних умов роботи мереж TETRA.
4. Провести комп’ютерне моделювання для оцінки ефективності розробленої моделі, визначити її продуктивність.

Об’єкт дослідження: процес управління ключами шифрування в телекомунікаційних мережах.

Предмет дослідження: теоретичний аналіз, алгоритми генерації, розподілу та оновлення ключів шифрування у мережах TETRA.

Методи дослідження. Для досягнення поставленої мети використовувалися аналітичні методи для вивчення існуючих рішень у сфері шифрування, методи математичного моделювання для розробки оптимальної моделі управління ключами, а також комп'ютерне моделювання для тестування її ефективності.

Наукова новизна. Наукова новизна роботи полягає у розробці моделі управління ключами шифрування для мереж TETRA, що впроваджує адаптивні алгоритми шифрування. Це забезпечує підвищену стійкість системи до сучасних кіберзагроз, підвищення швидкості обробки даних та можливість динамічного управління ключами в умовах високого навантаження.

Практичне значення здобутих результатів. Результати роботи можуть бути використані для вдосконалення існуючих систем шифрування в мережах TETRA, що дозволить підвищити їх захищеність, знизити затримки у передачі даних та забезпечити адаптивність мережі до змін у навантаженні. Це має значний практичний потенціал для впровадження в організаціях, які використовують мережі TETRA для забезпечення критично важливого зв'язку.

Публікації. Описані в збірнику «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ»

Структура роботи. Робота складається з пояснювальної записки. Пояснювальна записка складається із вступу, чотирьох розділів, висновків, списку використаних джерел, та додатку. Обсяг роботи: пояснювальна записка – аркушів формату А4.

РОЗДІЛ 1

АНАЛІТИЧНА ЧАСТИНА

1.1 Що таке TETRA

Наземне транкінгове радіо є стандартом, визначеним Європейським інститутом телекомунікаційних стандартів, який є організацією, відповідальною за публікацію телекомунікаційних стандартів для обов'язкового використання в Європі.

За даними SELEX Communications (2007), TETRA є першим справді цифровим стандартом PMP. До TETRA використовуваний стандарт називався MPT1327, однак цей стандарт був аналоговим і не мав усіх характеристик цифрового зв'язку.

Попри те, що TETRA була створена ETSI, вона отримала схвалення в усьому світі та використовується в багатьох інших частинах світу за межами Європи, де вона не є обов'язковою, але була прийнята для мереж зв'язку в надзвичайних ситуаціях і безпеки.

TETPA можна розглядати як окремий рівень над загальною технологією PMR, додаючи послуги, спеціально розроблені для організацій громадської безпеки.

Як зазначає ETSI (2016), у стандарті TETRA є унікальні служби PMR, такі як:

- швидкий доступ до викликів і мінімізація затримок: швидкий доступ до дзвінків зазвичай здійснюється за допомогою кнопки «Натисни і розмовляй» (PTT), яка забезпечує пряме з’єднання з попередньо вибраною розмовною групою.
- прямий режим роботи (DMO): мобільні станції PMR можуть працювати безпосередньо одна з одною (враховуючи той факт, що вони знаходяться на певній відстані) без потреби в базовій станції.
- шифрування високого рівня (повітряний інтерфейс і E2EE з різними алгоритмами)
- пріоритетні виклики: користувач може, наприклад, здійснити екстрений виклик, який може зайняти ресурси мережі, які вже
- використовуються менш важливим викликом.

- високошвидкісна передача даних за допомогою TETRA Enhanced Data Services
- TETRA використовує множинний доступ із тимчасовим розподілом (TDMA) для розподілу ресурсів у радіоінтерфейсі (AI), кожен TBS працює з одним основним каналом керування (MCCH), який відповідає за керування сигналізацією, тоді як канали трафіку (TCH) передають голос або дані відповідно.

У TETRA TBS може бути відповідно налаштований із попередньо визначеною кількістю вторинних каналів керування (SCCH), які служать допоміжними каналами для MCCH у разі високого трафіку сигналізації на цьому конкретному TBS.

Зараз TETRA переживає трансформацію від суто цифрового PMR до гібридного зв'язку завдяки новому спектру доступних технологій (таких як LTE), які не підтримують специфічні вимоги TETRA, але при використанні з TETRA комбінація дозволяє вища пропускна здатність даних, водночас використовуючи особливі переваги TETRA, такі як груповий і екстрений зв'язок.

1.1.1 Системи TETRA

Як описано Secure Land Communications (2015), продукти TETRA варіюються від інфраструктури, що включає комутатори/обмінники трафіку та базові станції, через апаратне забезпечення кінцевого користувача, наприклад портативні радіостанції та диспетчерські робочі станції, аж до програмних додатків, таких як пакети для керування радіозв'язком. абонентів або для перегляду відстеження в реальному часі радіостанцій, розміщених у полі.

SLC розробляє, тестує, розгортає та обслуговує основні апаратні та програмні продукти TETRA, такі як обмінники та базові станції. Інші менші продукти також розробляються та тестуються, такі як TETRA Connectivity Server (TCS), який служить інтерфейсом між системою TETRA та додатками сторонніх розробників шляхом реалізації інтерфейсу прикладного програмування (API), здатного отримувати та передавати команди для взаємодії між третіми сторонами. вечірнє обладнання та магістраль TETRA.

Для проєкту, пов'язаного з цією дисертацією, я зосередився лише на дуже невеликій частині системи, тобто розподілі ключів для шифрування трафіку

голосових повідомлень і коротких даних; цей трафік розподіляється через мережу за допомогою протоколу під назвою Over The Air Keying (OTAK). У реалізації SLC основою наскрізного шифрування OTAK є Key Management Facility (KMF); Функція цього KMF полягає в тому, щоб відстежувати у своїй базі даних ключі для шифрування зв'язку та координувати їх використання, завантажуючи їх по повітрю в TP, які були зареєстровані в ньому та які підтримують доставлення ключів шифрування по повітрю..

Для нашого конкретного випадку варто зауважити, що ядро рішення, створеного цим проєктом наскрізного шифрування, KMF, діє як стороння програма для досягнення з'єднання з мережею TETRA через TCS API для доставлення ключів шифрування та іншої сигналізації.

1.2 Інтеграція та перевірка

«Інтеграція - це процес об'єднання всіх тестованих модулів програми в повну систему». (Бішоп, 2008, стор. 322).

Те, що Бішоп (2008) описав у цьому реченні своєї книги, є саме тим, що ми зробили в цьому проєкті.

У нашому випадку через великий перелік підсистем, залучених у рішенні E2EE, інтеграція та верифікація розділені на різні області, тестовані в географічно окремих місцях. У нашій перевірці системи, ці одиниці: DXT, TBS, TH1n (TETRA Radio) і KMF. Інші пристрої, такі як диспетчерські додатки або SCT (додаток для програмування смарт - карт).

Основна мета наших тестів полягає в тому, щоб після інтеграції переконатися, що 4 призначені нам блоки працюють належним чином, не втручаючись один у роботу іншого. Крім того, наші тести зосереджені саме на перевірці впливу рішення E2EE, що використовує OTAK, на ШІ.

1.3. Симетричне шифрування

Існує два типи методів шифрування: симетричні та асиметричні. Для наших цілей ми зосереджуємось на симетричному шифруванні, оскільки рішення цього проєкту на основі систем TETRA використовує симетричне шифрування для шифрування/дешифрування голосових викликів між користувачами.

Однак ми повинні знати, що симетричне шифрування використовує лише один ключ для шифрування та Дешифрування даних, що спрощує його роботу, однак проблема полягає в тому, щоб розподілити ключі на всі вузли безпечним способом, тому рішення КМЕ було створено.

Як зазначали Столлінгс і Браун (2008), симетрична система шифрування складається з п'яти компонентів:

- у нас є відкритий текст, який є нашим оригінальним повідомленням, яке можна читати чітко
- також у нас є секретний ключ, який використовується алгоритмом шифрування для створення
- зашифрований текст, це не що інше, як транспозиція та перестановка відкритого тексту за допомогою
- алгоритм шифрування, цей визначає лише основи виконання перестановок і транспозицій, але точні операції вказує секретний ключ.
- п'ятий елемент, алгоритм дешифрування, є не що інше, як алгоритм шифрування, який виконується у зворотному порядку.

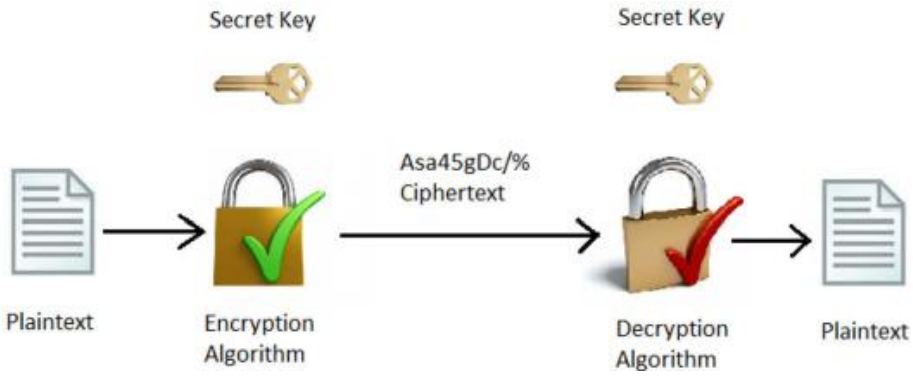

Рис. 1.1. Ілюстрація 5 елементів у зашифрованому зв’язку

1.4 Загальні концепції безпеки в системах TETRA

Системи TETRA багаті функціями безпеки, згідно з Airbus Defence and Space Фінляндії (2015, d), існує, загалом, 5 сфер, де безпека так чи інакше може бути помітна в мережах TETRA.

Область перша: автентифікація.

Якщо мережа налаштована на автентифікацію, даний користувач повинен увійти в мережу, виконавши механізм автентифікації, незалежно від типу пристрою, який він використовує (TR або диспетчерська станція).

Область друга: функції безпеки.

Можна вжити кілька заходів для забезпечення безпеки з погляду зору роботи. Такими заходами можуть бути, наприклад, прослуховування навколишнього середовища для сценаріїв, пов'язаних із захопленням заручників, вимкнення/увімкнення функцій у разі викрадення TR, обмеження прав диспетчерів, щоб вони могли використовувати лише певні функції або запис дзвінків для аудиту та законного перехоплення.

Область третя: захист нашого трафіку від сторонніх.

Проти цієї проблеми можна вжити три заходи. Першим і найважливішим заходом захисту трафіку є наскрізне шифрування, яке забезпечує безпеку від однієї кінцевої точки системи до іншої, і є предметом цієї дипломної роботи. Другим заходом є шифрування радіоканалів між TR і TBS. І третім заходом є захист зв'язків між DXT і TBS за допомогою IPsec (не розглядається в цій дипломній роботі).

Область четверта: менеджмент.

Безпека в мережі також стосується її керування. У реалізації SLC систем TETRA пристроями можна керувати віддалено за допомогою захищених з'єднань (SSH і SFTP), а дії користувачів також можна реєструвати на сервері аудиту.

Область п'ята: відмова в обслуговуванні.

Попри те, що це не призводить до викрадення даних, це призведе до катастрофи, якщо це буде виконано, щоб протистояти цьому, базові станції підготовлені з методами виявлення перешкод, щоб уникнути цієї проблеми.

Далі в цій роботі я поясню автентифікацію та розрізню типи шифрування трохи детальніше.

1.5 Аутентифікація

Хоч те, що автентифікація не є функцією, яка буде модифікована та/або протестована під час цього проекту, короткий огляд її необхідний, щоб мати загальні знання про функції безпеки, доступні в мережах TETRA, особливо тому, що ця функція вже використовується в мережі наших клієнтів.

Як описано у фінському Cassidian (2013), «Автентифікація - це функція, яка дозволяє інфраструктурі перевірити, чи мобільний абонент або користувач робочої станції дійсний для роботи в системі».

У документі Cassidian (2013) з Фінляндії вказано типи автентифікації, що використовуються в системах TETRA, ми можемо узагальнити їх як 3 типи: автентифікація мобільного абонента, автентифікація користувача робочої станції та розповсюдження ключа автентифікації.

Для зручності та тому, що це найбільш відповідний тип автентифікації для наших цілей, я коротко опишу автентифікацію мобільного абонента.

У системах SLC аутентифікація мобільного абонента є взаємною, тобто спочатку мобільний абонент повинен пройти аутентифікацію в мережі, а потім мобільний абонент запитує мережу про аутентифікацію також. Це вказано у Finnish Cassidian (2013, сторінка 15) разом із процедурою автентифікації, яка пояснюється нижче.

У спрощеному вигляді процедура автентифікації виглядає наступним чином:

- мобільний абонент реєструється в мережі та надсилає оновлену інформацію про розташування.
- мережа надсилає абоненту запит на основі 3 факторів: алгоритм аутентифікації, випадкові числа та ключ аутентифікації.
- мобільний абонент розраховує відповідь на виклик на основі ключа аутентифікації, попередньо збереженого на його SIM - карті, і надсилає його назад у мережу.

- коли мережа перевіряє відповідь абонента, вона дозволяє йому доступ до мережі.

Щоб це сталося, специфічні дані абонента (ключ автентифікації та індивідуальний ідентифікатор абонента Tetra) повинні бути заздалегідь запрограмовані або надіслані абоненту мобільного зв'язку безпечним способом, вони зберігаються в обладнанні абонента мобільного зв'язку (або на SIM - картці, або в радіоприймачі). себе).

Третій елемент необхідний під час автентифікації: алгоритм автентифікації, однак, може бути доставлений мережею, коли він забезпечує виклик, на який повинен відповісти мобільний абонент.

1.6 Концепція crypto Group

У системах TETRA Crypto Group (CG) - це об'єкт, який підтримує зв'язок між ключами шифрування трафіку і діапазоном номерів абонентів у мережі.

У системах TETRA все радіообладнання налаштовано за допомогою індивідуального короткого ідентифікатора абонента (ISSI), який є особистим телефонним номером цього радіо; ці ISSI потім призначаються групі користувачів (UG), яка є мостом між ISSI та CG. Якщо UG має діапазон ISSI, йому також можна призначити діапазон CG, і TEK, що містяться в цих CG, буде доставлено до діапазону ISSI.

Це поняття трохи важко зрозуміти лише словами, щоб зробити його більш зрозумілим; Я наводжу приклад цього механізму на рисунку 1.2.

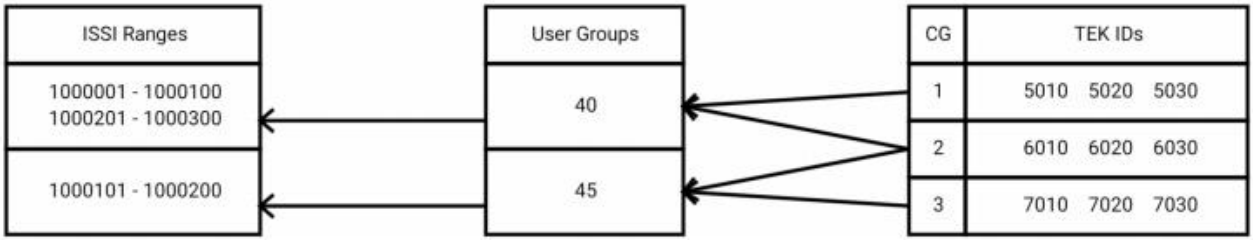

Рис. 1.2. Ілюстрація 5 елементів у зашифрованому зв’язку

У прикладі, представленому на рисунку 1.2, ми можемо побачити 3 криптогрупи, які містять 3 ключі шифрування трафіку відповідно, які можуть використовуватися будь - яким TETRA Radio для шифрування свого трафіку; однак існує потреба призначити ці ТЕК певним радіостанціям TETRA, щоб домовитися про те, хто має використовувати які ключі.

У центрі ми бачимо UG 40, який зіставлено з діапазонами ISSI від 1000001 до 1000100 і від 1000201 до 1000300; цю групу користувачів також зіставлено з CG 1 і 2. Завдяки цьому відображенню ми призначили згадані діапазони ISSI ідентифікаторам ТЕК з CG 1 і 2.

Те ж саме відбувається з UG 45, з одного боку, він зіставляється з діапазоном ISSI від 1000101 до 1000200, а з іншого - з CG 3, тому радіостанції TETRA в діапазоні від 1000101 до 1000200 можуть використовувати ТЕК з ID 7010, 7020 і 7030.

Такий механізм відображення корисний, оскільки ми можемо розділити діапазони ISSI на різні частини та призначити їх окремо для різних UG, як у нашому прикладі, коли діапазон ISSI, призначений UG 45, насправді є проміжним діапазоном між діапазонами, призначеними UG 40.

Крім того, розділивши ТЕК на CG, ми можемо переконатися, що TR отримають деякі ТЕК, які будуть використовуватися лише всередині певного діапазону (яким може бути, наприклад, організація, UG 40, що належить поліції, а UG 45 - пожежній частині).), а інші ТЕК спільно використовуються з іншими UG (які можна використовувати, наприклад, якщо є потреба у співпраці між відділами).

1.7 Розподіл ключів

«Якщо A і B мають зашифроване з'єднання зі сторонньою стороною C, C може доставити ключ за зашифрованими посиланнями до A і B». (Столлінгс і Браун, 2008, стор. 618).

KMF було створено, щоб бути надійним джерелом усіх мобільних (і немобільних) пристроїв у мережі, Механізм управління ключами (KMF) є центральним елементом системи зашифрованих з'єднань, він відповідає за підтримку всіх пристроїв, які

використовуються з E2EE, у робочому стані в мережі, шляхом надання їм Crypto Groups, які містять необхідні ключі для встановлення зв'язку з рештою дозволених пристроїв, усе це здійснюється через зашифроване з'єднання між KMF та одержувачами ключів. Система використовує різні ключі для різних цілей.

Ключі для наскрізного шифрування, як визначено стандартом TETRA, доставляються через повідомлення служби коротких даних (SDS), які використовуються як носій для протоколу OTAK у всіх системних рішеннях TETRA.

1.8 Повітряний інтерфейс і наскрізне шифрування

По суті, шифрування повітряного інтерфейсу - це шифрування, яке виконується між TBS і TR, воно не включає жодних інших частин мережі, тобто голос/дані вільно передаються по всій дротовій мережі між TBS, що надсилає, і приймає., з цієї причини необхідно впровадити E2EE. Наскрізне шифрування, на відміну від шифрування штучного інтелекту, шифрує голос/дані, оскільки вони залишають RT, що надсилає, і переміщуються в зашифрованому вигляді до місця призначення, лише тоді голос/дані розшифровуються для отримання.

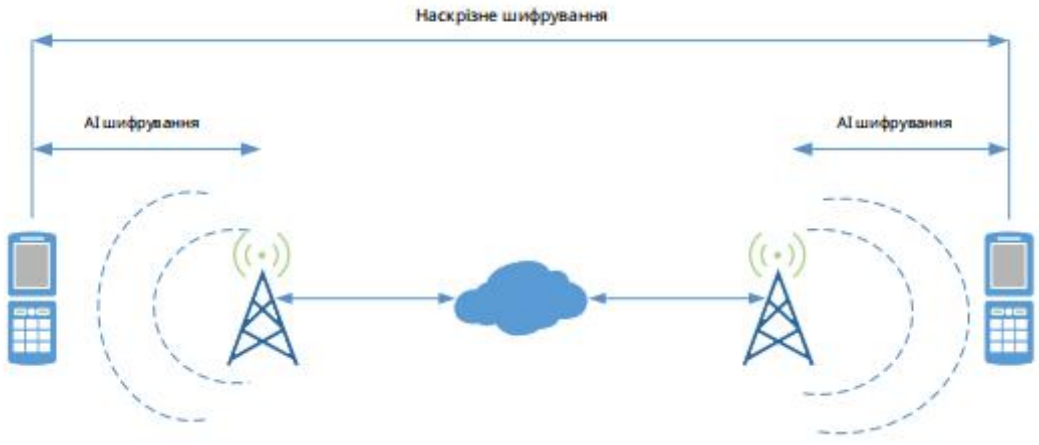

Рис. 1.3. Різниця між повітряним інтерфейсом і наскрізним шифруванням

Як пояснюється в Stallings and Brown (2008), E2EE не можна використовувати окремо, через те, що якщо всі дані зашифровані, проміжні комутатори не можуть бачити адресу призначення, з цієї причини в E2EE лише корисне навантаження

зашифровано, а заголовок залишається відкритим. Для подолання цієї слабкої сторони використовується шифрування повітряного інтерфейсу, яке шифрує весь пакет даних (заголовок і вже зашифроване корисне навантаження), які передаються через повітряний інтерфейс.

1.9 Висновки до розділу 1

У розділі описано основні принципи роботи мереж TETRA, їх переваги у порівнянні з аналоговими стандартами, функції безпеки, включаючи автентифікацію та шифрування. Продемонстровано глибоке розуміння основних механізмів управління ключами.

РОЗДІЛ 2
ОСНОВНА ЧАСТИНА

2.1. Критерії якості

Метою цього проекту, є надання зрілого рішення з прийнятною якістю, піклування про те, щоб не впливати на інші частини системи, одночасно вводячи нові функції, пов'язані 3 E2EE, і ефективно їх використовувати.

Це перша версія E2EE, розроблена SLC, яка використовує доставку ключів ОТАК для великих мереж, з цієї причини, і через обмеження бюджету та часу не очікується, що вона надасть повне рішення з усіма включеними функціями натомість, деякі функції управління були виключені, і зусилля були зосереджені в основному на експлуатаційних характеристиках, маючи на увазі, що більшість основних аспектів операцій повинні виконуватися з високою якістю, а інші незначні проблеми можна залишити позаду, якщо вони не впливають на операції, ці проблеми будуть вирішені в наступних версіях цього рішення.

2.2. Використані алгоритми

У проєкті планується впровадження 2 алгоритмів шифрування в приміщеннях замовника. По - перше, алгоритм Advanced Encryption Standard із довжиною ключа 256 бітів реалізовано як перехід від поточного стану безпеки мережі до E2EE з можливістю доставляння ОТАК, коли цей алгоритм буде використовуватися та працюватиме належним чином, алгоритм, розроблений спеціально для клієнта та викликаний для цієї мети алгоритм клієнта (CAlg) реалізовано, щоб налаштувати безпеку для цього конкретного клієнта.

2.3. Розширений стандарт шифрування (AES256)

За словами Столлінгса та Брауна (2008), AES - це симетричний алгоритм блочного шифрування з довжиною блоку 128 біт і підтримкою ключів до 256 біт. Як згадувалося у їхній книзі, Столлінгс і Браун стверджують, що симетричний алгоритм блокового шифрування створює вихідний блоковий шифр того самого розміру, що й блок відкритого тексту, прийнятий як вхідний, і всі вхідні блоки тексту мають фіксовану довжину.

Робота Алгоритму AES простими словами, як пояснено в Stallings and Brown (2008), виглядає наступним чином:

- відкритий текст розглядається як матриця байтів, ці байти беруться по 4 за один раз і поміщаються в масив під назвою «Стан», цей масив містить блок із 4 слів по 32 біти (для блоку з загальних 128 бітів). Потім змінюється кількома перетвореннями.
- перше перетворення це підставляння, для цього використовується таблиця під назвою S - box, для простоти ця таблиця не показана в цьому документі, однак ми повинні розглядати її як просту таблицю, яка відображає кожне шістнадцяткове значення в нове значення (яке є постійним для всіх підстановок).
- друге перетворення зсув рядків, проста перестановка виконується рядок за рядком.

Оскільки ми працюємо з матрицею, кожен рядок містить 4 слова по 8 бітів, тобто 32 біти на рядок, кількість пробілів, які байт зміщує вліво, залежить від позиції байта в матриці, докладне пояснення цієї операції виходить за рамки цієї дипломної роботи.

- наступне перетворення використовує рівняння над скінченними полями, і його метою є змішування стовпців, для цієї операції кожен стовпець працює окремо, і кожне значення кожного стовпця відображається на нове значення, яке є функцією всіх байтів у стовпці; для простоти точна операція тут описана не буде.
- останнім і найважливішим перетворенням є раунд, до якого ми додаємо наш секретний ключ. У цьому раунді ми просто виконуємо операцію XOR з поточним блоком даних і частиною нашого ключа.

Весь цей процес повторюється 9 раундів (ще 9 разів) і закінчується 10 тис.раунд. із 3 етапів (замість 4 етапів). Етапи одного раунду показано на Рис. 2.1:

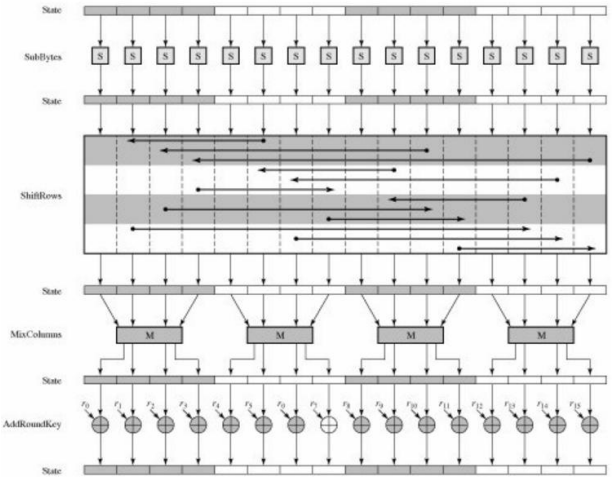

Рис. 2.1. Робота AES256. Взято зі Столлінгса та Брауна (2008)

2.4. Алгоритм клієнта (Calg)

У рамках рішення E2EE для кожного клієнта можна реалізувати індивідуальний алгоритм шифрування; цей алгоритм можна використовувати замість алгоритму AES256, який зазвичай використовується для шифрування у комунікаційних систем.

З міркувань безпеки налаштований алгоритм для клієнта, для якого розроблено це рішення, не відомий нікому за межами організації клієнта.

Спочатку рішення реалізовано за допомогою алгоритму AES256, а через певний період часу, коли рішення вже буде повністю запущено, буде розгорнуто клієнтський алгоритм, щоб замінити загальний алгоритм AES256.

Важливо зазначити, що клієнт може мати свій власний алгоритм, якщо він цього бажає.

2.5. Ключі шифрування, які використовуються в цьому рішенні

Ця робота зосереджується на дослідженні та описі Key Management Facility - нової функції, розробленої для управління ключами в системі шифрування.

Особливу увагу приділено ключам, що безпосередньо взаємодіють із цією функцією, з метою забезпечення їх ефективної інтеграції та функціонування у загальній архітектурі системи.

2.5.1. Ключі для зв'язку (ключ шифрування трафіку)

Згідно з Airbus Defense and Space Фінляндії, ключі, які використовуються для шифрування аудіо та SDS - повідомлень у їхніх системах, називаються ключами шифрування трафіку (TEK). Ці ключі використовуються для шифрування від одного кінця до іншого, дозволяючи, щоб передавати зашифровані дані через всю систему та бачити їх у чистому режимі лише в джерелі та пункті призначення.

У мережі клієнта буде відокремлено те, як генеруються та керуються TEK, це відокремлення буде залежати від організації, наприклад, якщо в країні, про яку йдеться, є кілька відділів, які використовують систему TETRA (пожежна служба, поліція, армія тощо).), їх можна розділити на організації, щоб тримати їх ізольованими одна від одної, і з цієї ж причини TEK генеруватимуться локально в організаціях, у яких вони використовуватимуться, тоді організації повинні будуть передати ключі до KMF поза смугою (OOB), щоб мати їх у базі даних KMF, щоб потім поширювати їх по повітрю серед призначених користувачів.

Загальна концепція генерації, управління та розподілу TEK виглядає так на рисунку 2.2.

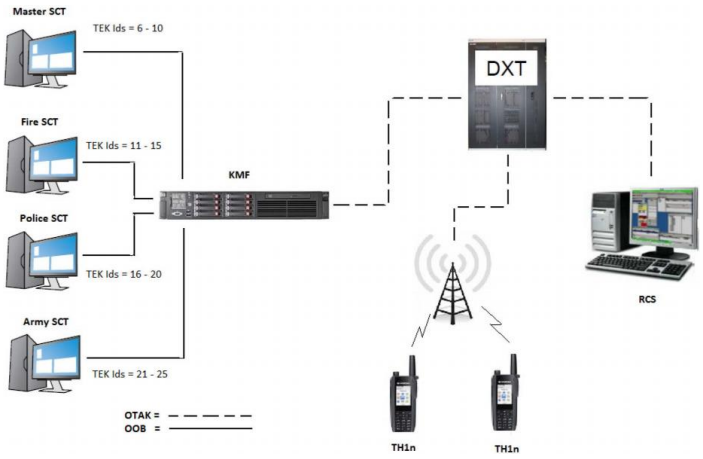

Рис. 2.2. Приклад розподілу TEK за організаціями

Кожен ключовий домен у нашому рішенні складається з 4550 ключів, і ідентифікатори ключів відповідно розподіляються між доменами, від найменшого до найбільшого. Наприклад, у доменах від 0 до 9 ідентифікатори, які містяться в кожному домені, виглядатимуть так:

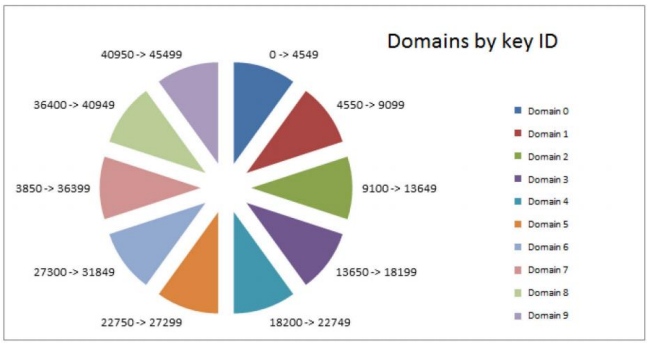

Рис. 2.3. – Приклад ідентифікаторів ключів у різних доменах

У випадку замовника вся організація поділена на відділи, і кожному відділу призначається набір ідентифікаторів домену для використання, отже, кожен відділ має власний унікальний набір ідентифікаторів ключів трафіку, таким чином кожен відділ вироблятиме та поширюватиме власні ключі для своїх користувачів, і ідентифікатори ключів не будуть збігатися. Єдиний випадок, коли один (або кілька) доменних ідентифікаторів використовується багатьма відділами, це коли мова йде про спілкування між відділами, наприклад, під час використання груп співпраці у випадку стихійного лиха (наприклад, урагану), користувачі з різних відділи повинні безпечно спілкуватися один з одним, і, отже, вони повинні мати спільні розмовні групи та ключі для шифрування спілкування в цих розмовних групах.

Одним із завдань інструменту Smart Card є створення ключів, будь то ключі керування чи ключі шифрування трафіку. Як показано на малюнку 2.2, у змодельованій ситуації існує 4 SCT, де 3 з них належать до певних відділів (пожежної служби, поліції та армії), ці SCT виробляють ключі шифрування, що належать їхній власній організації, які використовуються для внутрішнього відділу спілкування. На додаток до цих SCT, є 4 тисSCT під назвою Master SCT, роль цього

SCT полягає у створенні ключів, які будуть доставлені користувачам усіх відділів для забезпечення зв'язку між відділами.

2.5.2. Ключі для Tetra Radio (KEK, SEK)

Окрім ключів шифрування трафіку, у радіостанціях TETRA використовуються ще 2 ключі, ці ключі, які називаються ключами шифрування ключів (KEK) і ключами шифрування сигналів (SEK), використовуються лише для цілей керування. Вони не призначені для надсилання. по повітрю, і вони не шифрують голос або передачу даних.

Як пояснює фінська філія Airbus Defense and Space (2015), KEK і SEK використовуються для шифрування TEK, як показано на рисунку 2.4.

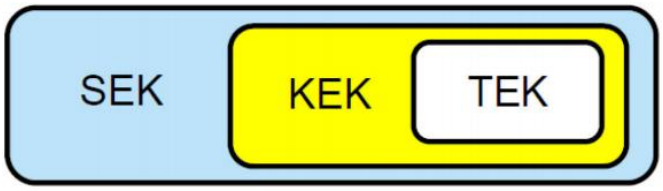

Рис. 2.4. Ключ шифрування трафіку, запечатаний ключами керування, взятий із Finnish Airbus Defense та Космос (2015)

Як ми бачимо на Рисунок 2.4, під час доставляння ключів шифрування по повітрю ключі, призначені для шифрування голосу та даних (TEK), спочатку шифруються дані в ключі керування під назвою Key Encryption Key, який має функцію encrypt keys (як говорить його назва), у нашому випадку він шифрує TEK. Весь цей пакет, сформований TEK і KEK, у свою чергу, запечатаний/зашифрований іншим ключем керування, який називається сигнальним ключем шифрування, як випливає з назви, SEK призначений для показу в інтерфейсі сигналізації системи.

Коли цей пакет сформовано, як описано вище, він надсилається через інфраструктуру комутації та керування (SwMI) і, нарешті, по повітрю до TR у формі повідомлення SDS.

На стороні TR KEK і SEK повинні бути заздалегідь запрограмовані в смарт - картку (SC), щоб термінал міг використовувати ці ключі для дешифрування

повідомлень ОТАК і відновлення ТЕК, що міститься в них; це означає, що для доставки ключів керування (KEK/SEK) вручну як до TR, так і до КМГ необхідно виконувати позасмугові операції.

Смарт - карти, які наразі використовуються радіотерміналами в мережі наших клієнтів, не підтримують обмін повідомленнями ОТАК, і всі SC абонентів повинні бути змінені, щоб запровадити прошивку, що підтримує ОТАК, з цієї причини зручно ініціалізувати та завантажити нові SC. з їх відповідними KEK/SEK одночасно. У плані міграції розглядається це питання, і наразі планується масове програмування SCs перед їх доставкою користувачам.

Інфраструктура відкритих ключів не існує в мережах TETRA, оскільки мережі TETRA розроблені таким чином, щоб бути максимально захищеними, і більшість інфраструктур Інтернету (наприклад, сервери відкритих ключів) не використовуються; 3 цієї причини наша система є симетричною системою шифрування і потребує використання позасмугових операцій для доставки ключів керування, які пізніше використовуються для шифрування ТЕК; це пов'язано з бажанням клієнта не Використовувати публічні методи.

2.5.3. Ключі для KMF (FEK, BEK, IEK)

Крім згаданих раніше ключів, у цьому рішенні використовуються інші ключі шифрування, які не призначені для використання в цілях ОТАК, а замість цього для цілей Out Of Band (OOB), ці такі ключі, які називаються ключами шифрування файлів, ключами резервного шифрування і внутрішній ключ шифрування використовуються здебільшого всередині KMF, за винятком FEK, який використовується в усьому некінцевому обладнанні (SCT, KSCC, КМЕ), коли ТЕК транспортуються ООВ з одного місця в інше.

FEK

Ключ шифрування файлів, який є найважливішим з усіх цих 3 ключів, використовується для шифрування всього, що потрібно перемістити з одного комп'ютера на інший.

Найпоширенішим використанням цього ключа є шифрування TEK для транспортування між SCT і KME; наприклад, у випадку, коли ми маємо головний SCT, який створює TEK для використання різними організаціями, а отже, різними KME.

На Рисунок 2.5 показано головний SCT, який відповідає за генерацію ключів для 2 KMF, кожен з яких відповідає різним відділам; у нашому прикладі один KMF обслуговує мережу, яку використовує поліція, а інший - мережу, яку використовує пожежна служба. Ці 2 мережі зазвичай працюють ізольовано одна від одної; однак у разі критичної ситуації, наприклад великої аварії чи стихійного лиха, обидва відділи мають спілкуватися один з одним. KMF, які використовуються в кожній мережі, зазвичай генерують ключі для своїх власних груп розмови, але ключі для спільних груп розмови між цими мережами не можуть бути згенеровані жодною з цих KMF, оскільки вони повинні бути спільними. З міркувань безпеки офіцер безпеки генерував би ключі спільних груп і розповсюджував їх OOB до KMF. У цьому процесі FEK використовувався 6 для запечатування файлів, що транспортуються OOB від Maser SCT до KMF.

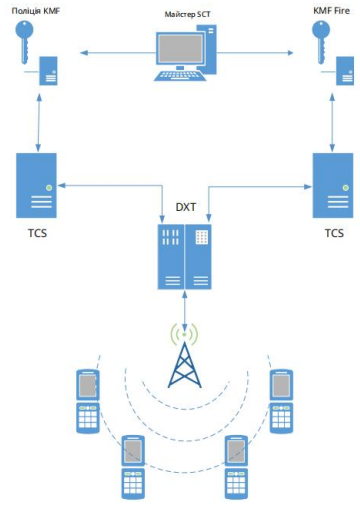

Рис. 2.5. Основні ключі генерації SCT для кількох KMF

BEK

Кожен KME запускає власну базу даних, і щовечора виконується резервне копіювання цієї бази даних, з міркувань безпеки ця

резервна копія шифрується за допомогою ключа шифрування резервної копії. Цей ключ використовується виключно для цієї мети і не має іншого використання.

IEK

Відповідно до Finnish Airbus Defense and Space (2015, a), внутрішній ключ шифрування використовується лише для шифрування зв'язку всередині даного KMF, коли дані переміщуються від одного компонента до іншого всередині того самого сервера.

Усі ці ключі, FEK, BEK та IEK, мають бути однаковими в усіх KMF, що належать одному конкретному клієнту. У ситуації аварійного відновлення, наприклад, коли сталася пожежа на сайті одного сервера, але ми маємо сховище даних на сайті другого сервера, ми можемо взяти резервну копію, яка зберігалася на сайті другого сервера, і використовувати її для відновлення інформації на новому сервері.

2.6. Типи пристроїв, що використовуються в проекті

У цьому розділі я поясню найважливіші елементи рішення E2EE.

2.6.1. Механізм керування ключами (KMF)

Це найважливіший елемент у рішенні, запропонованому цим проектом, і елемент/область, на якій я найбільше зосереджуюсь у своїй дисертації.

Цей елемент є сервером, який керує автоматичним розподілом ключів шифрування трафіку по повітрю на всі радіостанції в мережі, а також розподілом до іншого немобільного обладнання, такого як системи радіоконсолі (диспетчерські робочі станції, які використовуються операторами в основному офіс для зв'язку з польовими агентами) і шлюзи запису (записувачі це пристрої, які використовуються для запису всього спілкування в мережі).

Окрім попереднього згаданого завдання, KMF також координує використання TEK у зберіганні всього E2EE - сумісного обладнання в мережі. У мережах TETRA E2EE використовує 3 ключі: минулий, активний і майбутній; це налаштування має на меті безперервне використання зашифрованого зв'язку, навіть якщо закінчується термін дії старих ключів і починають використовуватися нові ключі.

Наприклад, якщо закінчується термін дії ключа в Crypto Group, деякі радіостанції змінять ключ на новий раніше за інших; якщо лише один ключ знаходиться у внутрішній пам'яті в певний момент часу, зв'язок буде втрачено на час між однією стороною та іншою стороною в каналі зв'язку для зміни ключів. З іншого боку, якщо наразі активний ключ залишається збереженим у внутрішній пам'яті пристрою, але він лише позначений як минулий, тоді буде отримано виклик від іншої радіостанції, яка зашифрована цим ключем (оскільки інша радіостанція ще не змінений на новий ключ) призведе до того, що обладнання кінцевого користувача зможе використовувати «минулий» ключ для успішного розшифрування виклику та спілкування. KMF сприяє цьому процесу, надсилаючи повідомлення про активацію «майбутнього» ключа по повітрю до всіх радіостанцій TETRA, що підтримують E2EE, після чого йде повідомлення «завантаження ключа».

На рисунку 2.6 проілюстровано базовий сценарій, де 2 TR мають різні ключі як «активний» ключ для шифрування голосових викликів.

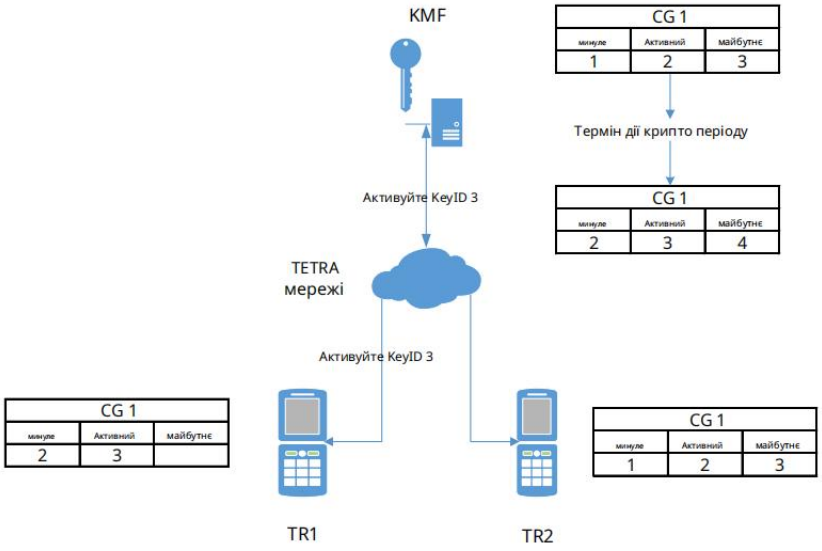

Рис. 2.6. Активація майбутнього ключа в CG1

Припустимо, що дана організація має розмовну групу, яка використовує ТЕК в CG 1, і CG 1 керується KMF цієї організації; на малюнку для простоти я проілюстрував лише відповідні елементи. Припустимо також, що CG 1 має три ключі:

- ідентифікаційний номер ключа або минулий ключ дорівнює 1
- ідентифікаційний номер ключа або активний ключ дорівнює 2
- ідентифікаційний номер ключа або ключ майбутнього дорівнює 3

Як показано на рисунку 2.6, із часом термін дії цього активного ключа добігає кінця, отже, KMF автоматично скасовує минулий ключ для цього CG і переміщує активний стан у минулий стан; Майбутній ключ переходить у активний стан у той самий час, коли KMF генерує новий ключ і переміщує його в майбутній стан. Після того, як це зроблено внутрішньо, KMF починає доставляти ключі всім абонентам. У великій мережі, де КМЕ обслуговує тисячі абонентів, не всі радіоприймачі отримають повідомлення про активацію та нове повідомлення про завантаження ключа одночасно з іншими радіостанціями, головним чином через обмеження можливостей ШІ та доступність основного керування канал радіоінтерфейсу TETRA; через це одна радіостанція може отримати повідомлення про активацію за багато годин (або навіть днів) на малюнку показано, що одна з радіостанцій вже змінила активний ключ на ключ з ідентифікатором 3, тоді як інша залишилася з попередньою конфігурацією, ми також бачимо, що клітинка для ключа Future порожня, тому що повідомлення KEY LOAD потрібно надіслати на радіо, коли КМЕ створює новий ключ. У конфігурації, показаній на малюнку, ми бачимо важливість наявності ключів Past і Future, якщо TR2 намагається викликати TR1 і шифрує зв’язок за допомогою ключа ID 2, TR1 може розшифрувати його, оскільки ключ все ще знаходиться в пам’яті; однак, якби у нас був лише один ключ, зв’язок був би неможливим.

2.6.2. Multi Generic Encryption Module (MGEM)

Для цілей шифрування/дешифрування однією з найважливіших частин у KMF є Multi Generic Encryption Module (MGEM), це плата на сервері, яка відповідає за шифрування/дешифрування всього вихідного/вхідного зв'язку.

Оскільки в КМЕ немає вхідного/вихідного аудіо, єдиним зв'язком, що проходить через MGEM, є повідомлення SDS для цілей OTAK. Для кожного повідомлення OTAK, яке надходить/виходить із KMF, MGEM шифрує/дешифрує TEK та інші дані,

як описано в розділі «4.3.2. Ключі для радіостанцій Tetra». Уся комунікація, якою обмінюються KMF і певний абонент, завжди шифрується за допомогою ключів керування (KEK/SEK), не має значення, чи це асоціація, завантаження ключа, повідомлення активації чи будь - який інший тип інструкцій.

MGEM також використовується в радіоконсольних системах для шифрування/дешифрування зв'язку. У такому обладнанні MGEM поєднується з іншою комп'ютерною платою під назвою xGear16, яка передає аудіопотоки; однак, оскільки функціональні можливості шифрування для RCS не тестувалися в нашій лабораторії в Гельсінкі, це виходить за рамки цієї дисертації, і я не буду вдаватися в подробиці. MGEM виглядає так, як показано на рисунку 2.7 нижче:

Рис. 2.7. MGEM, взято з Finnish Airbus Defence and Space (2015, b)

2.6.2.1 Модуль смарт - картки та смарт - картка для KME

На малюнку 10 можна побачити маленьку дочірню плату, вставлену в MGEM, яка містить 5 смарт - карт; це називається модулем смарт - картки (SCM), і він використовується в кожному MGEM для зберігання SC, які містять відповідні ключі для шифрування/дешифрування зв'язку.

У контексті KME SCM містить смарт - карти для засобу керування ключами (або скорочено SC4KMP). Ці типи смарт - карток відрізняються головним чином ємністю від SC, що використовуються в радіотерміналах. Сам KMF розроблений для підтримки приблизно 40 000 користувачів, щоб обмінюватися інформацією з такою кількістю користувачів, SC4KMF повинен мати більшу ємність, ніж ті, що

використовуються в TR, кожен SC4KMF має ємність для зберігання понад 2000 пар ключів керування (КЕК/SEK). Загалом версія 1 KMF може містити 20 SC, розподілених у 2 MGEM, де кожен MGEM може містити 1 SCM, а 1 SCM може містити до 10 SC (5 на кожну сторону).

2.6.2.2. Ключ автентифікації для MGEM

Апаратні засоби MGEM і SC, які використовуються в радіодиспетчерах і KMF, по суті, однакові, але програмне забезпечення відрізняється; MGEM і SC4KMF використовують спеціальний ключ автентифікації для спільної роботи; цей ключ залежить від глобального місцезнаходження клієнта та містить конкретні дані для кожного клієнта, які не можна використовувати в приміщеннях іншого клієнта. У SC4KMF також завантажується різне мікропрограмне забезпечення залежно від географічного регіону та клієнта, до якого вони належать, таким чином SC4KMF не можна Використовувати повторно.

2.6.3. Конфігуратор смарт - карт KMF (KSCC)

Конфігуратор смарт - карт KMF - це інструмент, розроблений з єдиною метою ініціалізації та програмування смарт - карт для KME. Цей інструмент не можна використовувати для програмування будь - яких інших типів смарт - карт (як, наприклад, 5C для радіостанцій TETRA).

Це дуже простий інструмент, яким легко користуватися; цей інструмент прийматиме SC4KMF і створюватиме ключі на основі алгоритму, що міститься у мікропрограмі SC, який у нашому випадку є розширеним стандартом шифрування з 256 - бітним ключем. Під час генерації ключів для SC4KMF KSCC створить набір, що містить FEK, BEK та IEK; після створення цих ключів інструмент дає нам можливість зберегти ключі на самому SC, на локальному комп'ютері або на ключі безпеки (пояснення в наступному розділі).

Згенеровані ключі мають бути збережені на всіх смарт - картках, які використовуватимуться в призначеному KME, щоб смарт - картки працювали, коли їх вставлено в MGEM KMF. Причина полягає в тому, що FEK

використовуватиметься в KMFy case ТЕК імпортуються з SCT (наприклад, головного SCT) у KMF, а ВЕКта ІЕК використовуватимуться внутрішньо для резервного копіювання та внутрішньої передачі інформації.

2.6.3.1. Аксесуари KSCC - інструмент домену користувача (UDT) для KSCC і ключів безпеки

Інструмент домену користувача (для KSCC, не плутати з UDT для SCT) - це ще одна програма, яку необхідно Використовувати перед виконанням будь - яких операцій у KSCC. Єдиною метою UDT для KSCC є створення авторизованого користувача, якому потім буде дозволено ввійти та виконувати операції в KSCC. Особа, відповідальна за використання UDT і створення авторизованих користувачів KSCC, має бути особою, яка не пов'язана з жодною діяльністю в KSCC. Цей захід додає додатковий рівень безпеки до загального процесу. Процес роботи всього механізму описаний на рисунку 2.8:

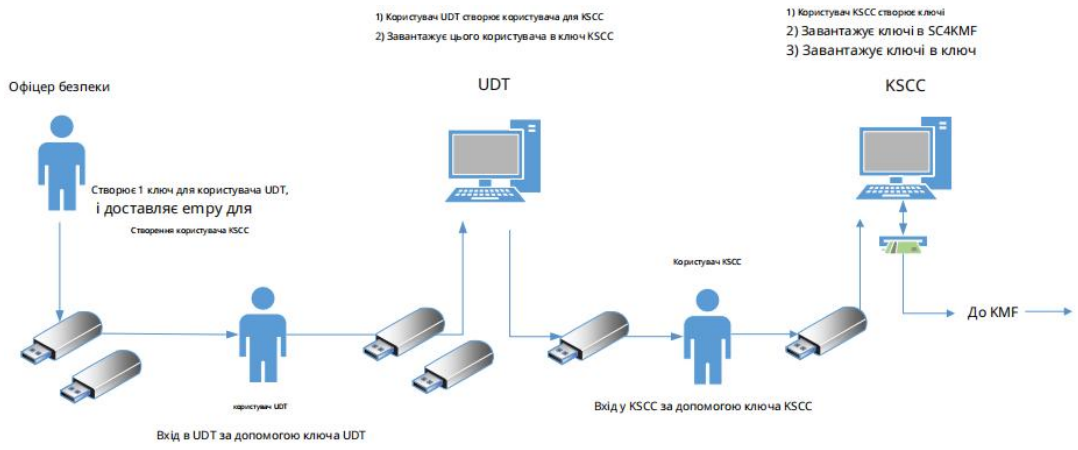

Рис. 2.8. Процес роботи KSCC

На рисунку 2.8 ми можемо побачити процес, який необхідно виконати для роботи KSCC і налаштування смарт - карт для КМЕ

Оператор повинен мати ключ безпеки для використання KSCC, а також для використання UDT для KSCC, який є різновидом електронної ідентифікації. Без захисного ключа програми створять виняток безпеки та завершать роботу.

Оператор UDT повинен мати ключ безпеки, щоб увійти до свого облікового запису в UDT; Офіцер служби безпеки компанії відповідає за видачу правильно налаштованого ключа. Після того, як користувач UDT отримає цей ключ від офіцера безпеки, він може увійти до свого облікового запису в UDT і створити користувача для KSCC; після створення цього користувача він повинен завантажити цю інформацію в інший ключ безпеки, який буде доставлено особі, відповідальній за роботу KSCC.

Користувач KSCC може увійти в KSCC і створити необхідні ключі для налаштування SC4KMF (FEK/ВЕКЛЕК) після отримання ключа безпеки KSCC, а потім завантажити ці ключі в смарт - карти.

Нарешті, якщо TEK імпортуватимуться з SCT до KMF за допомогою зовнішнього каналу, як, наприклад, ключі шифрування міжорганізаційної групи, тоді користувач KSCC повинен завантажити FEK у свій ключ безпеки та перенести його OOB до SCT, щоб мати можливість запечатати TEK переміщувати разом із ФЕК для безпечного транспортування. Коли KMF отримає вихідні TEK, він зможе розпечатати контейнер, оскільки FEK уже завантажено в смарт - картки, вставлені в його Multi Generic Encryption Module.

2.6.4. Сервер підключення TETRA (TCS)

Від Finnish Airbus Defence and Space (2015, с) «Сервер зв'язку TETRA (TCS) забезпечує інтерфейс високого рівня для безпечного та ефективного підключення додатків клієнтів до системи TETRA. Цей інтерфейс називається TCS Application Programming Interface або TCS API».

Коротше кажучи, ми могли б сказати, що TCS є дверима між системами TETRA SLC та рештою світу, коли мова йде про користувацькі програми, які повинні виконувати певну роботу в системах TETRA SLC.

Існують інші інтерфейси систем TETRA, наприклад, голос передається через TVG (голосовий шлюз TETRA), а також міжсистемний інтерфейс (ISI) і загальний 4 - провідний інтерфейс (G4WI) для інших цілей; однак, коли йдеться про передачу

сигналів між мережею TETRA та програмами сторонніх розробників, TCS є мостом, який потрібно використовувати.

Для цілей цієї дисертації важливим є лише з'єднання через TCS, тому я не буду пояснювати решту інтерфейсів системи TETRA.

TCS API - це частина програмного забезпечення, яку можна запускати на звичайному комп'ютері з Windows 7 або на сервері Windows; сервер Windows використовується для цілей ОТАК, причиною цього є те, що TCS, який працює на комп'ютері з Windows 7, здебільшого призначений для роботи разом із програмою диспетчера, для якої використовується програмне забезпечення TCS для одного користувача. Для цілей ОТАК; однак TCS може бути окремим загальним багатокористувацьким сервером, який може використовуватися KMF та іншими сторонніми програмами одночасно.

2.6.5 Базова станція TETRA (TBS)

У стільниковому зв'язку «BTS забезпечує прямий зв'язок із мобільними телефонами». Пул, І. (2006). За словами цього автора, базова станція є сполучною ланкою між мобільним обладнанням та мережевою інфраструктурою, оскільки ця базова станція складається з самих антен та електроніки, відповідальної за мультиплексування та посилення сигналів; Крім цього, є контролер базової станції, який відповідає за управління ресурсами базової станції та за зв'язок із центром комутації.

У випадку SLC усі елементи, згадані вище, знаходяться разом в одному фізичному пристрої, TBS містить контролер базової станції, радіоприймачі, радіочастотні мультиплексори та джерела живлення; він здатний передавати сигнали, голос і трафік даних до DXT, а також діяти як автономне обладнання, маршрутизуючи голосові дзвінки в радіостанціях безпосередньо під його покриттям.

З точки зору E2EE, для TBS немає особливої ролі, його єдина мета - передавати повідомлення ОТАК до та з радіостанцій TETRA. TBS відіграє основну роль у шифруванні повітряного інтерфейсу та автентифікації мобільних абонентів, однак ця тема не охоплюється цією тезою, тому я не буду вдаватися в подробиці.

2.6.6 Радіо TETRA (TR)

Це мобільні пристрої, які використовуються для мереж TETRA, вони не схожі на звичайні комерційні телефони, оскільки робоче середовище є зовсім іншим, і вони повинні бути стійкими до більш екстремальних сфер роботи порівняно зі звичайними споживчими телефонами. Деякі радіостанції TETRA підтримують наскрізне шифрування. використовуючи ОТАК для доставки ключів, ми використали модель TH1n radio.

2.6.7 Смарт - карти для TP

Існує 2 різні типи смарт - карт: ті, які призначені для використання в MGEM KME, а решта, які можна використовувати в TR і RCS. Останні мають мікропрограму, призначену для зберігання лише 1 пари ключів керування, а решту можна заповнити криптогрупами та ТЕК.

SC для радіостанцій TETRA також розроблено для дистанційного керування в тому сенсі, що їхні ключі можна стерти по повітрю у разі втрати або викрадення радіостанцій.

Смарт - карти для радіостанцій TETRA потрібно налаштувати лише один раз вручну під час ініціалізації, щоб записати в них адресу індивідуального короткого ідентифікатора абонента (ISSI) KMF і їхню власну пару ключів керування (KEK/SEK); маючи цю інформацію, SC може зв'язатися з KMF, коли TR увімкнено, щоб запитувати ТЕК.

2.6.8 Інструмент смарт - карт (SCT) для TR

Інструмент смарт - карт - це програмне забезпечення, яке використовується для налаштування абонентських SC як із радіостанцій TETRA, так і з систем радіоконсолі. Окрім налаштування SC, SCT також може створювати ключі, які будуть використовуватися як ключі шифрування трафіку; наприклад, якщо ключі потрібно розповсюдити кількома KMF, як у випадку міжорганізаційних Crypto Groups. Рисунок 2.9 є прикладом SCT:

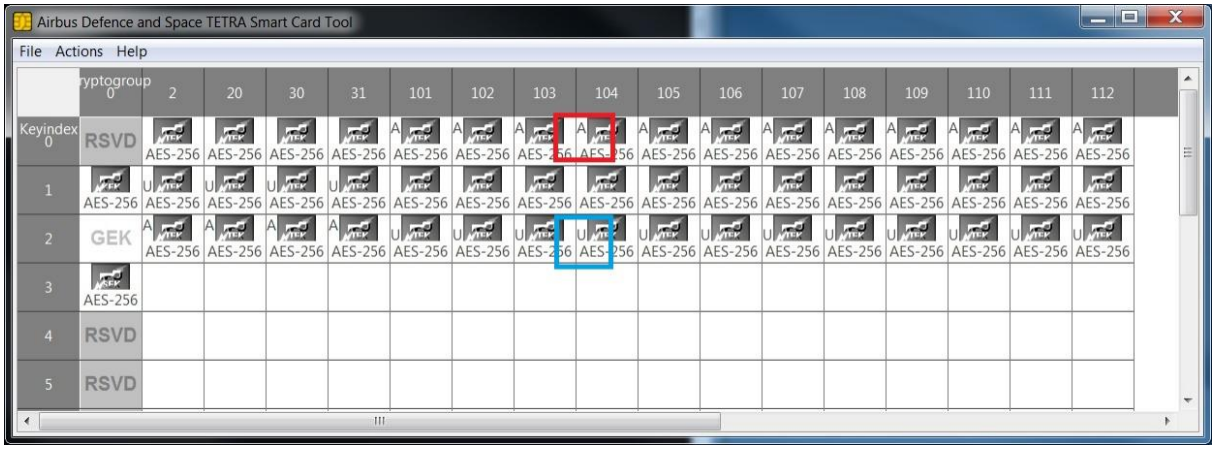

Рис. 2.9. Приклад інструменту Smart Card

На рисунку 2.9 ми можемо побачити, як виглядає KeyStore смарт - картки; у цьому конкретному SC ми маємо 16 CG, які мають по 3 TEK, для кожної групи з 3 ключів є один у стані «Минулий», позначений літерою «U» (скорочення від «Використано»), інший у стані <<Активний», позначений знаком «A», і немаркований ключ, який знаходиться в стані «Майбутнє» і ще не Використовувався. У лівій частині ми також бачимо 2 ключі в стовпці Crypto Group 0, і хоча це не показано, цими ключами є ключ шифрування ключа та ключ шифрування сигналізації. У цьому прикладі відповідні слоти вже заповнені; однак, оскільки CG0 не використовується для ключів трафіку, слоти в його стовпці позначені відповідно до типу ключа, який він утримує, у момент ініціалізації SC можна побачити KEK або SEK, Вигравірувані в них.

2.6.9 Майстер та організаційні SCTs

На рисунку 2.10 ми бачимо, що існує так званий Master Smart Card Tool разом із кількома департаментськими SCT, які постачають ключі шифрування трафіку з різних доменів до 2 KMF для надсилання по повітрю.

Роль цього головного SCT полягає в тому, щоб надати однаковий набір ключів для кількох KMF, щоб розповсюдити його всім користувачам в організаціях, які обслуговують ці KMF.

На рисунку 2.10 ми бачимо, що один KMF підключений до SCT свого відділу та до головного SCT; наприклад, у випадку пожежної служби, він має KMF, позначений на ілюстрації як «Fire KMF», який, у свою чергу, підключений до Fire SCT і водночас до головного SCT.

Припустімо, що пожежна служба має внутрішню групу розмови з номером 6002563, і що ця група розмови пов'язана з CG1, у той же час існує міжорганізаційна група розмови з номером 2008541, і ця міжорганізаційна група розмови призначена CG2.

У нашому прикладі Fire SCT згенерує ключі для CG1 і доставить їх (OOB) до Fire KMF. У той же час Master SCT генеруватиме ключі для CG2 і доставлятиме їх (OOB) не лише до Fire KMF, але й до Army KMF; таким чином користувачі пожежної служби зможуть спілкуватися один з одним через групу розмов 6002563 у груповому виклику, зашифрованому за допомогою ключів, що містяться в C61 які доставляються від Пожежної КМФ користувачам Пожежної частини. Крім того, якщо необхідно, користувачі пожежної служби зможуть спілкуватися з користувачами армійської служби через міжорганізаційну розмовну групу 2008541 у груповому дзвінку, зашифрованому за допомогою ключів, що містяться в CG2, які були доставлені користувачам обидві організації їхніми відповідними KMF.

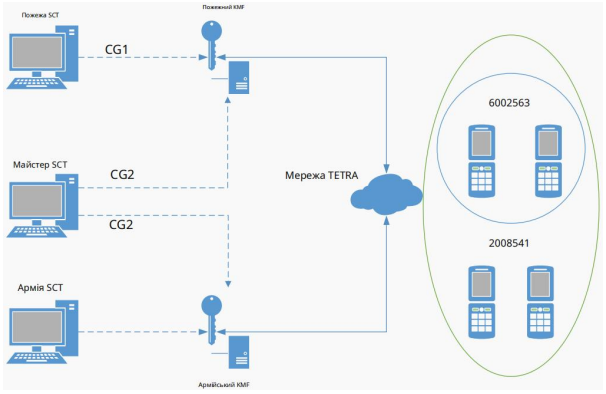

Рис. 2.10. Головний SCT доставляє ключі до кількох KMF

У нашому попередньому прикладі ми припускаємо, що KMF покладаються на відділ SCT для генерації ключів; Я пояснив це так, щоб зробити роль магістра SCT більш зрозумілою. Однак насправді TEK для внутрішньовідомчої організації

генеруються локально у відповідних KMF для зручності, а Master SCT генерує лише спільні TEK.

2.7 Аксесуари SCT (UDT і ключі безпеки)

SCT також використовує інструмент домену користувача подібним чином, як і KSCC, це служить додатковим заходом безпеки, оскільки ним керує інша особа, роль якої полягає лише у створенні користувачів і призначенні цим користувачам ключового домену для використання в SCT.

Концепція ключів SCT і UDT в принципі така сама, як і в KSCC, з кількома відмінностями:

- KSCC є програмним забезпеченням, похідним від SCT, тому супутні елементи та процес роботи дуже схожі; однак, будучи батьківським програмним забезпеченням, програмне забезпечення SCT має багатший дизайн.
- SCT використовує різні діапазони доменів для створення TEK, на відміну від KSCC, який використовує лише 1 діапазон доменів для створення FEKIEK/BEK.

Рисунок 2.11 ілюструє процес використання SCT; процес дуже подібний до процесу на рисунку 2.8, що відповідає KSCC, за винятком етапів, що виконуються на етапах UDT і SCT, які відрізняються:

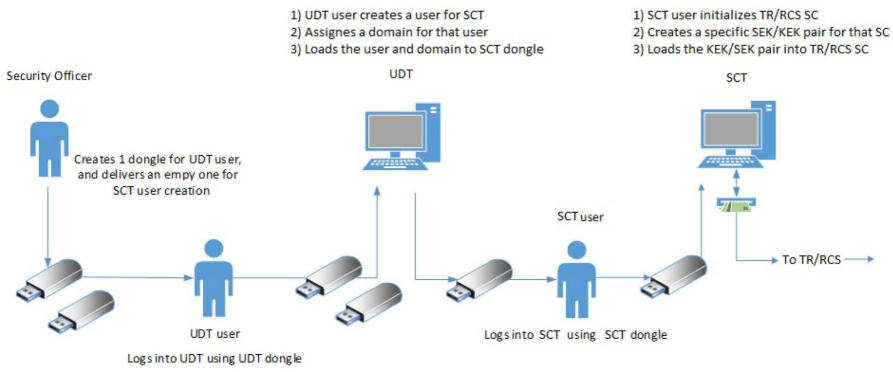

Рис. 2.11. Процес створення та використання користувача SCT

Необхідно чітко пояснити, що UDT, який використовується для SCT і KSCC, не є однаковим, кожен інструмент (SCT і KSCC) має власну версію User Domain Tool, і

користувачі, створені, наприклад, в UDT з SCT, не будуть працювати в KSCC і навпаки.

2.8. Сертифікати шифрування

Для додаткового рівня безпеки в OOB - управлінні ключами рішення E2EE використовує сертифікати SMIME поверх файлів, зашифрованих FEK.

Щоразу, коли файл, яким би він не був (TEK, асоціації, KEK/SEK тощо), переміщується з одного комп'ютера на інший через зовнішню пам'ять, файл автоматично запечатується сертифікатом SMIME, попередньо встановленим на комп'ютері, де створюється файл. Щоб розшифрувати файл, на цільовому комп'ютері має бути встановлено такий же сертифікат.

SMIME не використовується під час надсилання повідомлень OTAK, він використовується лише для цілей управління OOB.

2.9. Цифровий обмін для TETRA (DXT)

У стільникових системах центр комутації мобільних пристроїв є найважливішим компонентом усієї мережі; у реалізації TETRA від SLC цей пристрій називається Digital exchange for TETRA (DXT), і його основна мета полягає в маршрутизації голосових викликів і даних між усіма абонентами в мережі.

За всю історію було багато моделей DXT. Понад 20 років тому DXT являв собою величезну комутаційну шафу, яка могла легко вмістити цілу маленьку кімнату; однак на момент написання цієї дисертації DXT - це коробка, менша за посудомийну машину, і використовує передову телекомунікаційну обчислювальну архітектуру (ATCA); більшість його компонентів є віртуальними комп’ютерними блоками, які виконують функції того, що колись було величезними фізичними пристроями, розміщеними в безперервному масиві шаф. На рисунку 2.12 нижче показано зображення DXT:

Рис. 2.12. DXTA від SLC, взято з Sturtzel, A. (2015)

DXT має багато різних інтерфейсів і здатний підключатися до різних пристроїв, щоб отримати їхні послуги для різних цілей.

Деякі з основних завдань і функцій DXT перераховані нижче; послуги з третього пункту і далі можуть або не можуть використовуватися залежно від клієнта:

Ведіть числове дерево для маршрутизації трафіку

- перемикайте дзвінки та передачу даних між різними абонентами
- керуйте магістральними з’єднаннями з іншими DXT
- керуйте послугами зарядки
- управління статистикою (трафіку, навантаження тощо) і звітністю
- разом із розширеним шлюзом пакетних даних маршрутизує пакетні дані до місця призначення

- спілкуйтеся із зовнішніми системами, такими як PSTN, PABX, ISDN та іншими стільниковими радіомережами

- Підключайте до мережі TETRA різні програми, такі як голосові диспетчери, програми керування, центри моніторингу мережі тощо.

Через великий характер цього конкретного пристрою знадобився 6 цілий документ, щоб описати кожну його функцію, з цієї причини та оскільки ця дисертація зосереджена на управлінні безпекою та шифруванням, я не буду вдаватися в подробиці щодо комутації телефонії.

2.10 Від створення ключа до встановлення виклику, пояснення процесу

У будь - якому механізмі шифрування рекомендується змінювати ключі шифрування кожен певний період, тому в нашій системі наскрізного шифрування ключі, які використовуються для зв'язку, змінюються на регулярній основі, яку може налаштувати користувач. У випадку наших тестів у лабораторії ми використовували 1 годину для закінчення періоду крипто; однак у клієнтській мережі це може тривати кілька тижнів.

У цьому розділі спочатку я коротко поясню, як генеруються ключі, потім, коли ключі готові, їх потрібно розповсюдити, я поясню сигналізацію щодо їх розподілу у другому розділі; і в кінці, коли ключі знаходяться в обладнанні кінцевого користувача, я пояснюю, як встановлюється виклик.

2.11 Генерація ключів

Ключі генеруються двома способами в нашому рішенні наскрізного шифрування: безпосередньо всередині Key Management Facility перед розповсюдженням серед усіх абонентів або у зовнішньому програмному забезпеченні, розміщеному на іншому комп'ютері під назвою Smart Card Tool.

Коли всі радіостанції TETRA, які мають спілкуватися, обслуговуються одним KMF, тоді цей KMF може самостійно генерувати та розповсюджувати ключі, як показано на рисунку 2.13:

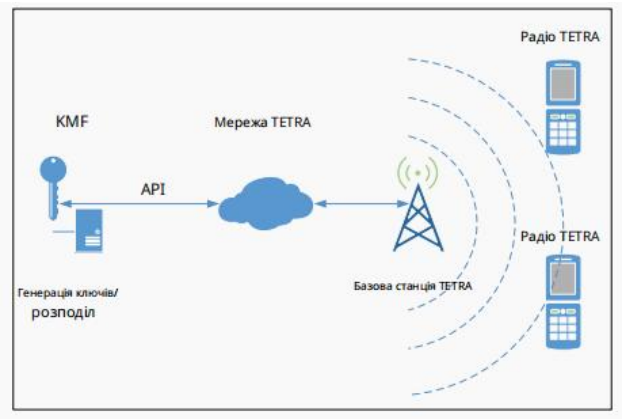

Рис. 2.13. Ключі, згенеровані в KMF

Однак, коли радіостанції TETRA, які мають спілкуватися, обслуговуються різними KMF, як показано на рисунку 2.14, де KMF 1 обслуговує TR 1, а KMF 2 обслуговує TR 2, зовнішнє програмне забезпечення має згенерувати ключі та передати їх відповідному КМФ для їх розподілу; інакше, якби один із KMF генерував їх, інший не мав би уявлення про те, які ключі розподіляються

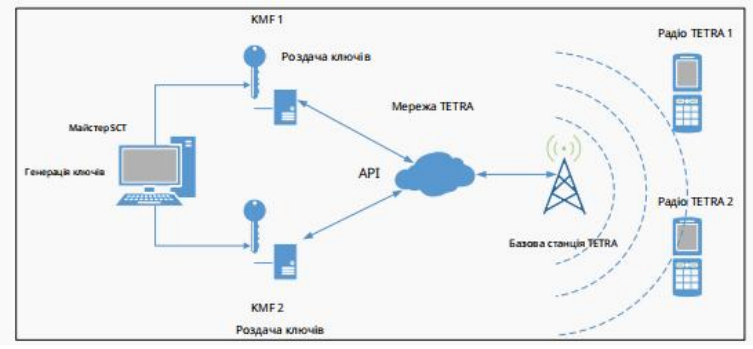

Рис. 2.14. Ключі, згенеровані поза KMF

У нашому рішенні наскрізного шифрування сторона, відповідальна за генерацію ключів, розміщує фізичну плату, що містить машину для генерації ключів. Ця плата, яка називається Multi Generic Encryption Module, містить ряд розумних Картка, яка, у свою чергу, містить алгоритм, необхідний для генерації ключів.

2.12. Обмін ключами

Спочатку потрібно виконати кілька кроків для генерації та обміну ключами, щоб встановити успішний виклик із наскрізним шифруванням за допомогою цього рішення. Ці кроки, а також інші деталі сигналізації описані нижче:

- Як попередня умова, всі пристрої, призначені для роботи в режимі наскрізного шифрування, повинні спочатку отримати належним чином налаштовану смарт - карту (SC), ці смарт - карти повинні бути попередньо запрограмовані набором ключів керування (Key Encryption Key/Signaling Encryption Key), які використовуються для розшифровки ключів, які використовуються для зв'язку (ключі шифрування трафіку), коли вони отримані в зашифрованому вигляді в повідомленнях за допомогою протоколу Over The Air Keying (OTAK).

Під час попереднього програмування смарт - картки також має бути включений індивідуальний короткий ідентифікатор абонента (ISSI) засобу керування ключами (KMF), таким чином радіостанції TETRA (TR) зможуть зв'язатися з KMF під час реєстрації, щоб отримати решта необхідної інформації.

Оскільки в мережі замовника є тисячі користувачів мобільного зв'язку, усі необхідні смарт - карти спочатку будуть масово запрограмовані, а потім роздані всім користувачам.

- Після того, як SC належним чином попередньо запрограмовано та вставлено в TR, його потрібно ввімкнути, і коли це станеться, TR зареєструється в мережі TETRA звичайним способом, у той же час TR надішле повідомлення про реєстрацію до КМЕ, щоб зареєструватися як клієнт для прийому повідомлень протоколу ОТАК, зробивши таким чином себе доступним для отримання повідомлень ОТАК, що містять ТЕК, які пізніше використовуватимуться для шифрування/дешифрування зв'язку (голосових викликів і текстових повідомлень). Це реєстраційне повідомлення зашифровано за допомогою КЕК, попередньо запрограмованого в SC.
- Коли КМЕ вперше отримує реєстраційне повідомлення (перший раз, коли вмикається наскрізне шифрування TR), він пов'язує адресу ISSI, з якої воно було

отримано, разом із ключем керування (КЕК), у якому реєструється повідомлення було зашифровано; таким чином KMF знає, хто який ключ використовує для сигналізації (обмін повідомленнями протоколу ОТАК).

- Після того, як KMF зареєструє даний TR у своїй базі даних, він шукатиме групу користувачів (UG), до якої належить TR, і надасть усі асоціації та ключі шифрування, що відповідають цій конкретній групі користувачів TETRA Radio.
- Коли розглянутий TR отримає всі асоціації та ключі шифрування, що відповідають його UG, він зможе почати обмін даними з іншими TR.

Перш ніж я продовжу пояснювати процедуру встановлення наскрізного шифрованого виклику, я хочу представити у графічній формі описані раніше кроки з 1 по 5.

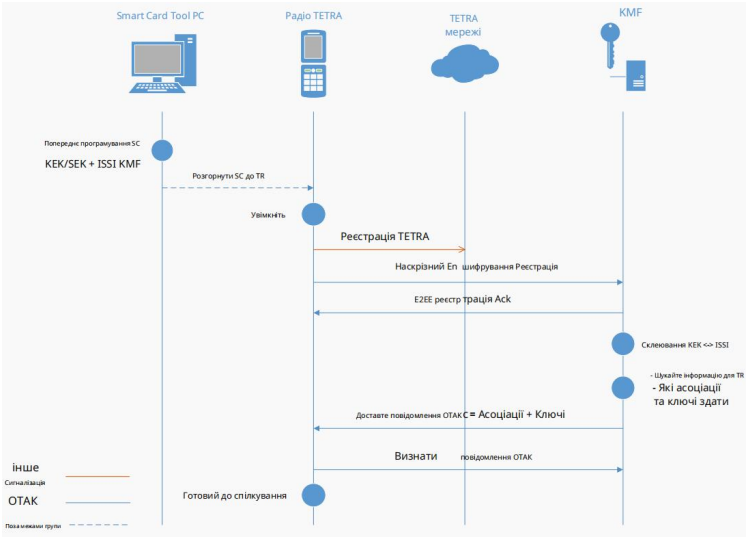

Рис. 2.15. – Діаграма послідовності для сигналізації обміну ключами

2.13. Встановлення виклику

Після завершення всіх сигналів для доставки ключів шифрування, TR може розпочати обмін даними. Процедура встановлення виклику за допомогою нашого рішення наскрізного шифрування така:

- користувач набирає номер для індивідуального виклику або натискає кнопку Push - To - Talk у попередньо вибраній розмовній групі, щоб почати виклик.

- давайте зосередимося на випадку індивідуального дзвінка на цьому прикладі. Коли користувач натискає кнопку «Набрати», TR шукає у своєму SC список асоціацій, попередньо наданих KME, коли він знаходить відповідний відповідник для адреси призначення, він шукає «активний» ключ шифрування, що міститься в Crypto Group зіставляється з адресою призначення.
- знайшовши правильний ключ шифрування, TR шифрує голосовий виклик цим криптоключем і починає надсилати голосові пакети (на основі TDMA з комутацією каналів) через мережу.
- кроки 1 - 3 припускають, що відповідний ключ було доставлено на інший кінець голосового виклику за допомогою процедури, описаної в розділі, отже, одержувач може відповісти на виклик і розшифрувати його.

І останнє, але не менш важливе, ось графічне представлення процедури встановлення виклику за допомогою нашої системи наскрізного шифрування:

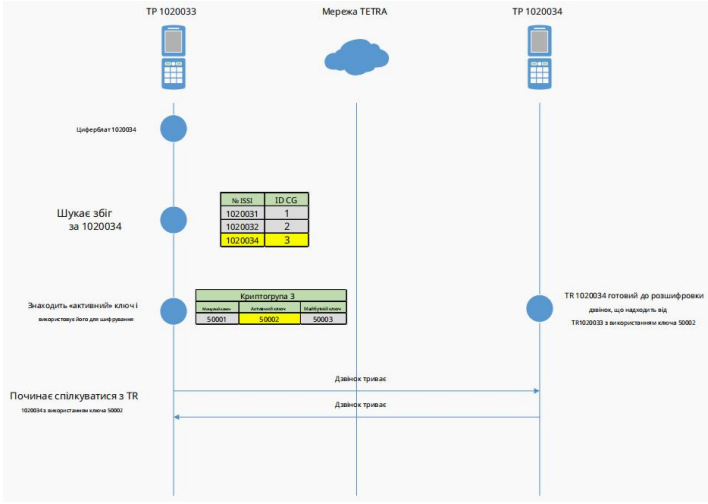

Рис. 2.16. Процес встановлення виклику за допомогою нашої системи наскрізного шифрування

2.14 Висновки до розділу 2

Описані основні алгоритми шифрування, критерії якості реалізації системи та впровадження рішення OTAK для розподілу ключів у великих мережах. Особливу увагу приділено AES-256 як стандарту для впровадження систем безпеки.

РОЗДІЛ 3

НАУКОВО - ДОСЛІДНА ЧАСТИНА

3.1 Визначення плану симуляції

Для даного етапу було розроблено і сформульовано план виконання індивідуального завдання, орієнтований на проведення симуляційних досліджень та змодельованих ситуацій. Основна увага приділялася моделюванню роботи механізмів шифрування в умовах варіативного навантаження на мережу. Було використано віртуальне середовище для створення сценаріїв тестування, що включало всі необхідні компоненти мережі TETRA. Цей підхід дозволив точно відтворити мережеві умови без необхідності натурного експерименту.

3.2 Профіль навантаження та фоновий трафік

У процесі дослідження використовувалося моделювання для аналізу функціонування Key Management Facility (KMF). Для цього було розроблено детальну модель, яка враховувала потоки даних, обробку ключів шифрування та сценарії виникнення збоїв у мережі. Симуляція проводилася за допомогою спеціалізованого програмного забезпечення, що забезпечувало масштабованість та високу точність отриманих результатів.

Особливу увагу приділено оцінці продуктивності системи при підвищеному навантаженні. Змодельовано ситуації з високою кількістю користувачів, що одночасно здійснюють запити до KMF, та вивчено стійкість системи до кіберзагроз.

Профіль навантаження складається з двох частин: поточного трафіку, що вже є в мережі, і нового трафіку, пов'язаного з OTAK. Поточний трафік, що отримав назву «фоновий трафік», включає різноманітні повідомлення, такі як групові та індивідуальні дзвінки, передача даних (SDS) та інші типи комунікацій. Цей трафік

здійснюється до, під час і після введення нового трафіку обміну повідомленнями OTAK.

Новий трафік, який позначено як «трафік OTAK», охоплює всі повідомлення, необхідні для реєстрації, отримання та підтвердження повідомлень, що надсилаються KMF на радіостанції TETRA. Це включає ключі шифрування, асоціації для їх використання, активацію ключів та інші повідомлення, що стосуються процесу управління ключами та обміну даними.

У наведеній нижче таблиці описано розбивку сигналізації в одиницях за одиницю часу. За оцінками, на базову станцію в будь-який момент часу припадає в середньому 65 тетрарадіостанцій, тому наступні суми базуються на цьому числі.

Таблиця 3.1

Фоновий трафік для тестування ШІ

Протокол	Напрямок	Сума	Тривалість (с)	Повторення	Коментарі
Груповий виклик		325	20	годину	
Пізній вступ	ВНИЗ	1		друге	Як трансляція
Індивідуальний дзвінок		65	180	годину	
Виклик PSTN/PABX		65	180	годину	
Індивідуальний статус	Будь-який	65		годину	16 біт
Індивідуальний SDS	Будь-який	65		годину	64 символи. Визнано
Статус групи	Будь-який	65		годину	16 біт
Група SDS	Будь-який	65		годину	64 символи. Визнано
Управління групою SDS	ВНИЗ	129		Робоча зміна	
Роумінг (Inter-DXT)		129		годину	
Передача (Intra-DXT)		65		годину	
Пакет даних		104,4643			milli-earlang
AVL	вгору	129		хвилина	

З огляду на специфіку тестування, запропонований трафік визначається на основі обсягу трафіку, що генерується одним абонентом, помноженого на кількість абонентів, які обслуговуються однією базовою станцією. В загальному вигляді обсяг трафіку на одного абонента виглядає наступним чином:

- 5 групових дзвінків тривалістю по 20 секунд кожен на годину на одного абонента
- 1 індивідуальний дзвінок тривалістю 3 хвилини на годину на одного абонента
- 1 дзвінок до зовнішніх систем (наприклад, PSTN) тривалістю 3 хвилини на годину на одного абонента
- 1 індивідуальне повідомлення про статус обсягом 16 біт на абонента на годину
- 1 індивідуальне повідомлення SDS (і його підтвердження) довжиною 64 символи на абонента на годину
- 1 повідомлення про статус обсягом 16 біт для групи на абонента на годину
- 1 повідомлення SDS (і його підтвердження) довжиною 64 символи для групи на абонента на годину
- 2 абоненти, що переміщуються в/з зони, на яку поширюється інший DXT (роумінг), на годину
- 1 абонент, що переміщується до/з зони, охопленої іншою TBS, але тим самим DXT (хендовер), на годину
- Загалом 104,46 міліерланга пакетних даних, що передаються в TBS на годину
- Щохвилини кожному абоненту надсилається 2 автоматичні повідомлення про місцезнаходження автомобіля
- Додатково до попереднього трафіку, сигнал пізнього входу надсилається щосекунди як трансляція в ШІ.

Ці показники забезпечують реалістичне моделювання навантаження на мережу під час тестування, що дозволяє оцінити вплив обміну повідомленнями OTAK на загальну ефективність радіоінтерфейсу.

У мережі замовника робочий день поділяється на чотири зміни, кожна з яких триває 6 годин. Враховуючи, що працівники вмикають свої мобільні радіостанції на початку робочої зміни, можна зробити висновок, що більшість реєстрацій у мережі

відбуваються в короткі проміжки часу, що повторюються кожні 6 годин. Ці часові вікна зазвичай тривають кілька хвилин, залежно від кількості людей та відділів, де вони працюють.

Встановлено, що більшість користувачів вмикають свої радіостанції та реєструються протягом 5-15 хвилин після початку робочих змін. З огляду на цю інформацію, для тестування було визначено три основні часові рамки: перша - найгнучкіша, коли всі абоненти реєструються протягом 15 хвилин; друга - коли всі абоненти реєструються за 10 хвилин; і третя - найбільш навантажена, коли всі абоненти реєструються за 5 хвилин після початку робочої зміни.

З огляду на цю інформацію, а також враховуючи критерії фонового трафіку і кількість абонентів, яких потрібно включити до TBS, була створена відповідна таблиця для подальшого аналізу та тестування.

Таблиця 3.2

Реєстрації за робочу зміну в ТБШ для тестування

<table>
<tr><td colspan="6">Одна робоча зміна</td></tr>
<tr><td colspan="6">Сигнальні повідомлення для реєстрації 65 ТР</td></tr>
<tr><td>Випадок 1</td><td>Випадок 2</td><td>Випадок 3</td><td colspan="3">Трафік загальний для всіх випадків</td><td></td></tr>
<tr><td colspan="3">час</td><td></td><td>Протокол</td><td>Напрямок</td><td>#</td></tr>
<tr><td rowspan="5">перше
3 хвилин</td><td rowspan="5">перше
6 хвилин</td><td rowspan="5">перше
9 хвилин</td><td>Розташування
Оновлення
Попит</td><td>вгору</td><td colspan="2">55</td></tr>
<tr><td rowspan="2">Взаємний
Аутентифікація</td><td>вгору</td><td colspan="2" rowspan="2">110</td></tr>
<tr><td>вниз</td></tr>
<tr><td>прийняти</td><td>вниз</td><td colspan="2">55</td></tr>
<tr><td>Група
Звітність</td><td>вниз</td><td colspan="2">NA</td></tr>
<tr><td rowspan="5">Далі
2 хвилин</td><td rowspan="5">Далі
4 хвилин</td><td rowspan="5">Далі
6 хвилин</td><td>Розташування
Оновлення
Попит</td><td>вгору</td><td colspan="2">10</td></tr>
<tr><td rowspan="2">Взаємний
Аутентифікація</td><td>вгору</td><td colspan="2">20</td></tr>
<tr><td>вниз</td><td colspan="2">20</td></tr>
<tr><td>прийняти</td><td>вниз</td><td colspan="2">10</td></tr>
<tr><td>Група
Звітність</td><td>вниз</td><td colspan="2">NA</td></tr>
</table>

У таблиці 3.2 представлені три часові рамки, на основі яких я буду проводити тестування. Ці часові вікна позначені як Випадок 1, Випадок 2 і Випадо 3, причому

кожне з них поділяється на два інтервали часу: перший займає 3/5 загальної тривалості, а другий - 2/5 цієї тривалості для кожного випадку.

Оскільки більшість абонентів (85%) реєструються на початку вказаних мною часових проміжків (5, 10 і 15 хвилин), я визначив, що перші 3/5 часу будуть відведені для реєстрації 85% користувачів, які підключаються на самому початку робочої зміни. Останні 2/5 часу я використовую для реєстрації решти 15% абонентів.

Таким чином, у таблиці показано, що загальна кількість абонентів (65) розподілена таким чином: 55 абонентів реєструються протягом перших 3/5 часу, а 10 абонентів - протягом наступних 2/5 часу.

У правій частині таблиці я відобразив сигнальні повідомлення, що використовуються під час реєстрації мобільних радіостанцій. Стандартний протокол реєстрації у системі TETRA виглядає досить просто:

- Абонент мобільного зв’язку вмикається та надсилає на базову станцію запит на оновлення розташування, щоб повідомити про своє включення.
- Базова станція надсилає виклик на радіостанцію для перевірки її автентичності.
- Радіостанція відповідає на виклик.
- Базова станція надсилає повідомлення про прийняття, і зв'язок може бути встановлений.
- Далі базова станція надсилає звіт про групи, які будуть використовуватися радіостанцією.

Трафік, що утворюється під час цієї реєстрації, разом з фоновим трафіком, є типовим для початку кожної робочої зміни в мережі клієнта. Це є основним навантаженням, яке відповідає умовам реальної мережі клієнта. Мета полягає не лише у тестуванні цього трафіку, а й у перевірці трафіку OTAK, який буде вводитися під час впровадження рішення E2EE. Для цього необхідно визначити трафік OTAK як на етапі впровадження рішення, коли все обладнання переходить на використання E2EE з бездротовими ключами, так і впродовж решти часу, коли здійснюється регулярна реєстрація та зміна ключів радіостанцій без необхідності в початковій конфігурації.

3.3 OTAK

Відповідно до зібраних даних клієнта, які стосуються архітектури мережі та очікуваної доставки ключів для цілей E2EE, визначеної їхнім криптографічним планом, я здійснив розрахунок середньої кількості повідомлень OTAK, які очікуються в мережі клієнта. Це дозволило створити основу, на якій будується наш план тестування та тестове середовище. Було розглянуто три основні сценарії, що визначають основне навантаження трафіку E2EE OTAK, які я поясню нижче.

Етап початкової конфігурації та розгортання

У моделюванні інтеграції рішення в мережу замовника було передбачено поступове налаштування TR на E2EE з підтримкою OTAK. Для імітації цього процесу використано математичну модель, яка поступово збільшує параметри трафіку OTAK, що дозволяє оцінити ефективність розподілу ключів у масштабованій мережі. Важливо враховувати, що трафік OTAK під час перших реєстрацій значно вищий, ніж під час стандартної реєстрації TR, оскільки на етапі першої реєстрації TR отримує всю конфігурацію шифрування відразу від KMF, що створює велике навантаження на мережу.

На рисунку 3.1 представлено результати моделювання 10-кратного збільшення навантаження трафіку OTAK під час початкової реєстрації для 64 смарт-карт (середня кількість TR, яка змодельована для TBS протягом кожної робочої зміни).

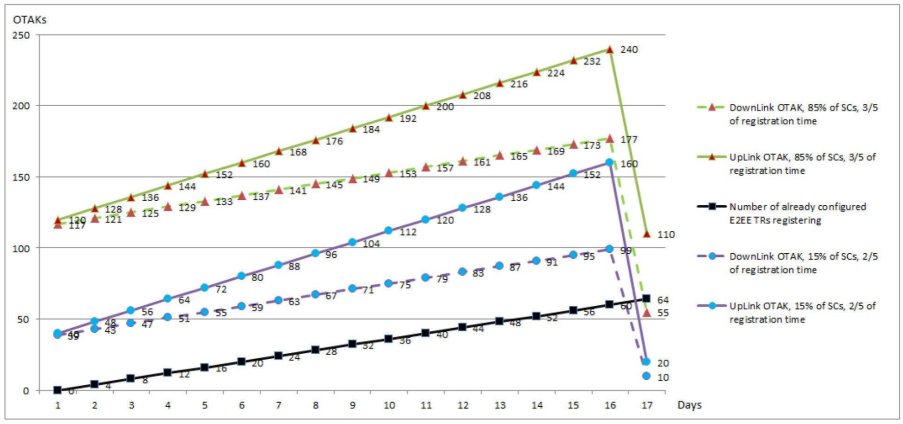

Рис. 3.1. 10-кратне навантаження очікуваного трафіку OTAK за робочу зміну в TBS

Регулярна реєстрація на кожну робочу зміну

У правій частині графіка на рисунку 20 змодельовано значне зменшення лінії, що демонструє зниження обсягу трафіку OTAK після початку робочої зміни. Це пов'язано з тим, що модель передбачає реєстрацію всіх TR у мережі на ранніх етапах, виключаючи необхідність додаткової початкової конфігурації.

Закінчення крипто-періоду

У змодельованій ситуації завершення крипто-періоду потребує оновлення всіх криптогруп (CG), налаштованих на цей період. Симуляція передбачає, що KMF генерує нові випадкові шифрувальні ключі та розподіляє їх до TR, що містять ці CG. Для забезпечення більшої стійкості модель була налаштована так, щоб термін дії всіх CG у межах певного KMF завершувався одночасно, що дозволило оцінити вплив одночасної генерації та доставки ключів на всі Tetra Radio в системі.

Обчислення кількості повідомлень OTAK після завершення крипто-періодубуло розділено на два основні випадки: перший - моделювання доставки повідомлень OTAK до поточних онлайн-радіостанцій TETRA (які працюють під час робочої зміни), другий - симуляція доставки до автономних радіостанцій TETRA, які не були онлайн під час генерації нових ключів, але отримують їх після повторного підключення.

У таблиці 3.3 представлено результати моделювання кількості повідомлень OTAK, які необхідно надіслати середній кількості онлайн-радіостанцій TETRA, що обслуговуються базовою станцією TETRA протягом певної робочої зміни, у випадку одночасного оновлення всіх CG (відповідно до криптографічного плану клієнта.

Таблиця 3.3

Повідомлення OTAK, надіслані онлайн-радіостанціям після закінчення крипто-періоду

OTAK терміну дії криптографічного періоду, надіслані до поточних онлайнових TR		
Смарт-карти		
64,28	~ 65	
	DownLink OTAK	UpLink (Acks)
	520	520

У випадку, коли повідомлення OTAK надсилаються до радіостанцій TETRA, які перебувають в автономному режимі під час оновлення ключа, обчислення повинні бути адаптовані відповідно до специфіки їх підключення. Оскільки не очікується, що ці радіостанції одразу підключаться до мережі, реєстраційний трафік розподіляється таким чином: 85% реєстрацій відбуваються протягом перших 3/5 часу, а решта 15% - протягом наступних 2/5 часу.

У таблиці 3.4 наведено розрахований обсяг трафіку OTAK для зазначених відсотків TR та тривалості реєстрації.

Таблиця 3.4

Трафік повідомлень OTAK для оновлення ключа, коли TR стають доступними

OTAK терміну дії криптографічного періоду, надіслані до TR наступного разу, коли вони виходять в Інтернет (включаючи реєстрацію)				
Смарт-карти	85 % від загальної кількості СК		15 % від загальної кількості СК	
64	54,4	~ 55	9,6	~ 10
	DownLink OTAK	UpLink (Acks)	DownLink OTAK	UpLink (Acks)
	495	550	90	100

У наступному розділі пояснюється, як заданий обсяг трафіку, описаний у цьому профілі навантаження, використовується для запланованих тестових випадків на етапі перевірки

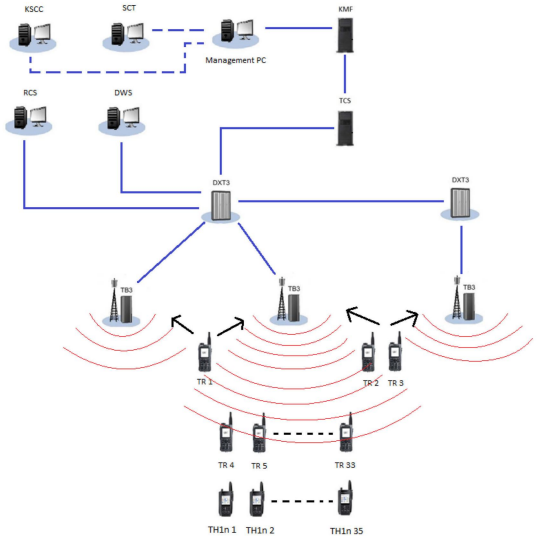

Рис. 3.2. Мережа для тестування повітряного інтерфейсу

На рисунку 3.2 представлена мережа, розроблена для підтримки необхідного обсягу трафіку, характерного для мережі клієнта. Для спрощення та зосередження на основних компонентах, на схемі не зображено всі елементи мережі, такі як комп'ютери моніторингу або сервер CDD, оскільки вони не впливають безпосередньо на потік трафіку, пов'язаний з рішенням E2EE. Лише ті елементи, які безпосередньо взаємодіють з E2EE, відображені на малюнку.

Короткий опис призначення основних елементів тестової мережі:

ПК керування: розташований у верхній частині малюнка, цей комп'ютер на базі Windows 7 використовується для загального керування елементами E2EE в мережі. Він оснащений програмним забезпеченням KSCC та SCT для налаштування конфігурацій смарт-карток. Також має віддалене з'єднання з KMF для виконання операцій через графічний інтерфейс або для налагодження виявлених дефектів за допомогою файлів журналу.

KMF: забезпечує дистанційне IP-з'єднання з ПК керування та підключення до мережі TETRA (DXT) через TCS API для доставки ключових матеріалів E2EE призначеним одержувачам.

DXTS: відповідають за комутацію голосових та даних у мережі TETRA. Підключені безпосередньо до базових станцій TETRA, які передають пакети кінцевим користувачам (радіотерміналам). Також з'єднані з RCS, DWS (диспетчерськими робочими станціями) та сервером TCS, який діє як міст між мережею TETRA та зовнішніми мережами/KMF.

RCS та DWS: у цій тестовій мережі RCS використовується для прийому групових голосових викликів. Зазвичай для створення групового дзвінка необхідні принаймні дві радіостанції (TR), однак RCS може одночасно обробляти кілька відкритих групових викликів, що зменшує кількість необхідних TR для фонового трафіку. DWS використовується для виконання операцій керування всередині мережі TETRA, таких як додавання абонентів або зміна організацій.

TBS: у мережі є три TBS, але для наших тестів контролюється лише один. Інші два TBS використовуються для передачі даних та роумінгу, що забезпечує фоновий трафік.

Радіостанції TETRA: існує два типи TR: одна група позначена як «TH1n», інша - «TR». У системах SLC лише радіостанції TH1n підтримують OTAK E2EE. Оскільки вони часто вмикаються та вимикаються, їх використовують виключно для обміну сигналами OTAK з KMF. Інший тип, позначений як «TR», є старою моделлю, яку використовують лише для створення фонового трафіку, такого як дзвінки, повідомлення, передачі тощо.

3.4 План тестування та визначення тестового покриття

Дослідження повітряного інтерфейсу зосереджено на симуляційному моделюванні сигналізації, яка виникає під час обміну повідомленнями E2EE OTAK через цей інтерфейс. Метою є ідентифікація вузьких місць та можливих дефектів, спричинених нововведеним рішенням. Це досягається шляхом створення моделей пікових навантажень трафіку на інтерфейсі та аналізу їхнього впливу на змодельовану поведінку пристроїв у потоці трафіку OTAK.

Для реалізації цього завдання був розроблений план симуляції, який включає різні сценарії використання трафіку E2EE OTAK, характерні для мережі клієнта, з акцентом на моделювання ситуацій із високим рівнем навантаження в конкретні часові інтервали.

На малюнку 3.3 представлена концепція симуляції E2EE OTAK через радіоінтерфейс. Схема включає 28 симуляційних сценаріїв, які формують основу моделювання E2EE OTAK через повітряний інтерфейс. Ці сценарії поділяються на 4 основні групи, кожна з яких відповідає найбільш критичним фазам змодельованого трафіку OTAK, передбаченого для мережі клієнта.

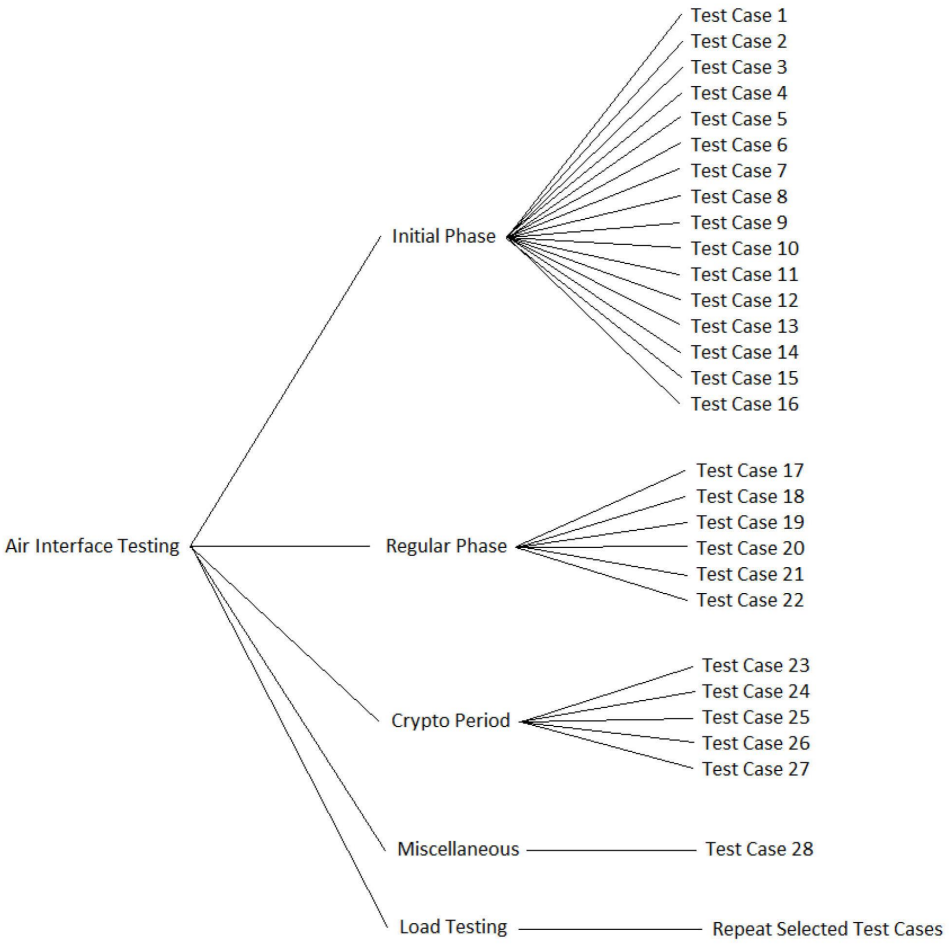

Рис. 3.3. – Розподіл тестування повітряного інтерфейсу

На рисунку 3.3 зображено підрозділи тестування ШІ, які відповідають різним обчисленням трафіку OTAK. У першому підрозділі моделювання радіоінтерфейсу (початкова фаза) включено 16 симуляційних сценаріїв. Враховуючи, що в мережі замовника середня кількість SC, які активні у TBS в конкретний момент часу, становить 3,5, результати моделювання можна підсумувати в таблиці 3.5.

Таблиця 3.5

Кількість повідомлень UL та DL OTAK, які враховуються для тестових випадків початкової фази

Початкові конфігурації на робочу зміну на TBS				
Смарт-карти	85 % від загальної кількості СК		15 % від загальної кількості СК	
3,571428571	3,04 ~ 3		0,535714286 ~ 1	
	DownLink OTAK	UpLink (Acks)	DownLink OTAK	UpLink (Acks)
	117	120	39	40

Щоб пояснити таблицю 3.5, слід врахувати такі моменти:

- Кожен DXT обслуговує в середньому 58,3 TBS.
- Кожен DXT обслуговує в середньому 15 000 SC від TR, що, розділене на 58,3 TBS, дає середнє значення 257,28 SC, які обслуговуються одним TBS в одному DXT.
- У мережі буде здійснено переміщення 1000 смарт-карт на E2EE з можливістю OTAK на день.
- У мережі клієнта функціонує 12 DXT.
- 1000 SC, переміщених на OTAK на день у всій мережі, в середньому означають, що на кожен DXT буде переміщено 83,33 SC.
- 83,33 SC, переміщених на DXT, поділених на 58,3 TBS, що обслуговуються DXT, дають нам середнє значення 1,42 SC на кожен TBS на день.
- У мережі клієнта працює 4 зміни по 6 годин.
- 1,42 SC, переміщених на кожен TBS на день, поділені на 4 робочі зміни, дають середнє значення 0,35 SC на кожну зміну.

Оскільки 0,35 SC на день на кожен TBS є недостатнім для моделювання здатності AI у критичних умовах, у симуляції було вирішено збільшити це число в 10 разів для отримання більш репрезентативного обсягу змодельованого трафіку. Це значення відображено в таблиці 3.5 у стовпці "Смарт-карти".

Відомо, що на початку робочої зміни більшість користувачів (приблизно 85%) реєструються в мережі, в той час як решта (приблизно 15%) підключаються після короткої паузи. Це сформувало основні показники, наведені в таблиці 3.5, де повідомлення OTAK для 3 SC (округлене значення для 85% TR) відокремлені від решти повідомлень OTAK для 1 SC (округлене для решти 15% TR).

Оскільки тестування відбувається через ШІ, немає необхідності аналізувати трафік на більше ніж 1 TBS. Це означає, що в тестовій мережі, представленій на малюнку 21, достатньо використовувати лише 4 радіостанції TH1n одночасно. Проте, з метою забезпечення стійкості та враховуючи наявність 35 радіостанцій TH1n під час тестування, було вирішено застосувати всі ці радіостанції для створення більшого навантаження на мережу та досягнення пікових значень.

3.5 Початкова фаза тестування

Початкова фаза моделювання складається з 16 симуляційних сценаріїв, у яких моделюється перенесення в середньому 4 смарт-карток на OTAK протягом однієї робочої зміни, а таких змін у симуляції передбачено 4 за день. Для змодельованого перенесення всіх 256 смарт-карт, які обслуговуються одним TBS у мережі клієнта, необхідно 16 симуляційних днів. Реальна міграція була змодельована із врахуванням тривалості близько півроку, оскільки кількість смарт-карт, які переходять, становить не 4, а 3,57 на TBS, поділені на 10. Проте для цілей симуляції таке спрощене припущення є виправданим.

Рисунок 3.4 є адаптованою версією попереднього малюнка. У ньому кожен "День" відповідає окремому тестовому сценарію. У перший день всі TR ще не налаштовані на OTAK E2EE, а щодня під час кожної робочої зміни передбачається міграція 4 TR. Графік відображає поступове збільшення кількості налаштованих TR із кроком 4. Передбачається, що користувачі TR залишаються в межах своєї робочої зміни, і жоден користувач не переходить із першої зміни до наступних. Таким чином, на другий день у першій робочій зміні налаштовані TR будуть лише ті, які були переведені в перший день у цій самій зміні.

На рисунку також відображено змодельований поділ користувачів на групи 85% і 15%. Часові інтервали, зазначені як 3/5 і 2/5, моделюють перші три хвилини у початковому періоді часу та дві хвилини у другому. Ці рамки були визначені на основі змодельованих сценаріїв, базованих на статистичних даних з мережі клієнта.

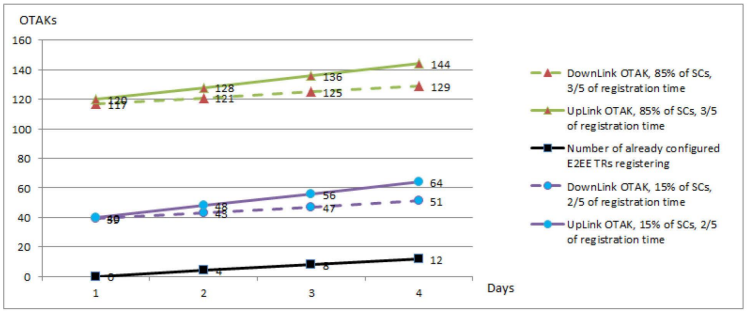

Рис. 3.4. Кількість повідомлень OTAK, що відповідають 4 першим тестовим випадкам початкової фази

На рисунку 3.4 представлено 16 тестових сценаріїв, але часові рамки, що відповідають рисунку 3.4, слід інтерпретувати як три окремі набори: перший - "Перші 3 хвилини і наступні 2 хвилини", другий - "Перші 3 хвилини і наступні 4 хвилини", і останній - "Перші 9 хвилин і наступні 6 хвилин". Це означає, що симуляції потрібно виконувати тричі для кожного сценарію, використовуючи різні часові рамки, що в підсумку охоплює тривалість 5, 10 і 15 хвилин відповідно. Такий підхід дозволяє змоделювати поведінку мережі при різних інтервалах застосування трафіку, адже в реальних умовах неможливо, щоб усі користувачі одночасно активували свої пристрої, тому тестування одного сценарію було б недостатнім.

На рисунку 3.4 значення "OTAK" вказують на кількість очікуваних повідомлень (UL і DL), якими обмінюються всі TR у межах одного TBS і KMF. Зазначено, що кількість повідомлень UL OTAK перевищує DL, оскільки протокол сигналізації OTAK передбачає додаткове повідомлення в напрямку UL. Наприклад, у "День 1" для інтервалу часу, відповідного 3/5 (тобто 3, 6 або 9 хвилин), кількість повідомлень становить 117 для DL і 120 для UL. Це обумовлено тим, що при початковій реєстрації трьох TR у KMF додаткове UL-повідомлення підвищує загальну кількість UL на 3 одиниці порівняно з DL, враховуючи застосований криптоплан.

Через обмеження конфіденційності не можна розкривати методологію обчислення кількості OTAK-повідомлень, які обмінюються кожним TR під час його реєстрації. Проте можна зазначити, що ці кількості є результатом налаштувань криптогруп та асоціацій, визначених у криптоплані, що використовується в KMF. У тестовій лабораторії кількість повідомлень для одного TETRA-радіо становить 40 DL та відповідну кількість UL.

3.6 Різні тестові випадки

Симуляційний сценарій, описаний у цьому розділі, досліджує здатність KMF управляти доставкою ключів у разі змодельованого збою дротової мережі, що з'єднує його з DXT через TCS. Суть моделювання полягає у створенні сценарію

недоступності TCS для KMF під час процесу доставки ключів, а потім у перевірці, що після змодельованого повторного підключення TCS система успішно відновлює процедуру без помилок.

KMF змодельовано з підтримкою підключення до кількох TCS через різні мережеві інтерфейси, що дозволяє досліджувати використання альтернативних маршрутів у разі відмови одного з мережевих з'єднань. Проте ця функціональність уже була перевірена під час попередніх етапів симуляції продукту й не входить до сфери цього дослідження.

Крім описаного симуляційного сценарію, передбачено можливість додавання потенційних майбутніх симуляцій до цього розділу.

Тестування навантаження

Метою цього етапу було повторити найскладніші тестові випадки з підвищеним рівнем фонового трафіку. Це досягалося шляхом збільшення кількості криптогруп і асоціацій у конфігурації KMF, щоб забезпечити більш інтенсивне навантаження на систему та оцінити її стійкість.

3.7 Етап тестування ШІ

Симуляція розпочалася після завершення підготовчого етапу, який включав дослідження всіх необхідних аспектів налаштування, конфігурації та обслуговування KMF, а також розгортання відповідного симуляційного середовища.

На початковому етапі симуляції були ідентифіковані ключові недоліки, які було змодельовано для аналізу й передачі на виправлення. Після внесення необхідних змін розпочався наступний симуляційний цикл, спрямований на перевірку усунення недоліків та виявлення нових потенційних проблем. Процес моделювання та усунення дефектів проходив у кілька повторюваних ітерацій до досягнення повного вдосконалення системи.

Симуляція охоплювала дослідження роботи радіостанцій, змодельованих для управління ключами OTAK, включаючи ідентифікацію можливих помилок у їх роботі. Особлива увага приділялася симуляційному аналізу трафіку через

повітряний інтерфейс, а також оцінці відповідності компонентів мережі встановленим вимогам.

Основна увага зосереджувалася на змодельованих процесах, пов’язаних із E2EE, зокрема на управлінні ключами в різних елементах системи, таких як KMF та смарт-карти радіостанцій. Головними завданнями було створення симуляційних моделей налаштування та підтримки KMF, дослідження поведінки системи під час змодельованих збоїв, передача інформації про виявлені недоліки відповідним командам для аналізу, а також подальший контроль результатів моделювання. Це дозволило підтвердити готовність системи до реального впровадження.

Змодельована ситуація вимагала постійної координації дій та аналізу результатів для формулювання висновків. Після виконання тесту здійснювалася перевірка журналів у KMF, що дозволяло відстежувати точну послідовність подій і визначати помилки, які виникали в ході симуляції роботи сервера. Аналіз журналів проводився також на рівні компонентів мережі, таких як DXT-TBS і TRs, з метою ідентифікації потенційних проблем і їх розташування в моделюваній системі.

Цей підхід забезпечував глибоке розуміння роботи системи, дозволяючи виявляти причини відхилень і своєчасно вживати необхідні заходи для корекції результатів симуляції. Результати такого аналізу були важливими для вдосконалення компонентів моделюваної системи, їхньої взаємодії та загальної стабільності.

3.8 Дефекти

Протягом симуляцій було ідентифіковано 24 недоліки, які демонстрували різний рівень впливу на функціонування системи. Деякі з них суттєво впливали на змодельованих користувачів і були одразу очевидними, тоді як інші проявлялися лише за певних змодельованих умов, але могли викликати серйозні проблеми зі стабільністю мережі. Також були менш важливі недоліки, які, попри відсутність критичного впливу, потребували усунення для забезпечення повної надійності системи.

Таблиця 3.6

Основні проблеми, виявлені під час тестування E2EE через ШІ

Суворість	Проблема	Опис	Як було виявлено
Критична	Резервне копіюванн я заважає доставці повідомле нь OTAK	Під час виконання автоматичного резервного копіювання, якщо воно збігається із завершенням криптоперіоду, KMF припиняє свою роботу та не доставляє повідомлення OTAK. Це відбувається через конфлікт обробки завдань резервного копіювання та доставлення ключів.	Помилка була виявлена під час тестування з коротким криптоперіодом, коли резервне копіювання, налаштоване на певний час, збіглося із завершенням криптоперіоду.
Критична	Збої криптомо дуля	Криптомодуль KMF може переходити у фатальний стан, коли ключі для нового криптоперіоду не були доставлені вчасно через перевантаження мережі, або коли реєстрація SC не вдалася. Це супроводжується сигналізацією тривоги та зміною індикатора криптомодуля на червоний у графічному інтерфейсі.	Помилки були виявлені під час тестування, яке включало створення високого навантаження в радіомережі та штучні збої в реєстрації SC.
Критична	Неправил ьна послідовн ість номерів у повторній передачі OTAK	При повторних спробах доставки OTAK KMF не завжди оновлює порядковий номер повідомлення. Це призводить до проблем, коли TR уже підтвердив попереднє повідомлення, але KMF інтерпретує це як нове.	Ця проблема була виявлена при аналізі сигналізації з високим мережевим навантаженням, яке включало фоновий трафік і сценарії з частими колізіями.
Критична	Невідпові дність порядку підтвердж ень рівнів зв'язку та додатків	У разі перевантаження мережі підтвердження рівня додатків може надійти до KMF раніше за підтвердження рівня зв'язку, що призводить до помилок у процесі доставки OTAK. Наприклад, KMF може повторно передавати повідомлення, яке вже було успішно доставлене.	Ця проблема потребувала детального аналізу всіх журналів системи, включаючи KMF, DXT, TBS і TR, під час роботи з високим навантаженням.

Для покращення аналізу виявлені недоліки були класифіковані за рівнем важливості. Критичні та основні проблеми об’єднано в одну групу, недоліки середньої важливості — в іншу, а менш значущі недоліки винесено в окрему

категорію. У цьому аналізі представлені найбільш значущі приклади, тоді як менш важливі дефекти було виключено для спрощення й уникнення зайвої деталізації.

Більш детальний опис кожного критичного дефекту подається після відповідних таблиць для забезпечення глибшого розуміння характеру цих проблем і їхнього потенційного впливу на систему.

Потік очікуваного трафіку OTAK в ідеальних умовах з точки зору KMF проілюстровано на наступному зображенні:

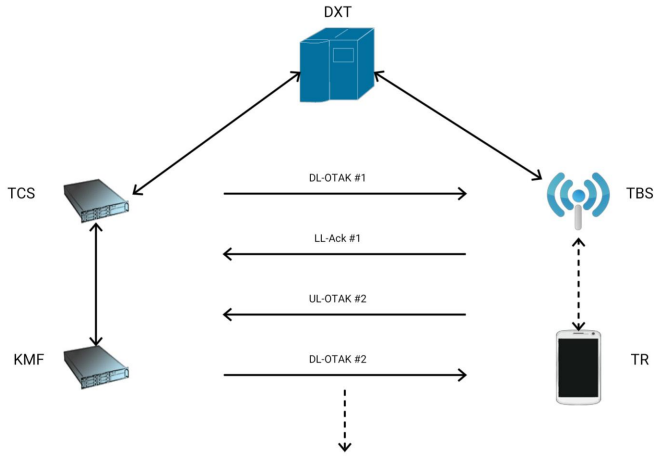

Рис. 3.5. Транспортний потік OTAK в ідеальних умовах

На ілюстрації представлено схему обміну повідомленнями OTAK, спрощену для кращого розуміння. Цей процес включає два рівні: базовий рівень, позначений як Link Layer (LL), і прикладний рівень (OTAK). При передачі повідомлень KMF спершу очікує підтвердження на рівні LL, а потім відповідь на рівні OTAK у вигляді UL-OTAK, яка підтверджує отримання попереднього DL-OTAK кінцевим користувачем.

Хоча на ілюстрації відображено ідеальний порядок передачі, у змодельованих умовах цей порядок не завжди зберігався. Під час симуляції було зафіксовано, що через перевантаження мережі, особливо на інтерфейсі AI, LL-Ack іноді надходив із запізненням порівняно з UL-OTAK. Оскільки система KMF не була адаптована до такого сценарію, це призводило до змодельованих помилок.

У поданому прикладі проілюстровано ситуацію для кращого розуміння. KMF спочатку передає DL-OTAK, умовно позначений як №1. Потім він отримує UL-OTAK №1, у той час як LL-Ack для цього повідомлення відсутній через затримку в мережі. Система продовжує передачу наступного DL-OTAK (№2) для того самого користувача. Коли ж LL-Ack, затриманий у мережі, нарешті надходить із запізненням, він невірно зіставляється з DL-OTAK №2. У разі, якщо цей LL-Ack є негативним, система хибно визначає збій для OTAK №2 і запускає повторну передачу цього повідомлення, що є помилкою.

3.9 Дефекти середньої важливості

У таблиці представлено дефекти середньої важливості, ідентифіковані в процесі симуляцій. У більшості випадків ці недоліки не викликають критичних збоїв у роботі змодельованої мережі або системи шифрування E2EE, проте деякі з них можуть призвести до серйозних проблем за певних змодельованих умов.

Таблиця 3.7

Дефекти середньої важливості, виявлені

Суворість	Проблема	Опис	Як було виявлено
Середня	KMF не виконує команди при неправильному часовому поясі	Алгоритм роботи KMF включає порівняння часу на сервері з позначками часу у завданнях, що стоять у черзі бази даних. Якщо сервер налаштовано на від'ємний часовий пояс (схід від GMT), KMF не може надіслати OTAK через помилку.	Проблема виявлена під час тестування, коли сервер було налаштовано на часовий пояс, відмінний від стандартного GMT.
Середня	Повільне відображення журналів у графічному інтерфейсі	При відкритті вкладки журналів графічного інтерфейсу завантажується вся таблиця з бази даних, що призводить до її зависання при великій кількості записів.	Помічено після накопичення великої кількості записів у базі даних під час тестування.

Продовж. табл.3.7

Середня	Надмірне навантаження при активації ключів OTAK	Якщо TR перебуває поза мережею кілька криптоперіодів, KMF зберігає завдання активації ключів для цих періодів. Коли TR підключається, всі ці завдання активуються одночасно, перевантажуючи мережу.	Виявлено під час тестів, коли кілька TR залишалися поза мережею протягом тривалого часу.
Середня	Тривалий час ручного запиту ключів	Під час запиту оновлення ключів шифрування через TR процедура займає занадто багато часу, що змушує користувача чекати або скасувати операцію.	Проблему зафіксовано при тестуванні функціональності TR у специфічних сценаріях.
Середня	Усі повідомлення OTAK позначені як високопріоритетні	KMF надсилає всі повідомлення OTAK із позначкою високого пріоритету, навіть якщо вони не є критичними. Це призводить до зменшення пропускної здатності для більш важливого трафіку.	Виявлено під час спроби налаштувати пріоритети трафіку OTAK у тестовій мережі.
Середня	Неможливість запустити службу KMF через помилку автентифікації	Під час запуску служби KMF виникає помилка автентифікації між компонентами SC4KMF і MGEM, що блокує роботу системи.	Виявлено під час початкових спроб налаштування та запуску програмного забезпечення.
Середня	Повторна передача повідомлень OTAK для недоступних TR	KMF повторно надсилає повідомлення OTAK, навіть якщо TR був вимкнений вручну та недоступний. Це створює марне навантаження на мережу.	Проблему виявлено під час тестування в умовах недоступності TR.
Середня	Довготривале виконання команд графічного інтерфейсу	Команди з видалення конфігурацій шифрування та перезавантаження ключів не мають високого пріоритету, через що виконуються з затримкою.	Помічено під час роботи з графічним інтерфейсом у ручному режимі.

Окремо представлено менш важливі дефекти, які не мають критичного значення та не повинні впливати на першу версію KMF. Однак вони заслуговують на увагу і мають бути враховані під час розробки наступної версії системи.

Таблиця 3.8

Незначні дефекти, виявлені під час тестування OTAK E2EE через ШІ

Суворість	Опис проблеми	Як її виявлено	Ідентифікатор
незначна	Резервне копіювання, що виконується щодня о 1:00, перешкоджає роботі криптомодуля KMF, якщо криптоперіод завершується одночасно або під час виконання резервного копіювання. Це призводить до збоїв у доставці повідомлень.	Під час тестування з короткими криптоперіодами, налаштованими щогодини, проблема виникла через перетин із резервним копіюванням.	1
незначна	Криптомодуль KMF подає сигнал тривоги через відсутність ключів для поточного криптоперіоду або збій реєстрації SC, що призводить до фатального стану.	Виявлено під час введення радіочастотних перешкод та перевантаження мережі, що ускладнювали доставку ключів або успішну реєстрацію SC.	2
незначна	Відсутність коректного збільшення порядкового номера при повторних спробах доставки повідомлень OTAK, що спричиняє збої у взаємодії з TR.	Проблема виникла під час аналізу сигналізації у мережі з високим навантаженням і умовами загасання, які створили численні колізії доступу.	3
незначна	Некоректний порядок підтверджень: підтвердження рівня додатків приходить перед підтвердженням рівня зв'язку, що викликає повторну відправку повідомлень.	Проблема виявлена під час налагодження з високим навантаженням та детальним аналізом журналів KMF, DXT, TBS і TR.	4

Таблиця містить перелік незначних дефектів, виявлених під час тестування. Хоча ці недоліки не мають критичного впливу на функціонування системи, вони заслуговують на увагу. Ці дефекти не є пріоритетними для включення до першої версії KMF, проте їх необхідно врахувати під час розробки наступної версії, щоб забезпечити подальше вдосконалення системи.

3.10 Висновки до розділу 3

У розділі 3 досліджено ефективність системи управління ключами шифрування (KMF) у мережах TETRA через симуляцію та тестування. Визначено, що запропоновані алгоритми забезпечують надійну та автоматизовану доставку ключів за допомогою механізму Over The Air Keying (OTAK), що значно підвищує ефективність та безпеку системи. Тестування охоплювало різні сценарії навантаження, виявлення дефектів та їх аналіз, що дало змогу вдосконалити адаптивність системи до реальних умов роботи. Отримані результати демонструють переваги використання розроблених рішень, які забезпечують захист даних, мінімізують ризики кіберзагроз та сприяють стабільності системи в умовах високого трафіку, що робить їх придатними для впровадження у критично важливих телекомунікаційних мережах.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Значення адаптації в трудовому процесі.

Трудова діяльність людини нерозривно пов'язана з виробничим оточенням. Ефективне виконання роботи працівником можливе лише при наявності оптимальних зовнішніх умов. У разі зміни цих умов на несприятливі, організм людини активує спеціальний механізм адаптації, який забезпечує стійкість внутрішнього середовища або його припустиму зміну. Адаптація є важливим інструментом у запобіганні травматичних ситуацій, нещасних випадків під час праці та має велике значення для охорони праці.Адаптація - це процес, за допомогою якого організм та його органи адаптуються до змінних умов зовнішнього середовища.

Адаптація в трудовій сфері може приймати різні форми, у науковій літературі визначаються такі як фізіологічна, психологічна, соціальна та професійна [43,44,45,46,47].

Фізіологічна адаптація включає комплекс фізіологічних реакцій, які сприяють пристосуванню організму до змін зовнішніх умов і збереженню стійкості його внутрішнього середовища, що називається гомеостазом. Гомеостаз передбачає динамічну рівновагу між організмом та зовнішнім середовищем, забезпечуючи стійкість основних фізіологічних функцій людського організму. Адаптаційний механізм полягає у внутрішніх змінах, які відбуваються в організмі, щоб відповісти на зміни у зовнішньому середовищі. Це включає зміни чутливості аналізаторів, розширення фізіологічних резервів організму та модифікацію певних параметрів функцій організму в межах допустимого. Фізіологічна адаптація дозволяє підтримувати стабільність організму під впливом холоду, тепла, недостатнього кисню, зміни атмосферного тиску та інших факторів. При цьому реактивність організму та його початковий функціональний стан впливають на процес фізіологічної адаптації.

Фізіологічна адаптація до роботи є активним процесом, і за сприятливих умов виробничого середовища та оптимальних навантажень вона підвищує стійкість і продуктивність організму, розширює його резервні можливості та зменшує ризик захворювань і травматизму. Однак коливання умов праці мають свої межі, і якщо інтенсивність впливу факторів виробничого середовища перевищує можливості адаптації організму, можуть виникнути патологічні зміни в фізіологічних системах, що призводить до зниження стійкості та погіршення здоров'я.

Психологічна адаптація відображає процес, за яким особистість намагається встановити оптимальну гармонію з оточуючим середовищем під час виконання своєї діяльності. Різні фактори, такі як швидкість обробки інформації, пам'ять, сприйняття та реакція на стресові ситуації, впливають на процес психологічної адаптації. При виконанні праці психологічна адаптація залежить від особистих характеристик працівника, його психічного стану, реакцій на стрес та конкретних умов праці.

Соціальна адаптація відображає процес пристосування працівника до системи взаємодії у робочому колективі, включаючи норми, правила, традиції та цінності. Під час соціальної адаптації працівник засвоює різноманітну інформацію про колектив, в якому працює, і про систему професійних та особистих відносин. Цей процес може вимагати часу та зусиль, але в результаті працівник стає більш інтегрованим у колектив та здатним ефективно взаємодіяти з іншими працівниками.

Кожен з видів адаптації важливий для успішного функціювання працівника в трудовій діяльності. Фізіологічна адаптація дозволяє зберегти стійкість організму і здоров'я в умовах різних фізичних навантажень і впливів довкілля. Психологічна адаптація сприяє розвитку ефективних когнітивних та емоційних стратегій, що допомагають працівнику успішно впоратися з різними викликами та стресовими ситуаціями. Соціальна адаптація допомагає створити гармонійні відносини в колективі та впливає на задоволеність праці та загальний клімат у робочому середовищі. Всі ці види адаптації взаємопов'язані і спільно впливають на пристосування працівника до трудової діяльності і його успішність.

Якщо процес соціальної адаптації протікає незадовільно, це може призвести до підвищення рівня стресу на роботі, що може вплинути на поведінку працівника і спричинити між особові конфлікти або нещасні випадки.

Професійна адаптація - це процес пристосування до трудової діяльності в усіх її аспектах, включаючи адаптацію до робочого місця, інструментів і засобів праці, об'єктів та матеріалів, особливостей технологічних процесів, робочого графіку і т.д.

Професійна адаптація проявляється у розвитку стійкого позитивного ставлення працівника до своєї професії, набутті необхідного рівня вмінь і навичок, формуванні властивостей, необхідних для якісного виконання роботи. Вона визначається необхідним мінімумом знань і навичок, які працівник отримав під час навчання на спеціальності, ступенем відповідальності, практичністю, діловитістю і т.д. Адаптація вважається завершеною, коли працівник досягає кваліфікації, яка відповідає наявним стандартам.

Кожен з розглянутих видів адаптації впливає на працездатність та здоров'я працівника, формує певний рівень чутливості і стійкості до психоемоційного навантаження, яке, у разі негативного розвитку, може суттєво змінити надійність професійної діяльності.

4.2 Психофізіологічне розвантаження для працівників

За умови високого рівня робіт з ЕОМ рекомендується психофізіологічне розвантаження у спеціально обладнаних приміщеннях (кімнати психофізіологічного розвантаження) під час регламентованих перерв або в кінці робочого дня.

При проведенні сеансів психофізіологічного розвантаження рекомендується використовувати деякі елементи методу аутогенного тренування, який ґрунтується на свідомому застосуванні комплексу взаємопов’язаних прийомів психічної саморегуляції й виконанні нескладних фізичних вправ зі словесним самонавіюванням.

Згідно ‘’ДСанПіН 3.3.2.007-98’’ [48] наведено перелік протипоказань з боку органів зору та загальних (соматичних) протипоказань, які забороняють роботу на ЕОМ, а також комплекс вправ для поліпшення здоров’я і підвищення працездатності.

Зменшення негативного впливу шкідливих випромінювань і речовин

Для зменшення негативного впливу шкідливих випромінювань від дисплеїв ВДТ і комп’ютерів і поліпшення самопочуття працюючих використовують приекранні фільтри, а для зниження величини потенціалу зарядів статичної електрики рекомендують застосовувати антистатичне покриття підлоги та зволоження повітря. Від торсійної компоненти штучних електромагнітних випромінювань та полів технічних гарантованих засобів захисту поки що не знайдено.

Для запобігання дії шкідливих речовин встановлюють місцеву припливно-витяжну вентиляцію.

Зниження шуму

З метою зниження шуму до санітарно-гігієнічних норм застосовують шумопоглинаючі засоби, вибір яких визначається інженерно-акустичними розрахунками. В якості шумопоглинаючих засобів використовуються негорючі або важкогорючі перфоровані плити, панелі, мінеральна вата, підвісні стелі та інше.

Забезпечення необхідного освітлення

Приміщення для роботи з ВДТ і ПЕОМ повинні мати природне та штучне освітлення. Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природної освітленості (КПО) не нижче ніж 1,5%. У разі переважної роботи з документацією можуть додатково встановлюватися світильники місцевого освітлення. Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300–500лк. Світильники місцевого освітлення не повинні створювати відблисків на поверхні екрану дисплею.

Забезпечення нормального мікроклімату

Нормативні параметри мікроклімату для приміщень з ВДТ та ПЕОМ мають знаходяться в межах: для температури 21–250с, для відносної вологості –40– 60%,

для швидкості руху повітря – 0,1–0,2м/с і мало залежати від пори року та категорії робіт.

Для підтримки допустимих значень мікроклімату та іонного складу повітря необхідно передбачати установки і прилади зволоження або штучної іонізації та кондиціонування повітря

4.3 Висновки до розділу 4

У підрозділі з охорони праці проаналізовано питання адаптації працівників до трудового середовища, зокрема фізіологічної, психологічної, соціальної та професійної адаптації, а також їхнього впливу на здоров’я, працездатність і безпеку праці.

У підрозділі з безпеки в надзвичайних ситуаціях проаналізовано питання психофізіологічного розвантаження працівників, забезпечення нормативного мікроклімату, зниження впливу шкідливих факторів, таких як шум, випромінювання та шкідливі речовини, а також заходи щодо покращення умов освітлення.

ЗАГАЛЬНІ ВИСНОВКИ

Було ідентифіковано багато недоліків, включаючи критичні, які могли призвести до значного погіршення або повного виходу з ладу частини змодельованої мережі клієнта, якщо б ці проблеми виникли у реальних умовах експлуатації.

Симуляція через радіоінтерфейс відіграла ключову роль у дослідженні рішення наскрізного шифрування. Це пов’язано з тим, що радіоінтерфейс є найбільш уразливим місцем у будь-якій бездротовій чи стільниковій мережі через фізичні обмеження та специфіку використання радіочастотного спектру.

Отримані результати симуляцій забезпечили створення більш надійного та вдосконаленого продукту. Це значно покращило функціональність системи управління ключами (KMF) та її інтеграцію з існуючим рішенням наскрізного шифрування. Верифікація підтвердила коректну роботу нових функцій, зокрема механізму Over The Air Keying (OTAK), який забезпечив ефективніший та автоматизований спосіб доставки ключів шифрування кінцевим користувачам у порівнянні з попередніми методами.

Розроблені вдосконалення сприяють підвищенню продуктивності як системи, так і клієнтського обладнання, пропонуючи зручний та ефективний інструмент для розповсюдження ключів. Це приносить вигоди як для компанії, так і для клієнтів, які тепер отримують більш надійне та автоматизоване рішення для щоденних комунікацій.

Під час подальших ітерацій симуляцій і розробки програмного забезпечення було визначено напрямки для вдосконалення, що дозволять усунути виявлені недоліки та додати нові функції в майбутньому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Химич, Г., Дунець, В., Дуда, С., Паляниця, Ю., & Корнєєв, К. (2023). Двополяризаційна антена Ягі-Уда метрового діапазону довжин хвиль. Вісті вищих учбових закладів. Радіоелектроніка, 66(11), 680-688.
2. Khvostivska, L., Khvostivskyi, M., Dediv, I., Yatskiv, V., & Palaniza, Y. (2023, June). Method, Algorithm and Computer Tool for Synphase Detection of Radio Signals in Telecommunication Networks with Noises. CEUR Workshop Proceedings. Proceedings of the 1st International Workshop on Computer Information Technologies in Industry 4.0. 173-180. 2023..
3. Velychko, D., Osukhivska, H., Palaniza, Y., Lutsyk, N., & Sobaszek, Ł. (2024). Artificial Intelligence Based Emergency Identification Computer System. Advances in Science and Technology. Research Journal, 18(2). 2024.
4. Драґан, Я. П., Грицюк, Ю. І., & Паляниця, Ю. Б. (2015). Системний аналіз–засіб обґрунтування математичної моделі досліджуваного об'єкта як системи. In Advanced Information and Communication Technologies-2015: Proceedings of 1st International Conference (AICT'2015) (pp. 159-161). Advanced Information And Communication Technologies-2015.
5. Химич, Г., Дунець, В., Дуда, С., Паляниця, Ю., & Корнєєв, К. (2023). Двополяризаційна антена Ягі-Уда метрового діапазону довжин хвиль. Вісті вищих учбових закладів. Радіоелектроніка, 66(11), 680-688.
6. Бішоп, М. (2008)Вступ до комп’ютерної безпеки . 4тисред. Вестфорд, Массачусетс: Addison - Wesley.
7. ETSI (2016)TETRA . Доступно за адресою:http://www.etsi.org/technologies - clusters/technologies/tetra [Дата
8. звернення: 29тисЛютий 2016]
9. Фінляндія. Airbus Defence and Space. (2015, a).ОГЛЯД КУРСУ TETRA E2EE (рішення E2EE на основі KMF із використанням
10. OTAK) .

11. Фінляндія. Airbus Defense and Space (2015, b).Опис продукту диспетчерської робочої станції TETRA
12. (DWS). Фінляндія: Airbus Defence and Space. (Випуск системи TETRA 6.5 – 7, DN05221844 - 10 - 0en).
13. Фінляндія. Airbus Defense and Space (2015, c). Опис продукту TCS. Фінляндія: Airbus Defence and
14. Space. (TETRA System Release 6.0 - 7.0, DN0116031 - 20 - 0en).
15. Фінляндія. Airbus Defense and Space (2015, d). Курс навчання. Фінляндія: Airbus Defence and Space. (Курс
16. системи TETRA, ED07.01en).
17. Фінляндія. Кассидіан (2013).Аутентифікація в системі TETRA. Фінляндія: Cassidian. Компанія EADS.
18. (TETRA SYSTEM RELEASE 6.0 – 6.5, TRASYSAPP00003 - 02 - 3en).
19. Фортуна (2016)Ще один великий додаток для обміну повідомленнями приєднується до групи наскрізного шифрування . Доступно за
20. адресою: http://fortune.com/2016/04/19/viber - e2e - encryption/ [Дата звернення: 27тисквітень 2016]
21. Кеттерлінг Х. (2003)Введення в цифрове професійне мобільне радіо . Норвуд, США: Artech House
22. Books.
23. Нью - Йорк Таймс (2016)WhatsApp представляє наскрізне шифрування . Доступно за адресою: http://
24. www.nytimes.com/2016/04/06/technology/whatsapp - messaging - service - introduces - fullencryption.html?_r=0 [Дата
25. звернення: 27тисквітень 2016]
26. Пул І. (2006)Пояснення стільникового зв’язку: від основ до 3G . GBR: Newnes: Jordan Hill.
27. Безпечний наземний зв'язок (2015)Рішення [онлайн] Доступно з: http://
28. www.securehybridcomms.com/solutions [Дата звернення: 13тисжовтень 2015 р.]

29. SELEX Communications (2007)Знайомство з TETRA . Доступно за адресою: http://www.ok1mjo.com/all/tetra/
30. vseobecne_informace/TETRA_Selex_Introduction_to_TETRA_Terrest rial - Trunked - RAdio.pdf [Дата звернення: 29тис
31. Лютий 2016]
32. 68
33. Столлінгс В. і Браун Л. (2008)Принципи та практика комп'ютерної безпеки . Верхня річка Седл: Пірсон Прентіс
34. Холл.
35. Штурцель, А. (2015)Airbus Defense and Space представляє новий сервер DXTA Tetra з більшою місткістю та
36. новими можливостями . Доступно за адресою:http://www.airbusgroup.com/int/en/news - media/press - releases/
37. Airbus - Group/Financial_Communication/2015/05/20150520_airbus_defence_and_space_d xta_tetra_server.ht ml
38. [Дата доступу: 17 лютого 2016 р.]
39. TCCA (2016)Безпека TETRA . Доступно за адресою:http://www.tandcca.com/about/page/12027 [Доступ: 2nd
40. Березень 2016]
41. WhatsApp (2016)Огляд шифрування WhatsApp Технічна документація . Доступно за адресою: https://
42. www.whatsapp.com/security/WhatsApp - Security - Whitepaper.pdf [Дата звернення: 27тисквітень 2016]
43. Лукашевич Н. П. Виробнича адаптація як елемент трудовий кар'єри працівника. — К.: Знання, 2004.
44. Шекшня С.В. Управління персоналом сучасної організації. – М., 2006.
45. Комісарів Т.А. Управління людськими ресурсами. – Видавництво «Справа», 2002.

46. Вершиніна Т. Н. Взаємозв’язок плинності і виробничої адаптації робітників. — К., 2004.
47. Іванова Е. М. Основи психологічного вивчення професійної діяльності. — М., 2002
48. Котиков И. Д. Цивілізація й адаптація. — М.: Прогрес, 2000.

ДОДАТКИ

Додаток А

Копія тези

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XIII Міжнародної науково-практичної конференції молодих учених та студентів
11-12 грудня 2024 року

УКРАЇНА
ТЕРНОПІЛЬ – 2024

Матеріали XIII Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль,11-12 грудня 2024 року

УДК 621.391

О.П. Трухан, Ю.Б. Паляниця, канд. техн. наук, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МАТЕМАТИЧНА МОДЕЛЬ КЛЮЧІВ ШИФРУВАННЯ В МЕРЕЖАХ TETRA ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

O.P. Truhan, Y.B. Palaniza, PhD.

MATHEMATICAL MODEL OF ENCRYPTION KEYS IN TETRA NETWORKS FOR TELECOMMUNICATION SYSTEMS

У даній роботі досліджується методика впровадження математичної моделі ключів шифрування для забезпечення безпеки зв’язку в мережах TETRA. Зокрема, реалізується наскрізне шифрування (E2EE) з використанням механізму Over The Air Keying (OTAK), що дозволяє автоматизувати розподіл ключів без фізичного доступу до пристроїв. У межах проекту здійснено системне тестування, виявлення дефектів, а також оптимізацію параметрів передачі ключів у середовищі з високим навантаженням.

Запропоноване рішення найбільш оптимально інтегрується з системами, що використовують стандарт GMR (GEO Mobile Radio Interface). Воно може бути застосоване в мережах із геостаціонарними супутниками (GEO), що оперують у Ku- та Ka-діапазонах, оскільки вони забезпечують високу пропускну здатність для сигналізації OTAK.

Також система може працювати з іншими телекомунікаційними стандартами, наприклад, DVB-S2X для широкомовлення та VSAT для фіксованого зв’язку, що дозволяє адаптувати рішення до спеціалізованих потреб, таких як навігаційні системи або віддалені мережі.

Модуляції та методи передачі

Для забезпечення стійкості передачі використовуються сучасні схеми модуляції:

QPSK (Quadrature Phase Shift Keying) для базової надійності;

8PSK (8 Phase Shift Keying) для підвищеної пропускної здатності;

OFDM (Orthogonal Frequency Division Multiplexing) для зменшення інтерференції між каналами.

Для підвищення точності та надійності передачі даних у телекомунікаційних мережах з шумами можуть бути використані методи синфазного виявлення радіосигналів, що базуються на спеціалізованих алгоритмах та комп'ютерних інструментах [4].

Результати дослідження

Створено математичну модель розподілу ключів у мережах TETRA.

Виявлено та усунено понад 10 критичних дефектів у процесі інтеграції рішення OTAK.

Збільшено ефективність передачі ключів, що дозволило масштабувати мережу до тисяч активних користувачів.

Результати свідчать про доцільність впровадження механізму OTAK для захищеного зв’язку у великих мережах.

Література

1. Stallings, W., Brown, L. Computer Security: Principles and Practice. Pearson Education, 2008.
2. Airbus Defence and Space. Security features in TETRA systems. 2015.
3. ETSI. TETRA standardization documentation. 2016.
4. https://scholar.google.com.ua/citations?view_op=view_citation&hl=uk&user=_80WiBwAAAAJ&citation_for_view=_80WiBwAAAAJ:SeFeTyx0c_EC

СЕКЦІЯ: ФУНДАМЕНТАЛЬНІ ПРОБЛЕМИ ХАРЧОВИХ, БІО- ТА НАНОТЕХНОЛОГІЙ