МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

КОЧІЙ Андрій Васильович

Алгоритм підвищення рівня інформаційної безпеки IP-телефонії з врахуванням характеристик протоколів розподілених ключів / Algorithm for Increasing the Level of information security of IR-telephony taking into account the characteristics of distributed key Protocols

спеціальність: 123 - Комп'ютерна інженерія
освітньо-професійна програма - Комп'ютерна інженерія
Кваліфікаційна робота

Виконав студент групи КІм-21
А.В. Кочій

Науковий керівник
к.т.н., І.Р.Паздрій

ТЕРНОПІЛЬ - 2023

РЕЗЮМЕ

Кваліфікаційна робота на тему “Алгоритм підвищення рівня інформаційної безпеки IP-телефонії з врахуванням характеристик протоколів розподілених ключів” зі спеціальності 123 «Комп’ютерна інженерія» освітнього ступеня «магістр» написана обсягом сторінок і містить ілюстрацій, таблиць, 2 додатки та 50 джерел за переліком посилань.

Метою роботи є підвищення рівня інформаційної безпеки в захищених каналах IP-телефонії та скорочення часу, необхідного для встановлення безпечного з'єднання. Основними завданнями є розробка модифікації протоколу розподілу ключів для покращення імовірнісно-часових характеристик протоколу, розробка алгоритму виявлення порушника протоколів розподілу ключів, що ґрунтуються на алгоритмі Діффі-Хелмана.

Методи дослідження ґрунтуються на теорії побудови графів, основ криптографії, методах імітаційного моделювання, теорії ймовірності, теорії обробки та аналізу інформаційних даних.

У кваліфікаційній роботі запропонована модель порушника атаки на протоколи безпеки IP-телефонії. Запропонована оцінка імовірнісно-часових характеристик протоколів розподілу ключів. Запропонований алгоритм, який дозволяє виявляти активних порушників протоколу у каналі зв'язку, дозволяє знизити ймовірність успішної атаки НСД для порушника протоколів і може бути використаний при проектуванні, розробці та реалізації рішень захищеної IP-телефонії, які мають режим роботи без сервера, а також для вдосконалення існуючих рішень. Оцінки імовірнісно-часових характеристик можуть використовуватися в розрахунках при проектуванні рішень щодо захищеної IP-телефонії, які використовують у своєму складі протоколи розподілу ключів.

КЛЮЧОВІ СЛОВА: АЛГОРИТМ, ІМОВІРНІСНО-ЧАСОВІ ХАРАКТЕРИСТИКИ, IP-ТЕЛЕФОНІЯ, НЕСАНКЦІОНОВАНИЙ ДОСТУП.

RESUME

The qualification work on the topic "Algorithm for increasing the level of information security of IR-telephony taking into account the characteristics of distributed key protocols" from the specialty 123 "Computer Engineering" of the master's degree is written in the volume of pages and contains illustrations, tables, 2 appendices and 50 sources as listed links

The purpose of the work is to increase the level of information security in protected IP telephony channels and reduce the time required to establish a secure connection. The main tasks are the development of a modification of the key distribution protocol to improve the probabilistic-time characteristics of the protocol, the development of an algorithm for detecting a violator of key distribution protocols based on the Diffie-Hellman algorithm.

The research methods are based on the theory of graph construction, the basics of cryptography, simulation modeling methods, probability theory, the theory of information data processing and analysis.

In the qualification work, a model of the violator of an attack on IP telephony security protocols is proposed. Proposed assessment of probabilistic-time characteristics of key distribution protocols. The proposed algorithm, which allows detecting active protocol violators in the communication channel, reduces the probability of a successful NSD attack for a protocol violator and can be used in the design, development, and implementation of secure IP telephony solutions that have a serverless mode of operation, as well as for improvement of existing solutions. Estimates of probabilistic time characteristics can be used in calculations when designing solutions for secure IP telephony that use key distribution protocols.

KEYWORDS: ALGORITHM, PROBABILITY-TIME CHARACTERISTICS, IR-TELEPHONY, UNAUTHORIZED ACCESS.

ЗМІСТ

Вступ ……....6
Перелік умовних скорочень і позначень …….....10
1 Аналіз напряму досліджень в області захищеної IP-телефонії ……..…11
1.1 Принципи передачі голосової інформації в мережах з пакетною комутацією …….……..…11
1.2 Забезпечення якості та методи її оцінки в IP-телефонії ……...…...16
1.3 Забезпечення інформаційної безпеки IP- телефонії …….....24
1.4 Висновки до розділу 1. ……..31
2 Модель активного зловмисника для захищеної IP-телефонії ….……32
2.1 Загрози інформаційної безпеки в IP-телефонії ……..……....33
2.2 Узагальнена модель зловмисника ……35
2.3 Зовнішній порушник ……..……..……...…….40
2.4 Висновки до розділу 2.……48
3 Алгоритми вдосконалення протоколів розподілу ключів ……...……49
3.1 Підвищення безпеки ZRTP за рахунок автоматичної автентифікаційної перевірки рядка……...…....51
3.2 Виявлення порушника протоколів розподілу ключів, побудованих на алгоритмі Диффі- Хелмана …….……..…59
3.3 Експериментальне дослідження розробленого алгоритму ……..……66
3.4 Висновки до розділу 3 ……..……68
Висновки ……..……69
Список використаних джерел ……..…..70
Додаток А Довідка про використання ……75
Додаток Б Світлокопія публікацій……....76

ВСТУП

Сучасному світі розвитку телекомунікацій відповідають зростаючі обсяги трафіку в корпоративних мережах, зокрема, в мережах Інтернет-провайдерів.

Актуальність теми. Розробка нових протоколів, а також передача голосових пакетів у відкритому вигляді через мережі загального користування призвели до появи та стандартизації протоколів безпеки IP-телефонії. Протоколи були розділені на три групи відповідно до завдань, що вирішуються: забезпечення безпеки сигналізації, захист медіа-трафіку та розподіл ключів для медіа-трафіку.

Стандартизація протоколів, а також широке використання персональних комп'ютерів як терміналів користувача для послуг IP-телефонії призвели до розробки великої кількості програм IP-телефонії, включаючи програмне забезпечення з відкритим вихідним кодом. Це дозволяє розширювати можливості та використовувати додаткові алгоритми в програмах.

Робота присвячена дослідженню протоколів забезпечення інформаційної безпеки IP-телефонії, а також розробці пропозицій щодо вдосконалення цих протоколів з метою підвищення безпеки та ефективного функціонування по каналах зв'язку з різними параметрами. Тематика відповідає сучасній науковій проблематиці та є актуальною.

Мета і завдання дослідження. Метою є підвищення рівня інформаційної безпеки в захищених каналах IP-телефонії та скорочення часу, необхідного для встановлення безпечного з'єднання. Для досягнення поставленої мети слід провести дослідження існуючих протоколів безпеки IP-телефонії, їх параметрів, характеристик і особливостей, а також впливу протоколів на показники якості. У роботі слід запропонувати моделі порушника для оцінки безпеки IP-телефонії та методику оцінки імовірнісно-часових характеристик протоколу розподілу захищених ключів IP-телефонії. Основними завданнями є розробка модифікації протоколу розподілу ключів для покращення імовірнісно-часових характеристик

протоколу, розробка алгоритму виявлення порушника протоколів розподілу ключів, що ґрунтуються на алгоритмі Діффі-Хелмана, розробка пропозицій щодо модифікації протоколу Zimmermann Real-time Transport Protocol (ZRTP) для підвищення безпеки кореспондентів при взаємодії без сервера у топології клієнт-клієнт.

Об’єкт дослідження. Об’єктом дослідження є захищена IP-телефонія з протоколами розподілу ключів.

Предмет дослідження. Предметом дослідження є алгоритми та протоколи, що забезпечують інформаційну безпеку IP-телефонії, а також імовірнісно-часові характеристики цих протоколів.

Методи досліджень. Методи дослідження базуються на теорії побудови графів, основ криптографії, методах імітаційного моделювання, теорії ймовірності, теорії обробки та аналізу інформаційних даних.

Наукова новизна одержаних результатів. У роботі запропонована модель порушника, яка відрізняється від відомих аналогів врахуванням атаки на протоколи безпеки IP-телефонії. Запропонована оцінка імовірнісно-часових характеристик протоколів розподілу ключів. На відміну від існуючих, враховує особливості протоколів розподілу ключів, що враховують обмеження кількості повторних передач повідомлень. Описаний спосіб ідентифікації зловмисників, на відміну від існуючих, дозволяє виявляти активних порушників протоколу у каналі зв'язку, що використовується, за відсутності загального довіреного центру або ключа між кореспондентами, а також виявляти фірмових порушників. Модифікований протокол ZRTP, що відрізняється меншим часом успішного завершення, що знижує часові витрати під час роботи протоколу каналами зв'язку.

Практичне значення отриманих результатів. Виявлення порушника дозволяє автоматично виявити втручання порушника протоколів у зв'язок між кореспондентами для протоколу ZRTP без участі користувача. Алгоритм дозволяє знизити ймовірність успішної атаки НСД для порушника протоколів і може бути використаний при проектуванні, розробці та реалізації рішень

захищеної IP-телефонії, які мають режим роботи без сервера, а також для вдосконалення існуючих рішень. Оцінки імовірнісно-часових характеристик можуть використовуватися в розрахунках при проектуванні рішень щодо захищеної IP-телефонії, які використовують у своєму складі протоколи розподілу ключів.

Публікації та апробація КМР. За результатами КМР підготовлені тези на VIII Науково-практичну конференцію «Інтелектуальні системи та мережі» ЗУНУ, каф. КІ, 5 грудня 2023р. [Додаток А].

Впровадження результатів КМР. Впровадження практичних результатів КМР планується [Додаток Б].

У першому розділі розглянуто актуальні проблеми та існуючі підходи їх вирішення у сфері захищеної IP-телефонії. Зокрема, розглянуто основні компоненти та протоколи IP-телефонії, а також можливі сценарії встановлення з'єднань. Описано механізми та алгоритми, що застосовуються для забезпечення нормованого показника MOS, а також значень інших нормованих показників. Показано значення параметрів каналу зв'язку, за яких має сенс виконувати аналіз роботи протоколів IP-телефонії. Проаналізовано дослідження у галузі забезпечення безпеки IP-телефонії та виявлено відсутність досліджень про вплив протоколів безпеки на нормовані параметри функціонування мережі телефонії. Показано вплив протоколів безпеки на параметри функціонування мережі телефонії, виражене у виникненні затримки під час встановлення захищеного з'єднання між кореспондентами.

У другому розділі наведено визначення порушника та опис терміналу користувача. Показано сукупність атак, які може виконувати порушник задля досягнення НСД. Представлено модель активного порушника для захищеної IP-телефонії, яка враховує можливості цього порушника реалізувати атаку MITM на ПРК та інші атаки. Модель дозволяє розрахувати ймовірність успішної атаки, націленої на НСД. Показано, що особливу небезпеку становлять зовнішній та внутрішній порушники, які виконують атаку на обладнання оператора.

Представлено імовірнісну модель такого порушника. Показано, що найнебезпечнішою є атака MITM на протоколи розподілу ключів.

У третьому розділі запропонований алгоритм виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана. Алгоритм використовує декілька відкритих каналів зв'язку. Виявлення порушника відрізняється зниженою ймовірністю успішної атаки MITM, а також наявністю механізму визначення активного порушника в каналі зв'язку навіть за відсутності заздалегідь розподіленого загального ключа. Однак, даний алгоритм накладає обмеження на канали зв'язку, що використовуються. Він полягає в тому, що канали зв'язку повинні бути незалежні.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ

КЗ – канал зв'язку

НСД – несанкціонований доступ

ПРК – протокол розподілу ключів

ТФСК – телефонна мережа спільного користування

ТС – телефонна станція

МСЕ – Міжнародний Союз Електрозв'язку

1 АНАЛІЗ НАПРЯМУ ДОСЛІДЖЕНЬ В ОБЛАСТІ ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ

1.1 Принципи передачі голосової інформації в мережах з пакетною комутацією

Протоколи IP-телефонії поділяються на великі групи, а саме протоколи передачі медіа інформації по пакетних мережах, а також протоколи управління встановленням з'єднання.

У першу групу входить протокол RTP (Real-time Transport Protocol) [1], який використовується поверх UDP (User Datagram Protocol) протоколу. Сукупність протоколів RTP/UDP/IP забезпечує транспортний механізм для мовного трафіку.

Протоколи другої групи забезпечують управління виклику між абонентами. До цією групи відносяться протоколи SIP (Session Initiation Protocol) [2], H.323, MGCP (Media Gateway Control Protocol) [3]. Протоколи встановлення з'єднання можуть працювати як поверх UDP протоколу, так і по TCP (Transmission Control Protocol). Таким чином, сукупність протоколів (SIP/H.323/MGCP)/(UDP/TCP)/IP формують сигнальний механізмпередачі мовного та медіа трафіку.

Історично першим протоколом для IP-телефонії, який отримав широке поширення, став H.323, представлений Міжнародним Союзом Електрозв'язку у рекомендації H.323. Документ описує кілька протоколів, які спільно забезпечують роботу мультимедійних протоколів у мережах з негарантованою якістю обслуговування. Однак, H.323 має досить складну структуру, оскільки протокол спочатку розроблявся для інтеграції телефонної мережі спільного користування (ТФСК) з мережами передачі даних.

Управління викликами може бути реалізовано за рахунок використання протоколу MGCP, архітектура якого складається з кількох елементів:

− шлюз – Media Gateway, що виконує функції перетворення мовної інформації з ТФСК в мережу з комутацією пакетів;

− контролер шлюзів - Call Agent, керуючий шлюзами;

− шлюз сигналізації - Signaling Gateway (SG), що забезпечує передачу сигналізації, надходить з ТФСК, до контролеру шлюзів і в зворотному напрямі.

Особливостями MGCP є зосередження всього інтелекту розподіленого шлюзу в контролері і можливість поділу функцій контролера між декількома обчислювальними платформами.

Третім протоколом, що дозволяє здійснювати управління викликами, є SIP [4, 39, 40]. SIP базується на протоколі HTTP, має більш просту структуру у порівнянні з H.323 і MGCP. Завдання протоколу - зробити абонентські пристрої та шлюзи більш інтелектуальними, а також забезпечити розширюваність протоколу для підтримки додаткових послуг для користувачів. Підхід до побудови мереж IP-телефонії на базі протоколу SIP набагато простіший, ніж реалізація на H.323 і MGCP. Через це SIP протокол отримав широке застосування.

Крім наведеної вище класифікації протоколів IP-телефонії, можна додатково виділити кілька підсистем, що функціонують для надання послуг VoIP:

− підсистема забезпечення якості;

− підсистема безпеки IP-телефонії;

− підсистема білінгу і менеджменту IP- телефонії;

− підсистема додаткових послуг;

− підсистема забезпечення управлінням викликами і адресацією.

Підсистема забезпечення якості відповідає за підтримку якості телефонного зв’язку і включає в себе сукупність протоколів, алгоритмів і механізмів, працюючих для досягнення цієї мети.

Підсистема безпеки IP-телефонії відповідає за конфіденційність телефонних переговорів кореспондентів, а також інформації, що передається. Дана система включає в себе сукупність протоколів, механізмів і алгоритмів для забезпечення безпеки в мережі IP-телефонії.

Підсистема білінгу і менеджменту застосовується для обліку викликів

користувачів, тарифікації дзвінків і виконання взаєморозрахунків між користувачами (абонентами) і оператором надавання послугу.

Підсистема додаткових послуг відповідає за надання додаткових сервісів абонентам мережі IP-телефонії. До них відноситься забезпечення роумінгу та мобільності, надання додаткових сервісів, таких як відеодзвінки, інформаційні сервіси і т.д. Підсистема складається з протоколів надання додаткових послуг.

Підсистема управління викликами і адресації відповідає за виконання базових послуг VoIP, а саме:

- організацію викликів і маршрутизацію викликів;
- передачу голосового трафіку.

При описі системи IP-телефонії слід окремо виділити можливі сценарії взаємодії кореспондентів [29]. У загальному випадку сценарієм називається сукупність елементів, взаємодіючих при обробці дзвінка. У більш широкому сенсі, сценарієм може бути названа сукупність застосовуваних при обробці дзвінка протоколів, алгоритмів,механізмів, а також процедур їхньої взаємодії між собою для досягнення кінцевої мети.

При складанні прикладу сценарію доцільно ввести припущення, що в якості протоколу сигналізації в мережі IP-телефонії застосовується протокол SIP. При складанні схеми взаємодії слід враховувати, що по закону зв'язку, заборонено приєднання операторів один до одного за допомогою VoIP. З'єднання різних VoIP операторів дозволяється виконувати тільки через мережу ТФСК [5].

На рисунку 1.1 представлена принципова схема підключення оператора VoIP. На її прикладі розглянуто можливі варіанти сценаріїв обробки дзвінків елементами мережі IP-телефонії: користувачами (абонентами), IP-телефонними станціями (IP АТС, SoftSwitch), приграничними шлюзами E1. Для прикладу наведено два постачальники послуг IP-телефонії, а також оператор традиційної телефонії.

Оператор 1 надає VoIP сервіси абонентам, підключеним до мережі 1.

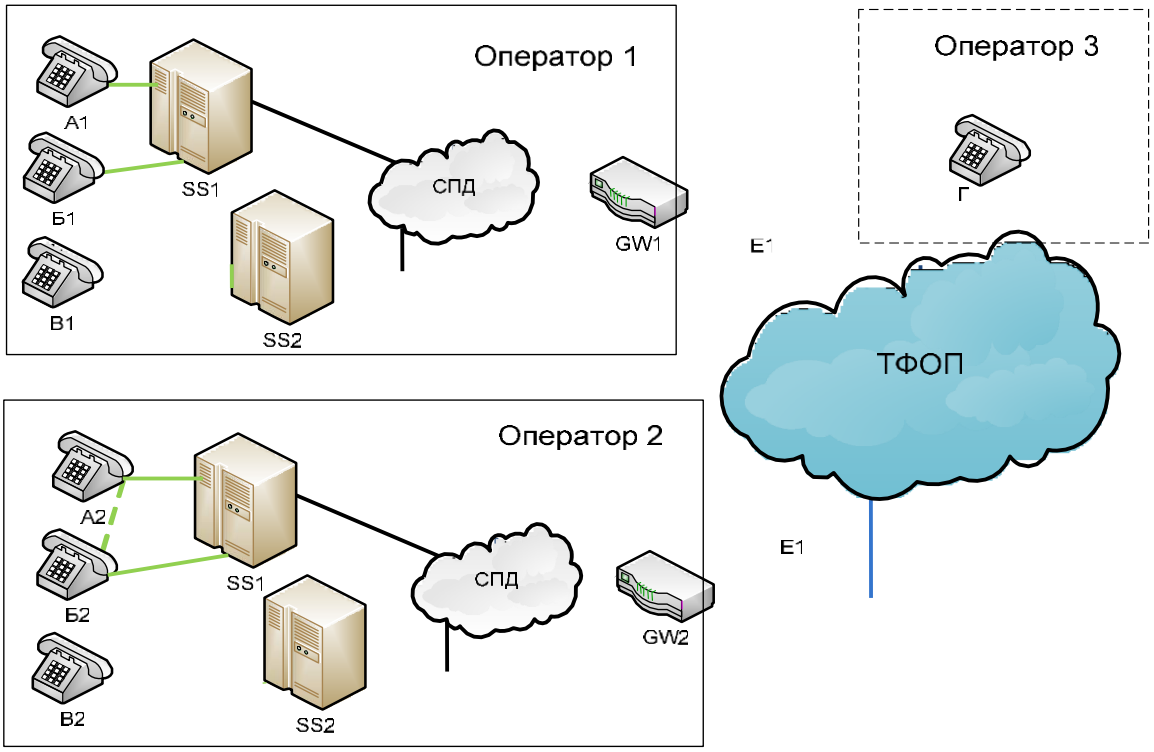


Рисунок 1.1 - Принципова схема підключення оператора VoIP

Оператор може використовувати кілька IP АТС, позначених SSx на рисунку, де x – порядковий номер IP АТС. Як правило, ймовірність виклику від абонента А1 іншому абоненту мережі того самого оператора (Б1 чи В1) вкрай мала для невеликих і середніх компаній. Найбільш поширені дзвінки абонентам, підключеним до іншим операторів.

Можливі наступні сценарії з'єднання:

– А1-SS1-GW1-ТФСК-GW2-SS2-В2 (VoIP абонент однієї компанії через ТФСК дзвонить VoIP абоненту іншого оператора);

– А1-SS1-GW1-ТФСК-Г (VoIP абонент однієї компанії через ТФСК дзвонить абоненту мережі ТФСК іншого оператора);

– А1-SS1-SS2-В1 (VoIP абонент одного оператора дзвонить іншому абоненту цього ж оператора, підключеного до додаткової IP АТС оператора);

– А1-SS1-Б1 (VoIP абонент одного оператора дзвонить іншому абоненту цього ж оператора, при цьому абоненти підключені до однієї IP АТС)

– А2-Б2 (VoIP абонент одного оператора дзвонить іншому абоненту, при цьому виклик здійснюється безпосередньо між кореспондентами, минаючи IP АТС). Такий спосіб використовується, коли необхідно організувати передачу абонентської лінії традиційної телефонії мереж IP. Спосіб організації зв'язку без АТС може застосовуватися в корпоративних мережах для організації внутрішнього службового зв'язку, а також між окремими кореспондентами глобальної мережі, які не мають підключення до однієї АТС, але мають потребу проведення сеансів телефонного зв'язку в захищеному режимі.

Описані сценарії показані також на рисунку 1.2.

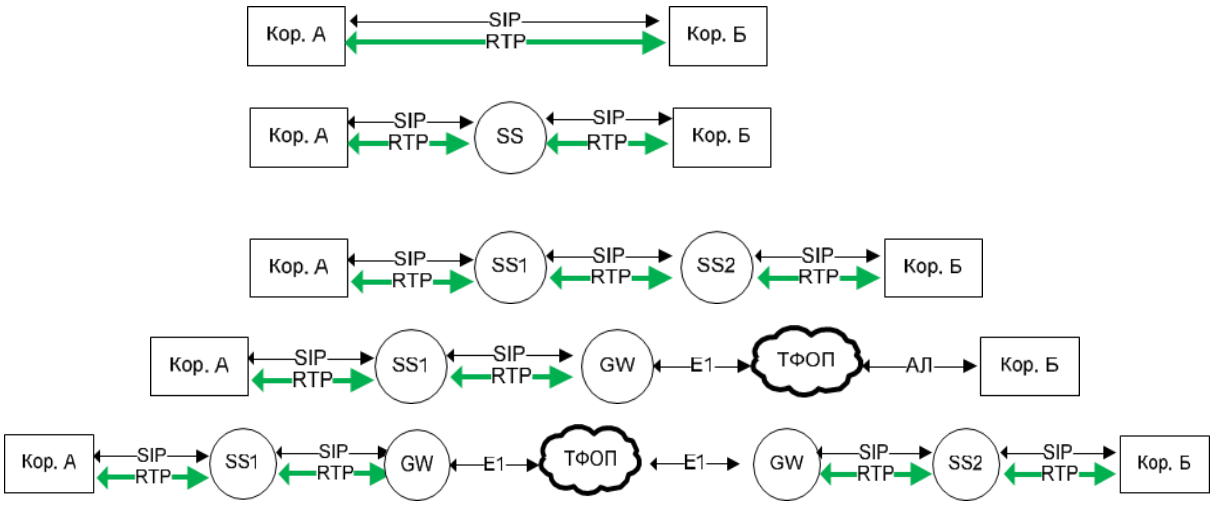


Рисунок 1.2 - Можливі сценарії встановлення з'єднання кореспондента VoIP

У всіх вищенаведених сценаріях при обробці викликів повинні виконуватись норми, визначені для телефонного зв'язку. Проте, у сценаріях можуть застосовуватись різні протоколи, алгоритми забезпечення безпеки. Можливе використання різних механізмів підтримки якості обслуговування при встановленні з'єднання між абонентами різних операторів. З цих причин, підсистема забезпечення якості та підсистема забезпечення безпеки IP-телефонії [6] вимагають більш детального вивчення.

1.2 Забезпечення якості та методи її оцінки в IP-телефонії

Міжнародний Союз Електрозв'язку (МСЕ) визначає якість наданих послуг як "сумарний ефект показників якості послуг, який визначає ступінь задоволеності користувача послуги" [7].

Найбільш популярним з показників якості IP-телефонії є оцінка MOS (Mean Opinion Schore), що визначається як середнє значення оцінок якості за п'ятибальною шкалою, отриманих великою групою слухачів-експертів [8]. Якість IP-телефонії визначається двома складовими - якістю мови та якістю сигналізації [9].

Якість мови включає в себе:

- діалог - можливість користувача зв'язуватися і розмовляти в реальному часі в повнодуплексному режимі з іншим користувачем;
- розбірливість - чистота і тональність мови;
- ехо - чутність власної мови;
- рівень – гучність мови.

Якість сигналізації включає:

- затримки при встановленні виклику - швидкість успішного доступу та час встановлення з'єднання;
- завершення виклику - час відбою та швидкість роз'єднання;
- DTMF - визначення і фіксація сигналів багаторазового набору номера.

При використанні захищеної IP-телефонії додатково з'являються показники:

- час виконання з'єднання, тобто час встановлення захищеного голосового каналу між кореспондентами, що використовують протоколи розподілу ключів;
- ймовірність успішної атаки порушника на IP- телефонію, працюючу в захищеному режимі;
- час і ймовірність успішного завершення протоколів забезпечення

безпеки.

У наш час IP-телефонія стає масовим явищем, тому на неї також можуть поширюватися норми, пред'явлені до традиційної телефонії. Для контролю показників якості IP-телефонії необхідно враховувати норми, що поширюються на пакетні канали зв'язку, а також норми, що поширюються на телефонію.

Для мережі передачі даних виділяють наступні показники:

- втрати - відношення коректно прийнятих пакетів до загальної кількості переданих пакетів;

- затримки - час, який потрібний для передачі пакету від точки відправкидо точки отримання;

- пропускна здатність - смуга пропускання доступна для передачі між кореспондентами;

- коливання затримки - різниця між затримками, що виникли при передачі різних пакетів.

Для мережі передачі даних різних класів трафіку в рекомендації ITU-T Y.1541 [10] вводяться норми на середню затримку, варіацію затримки, коефіцієнт втрачених пакетів, коефіцієнт помилок у прийнятому пакеті. Норми представлені в таблиці 1.1.

Таблиця 1.1 - Норми по рекомендації MCE

Характеристики мережі	Класи якості обслуговування (QoS)					
	0	1	2	3	4	5
Затримка доставки пакету IP, IPTD (мс)	100	400	100	400	1000	-
Варіація затримки пакету IP, IPDV (джиттер) (мс)	50	50	-	-	-	-
Коефіцієнт втрати пакетів IP, IPLR	10^{-3}	10^{-3}	10^{-3}	10^{-3}	10^{-3}	-
Коефіцієнт помилок пакетів IP, IPER	10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}	-

У рекомендації G.114 [11] для телефонної мережі сформовані нормативина односторонню затримку. Параметр не повинен перевищувати 400 мс при мережному планування. У документі наведено деякі значення затримок, які рекомендується використовувати в розрахунках при використання різних серед передачі та гібридних каналів передачі даних.

У рекомендації ITU-T Y.1291 [7] виділяється кілька основних конструктивних блоків, розподілених в трьох площинах.

Площина керування, містить механізми управління трактами, через які проходить трафік користувача. У склад цих механізмів входить управління допуском, маршрутизація для QoS і резервування ресурсів.

Площина даних містить механізми, працюючі безпосередньо з трафіком користувача. У склад цих механізмів входить управління буферами, запобігання перевантаження, маркування пакетів, організація черг та диспетчеризація, класифікація трафіку, правила його обробки та моделювання.

Площина адміністративного управління, містить механізми, що відносяться до експлуатації, адміністрування і адміністративного управління мережею. До складу цих механізмів входять: угода про рівні обслуговування (SLA), відновлення трафіку, вимір і реєстрація, а також задані правила доставки інформації.

У площині даних виконуються класифікація і маркування пакетів, застосовуються планування до пакетів, а також використовуються додаткові алгоритми обробки пакетів. Класифікація може виконуватися в залежності від CoS, MPLS-EXP, номери порту підключення кореспондента до мережного обладнання або MAC адреси відправника чи одержувача, Ethertype пакета, що відправляється, та інших ознак. Основним завданням класифікації є поділ пакетів на групи з метою їх наступною маркування з призначенням параметрів пакету:

- MPLS-EXP - три біти в MPLS для маркування QoS;
- біти CoS 802.1p;
- IP Precedence байт (ToS) або DSCP.

Інструмент планування застосовується для визначення, який кадр чи пакет буде першим виходити з інтерфейсу вузла мережі. Завдання вирішується за

рахунок застосування алгоритмів управління чергою, а також механізмів запобігання переповнення черги. Виділяють алгоритми управління чергою: SP, WRR, WFQ, CBWFQ, MDRR, LLQ (PQ+CBWFQ), WRED.

Опис алгоритмів наведено в [12]. Найбільш поширеним є застосування пріоритезації голосового трафіку в низькошвидкісних бездротових каналів зв'язку (КЗ).

Для забезпечення якості VoIP можуть застосовуватися механізми обмеження швидкості - policing або shaping. Policing - обмеження швидкості передачі даних без буфера. Shaping - обмеження швидкості передачі даних з проміжним буфером. Додатково може застосовуватися управління потоком Ethernet-механізм, що дозволяє попередити відправника про необхідності зупинити передачу даних на вказаному інтервалі часу через те, що приймає порт не може виконати обробку.

Для низькошвидкісних каналів додатково можуть бути застосовані механізми:

- фрагментація і чергування пакетів;
- механізми компресії (Compressed RTP - cRTP).

Так cRTP дозволяє стискати заголовок голосового пакету IP/UDP/RTP з 40 до 2-5 байт. Однак, даний механізм використовується тільки в межах одного фізичного каналу зв'язку.

До механізмів площини управління архітектурної моделі для підтримки QoS відносяться застосування RSVP (резервування ресурсів) на мережі, і навіть використання алгоритмів маршрутизації з урахуванням QoS. В якості вхідних даних алгоритми можуть використовувати значення полів в промаркованих пакетах та таблиці маршрутизації, що враховує різні параметри QoS для інтерфейсів обладнання та для різних маршрутів. Частина такого функціоналу підтримується, наприклад, протоколом маршрутизації OSPF. Механізми маршрутизації з урахуванням вимог QoS та додаткових можливостей протоколу OSPF описані в RFC 2676 [13].

До площини адміністративного управління відносяться механізми зміни

параметрів для VoIP трафіку, які застосовуються на користувальницьких терміналах, IP-телефонних станціях, а також на додаткових елементах мережі VoIP, таких, як RTP-проксі-сервери і прикордонні контролери сесій (SBC, Session Border Controller).

У світі ведуться активні дискусії про те, які моделі використовувати для оцінки якості сервісів, а також як оцінити ефективність обробки пакетів в мережі, які методики використовувати для оцінки якості наданих послуг. Ведуться активні розробки в напрямку оцінки QoS і QoE VoIP трафіку.

QoS (Quality of Service - якість обслуговування) за визначенням ITU – це колективний ефект роботи сервісів, що визначає ступінь задоволення користувача обслуговуванням.

QoE (Quality Of Experience - якість сприйняття) суб'єктивна міра оцінки роботи системи. QoE покладається на людську думку і відрізняється від якості обслуговування QoS, яке може бути точно виміряне. Наприклад, реакція людини при прослуховуванні музики через навушники базується не тільки на частотних характеристиках системи і спікерів, але і на чутливості слуху людини.

Для IP-телефонії MCE стандартизував математичну модель в рекомендації G.107 [14] для оцінки QoE, виходячи з параметрів якості терміналу та мережі. Ця модель отримала назву E-model і служить для розрахунку R-фактору.

Модель була широко використана для оцінки QoE в мережах IP-телефонії Японії. Така ж модель була потрібна для відеотелефонних сервісів. У результаті в лабораторії NTT був розроблений набір параметрів для оцінки сприйняття якості відеотелефонії, які згодом використовувалися в новій моделі для відеотелефонії. Використовуючи Е-модель, а також параметри каналу передачі даних іпараметри застосовуваної системи IP-телефонії, можна оцінити MoS (Mean Opinion Score) суб'єктивний рівень якості, що сприймається користувачем послуг IP-телефонії.

У рекомендації [14] наводиться відповідність R-фактору, описуваного та обчислюваного з використанням Е-моделі, та параметра MoS (Таблиця 1.3).

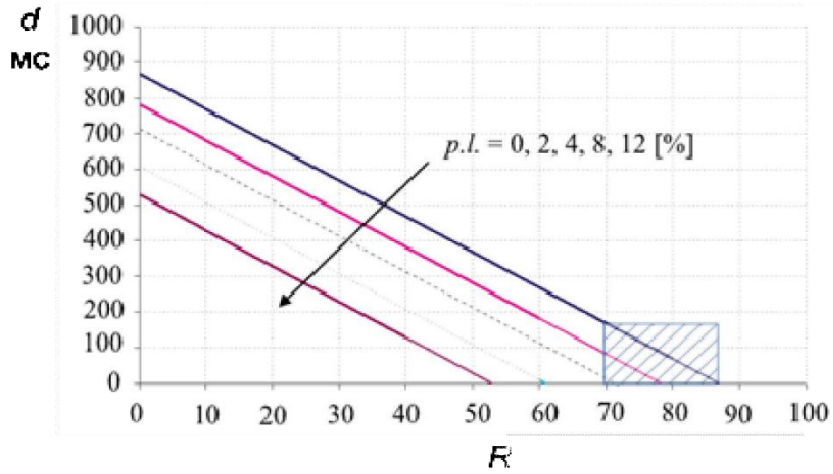
Таблиця 1.3 - Зв'язок R-фактору і MOS по рекомендації G.107

R-фактор	MoS (нижній поріг)	Задоволеність користувачів
90	4,34	Висока задоволеність
80	4,03	Задоволеність
70	3,60	Деякі користувачі не задоволені
60	3,10	Багато користувачів не задоволені
50	2,58	Майже всі користувачі не задоволені

На підставі таблиці 1.3 обрано нижню межу MOS 3.6, якій відповідає R=70. Необхідно визначити можливі параметри каналу зв'язку: затримку в каналі зв'язку (*d*) і втрати пакетів (*pl*), при яких буде досягатися значення R≥70.

У [15] розглядається вплив параметрів каналу зв'язку на якість послуг VoIP для різних кодеків: G.711, G.723 і G.729. Для цього виконується розрахунок MOS з використанням Е-моделі для різних затримок каналу зв'язку в інтервалі затримок 0-1200 мс, а також для втрати пакетів 0-12%.

На рисунках 1.4, 1.5 та 1.6 видно, як змінюється R в залежності від *pl* і від *d*. Додатково на графіках позначені умови, при яких забезпечується значення R ≥



70.

Рисунок 1.4 - Залежність R-фактору від втрати пакетів та затримки в каналізв'язку для кодеку G.723

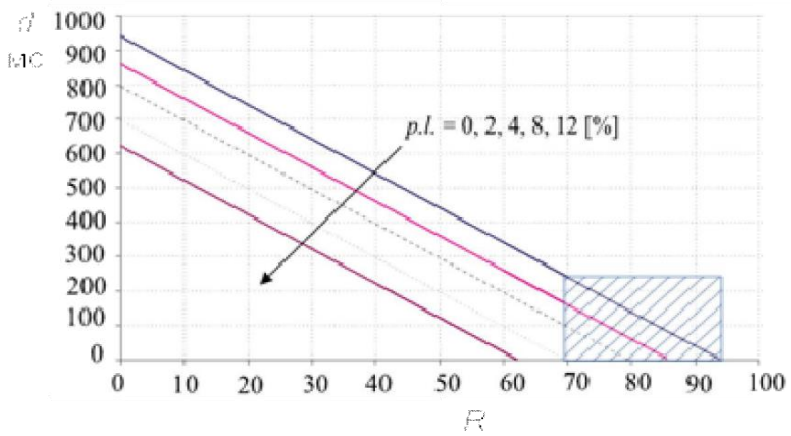


Рисунок 1.5 – Залежність R-фактору від втрати пакетів та затримки у каналі зв'язку для кодеку G.729

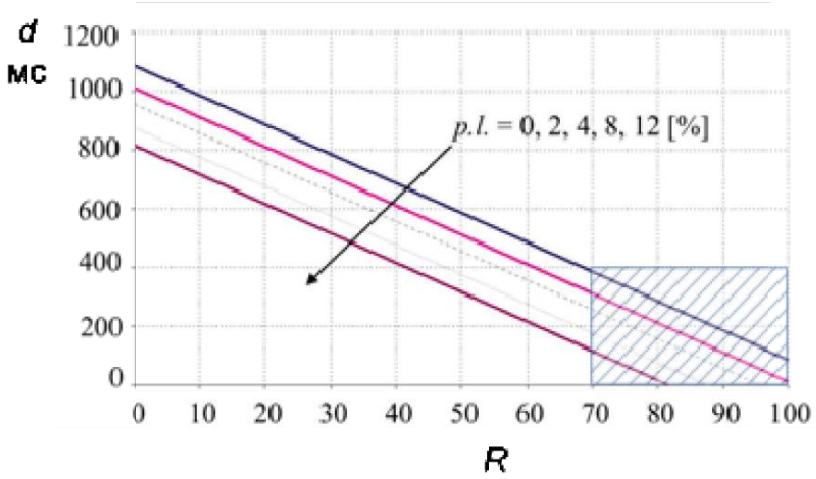


Рисунок 1.6 – Залежність R-фактору від втрати пакетів та затримки у каналі зв'язку для кодеку G.711

З рисунків 1.4-1.6 видно, що кодек G.711 забезпечує найбільше значення MOS при найгірших умовах в каналі зв'язку: максимальній затримці та втратах пакетів. Для *pl* = 0 умова *R* >=70 виконується для *d* <=300 мс, при *pl* =12, *R*>=70 виконується для *d* <=100 мс.

Подальший аналіз протоколів дотримання безпеки доцільно проводити для каналу зв'язку з параметрами *d*<=300 та *pl* <=12 при використанні кодеку G.711. У наступних обчисленнях також перевага надається кодеку G.711, як найбільш стійкому при роботі каналами зв'язку з помилками. Як вхідний параметр при розрахунках замість параметра *pl* зручно використовувати похідний параметр -

ймовірність бітової помилки в каналі зв'язку p_0 . Для цього необхідно визначити значення p_0 , еквівалентне pl =12 для кодеку G.711.

$$pl=1-(1-p_0)^{ps} \quad (1.1)$$

де ps - розмір пакету, біт.

Для кодеку G.711 допускаються розміри корисного навантаження 80160240 байт. При цьому розмір пакету з урахуванням заголовків складатиме відповідно 138,218,296 байт. p_0 визначається по формулі:

$$p_0 = 1 - 10^{\frac{lg\,(1-pl)}{ps}} \quad (1.2)$$

Розраховані значення наведено у таблиці 1.4. З таблиці видно, що максимальному значенню ймовірності помилки pl =12% відповідає $p_0 = 1{,}16\ 10^{-4}$. Відповідно, розрахунки необхідно виконувати для значень $p_0 \leq 1{,}16 \cdot 10^{-4}$.

Таблиця 1.4 – Залежність p_0 від pl для кодеку G.711

Имовірність втрати пакету, pl	Розмір пакету, ps , біт	Імовірність бітової помилки, p_0
0,12	138	$1{,}16\ 10^{-4}$
0,12	218	$7{,}33\ 10^{-5}$
0,12	298	$5{,}36\ 10^{-5}$

Тема забезпечення QoS широко обговорюється за кордоном: в університетах Центральної Флориди (Erol Gelenbe, Chair Professor, Ricardo Lent, doctor та ін.) [16], Карленгтонському університеті Канади (Lijing Ding, Ayman Radwan, Mohamed Samy El-Hennawey [17], Rafik A. Goubran, Ph.D., P.Eng) та ін.

Питання забезпечення QoS розглядається такими організаціями як MCE, IETF, IEEE, ETSI, 3GPP. Були прийняті ряд стандартів для якості QoS IP-телефонії та моделей із забезпечення якості IP-телефонії, але до сьогоднішнього часу не існує стандарту єдиного.

Однак, питання впливу протоколів забезпечення безпеки на якість IP-телефонії вивчені недостатньо і вимагають опрацювання та оцінки.

1.3 Забезпечення інформаційної безпеки IP- телефонії

У силу загальнодоступності використовуваних каналів передачі голосової інформації в IP мережах особливу актуальність набуває забезпечення конфіденційності VoIP-сервіси. Однак, багато VoIP-пристроїв не підтримують VPN (таблиця 1.4).

Таблиця 1.4 - Засоби захищеної IP-телефонії

Виробник	Засоби	Реалізація	Протокол захисту			Підтримка VPN
			Встановлення з'єднання	Медіатрафік	Розподіл ключів	
LinkSys	SPA8000	апаратна	SIPS/TLS	SRTP	немає даних	ні
LinkSys	Cisco SPA112	апаратна	SIPS/TLS	SRTP	немає даних	ні
Dlink	DVG-5008S	апаратна	немає даних	немає даних	немає даних	PPTP
AddPack	AP200	апаратна	SIPS/TLS	SRTP	немає даних	немає даних
Grandstream	GXW400x	апаратна	SIPS/TLS	SRTP	SDES	ні
UM-Labs	RC-2100	апаратна	SIPS/TLS	SRTP	ZRTP, SDES	немає даних
CounterPath	Eye-beam	програмна	SIP/TLS	SRTP	TLS	ні
3XC	3CX softphone	програмна	SIP/TLS	SRTP	ні даних	ні
Asterisk	IP PBX	програмна	SIP/TLS	SRTP	ZRTP	ні
FreeSwitch	IP PBX	програмна	SIP/TLS	SRTP	SDES	ні
Phoner	Phoner softphone	програмна	SIP/TLS	SRTP	ZRTP	ні

Для вирішення цього завдання можуть бути використані різні підходи:

− забезпечення прямого захищеного каналу між кореспондентами (наприклад, VPN-тунель);

− застосування спеціальних протоколів забезпечення безпеки для IP-сервісів.

Перший спосіб отримав широке застосування при побудові віртуальних корпоративних мереж, але для його реалізації кореспонденти повинні підтримувати протокол VPN. Однак, багато VoIP-пристроїв не підтримують VPN.

Для забезпечення безпеки досить часто застосовуються спеціальні протоколи забезпечення безпеки IP-телефонії. До спеціальних протоколів забезпечення безпеки IP-телефонії відносяться протоколи Secured SIP, SRTP, MIKEY, SDES, ZRTP, DTLS, S-MIME. Ці протоколи можна розділити на три категорії [18, 19, 29]:

− протоколи захисту сигналізації (Secured SIP);

− протоколи захисту медіаінформації (SRTP);

− протоколи генерації та розподілу ключів для протоколів захисту медіаінформації (MIKEY, SDES, ZRTP, DTLS).

Слід розглянути їх детальніше.

Протоколи захисту сигналізації призначені для забезпечення безпеки інформації про телефонні номери викликаючого та викликаного абонента, підтримуваних кодеках. Для вирішення цього завдання використовується Secured SIP (SSIP, SIP/TLS) [20]. Цей протокол працює по аналогії протоколу HTTPS, організовуючи тунель з використанням сертифікатів та відкритого ключа. між кореспондентом і сервером SSL Усі SIP-повідомлення (сигналізація) передаються цим тунелем. Недоліком протоколу є необхідність застосування інфраструктури відкритих ключів, що використовуються для організації TLS.

Для забезпечення конфіденційності при передачі мови широко використовується захищений протокол реального часу - Secure Real-time Transport Protocol (SRTP)[21], який реалізує функції криптографічного захисту - шифрування і автентифікації голосових повідомлень на основі алгоритму шифрування AES.

Криптографічний захист пакетів голосової інформації виконується протоколом SRTP в режимі реального часу і не вносить змін в імовірнісно-часові

характеристики протоколу RTP. Для його роботи необхідне попереднє формування криптографічних ключів [30]. Це завдання вирішує протокол розподілу ключів (ПРК).

Рекомендація RFC 3711 описує дві складові - власне протокол SRTP для перенесення та криптозахисту медіа даних, а також протокол SRTCP (Secure Real-time Transport Control Protocol) для управління медіа сесією. Основними завданнями протоколу SRTP є виконання наступних функцій:

- шифрування переданих голосових даних;
- автентифікація переданих повідомлень;
- захист від передачі повторних пакетів;
- збереження смуги пропускання, стиснення RTP заголовків.

Основними завданнями протоколу SRTCP є виконання наступних функцій:

- шифрування переданих даних;
- автентифікація переданих повідомлень.

Аутентифікація та шифрування можуть працювати незалежно один від одного. Таким чином, можливий варіант, коли шифрування вимкнено і SRTP використовується тільки з метою автентифікації. Обмеженням протоколу є те, що автентифікація повідомлення є обов'язковою в SRTP і не може бути відключена.

Протоколи третьої групи, по аналогії із спорідненими протоколами розподілу ключів у бездротових мережах [22, 28], призначені для генерації і розподілу ключів шифрування медіаінформації між кореспондентами. Для вирішення цього завдання можуть використовуватися протоколи MIKEY, SDES, ZRTP, DTLS.

Протокол обміну ключами MIKEY описаний у рекомендаціях RFC3830 [23] та RFC6309 [24]. MIKEY має кілька режимів роботи, що визначають спосіб формування секретного ключа сесії SRTP: режим попередньо встановленого ключа, режим відкритого ключа і режим Діффі-Хелмана. Причому другий і третій режими не захищають від атаки вторгнення (MiTM, Man In the Middle) та

вимагають реалізації механізму автентифікації повідомлень. Засобом для перенесення повідомлень протоколу може бути як SIP/SDP, так і протокол RTSP (Real Time Streaming Protocol).

SDES (Session Description Protocol Security) [25] описується RFC4568. Суть протоколу полягає в тому, що один із кореспондентів передає ключ до SIP повідомлення по сигнальному каналу. Кореспондент отримує його та використовує для шифрування. Однак при цьому обмін сигнальними повідомленнями має бути захищений від зловмисника. З цієї причини, SDES може використовуватись тільки за наявності SIP/TLS захищеного з'єднання з цифровим сертифікатом сервера. Також даний спосіб не забезпечує безпеки з кінця до кінця. Це означає, що коли з'єднання виконуватиметься через IP АТС, SDES буде виконувати розподіл ключів між кореспондентом А та IP PBX, між кореспондентом Б і IP-телефонної станцією, але не між кореспондентами А і Б безпосередньо.

Протокол DTLS [26] для SRTP описується в RFC 5764. Протокол описує формування медіа-сесій точка-точка з двома учасниками з жорстким фіксуванням портів UDP кореспондента та респондента. Повідомлення протоколи передають разом із RTP пакетами. Кожна сесія містить одну DTLS асоціацію та два SRTP контексти (для SRTP та SRTCP). Для організації сесії (DTLS-асоціації) кореспонденти виконують обмін повідомленнями, так званий DTLS handshake, що показано на рисунку 1.8. Так як в основі протоколу лежить TLS, він використовує інфраструктуру відкритих ключів (Public Key Infrastructure, PKI). Тому застосування TLS можливе теж тільки при наявності PKI.

Одним із найперспективніших протоколів генерації ключів є ZRTP [27]. Протокол застосовується у додатку для Android CsipSimple, програмних телефонах Jitsi, Phoner, програмних АТС FreeSwitch та Asterisk, апаратних VoIP шлюзах компанії UM-Labs.

Відмінною особливістю ZRTP протоколу є можливість підтримання безпеки з кінця в кінець, від одного кореспондента до іншого.

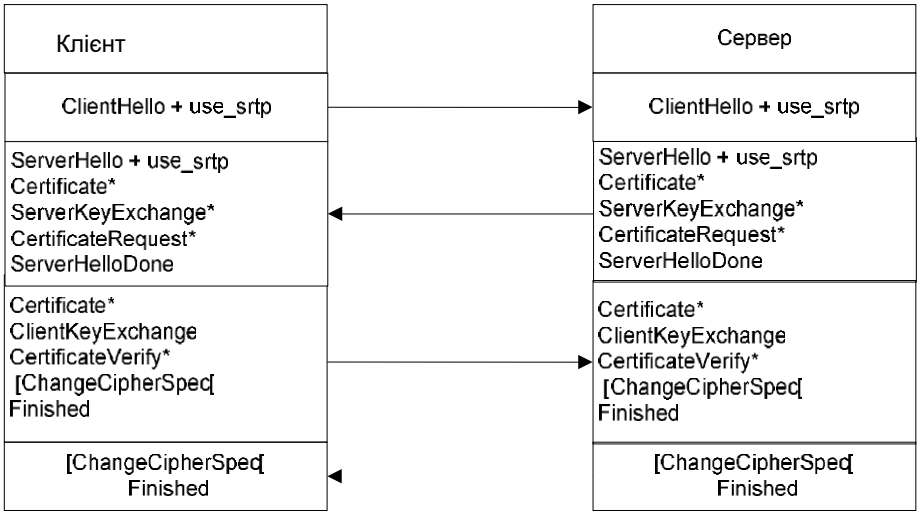


Рисунок 1.8 – Обмін повідомленнями DTLS

Завданнями протоколу ZRTP є:

− генерація ключових параметрів SRTP сесії;

− забезпечення конфіденційності повідомлень протоколу;

− забезпечення автентифікації кореспондентів;

− захист від атаки вторгнення посередині як з використанням, так і без використання інфраструктури відкритих ключів.

Протокол передбачає роботу кореспондентів по топології точка-точка, при цьому окремо виділяється можливість застосування протоколу при багатопотоковому режимі, коли необхідно організувати кілька захищених медіа потоків. Крім того, передбачений режим роботи з легітимним посередником, яким може бути, наприклад, корпоративна телефонна станція. Кожен з кореспондентів-учасників протоколу повинен мати встановлений ідентифікатор (ZID), який повинен бути унікальним. Особливістю протоколу обміну ключами по алгоритму Діффі-Хелмана є передача параметрів всередині RTP пакетів, залишаючи пакети сумісними з RTP/AVP профілем. У цьому випадку, несумісним пристроєм ZRTP пакети просто відхиляються та не впливають на встановлене з'єднання. Для автентифікації кореспондентів, а також випадків атаки вторгнення в середину (MiTM, Man in The Middle), протокол ZRTP передбачає використання короткого автентифікаційного рядка (SAS, Short Authentication String), а також частини

ключового матеріалу від попередніх сесій між кореспондентами.

Часто для забезпечення безпеки у сфері IP-телефонії використовують спеціальні протоколи. Такі протоколи охоплюють різні аспекти безпеки, включаючи захист сигналізації, медіаінформації та генерацію/розподіл ключів для захисту медіаінформації.

Кожен з цих протоколів спрямований на певний аспект захисту в рамках IP-телефонії. Secured SIP охоплює сигналізацію, SRTP захищає медіадані, а протоколи генерації та розподілу ключів (MIKEY, SDES, ZRTP, DTLS) забезпечують необхідні ключі для шифрування медіаінформації. Використання таких протоколів важливе для забезпечення конфіденційності та цілісності даних у мережі IP-телефонії.

Для підтримки безпеки передачі інформації про номери телефонні абонентів викликаного та викликаючого використовують протоколи захисту сигналізації. Для вирішення цього завдання використовується Secured SIP (SSIP, SIP/TLS) [20]. Цей протокол працює по аналогії протоколу HTTPS, організовуючи тунель з використанням сертифікатів та відкритого ключа. між кореспондентом і сервером SSL Усі SIP-повідомлення (сигналізація) передаються цим тунелем.

SRTP (Secure Real-time Transport Protocol) широко використовується для забезпечення конфіденційності при передачі голосу, використовуючи криптографічний захист, такий як шифрування і автентифікація голосових повідомлень на основі AES (Advanced Encryption Standard).

Одним з переваг SRTP є його можливість захищати голосову інформацію в режимі реального часу, не впливаючи на ймовірнісно-часові характеристики протоколу RTP (Real-time Transport Protocol), який використовується для передачі голосу в IP мережах. Це означає, що захист інформації відбувається без великого впливу на затримки або інші параметри, що є критичними для передачі голосу в реальному часі.

Протокол SRTP вимагає попереднього формування криптографічних ключів для своєї роботи. Це завдання вирішує протокол розподілу ключів (ПРК).

ПРК дозволяє генерувати, обмінювати та управляти ключами, які використовуються для шифрування та розшифрування голосових даних у SRTP, забезпечуючи потрібний рівень безпеки для передачі голосової інформації.

Для контролю цілісності переданихповідомлень кожне повідомлення ZRTP включає перевірочний код CRC, а також код автентифікації повідомлення MAC (Message Authentication Code). MAC обчислюється як ключова хеш-функція, яка узгоджується на першій фазі протоколу. Виявлення помилки тільки в хеш-повідомленні, як правило, означає виявлення атаки MiTM, оскільки спотворення за рахунок канальних помилок виявляються також під час перевірки CRC ZRTP пакетів.

Для аутентифікації кореспондентів, а також виключення атаки вторгнення в середину (MiTM, Man in The Middle), протокол ZRTP передбачає використання короткого аутентифікаційного рядка (SAS, Short Authentication String), а також частини ключового матеріалу від попередніх сесій між кореспондентами. Для контролю цілісності переданих повідомлень кожне повідомлення ZRTP включає в себе код CRC, а також код аутентифікації повідомлення MAC (Message Authentication Code).

Виявлення помилки тільки в хеш-повідомленні, як правило, означає виявлення атаки MiTM, оскільки спотворення за рахунок канальних помилок виявляються і при перевірці CRC ZRTP пакета.

Протокол виконується послідовно в чотири фази:

- виявлення;
- підтвердження;
- обчислення ключів;
- завершення.

У загальному випадку, ZRTP працює на самому початку розмови кореспондентів, відразу після завершення роботи протоколу SIP, як починає працювати в сторони протокол RTP.

1.4 Висновки до розділу 1

У першому розділі розглянуто актуальні проблеми та існуючі підходи їх вирішення у сфері захищеної IP-телефонії. Зокрема, розглянуто основні компоненти та протоколи IP-телефонії, а також можливі сценарії встановлення з'єднань. Описано механізми та алгоритми, що застосовуються для забезпечення нормованого показника MOS, а також значень інших нормованих показників. Показано значення параметрів каналу зв'язку, за яких має сенс виконувати аналіз роботи протоколів IP-телефонії.

Наведено набір протоколів безпеки IP-телефонії, а також класифікація протоколів та їх скорочений опис. Проаналізовано дослідження у галузі забезпечення безпеки IP-телефонії та виявлено відсутність досліджень про вплив протоколів безпеки на нормовані параметри функціонування мережі телефонії. Показано вплив протоколів безпеки на параметри функціонування мережі телефонії, виражене у виникненні затримки під час встановлення захищеного з'єднання між кореспондентами.

2 МОДЕЛЬ АКТИВНОГО ЗЛОВМИСНИКА ДЛЯ ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ

Злоумисник може вибрати різні способи атаки на систему IP- телефонії, працюючу в захищеному режимі, виходячи з особливостей протоколів забезпечення безпеки IP-телефонії. Існують кілька моделей порушника в IP-телефонії. Ймовірнісна модель порушника показана в [33] описує дії порушника, а також основні атаки при реалізації безпечної IP-телефонії на ОС Windows. Модель враховує різні типи атак, у тому числі, характерні саме для Windows під час використання криптографічних засобів операційної системи. Однак, дана модель не враховує, що ключі поширюються за допомогою протоколів розподілу ключів IP-телефонії, і припускає тільки попереднє встановлення пароля у обох кореспондентів. При атаці, спрямованої на несанкціонований доступ до інформації (НДІ), розглядається тільки ймовірність дешифрування переданого контенту методом перебору, а атака модифікація пакетів розглядається лише у разі успішної атаки отримання пароля при дешифрації перехоплених пакетів.

Загальна модель зловмисника також не враховує особливостей роботи безпечної IP- телефонії, при використанні кількох протоколів для забезпечення безпеки: захист сигналізації, захист медіа трафіку, розподіл ключового матеріалу, а також не описує атаки безпосередньо на ці протоколи. У роботі [35] запропоновано сукупність вимог, які пред'являються до мережі IP-телефонії, а також описуються основні загальні типи атак на систему IP-телефонії від середньостатистичного хакера. Однак, в роботі відсутня декомпозиція протоколів безпеки IP - телефонії на складові елементи і відсутній опис атак конкретно на ці протоколи. У роботі [34] описуються загальні принципи забезпечення безпеки, а також можливі дії порушників під час атак на систему IP-телефонії. При цьому не розглядаються атаки на протоколи розподілу ключового матеріалу, використовувані в IP- телефонії. Так як в існуючих моделях порушника, не

описується декомпозиція протоколів безпеки IP-телефонії, доцільно розробити нову модель порушника, яка враховує описані вище особливості.

Існуючі моделі не дозволяють визначити ймовірність успішної атаки - несанкціонований доступ до інформації на систему захищеної IP- телефонії, яка працює за схемою кореспондент-кореспондент, не враховують атаку людина всередині (MITM) на ПРК. Через те доцільно розробити таку модель злоумисника, яка дозволила б вирішити дане завдання.

2.1 Загрози інформаційної безпеки в IP-телефонії

Загроза безпеки інформації в IP-телефонії виникає в результаті доступу каналу між джерелом загрози і носієм (джерелом) інформації, що створює умови для порушення безпеки інформації. Актуальність загрози безпеки інформації визначається типом джерела загрози безпеки інформації, наявністю вразливості джерела інформації і середовищем поширення інформаційного сигналу.

За типом джерела загрози впливів на інформацію можна виділити:

− загрози, пов'язані з діяльністю організацій, які мають високий потенціал, оснащеність та мотивацію, обумовлені політичними,економічними, військовими і іншими цілями іноземних держав;

− загрози, пов'язані з діяльністю організацій, що мають мотивацію, обумовлену їх економічними, інформаційними і іншими цілями;

− загрози, пов'язані з діяльністю окремих фізичних осіб (злочинних елементів).

Способи впливу на інформацію визначаються можливостями джерела загроз. Джерело небезпеки – це підприємець, який здійснює несанкціонований доступи чи здійснює підготовку до дій з несанкціонованого впливу на інформацію є порушником інформаційної безпеки.

Далі, як порушник розглядається фізична особа, що випадково або навмисно чинить дії у своїх інтересах чи в інтересах організацій, наслідком яких є порушення безпеки інформації при її обробці технічними засобами в інформаційних системах.

Доцільно розглядати порушників з погляду наявності права постійного чи разового доступу до контрольованої зони (КЗ) [38 - 40]. Виділяється два типи порушників:

− порушники, які не мають права доступу до КЗ - зовнішні порушники;

− порушники, які мають право доступу до КЗ – внутрішні порушники.

Зовнішніми порушниками можуть бути:

− представники розвідувальних служб іноземних держав;

− представники терористичних і кримінальних структур;

− сторонні особи.

Внутрішніми порушниками можуть бути:

− працівники оператора;

− працівники сторонніх організацій – розробників чи постачальників програмного забезпечення та технічних засобів, що забезпечують супровід цих засобів для захищення об'єкту.

Забезпечення безпеки передачі мовлення в IP-телефонії здійснюється з застосуванням криптографічних протоколів:

− захищеного протоколу реального часу SRTP, який реалізує функції криптографічної інкапсуляції даних;

− протоколів, виконуючих функцію автоматичного розподілу ключів для сесій SRTP;

− протоколів захисту і сигналізації.

Враховуючи, що передача даних IP-телефонії здійснюється по мережах загального доступу, а VoIP термінали доступні будь-якій фізичній особі, то можна зробити висновок про актуальності загроз віддаленого доступу та можливості їх реалізації як зовнішніми порушниками, так і окремими категоріями внутрішніх порушників.

2.2 Узагальнена модель зловмисника

Під моделлю зловмисника розуміється опис сукупності практичних та теоретичних можливостей, знань, часу, місця дії, а також інших характеристик, властивих порушнику.

Під імовірнісною моделлю [stochastic, probabilistic model] розуміють модель, яка на відміну від детермінованої моделі містить випадкові елементи [36]. При заданні на в ході моделі деякої сукупності значень, на її виході можуть отримуватись різні між собою результати в залежності від дії випадкового фактору А.

Під математичною моделлю порушника розуміється модель, що містить випадкові елементи у вигляді ймовірностей успішного виконання окремих атак, формують одну загальну атаку, і визначають ймовірність досягнення кінцевої мети цієї атаки порушником. Щоб модель порушника була максимально корисною, вона повинна орієнтуватися на об'єкт захисту. Тому модель не може бути універсальною і синтезується виходячи з аналізу структури системи, ресурсів та способів їх використання.

Існуючі моделі порушника не враховують особливостей роботи безпечної IP-телефонії, що полягають у застосуванні кількох протоколів для забезпечення безпеки, а також не описують атаки безпосередньо на ці протоколи. Отже, доцільно розробити модель порушника, яка враховує ці особливості. Для цього необхідно розглянути схему взаємодії кореспондентів захищеної IP-телефонії для прямого з'єднання клієнт – клієнт при відсутності попередньо розподіленого ключа і можливі варіанти дії порушника.

Порушник може використовувати наступні стратегії:

− пасивну, використовуючи тільки перехоплення переданих даних;

− активну, використовуючи штатні засоби системи захисту та її недоліки для проведення атаки або додаткові засоби для впливу на систему з

метою виконання атаки.

Надалі розглядається порушник, який використовує активну стратегію атаки, що використовує вразливість протоколу Діффі-Хелмана, який лежить в основі більшості протоколів розподілу ключів (ПРК) IP- телефонії. Цей протокол захищає від атак пасивного порушника. Однак, він нестійкий до атаки Man In The Middle (MITM) активного порушника [5].

При здійсненні протиправних дій порушник може:

− перебувати в одній підмережі з об'єктом атаки, у тому числі мати права доступу будь-якого рівня в мережу або обладнання, на яке виконується атака;

− не перебувати в одній підмережі з об'єктом атаки або не мати прав доступу будь-якого рівня до мережі або до обладнання, на яке виконується атака.

VoIP терміналом користувача, як правило, є IP-телефон, шлюз IP-телефонії, або інший обчислювальний пристрій (стаціонарний комп'ютер або мобільний термінал: ноутбук, планшетний комп'ютер, смартфон і тощо) з встановленим спеціалізованим програмним забезпеченням IP-телефонії. Цей пристрій дозволяє користувачеві отримувати послуги IP-телефонії і виконувати аудіо або відео виклики до інших користувачів.

При розгляді атак на термінал користувача доцільно ввести припущення, що в одній підмережі з жертвою може перебувати тільки внутрішній порушник. Відповідно, деякі типи атак будуть доступні тільки для цієї категорії порушників.

Для досягнення мети НСД порушник при проведенні атаки може використовувати наступні існуючі загрози безпеки:

− навмисний несанкціонований доступ на обладнання оператора або користувача, отриманий за рахунок атаки перебору пароля чи іншої атаки на механізми забезпечення безпеки інформаційної системи (ІС), зі сторони внутрішніх або зовнішніх порушників, що володіють правами та повноваженнями на доступ до обладнання нижчого рівня, або не мають доступу до ньому;

− навмисний вплив на таблицю маршрутизації зі сторони зовнішніх або

внутрішніх порушників, а також використання штатного обладнання для часткового перенапрямлення трафіку користувачами. Вони володіють правами і повноваженнями на доступ до інформації в інформаційну систему;

− навмисний спеціалізований вплив на обмін повідомленнями ПРК, а також на інші передані дані кореспондентів, спрямований на порушення конфіденційності і цілісності переданих даних, зі сторони внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями на доступ до інформації в ІС;

− спеціальний вплив у вигляді атаки на шифр перехопленої інформації, переданої між кореспондентами, зі сторони внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями на доступ або перехоплення зашифрованої інформації в інформаційній системі з метою порушення конфіденційності і дешифрування даних;

− навмисний несанкціонований спеціальний вплив на програмне забезпечення одного або кількох кореспондентів зі сторони внутрішніх або зовнішніх порушників, які мають права та повноваження на доступ до обладнання та програмного використання забезпечення користувача;

− навмисне несанкціоноване встановлення додаткового обладнання на вузлі оператора з метою спеціального впливу на передану від користувачів інформацію зі сторони внутрішніх порушників, що мають права і повноваження доступу до вузла оператора;

− навмисний несанкціонований вплив на конфігураційні файли терміналу зі сторони внутрішніх і зовнішніх порушників, які мають права та повноваження доступу до терміналу користувача, з метою зміни налаштувань безпеки;

− навмисне несанкціоноване перехоплення авторизаційних даних для управління обладнанням користувача зі сторони внутрішніх порушників, які мають права та повноваження на доступ до даних, що передаються між комп'ютером користувача та терміналом користувача.

Для побудови моделі порушника проведений аналіз загроз і їх джерел. Використовуючи вразливість, активний порушник може виконувати комбінацію атак, яка може привести до досягнення НСД.

У якості основних можливих атак активного порушника [38] виділено:

− перебір пароля для доступу до управління обладнанням оператора чи користувача;

− організація перенапрямлення цілого або частини трафіку будь-яким доступним способом;

− виконання атаки MITM на ПРК і інші протоколи безпечної IP-телефонії;

− атака на шифр - перебір ключа до перехопленого медіа трафіку;

− встановлення закладки, модифікація програмного забезпечення (ПЗ) терміналу користувача;

− встановлення додаткового обладнання на вузлі оператора зв'язку;

− зміна налаштувань терміналу користувача для часткового відімкнення безпеки;

− перехоплення авторизаційних даних для управління терміналом користувача за рахунок прослуховування трафіку управління.

Перебір пароля до обладнання дозволяє отримати нелегітимному користувачеві контроль над атакованим обладнанням для подальшої організації атаки НСД. Складність атаки залежить: від протоколу управління, на який виконується атака (telnet, ssh, snmp, web тощо), від довжини використовуваних паролів, обчислювальних ресурсів порушника, та додатковихобмежень і захисних механізмів атакованого обладнання, а також від ширини каналу зв'язку між порушником і жертвою. Атака виконується з використанням спеціалізованого програмного забезпечення при наявності каналу зв'язку для віддаленого доступу до інтерфейсу управління обладнанням.

Організація проксування або перенапрямлення трафіку дозволяє порушнику частково або повністю пропускати через своє обладнання трафік легітимного кореспондента. Це може бути досягнуто за рахунок використання функції копіювання портів на обладнання оператора, за рахунок використання

маршрутизації на основі політик (policy based routing) , а також за рахунок інших механізмів, доступних на обладнанні оператора зв'язку з комутацією пакетів.

Атака на ПРК полягає в організації MITM і генеруванні ключів по черзі з кожним з кореспондентів [41]. Вона дозволяє порушнику ставати проміжним елементом між кореспондентами і прослуховувати або модифікувати передану інформацію. При цьому небезпека і поширеність даної атаки найбільш активно відзначається в різних джерелах [42 - 45].

Атака на шифр полягає в отриманні ключа шифрування за наявності зашифрованого повідомлення. Атака може виконуватися з допомогою спеціалізованого програмного забезпечення, яке здійснює перебір пароля на підставі часткової інформації про передані даних.

Встановлення закладки та модифікація програмного забезпечення терміналу користувача дозволяє порушнику отримувати контроль над обладнанням користувача і будь-якою інформацією, що проходить через термінал, а також виконувати відведення інформації на свій сервер з метою виконання атаки НСД.

Встановлення додаткового обладнання на вузлі оператора зв'язку, дозволяє порушнику виконувати модифікацію даних, що передаються між кореспондентами, без необхідності зміни маршрутизації на мережевому обладнання оператора. Атака виконується за рахунок включення між обладнанням оператора і кореспондента обладнання порушника, або підключення цього обладнання в мережу передачі даних оператора.

Зміна налаштувань терміналу користувача для зниження рівня безпеки може виконуватися за рахунок зміни таблиці маршрутизації на терміналі користувача, часткового відключення механізмів безпеки, наприклад, зміни режиму роботи протоколу SRTP на автентифікацію повідомлень без шифрування, модифікації даних телефонної книжки і і т.д.

Атака “Перехоплення авторизаційних даних користувача, які застосовуються для управління VoIP-терміналом”, може бути виконана внутрішнім порушником, який знаходиться в одній підмережі з легітимним

користувачем. Досягається атака шляхом перехоплення трафіку в момент авторизації користувача на VoIP терміналі за рахунок атаки на MAC-таблицю обладнання чи переналаштування мережевого обладнання.

2.3 Зовнішній порушник

Розробка моделі починається з аналізу алгоритмів дій порушника за кожною з перерахованих атак.

Слід проаналізувати модель для зовнішнього порушника, завданням якого є досягнення НСД шляхом захоплення обладнання оператора.

Для початку атаки порушник має визначити, на який ресурс чи який пристрій оператора почати виконувати атаку. Однією з можливостей отримати цю інформацію є використання команди tracert для визначення проміжних вузлів між порушником і жертвою. Відповідно, ці вузли з великою ймовірністю можуть приймати участь в обміні пакетами між двома кореспондентами.

Після вибору вузла порушник може спробувати захопити управління цим вузлом, виконуючи, наприклад, перебір пароля. Однак, технічно віддалене керування може бути заборонене для порушника з використанням списків доступу ACL (Access Control List).

Ймовірність p_{12} відображає подію, що віддалене керування з боку порушника відключено або у оператора встановлені ACL.

Ймовірність p_{13} відображає подію, зворотну до p_{12} , що існує можливість віддаленого підключення до пристрою оператора.

Порушник вибирає доступний протокол (telnet, SNMP, ssh, http/https або ін) віддаленого керування, на який буде виконувати атаку перебором пароля. Ймовірність успішного перебору пароля за обмежений час визначається, як

$$p_{34A} = F(l, D, T, C), \qquad (2.1)$$

де l - довжина логіна/паролю;

T - час, протягом якого потрібно виконати перебір;

D - додаткові обмеження протоколу та технічні можливості порушника;

C - швидкість каналу зв'язку, по якому виконується перебір.

Ймовірність p_{34A} відображає подію, що перебір пароля виконаний успішно і порушник отримав доступ до обладнання оператора. Ймовірність p_{32} відображає подію, що перебір пароля за обмежений час закінчився безуспішно.

У випадку успішного захоплення віддаленого управління, порушник може досягти НСД двома шляхами: виконати перебір пароля до трафіку і прослуховувати дані, або виконати атаку на механізм розподілу ключів і дешифрувати трафік з використанням отриманого ключового матеріалу. Однак, успішне виконання цих двох атак може не привести до позитивного результату з досягнення НСД, якщо немає можливості виконати атаку MITM на медіа трафік, створивши правила на обладнанні оператора. Вони дозволять порушнику пропускати трафік користувача через своє обладнання.

Ймовірність успішної атаки на медіа трафік можна визначити із співвідношення $1 - p_{42A} = 1$, якщо існує технічна можливість на обладнанні оператора створити правило для перенапрямки трафіку користувача в бік порушника. Якщо ж відсутня така технічна можливість, тоді $1 - p_{42A} = 0$.

Під атакою розуміється зміна маршруту передачі пакетів даних, щоб вони проходили через обладнання порушника. У разі успішного проведення атаки порушник намагається виконати одну з двох можливих атак: перебір ключа медіа трафіку або атаку на механізм розподілу ключів.

При цьому ймовірності відображають: імовірність, що порушник почав виконувати перебір пароля до медіа трафіку (p_{45A}) та ймовірність, що порушник розпочав атаку на механізм розподілу ключів VoIP (p_{46A}). Ймовірність p_{57} означає успішну атаку по перебору пароля. У цьому випадку порушнику стає доступним прослуховування медіа трафіку однієї конкретної розмови, а також модифікації даних при наявності проксування і швидкого дешифрування ключа.

Імовірність p_{52} відображає без успішне закінчення атаки по перебору пароля за обмежений час. Перехоплені дані можуть зберігатися у порушника як завгодно довго, однак актуальність перехоплених даних може старіти з часом. Так розшифровані через 100 років переговори можуть не принести ніякої користі порушнику, оскільки за цей час дані застаріють. T_{NAR_AKT} – час, протягом якого дані є актуальними – залежить від характер даних. T_{NAR_SRTP} – час, потрібний на перебір пароля, залежить від технічних потужностей порушника Nar_{TH}, використовуваних для захисту медіа даних криптографічних засобів та криптоалгоритмів Nar_K, від довжини ключа Nar_L, а також від ускладнюючих елементів (застосування ініціалізуючого вектора, додаткових лічильників і тощо) $Nar_{D.}$

$$p_{57A} = f(T_{NAR\_AKT,} T_{NAR\_SRTP}) = f(T_{NAR\_AKT}, Nar_{TH}, Nar_K, Nar_L, Nar_D) \quad (2.3)$$

$$p_{52A} = 1 - p_{57A} \quad (2.4)$$

Імовірність p_{67} визначає успішну атаку на механізм розподілу ключів. Під атакою розуміється вторгнення порушника в середину каналу зв'язку - момент обміну ключами між кореспондентами. Це дозволяє порушнику виробити два ключі – один для роботи з першим кореспондентом та другий до роботи з другим кореспондентом. Тим самим, під час розмови двох кореспондентів порушник виконує шифрування і дешифрування медіаданих з використанням своїх ключів. Ймовірність атаки залежить від наявності у порушника технічних і програмних засобів для проведення MITM на протокол розподілу ключів. Слід зазначити, що для проведення даної атаки потрібна розробка спеціалізованого програмного забезпечення, але не потрібні великі обчислювальні потужності.

Ймовірність p_{62} відображає без успішне виконання атаки і може бути визначена, як:

$$p_{62A} = 1 - p_{67A} \quad (2.5)$$

Для аналізу алгоритму використовується математичний апарат ймовірнісних графів [82], який дозволяє отримати для досліджуваного алгоритму оцінки середнього часу виконання та ймовірність успішного завершення.

На рисунку 2.1 представлений імовірнісний граф, що відповідає наведеному раніше алгоритму.

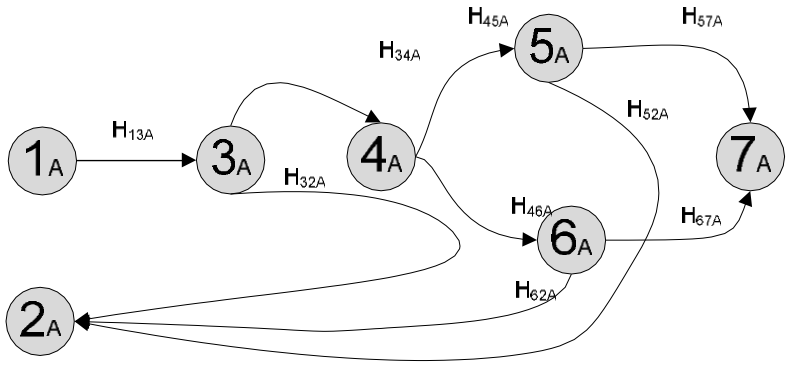


Рисунок 2.1 - Імовірнісний граф захоплення обладнання оператора зовнішнім зловмисником

Імовірнісний граф використовується для отримання похідної функції, відповідної переходу системи з початкового стану в кінцеве.

Кожній гілці графа відповідає похідна функція типу

$$H_{zy} = p_{zy} x^{Tzy}, \tag{2.6}$$

де p_{zy} - імовірність переходу в стан y з стану z,

T_{zy} - час, необхідний для переходу з стану z в стан y.

На графі виділена гілка, відповідна успішному виконанню атаки НСД та складена функція, що виробляє *H(x)* цієї гілки.

На графі відповідно до методики, наведеної в [82], представлені ймовірності:

$$P_{нсд_{ЦА}} = p_{13A}\, p_{34A}\, (p_{45A}\, p_{57A} + p_{46A}\, p_{67A}), \tag{2.7}$$

де p_{ijA} - імовірність переходу з вершини *i* графа в вершину *j*.

Доцільно проаналізувати модель для зовнішнього порушника, завданням якого є досягнення НСД. Завдання вирішується шляхом захоплення терміналу користувача. Алгоритм дій порушника наведено на рисунку 2.2. Розглянуто детальніше атаки, які може зробити порушник, в залежності від використання одним з кореспондентів шлюзу або персонального комп'ютера зі спеціалізованим програмним забезпеченням.

При використанні шлюзу найбільш ймовірною є атака з проксуванням всього трафіку через обладнання порушника. Атака виконується за схемою, зазначеною на рисунку 2.2, де IP1, IP2 - шлюзи користувачів, а Sн - сервер порушника зі спеціалізованим ПЗ.

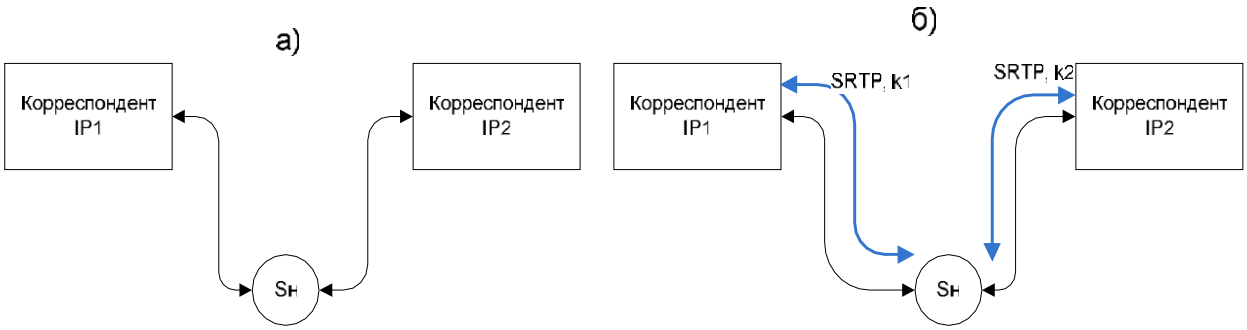


Рисунок 2.5 – Атака із проксуванням а) виконання ПРК; б) встановлений захищений канал

Для проведення цієї атаки порушнику потрібно в першу чергу захопити керування VoIP терміналом користувача і виконати його переналаштування. Наприклад, якщо у кореспондента в режимі точка-точка в телефонній книзі шлюзу введено поєднання номер – IP-адреса, то порушник може підмінити IP – адресу кореспондента Б у записнику кореспондента А на свій. Тим самим дзвінки з телефона кореспондента А приходитимуть на Sн. Сервер порушника виконує далі протоколи безпеки між собоюта кореспондентом Б від імені кореспондента А. Протоколи безпеки теж виконуються між кореспондентами Б і сервером

порушника. У результаті порушник отримує доступ до всією інформації, переданої від кореспондента А до кореспондента Б, у відкритому вигляді та за необхідності може не тільки прослуховувати, але й змінювати дані, передані між кореспондентами. Перенаправлення трафіку від кореспондента А на Sн можна здійснювати не тільки за рахунок заміни запису в адресній книжці, а й за рахунок зміни налаштувань на шлюзі кореспондента А, встановивши адресу свого Sн в якості проксі-сервера або основного сервера IP-телефонії.

При використанні комп'ютера з встановленим програмним шлюзом IP-телефонії найбільш реалізованими є атака з проксуванням всього медіатрафіку кореспондентів через Sн та використання програми-шпигуна на комп'ютері.

Перший тип атаки був описаний раніше. Атака з використанням програми-шпигуна полягає в установці на термінал користувача програмного забезпечення, яке надсилає голосові дані у відкритому вигляді з терміналу. Також передає всі вихідні та вхідні пакети з мережного інтерфейсу терміналу користувача на Sн для подальшої обробки. Тоді для доступу до переданої інформації порушник може вимкнути застосовувані на терміналі користувача А протоколи безпеки IP-телефонії, або, як мінімум, змінити режим роботи SRTP, вимкнувши шифрування переданих медіа даних.

Як правило, IP-телефони і шлюзи мають можливість віддаленогокерування, що використовується самими користувачами для їх налаштування. Обчислювальні пристрої також можуть мати віддалене управління, організоване внутрішніми засобами операційної системи, або з використанням додаткового програмного забезпечення. Однак, віддалене управління може бути також відключене користувачем, або можливості віддаленого керування можуть бути обмежені за рахунок застосування списків доступу.

Для успішного виконання атаки порушник має захопити віддалене управління користувацьким терміналом. У першу чергу, успіх атаки залежить від багатьох факторів.

При наявності віддаленого управління, порушнику для проведення атаки потрібно підібрати пароль або пару логін-пароль для авторизації на терміналі

користувача [46]. Передбачається, що IP адреса жертви відома порушнику заздалегідь. Підбір пароля або логіна-паролю залежить від протоколу віддаленого управління, на який виконується атака. Імовірність успішного перебору пароля має сенс оцінювати за кінцевий інтервал часу T , так як ймовірність успішного перебору пароля за нескінченне час буде дорівнює 1.

Ймовірність вибору однієї з двох атак визначається технічною оснащеністю порушника, а також наявністю у нього спеціалізованих інструментів та коштів.

Сенс першої атаки полягає в перехопленні голосової інформації в обхід протоколів IP-телефонії, або в вимкненні протоколів безпеки IP- телефонії чи зміні режимів роботи протоколів безпеки IP-телефонії, щоб можна було виконувати прослуховування.

Сенс другої і третьої атаки полягає в зміні налаштувань користувацького терміналу для реалізації атаки MITM, під час якої всі дані протоколів безпеки проходять через порушника. Це дозволяє йому контролювати передані голосові пакети, а також при необхідності виконувати модифікацію переданих даних. Фактично, при цій атаці порушник виконує з'єднання по черзі з кожним з кореспондентів, використовуючи протоколи забезпечення безпеки IP-телефонії, реалізуючи схему, представлену на рисунку 2.3.

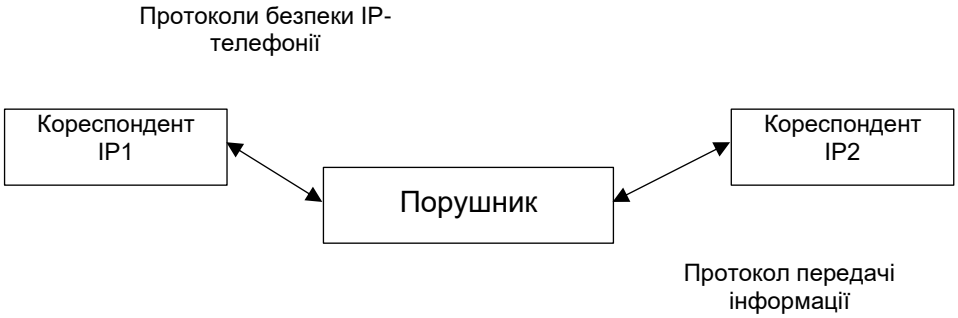


Рисунок 2.3 – Реалізація атаки MITM для всіх протоколів забезпечення безпеки VoIP

Вибравши одну з атак, порушник спробує виконати її для отримання несанкціонованого доступу до інформації, що передається. Однак існує

ймовірність безуспішного виконання обраної атаки, яка характеризується ймовірностями p_{72} та p_{62} відповідно.

Наприклад, атака “Зміна налаштувань терміналу користувача” може закінчитися безуспішно, якщо користувач помітить змінені налаштування та відновить свої налаштування, змінивши паролі доступу до терміналу або відключивши віддалене управління.

Використовуючи можливі алгоритми дій порушника, складений імовірнісний граф, представлений на рисунку 2.4.

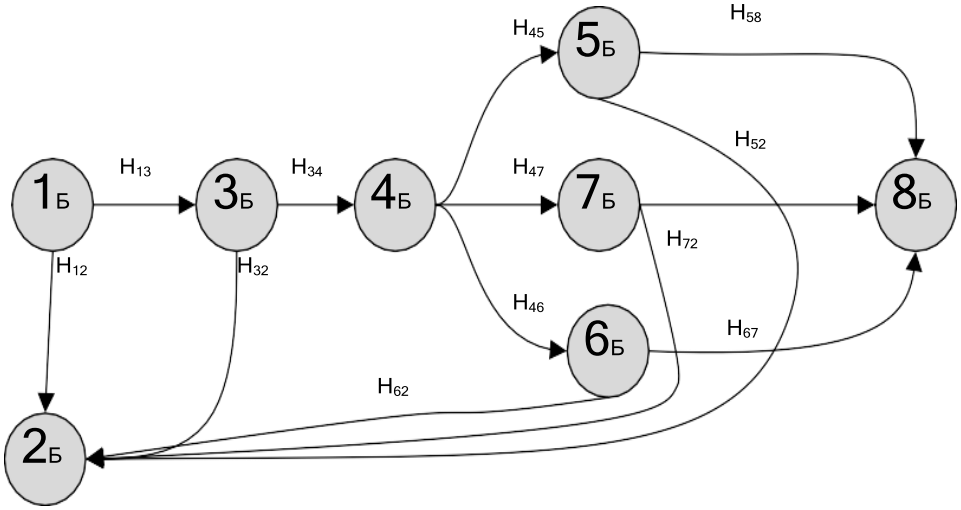


Рисунок 2.4 – Імовірнісний граф захоплення терміналу користувача зовнішнімпорушником

На графі виділено гілку, що відповідає успішному виконанню атаки НСД, та складена похідна функція *H(x)* цієї гілки.

Для графу відповідно з методикою, наведеною в [82], представлені $P_{НСД}$:

$$P_{НСД\text{-}ЦБ} = p_{13Б}\, p_{34Б}\, (p_{45Б}\, p_{58Б} + p_{46Б}\, p_{68Б} + p_{47Б}\, p_{78Б}), \qquad (2.10)$$

де $p_{ijБ}$ - ймовірність переходу з *i*- ї в *j*- у вершину графа.

2.4 Висновки до розділу 2

Наведено визначення порушника та опис терміналу користувача. Показано сукупність атак, які може виконувати порушник задля досягнення НСД. Представлено модель активного порушника для захищеної IP-телефонії, яка враховує можливості цього порушника реалізувати атаку MITM на ПРК та інші атаки. Модель дозволяє розрахувати ймовірність успішної атаки, націленої на НСД.

Показано, що особливу небезпеку становлять зовнішній та внутрішній порушники, які виконують атаку на обладнання оператора. Представлено імовірнісну модель такого порушника. Показано, що найнебезпечнішою є атака MITM на протоколи розподілу ключів.

3 АЛГОРИТМИ ВДОСКОНАЛЕННЯ ПРОТОКОЛІВ РОЗПОДІЛУ КЛЮЧІВ

Для дослідження імовірнісно-часових характеристик необхідно розглянути протоколи розподілу ключів захищеної IP-телефонії, на відповідність вимогам до ПРК, описаним в першому розділі:

– підтримка топологій клієнт-сервер і клієнт-клієнт (*К1*);

– функціонування без застосування додаткових протоколів між кореспондентами для реалізації функції розподілу ключів (*К2*);

– робота без передачі ключа каналом зв'язку у відкритому вигляді (*К3*);

– наявність механізму виявлення MITM без попередньо розподіленого ключового матеріалу між кореспондентами, а також без використання сертифікатів (*К4*);

– використання TCP/UDP портів для IP-телефонії (SIP/RTP), або TCP/UDP портів, використання яких узгоджено через встановлення з'єднання(*К5*).

У випадку виконання вимоги *Ki* =1, у протилежному випадку *Ki* = 0. Порівняння протоколів наведено в таблиці 3.1.

Таблиця 3.1 - Оцінка ПРК на відповідність вимогам

Опис вимоги до ПРК	Протоколи			
	DTLS	ZRTP	SDES	MIKEY
К1	1	1	0	1
К2	1	1	0	0
К3	1	1	0	1
К4	0	1	0	0
К5	1	1	1	1
$Q_{ПРК}$	4	5	1	3

Оцінка кожного з протоколів здійснюється згідно з формулою:

$$Q_{\text{ПРК}} = \sum_{i=1}^{5} К_i, \quad (3.1)$$

Протокол DTLS не відповідає четвертій вимогі, поданій у таблиці 3.1, оскільки розроблявся до роботи у топології клієнт - сервер і використовує встановлені сертифікати для захисту від MITM у обох кореспондентів. Тому для DTLS *К4* = 0.

На відмінність від інших протокол ZRTP має вбудований механізм SAS (Short Authentication String) для захисту від MITM. Тому для ZRTP *К4* =1. Для SDES та MIKEY *К4* = 0.

Протокол MIKEY не відповідає другій вимозі таблиці 3.1, тому що повідомлення протоколу можуть передаватися або в SIP/SDP-повідомлення, або поверх RTSP (Real Time Streaming Protocol).

В останньому випадку кореспонденти повинні додатково підтримувати протокол RTSP. Тому *К2* = 0 для MIKEY.

П'ята вимога під час роботи поверх RTSP протоколу не виконується, але при цьому виконується друга вимога. При роботі MIKEY поверх в SIP/SDP-повідомлення п'ята вимога виконується, але не виконується друга вимога. Так як при оцінки $Q_{ПРК}$ використовується *К2* =0, то *К1* = 1 для MIKEY.

Протокол SDES не відповідає першій та третій вимогам (*К1*=0 і *К3* = 0). Ключ передається між кореспондентами в явному вигляді в повідомленнях SDP та потребує їх додаткового захисту. Для захисту як правило використовується додатковий протокол SIPS. Однак, при з'єднанні клієнт-клієнт, коли у кореспондентів заздалегідь нема розподіленого ключового матеріалу, SIPS з'єднання з захистом від MITM організувати неможливо. Протокол SDES не відповідає також другій вимозі, оскільки для передачі даних протоколу SDES використовуються повідомлення SIP/SDP. Відповідно *К2* =0 для SDES.

3.1 Підвищення безпеки ZRTP за рахунок автоматичної автентифікаційної перевірки рядка

Протокол Діффі-Хелмана може бути повністю скомпрометований активним зловмисником. Тому при роботі протоколу необхідно забезпечити ідентичність вихідних даних. Через це протокол обміну ключами Діффі-Хелмана, зазвичай, застосовують по захищеному каналу передачі даних [50] , в якому неможливо виконати заміну переданих повідомлень. Також при використанні сертифікатів чи довіреного центру сертифікації, якому довіряють обидва кореспондента для здійснення автентифікації.

У разі потреби встановити захищене з'єднання між двома кореспондентами, вони, по перше, можуть не мати загальних сертифікатів (тобто. сертифікатів, які мають один і той же кореневий довірений центр), не мати загального довіреного центру сертифікації або розподілу ключів, а також можуть не мати захищеного каналу зв'язку між собою.

При наявності у кореспондентів сертифікатів, підписаних різними центрами сертифікації, неможливо перевірити справжність сертифікату, тому що кожен з кореспондентів може не довіряти центру сертифікації респондентів.

Для організації захищеного з'єднання між кореспондентами також потрібно виконати розподіл ключового матеріалу для цього з'єднання. Кореспонденти можуть використовувати симетричне або асиметричне шифрування. При використанні симетричного шифрування - один з кореспондентів повинен передати іншому секретний ключ. Якщо цей ключ стане відомим порушнику – передані у процесі сеансу зв'язку повідомлення будуть розшифровані порушником. При використанні асиметричного шифрування - інформація не буде прочитана порушником навіть у випадку перехоплення повідомлень. Однак - при обміні ключами для організації захищеного з'єднання у кореспондентів не буде можливості переконатися, що відкритий ключ передається між ними без модифікації порушником.

Аналіз проведених досліджень показує, що відомі протоколи розподілу ключів необхідно вдосконалювати у двох напрямках: підвищення безпеки та покращення ІЧХ протоколів.

Найбільш небезпечною атакою на протокол розподілу ключів є атака MITM. Завдання формування ключів в умовах вторгнення порушника в середину каналу зв'язку є актуальною і її вирішенню присвячено ряд наукових праць [86-90] . Особливістю даних робіт є те, що для формування ключів між кореспондентами використовується ефект незалежності випадкових процесів у різних точках середовища передачі сигналу. У протоколах формування ключів для IP-телефонії обмін повідомленнями реалізується на мережевому рівні і ефекти випадкових процесів серед передачі даних однакові у всіх точках на шляху передачі пакетів. Тому запропоновані підходи досить важко використовувати для розподілу ключів в IP-телефонії. Також проводяться дослідження по підвищенню безпеки протоколів [47-49]. Спорідненістю даних робіт є необхідність наявності спільного секрету між кореспондентами. Однак, це умова не завжди може бути виконана.

Одним з шляхів підвищення безпеки протоколу є зниження ймовірності вторгнення порушника до протоколу шляхом використання кількох незалежних каналів зв'язку. Для підвищення безпеки пропонується використовувати два підходи: підвищення безпеки за рахунок автоматизації перевірки автентифікаційного рядка по іншому каналу зв'язку та використання двох і більше каналів зв'язку для виконання протоколу розподілу ключів.

Захист від порушника в режимі клієнт-клієнт виконується за рахунок перевірки автентифікаційної рядки, яка передається по голосовому каналу в ручному режимі. Голосовий канал в цьому випадку є додатковим каналом зв'язку по відношенню до IP-каналу. Доцільно автоматизувати процес перевірки SAS. Існуючий метод не безпечний, тому що використовується один канал зв'язку, а сучасні засоби аналізу і синтезу мови дозволяють виконувати автоматичне вирізання рядки і заміну на рядок, синтезовану порушником.

Проведене практичне дослідження показало, що існує висока ймовірність наявності між кореспондентами незалежних непересічних маршрутів під час використання кількох каналів зв'язку. В основі пропонованих протоколів використано перевага легітимних кореспондентів над нелегітимними. Вона полягає в тому, що тільки легальні кореспонденти можуть отримувати повідомлення по двох і більше каналах зв'язку одночасно, володіючи інформацією про IP-адреси кореспондентів. При цьому ця інформація не є секретною для порушника. Слід відзначити, що метод модернізації протоколів розподілу ключів розглядається, як підвищення безпеки, але при цьому не забезпечує 100% достовірність.

Розглядаються кілька можливих варіантів модернізації протоколу розподілу ключів при використанні двох або трьох каналів зв'язку. В якості критеріїв оцінки використовуються значення наступних ймовірностей:

- ймовірність успішної атаки MITM $P_{УА}$;
- ймовірність виявлення атаки MITM $P_{ВІН}$;
- ймовірність успішного генерування спільного ключа $P_{КК}$.

Протокол ZRTP має механізм захисту від MITM. Полягає він у вербальній перевірці короткої автентифікації рядка SAS по мовному каналу між обома кореспондентами. Це означає, що після виконання протоколу ZRTP і встановлення мовного каналу в топології клієнт-клієнт без сервера, кореспонденти отримують значення SAS - обчислений текстовий рядок з комбінації символів.

$$SAS = f(hash(Hello)\ респондента || Commit || DHPart1 || DHPart2).$$

Один з кореспондентів вимовляє автентифікаційний рядок по мовному каналу, що встановився. Другий кореспондент звіряє SAS на своєму терміналі зі значенням, отриманим мовним каналом. Якщо SAS збігаються, значить, не має місце атака MITM, або має місце атака з підробкою SAS по мовному каналу зв'язку. Якщо SAS різняться, то це свідчить, що має місце атака MITM у каналі

передачі. Таким чином, при з'єднанні двох кореспондентів без участі сервера автентифікація виконується за рахунок знання кореспондентом голосу другого кореспондента, а також за рахунок неспотвореної передачі інформації двома каналами: по мовному каналу SRTP та каналу передачі даних.

Сучасні технології достатньо просто дозволяють виконувати як аналіз голосу кореспондентів, так і синтез мови, в тому числі синтез мови підробки голосу. Розглядаються два варіанти:

- кореспонденти знають голос один одного;

- кореспонденти не знають голос один одного.

У першому випадку, при з'єднанні кореспондент, що викликає, як правило, вимовляє вітання та ім'я сторони, що викликається. Після цього виконується вербальна перевірка SAS. Зібраних голосових даних може бути достатньо для синтезу мови кореспондента для заміни одних слів на інші з метою підміни SAS у голосовому каналі. У цьому випадку перевірка SAS пройде успішно навіть за наявності атаки MITM.

У другому випадку, коли кореспонденти не знають голоси один одного, не потрібно збору даних, так як синтез можна, напевне, виконувати з використанням будь-якого голосу.

У якості модернізації протоколу ZRTP пропонується додавання автоматизованої перевірки автентифікації рядка SAS.

Інформація про IP-адреси може бути передана між кореспондентами по телефону, по електронній пошті, при особистsq зустрічі, листом та іншими доступними методами. Відмінною особливістю є те, що інформація про IP-адреси не є секретною інформацією для порушника та може бути передана по відкритих каналах зв'язку. В цей час, як пароль для симетричного шифрування є секретним і розголошення приведе до можливості порушника дешифрувати передану інформацію за порівнянням довжини асиметричного ключа, загальна довжина двох IPv4 чи IPv6 адрес набагато менша. При перехопленні асиметричного ключа порушник може надсилати дані легітимному респонденту так само, як і легітимний кореспондент.

При використання IP-адрес додатковою мірою для підвищення безпеки є перевірка IP-адрес повідомлень відправника респондентом, а також можливість отримання всіх повідомлень, надісланих по двом каналам зв'язку, лише легітимними респондентами за відсутності атаки MITM одночасно в кількох каналах.

Даний метод підвищення безпеки ZRTP вимагає передачі лише одного повідомлення від кожного з кореспондентів по додатковому каналу зв'язку. Як другий канал зв'язку може виступати не обов'язково канал передачі даних, а й SMS, MMS, транспорт.

Особливістю підходу також є невисока складність розробки програмної реалізації протоколу за рахунок використання існуючих бібліотек [93, 94]. Значення SAS передається в додаток за результатами виконання протоколу ZRTP. Достатньо додатково передати цей параметр кореспондентові по іншому каналу зв'язку у відкритому або зашифрованому вигляді для реалізації автоматичної перевірки.

Недоліком методу підвищення безпеки в вигляді автоматизації перевірки SAS є виявлення порушника у каналі зв'язку безпосередньо після успішного виконання протоколу, а не під час виконання. Для оцінки можливості застосування кількох каналів зв'язку з метою підвищення безпеки необхідно вирішити наступні завдання:

− оцінити ймовірність наявності спільної точки в двох і більше каналах зв'язку;

− використання різних операторів зв'язку між кореспондентами;

− розробити алгоритм прийняття рішення про присутність порушника і оцінка ймовірності помилки можливих рішень.

Оцінку ймовірності показує високе значення ймовірності наявності двох та більше незалежних каналів зв'язку між кореспондентами, підключеними до різних операторів зв'язку.

Пропонується використовувати наступний алгоритм автоматичної перевірки SAS. Кореспонденти A та B виконують попередній обмін інформацією про IP-адресах IP_{A1}, IP_{A2}, IP_{B1}, IP_{B2}, де IP_{A1}, IP_{A2} - адреси кореспондента A та

IP_{B1} , IP_{B2} - адреси кореспондента В, а також налаштовують таблицю маршрутизації. Для установки захищеного з'єднання, кореспонденти А і В, виконують протокол ZRTP через канал зв'язку IP_1 - IP_{B1}. У результаті кожен обчислює значення SAS (див.рисунок 3.1). Кореспондент А відправляє SAS_A каналом зв'язку IP_{A2} - IP_{B2} кореспондентові В. Кореспондент В отримує SAS_A'. Кореспондент В відправляє SAS_B по каналу зв'язку IP_{A2} - IP_{B2} кореспондентові А. Кореспондент Аотримує SAS_B'.

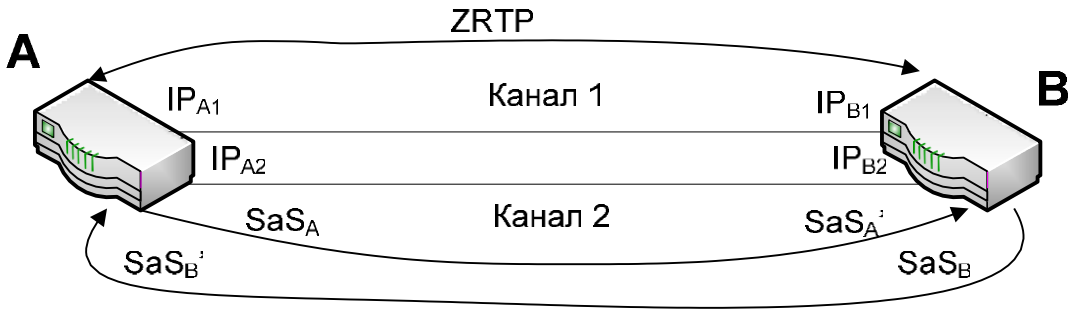


Рисунок 3.2 - Механізм автоматичної перевірки SAS

Кореспондент В виконує порівняння SAS_A' і SAS_B . Якщо вони збігаються, то це свідчить про відсутність активного порушника в двох каналах зв'язку, або присутній той самий активний порушник одночасно у двох каналах зв'язку. Якщо значення SAS не збігаються, кореспондент В отримує повідомлення від терміналу про наявності порушника в каналі зв'язку.

Кореспондент А виконує порівняння SAS_A і SAS_B'. Якщо вони збігаються, то це свідчить про відсутність активниго порушника в двох каналах зв'язку, або присутній той самий активний порушник одночасно у двох каналах зв'язку. Якщо значення SAS не збігаються, кореспондент А отримує повідомлення від терміналу про наявності порушника в каналах зв'язку.

Протокол фактично дозволяє виявити наявність активного порушника, працюючого в одному з двох каналів зв'язку.

Виконується розрахунок ймовірностей подій: $P_{УА}$, $P_{ВІН}$, $P_{КК}$.

Під успішною атакою розуміється подія, що порушник успішно реалізував атаку MITM, здійснивши обмін ключами з обома кореспондентами при використанні кількох каналів зв'язку, не виявивши себе під час проведення атаки. Це можливо лише в одному випадку, якщо один і той самий порушник може контролювати всі канали зв'язку, що використовуються кореспондентами, і виконувати синхронну модифікацію переданих повідомлень в кожному з каналів зв'язку.

Ймовірність успішної атаки $P_{УА\_SAS}$ для протоколу з автоматичною перевіркою SAS відповідає ймовірності події, що порушник може прослуховувати і виконувати модифікацію повідомлень в двох каналах зв'язку одночасно.

$$P\ УА2\_SAS = (P\ НІК)^2 \tag{3.1}$$

Під подією виявлення порушника визначається подія, що порушник виявлено кореспондентами в одному з використовуваних каналів зв'язку. Виявлення порушника дозволяє користувачам визначити, що може бути вироблений компрометований ключ, який дозволить порушнику дешифрувати і прослуховувати передану інформацію, а також виконувати модифікацію переданих повідомлень.

Під подією успішного генерування ключа розуміється, що порушника не виявлено в жодному з каналів зв'язку і кореспонденти виробляють ключ для подальшої роботи та шифрування переданих даних. Подія можлива тільки у випадку, якщо порушника нема ні в одному каналі зв'язку.

Ймовірність виявлення порушника $P_{ВІН\_SAS}$ для протоколу з автоматичною перевіркою SAS відповідає ймовірності знаходження порушника в одному каналі зв'язку за відсутності порушника в іншому каналі зв'язку.

Нехай сеанс ZRTP виконується по першому каналу зв'язку.

Ймовірність наявності порушника в першим каналі зв'язку при відсутностіпорушника у другому каналі зв'язку буде мати вигляд:

$$P_{HAP1K\_HE\_HAP2K} = (1 - P_{H1K})\, P_{H1K} \quad (3.2)$$

Ймовірність наявності порушника у другому каналі зв'язку за відсутності порушника в першим каналі зв'язку буде визначатися за аналогією з 3.2.

$$P_{BIH\_SAS} = 2(1 - P_{H1K})\, P_{H1K} \quad (3.3)$$

Під подією успішного генерування ключа розуміється, що порушника не виявлено в жодному з каналів зв'язку і кореспонденти виробляють ключ для подальшої роботи та шифрування переданих даних. Подія можлива тільки у випадку, якщо порушника нема ні в одному каналі зв'язку.

Імовірність успішного генерування ключа $P_{УК\_SAS}$ для протоколу протоколу з автоматичною перевіркою SAS відповідає ймовірності відсутності порушника в обох каналах зв'язку.

Ймовірність відсутності порушника в одному каналі зв'язку P_{HI_HAP} має вигляд:

$$P_{HI\_HAP} = 1 - P_{H1K} \quad (3.4)$$

Тоді:

$$P_{KK\_SAS} = P^2_{HI\_HAP} = (1 - P_{HIK})^2 \quad (3.5)$$

Однак, протокол з автоматичною перевіркою SAS не дозволяє визначити, який саме із каналів зв'язку атакує порушник. Також наявність порушника визначається тільки в результаті повного виконання протоколу і не може бути детерміновано в часі виконання протоколу. За цієї причини, слід розглянути додаткові варіанти модернізації протоколу ZRTP [48], в том числі варіанти, позбавлені вище описаних недоліків.

3.2 Виявлення порушника протоколів розподілу ключів, побудованих на алгоритмі Диффі- Хелмана

Для підвищення безпеки пропонується застосовувати метод виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана, що дозволяє виконувати розподіл ключів з використанням кількох каналів зв'язку одночасно і виявляти активного порушника.

В даний час наявність двох більше підключень в одного кореспондента достатньо поширене. Окремим випадком може бути користувач, який має бездротове підключення через 3G / 4G модем і одночасно має підключення до мережі Інтернет від оператора дротової широкосмугової мережі передачі даних.

Нехай існують два кореспонденти, які мають кожен по два і більше підключень в глобальній мережі Інтернет. Кожне підключення виконуєтьсячерез різних операторів зв'язку. Обидва кореспонденти мають публічну IP-адресу в кожному використовуваному каналі зв'язку. Кожен з кореспондентів передає іншому свої IP-адреси, які будуть використовуватися для встановлення зв'язку між кореспондентами. Дані можуть бути передані в словесній формі під час зустрічі, за допомогою електронної пошти чи поштового відправлення тощо, а також з використанням комбінації вищеописаних засобів зв'язку. Реалізація роботи протоколу ZRTP двома і більше каналами зв'язку вимагає інтеграцію багатоканального протоколу з протоколами SIP/RTP для вирішення наступних технічних завдань:

– визначення додаткових IP-адрес, а також UDP портів для виконання другої сесії протоколу, а також передачу цих параметрів до протоколу, клас протоколу або функцію протоколу;

– реалізація перевірки отриманих повідомлень Діффі-Хелмана по різних каналах зв'язку і виконання подальших дій за результатами перевірки;

– інтеграція з SIP та RTP протоколами, а також використання оригінальним

протоколом ZRTP узгоджені IP і UDP порти з цих протоколів.

У той же час, реалізація одночасного обміну повідомленнями ZRTP двом каналам зв'язку, а також реалізація перевірки ідентичності повідомлень, може вимагати набагато більших ресурсів. Для реалізації двоканального методу (2К) підвищення безпеки двом каналам зв'язку будуть передаватися однакові повідомлення обміну Діффі- Хелман. Ініціатор (бажаючий встановити захищене з'єднання) відправляє по двох каналах зв'язку два однакових повідомлення. Респондент отримує повідомлення, виробляє необхідні обчислення, а також перевіряє, що отримано однакові повідомлення. У разі, якщо отримані різні повідомлення, то має місце наявність активного порушника, виконуючого атаку MITM в одному з каналів,. Респондент відповідає, відправляючи по двох каналах зв'язку у відповідь повідомлення Діффі-Хелмана. Ініціатор отримує повідомлення та перевіряє – чи є повідомлення однаковими. Якщо повідомлення однакові – це означає що відсутній активний порушник в обох каналах зв'язку, або існує один і той же активний порушник в обох каналах зв'язку. Взаємодія кореспондентів при використанні модифікації ZRTP представлена на рисунку 3.2.

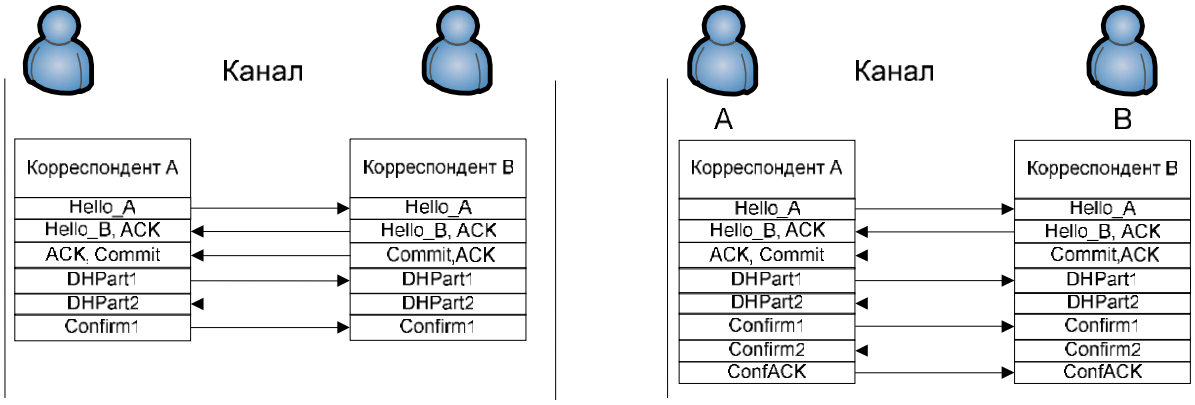


Рисунок 3.2 – Варіант взаємодії кореспондентів під час використання модернізованого протоколу ZRTP в режимі двоканального обміну.

Слід ввести ймовірність $P_{НІК}$, що порушник може виконувати атаку MITM в одному з каналів зв'язку. Ця ж ймовірність буде відповідати невдалій спробі виконання атаки MITM.

Виконується розрахунок ймовірностей подій: $P_{УА,} P_{ВІН,} P_{КК.}$

Під успішною атакою розуміється подія, що порушник реалізував атаку MITM, виконавши обмін ключами з обома кореспондентами по декількох каналах зв'язку. При цьому, порушник не виявив себе при проведенні атаки. Це стає можливим лише у випадку, коли один і той самий порушник може контролювати всі канали, що використовуються кореспондентами зв'язку та виконувати синхронну модифікацію переданих повідомлень у кожномуз каналів.

Ймовірність успішної атаки $P_{УА2}$ для двоканального протоколу відповідає $P_{Н2К}$ - ймовірності події, що порушник може прослуховувати та виконувати модифікацію повідомлень в 2 каналах зв'язку одночасно.

$$P_{УА2} = P_{Н2К} = (P_{Н1К})^2 \tag{3.7}$$

Виявлення порушника дозволяє користувачам визначити, що може бути вироблений компрометований ключ, що дозволяє дешифрувати і прослуховувати передану інформацію, а також виконувати модифікацію повідомлень. Ймовірність виявлення порушника залежить від числа використовуваних каналів зв'язку, а також від здатності алгоритму розподілу ключів визначити існування порушника у конкретному чи конкретних каналах зв'язку із сукупності використовуваних.

Ймовірність виявлення порушника $P_{ВІН2}$ для двоканального методу відповідає ймовірності знаходження порушника в одному каналі зв'язку при відсутності порушника в другом каналі зв'язку. Ймовірність наявності порушника в першим каналі зв'язку при відсутності порушника у другому каналі зв'язку буде мати вигляд:

$$P_{НАР1К\_НІ\_НАР2К} = (1 - P_{Н1К}) P_{Н1К} \tag{3.8}$$

Імовірність наявності порушника у другому каналі зв'язку за відсутності порушника в першим каналі зв'язку буде мати вигляд:

$$P_{НІ\_НАР1К\_НАР2К} = (1- P_{Н1К}) P_{Н1К} = P_{Н1К} - (P_{Н1К})2 \quad (3.9)$$

$$P_{ВІН2} = P_{НАР1К\_НЕТ\_НАР2К} + P_{НІ\_НАР1К\_НАР2К} = =2(1- P_{Н1К}) P_{Н1К} \quad (3.10)$$

Під успішним генеруванням ключа розуміється подія, що порушника не виявлено в жодному каналі зв'язку та кореспондентами вироблено ключ для шифрування переданих даних. Це можливо лише у разі відсутності порушника у використовуваних каналах зв'язку, або при використанні алгоритму розподілу ключів здатного визначати точне знаходження порушника в конкретному або конкретних каналах зв'язку із сукупності використовуваних.

Ймовірність успішного генерування ключа $P_{КК2}$ для двоканального протоколу відповідає ймовірності відсутності порушника в обох каналах зв'язку. Ймовірність відсутності порушника в одному каналі зв'язку $P_{НІ\_НАР}$:

$$P_{НІ\_НАР} = 1- P_{Н1К} \quad (3.11)$$

Тоді:

$$P_{КК2} = P^2_{НІ\_НАР} = (1- P_{Н1К})^2 \quad (3.12)$$

Розглядається інший варіант методу виявлення порушника з використанням трьох каналів передачі даних. Нехай по трьох каналам зв'язку передаються однакові повідомлення обміну Діффі-Хелмана. Ініціатор відправляє трьома каналами зв'язку три однакові повідомлення. Респондент отримує повідомлення, здійснює необхідні обчислення, а також перевіряє, що отримані однакові повідомлення з усіх трьох каналів зв'язку. У випадку, якщо отримані різні повідомлення, має місце наявність активного порушника, виконуючого атаку MITM, або порушник контролює одночасно усі три канали зв'язку. Респондент відповідає, відправляючи по трьох каналах зв'язку повідомлення у відповідь Діффі-Хелмана. Ініціатор отримує повідомлення і перевіряє чи є повідомлення однаковими. Можливі кілька варіантів роботи протоколу при використання методу виявлення порушника:

– якщо повідомлення однакові, то активний порушник відсутній у всіх каналах зв'язку, або існує активний порушник у всіх трьох каналах зв'язку;

– якщо одне повідомлення відрізняється від інших, значить або є один активний порушник в цьому каналі зв'язку, або присутні два порушника в двох інших каналах зв'язку;

– якщо усі повідомлення різні, значить, присутні два окремо діючі порушники, не мають між собою каналу зв'язку.

Таким чином, протокол дозволяє:

− за наявності одного порушника в одному із трьох каналів зв'язку визначити канал з порушником;

− при наявності порушника в двох каналах зв'язку виявити наявність порушника, без визначення каналів зв'язку, що містять порушника.

Проте протокол не дозволяє при знаходженні порушника у трьох каналах. зв'язку визначити наявність порушника. Відповідно, можна виділити два режими роботи методу підвищення безпеки: режим роботи з виявлення порушника (З-ВП) та режим роботи з винятком порушника (З-ІП).

При роботі в режимі ВІП у разі виявлення відмінності хоча б одного з трьох повідомлень протокол завершується з помилкою, повідомляючи користувача про наявності порушника в канал зв'язку. У разі роботи в режимі ІП при виявленні відмінності одного із трьох повідомлень формується повідомлення користувача про наявність порушника у конкретному каналі зв'язку. При цьому протокол продовжує роботу і враховує повідомлення лише з тих каналів зв'язку, де не виявлено порушника. Так забезпечується правильне виключення порушника. Ймовірність правильного виключення порушника для трьох канального протоколу відповідає події знаходження порушника в одному з каналів зв'язку та за його відсутності в двох інших каналах.

$$P_{ВІП} = 3\,P_{НІК}\,(1 - P_{НІК})^{2} \qquad (3.13)$$

Однак, за наявності активного порушника одночасно у двох каналах зв'язку з трьох можливих, а також синхронної модифікації повідомлень у двох каналах зв'язку порушником, механізм виключення може спричинити некоректне визначення каналу з порушником, що призведе до помилкового вибору двох каналів, що містять порушника, в якості надійних. Це дозволить порушнику успішно виконати обмін ключами з кореспондентами, здійснивши успішну атаку MITM.

Імовірність помилкового виключення відповідає ймовірності події, що порушник знаходиться одночасно в двох каналах зв'язку.

$$P_{ПОМ} = 3\,P^2_{Н1К}(1 - P_{Н1К}) \qquad (3.14)$$

Ця ймовірність буде також складовою ймовірності успішної атаки MITM. Розрахунок ймовірностей для протоколу трьохканального обміну. в режимі ВІП .

Ймовірність успішною атаки $P_{УАЗ\_ВІП}$ для трьохканального протоколу в режимі ВІП відповідає $P_{Н3К}$ - ймовірність події, що порушник може прослуховувати і виконувати модифікацію повідомлень в трьох каналах зв'язку одночасно.

$$P_{УАЗ\_ВІП} = P_{Н3К} = (P_{Н1К}\ \ 3 \qquad (3.15)$$

Ймовірність виявлення порушника для триканального протоколу в режимі ВІП відповідає ймовірності знаходження порушника в одному або двох каналах зв'язку при відсутності порушника в другом канал зв'язку. Імовірність наявності порушника в одному з каналів зв'язку за відсутності порушника в двох інших каналах зв'язку має вигляд:

$$P_{НАР1К\_НЕ\_НАР23К} = 3(1 - P_{Н1К})^2\,P_{Н1К} \qquad (3.16)$$

Ймовірність наявності порушника в двох з трьох каналів зв'язку при відсутності порушника в одному з каналів зв'язку буде мати вигляд:

$$P_{НІ\_НАР1К\_НАР23К} = 3(1 - P_{Н1К}) P_{Н1К}^{2} \tag{3.17}$$

$$P_{ОНЗ\_ВІП} = P_{НАР1К\_НЕ\_НАР23К} + P_{НІ\_НАР1К\_НАР23К} = 3(1 - P_{Н1К})^{2} P_{Н1К} + 3(1 - P_{Н1К}) P_{Н1К}^{2} \tag{3.18}$$

Ймовірність успішного генерування ключа $P_{ККЗ\_ВІН}$ для триканального протоколу у режимі ВІП відповідає ймовірності відсутності порушника в трьох каналах зв'язку:

$$P_{ККЗ\_ВІН} = P3_{НІ\_ПОР} = (1 - P_{Н1К})3 \tag{3.19}$$

Виконується розрахунок ймовірностей $P_{УА}$, $P_{ВІН}$, $P_{КК}$ для протоколу трьохканального обміну в режимі ІН. Вірогідність успішної атаки $P_{УАЗ\_ІН}$ для триканального протоколу відповідає ймовірності події, що порушник може прослуховувати і виконувати модифікацію повідомлень в двох або трьох каналах зв'язку одночасно.

$$P_{УАЗ\_ІН} = (P_{Н1К})^{3} + 3(1 - P_{Н1К}) P_{Н1К}^{2} \tag{3.21}$$

Ймовірність виявлення порушника $P_{ОНЗ\_ІН}$ для трьохканального протоколу в режимі ІН відповідає ймовірності знаходження порушника в одному каналі зв'язку за відсутності порушника у двох інших каналах зв'язку та буде мати вигляд:

$$P_{ОНЗ\_ІН} = 3(1 - P_{Н1К})^{2} P_{Н1К} \tag{3.22}$$

Ймовірність успішною вироблення ключа $P_{УКЗ\_ІН}$ для триканального протоколу у режимі ІН відповідає ймовірності відсутності порушника у двох або трьох каналах зв'язку:

$$P_{ККЗ\_ІН} = (1 - P_{НІК})^3 + 3(1 - P_{НІК})^2 P_{НІК} \quad (3.22)$$

3.3 Експериментальне дослідження розробленого алгоритму

Отримані залежності для ймовірності успішної атаки MITM представлені на рисунку 3.3.

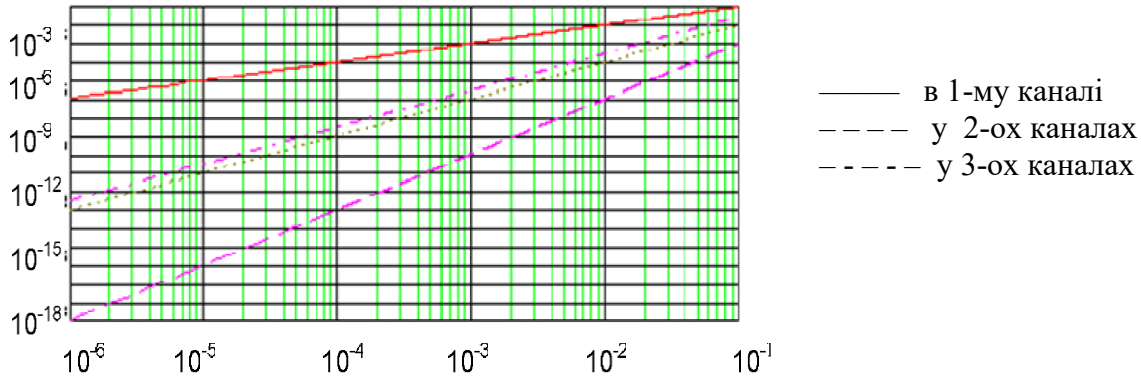


Рисунок 3.3 – Порівняння ймовірностей успішної атаки MITM

Отримана ймовірність виявлення порушника представлена на рисунку 3.4.

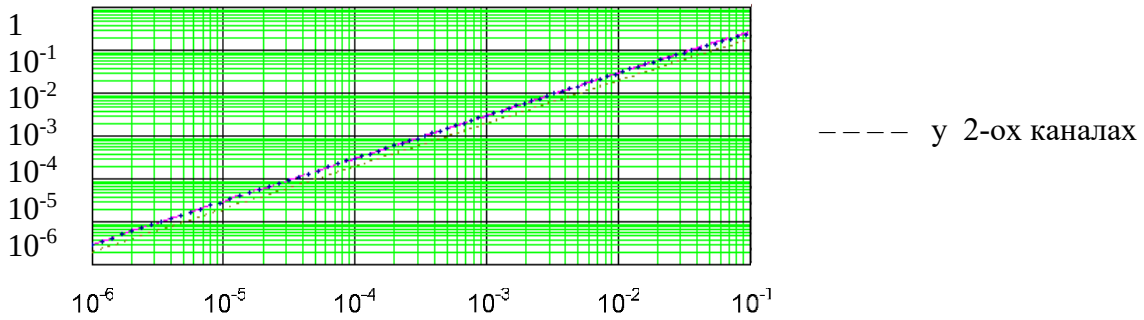


Рисунок 3.4 – Імовірність виявлення порушника

Отримані залежності для ймовірності успішної атаки MITM представлені на рисунку 3.5

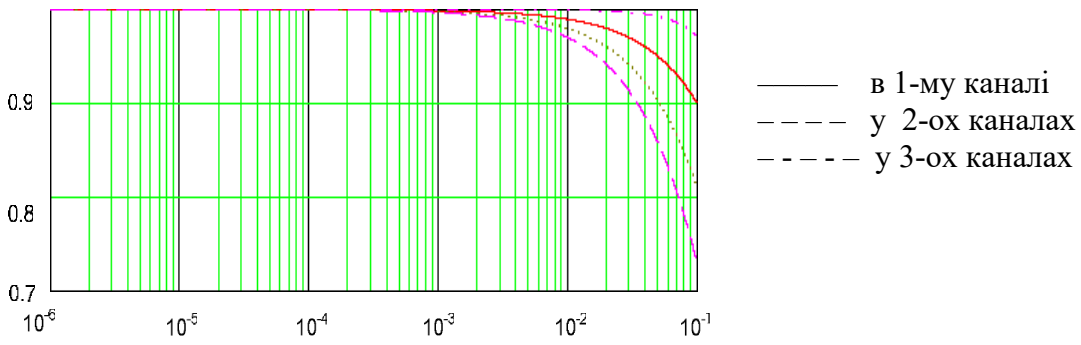


Рисунок 3.5 – Імовірність успішного генерування ключа

Модифікація протоколу для роботи по кількох незалежних каналах суттєво зменшує ймовірність успішної атаки MITM. Ефективність захисту зростає із збільшенням числа незалежних каналів. Модифікація в режимі виявлення порушника з використанням трьох каналів зв'язку має найбільшу ймовірність виявлення порушника, а також найменшу ймовірність успішної атаки порушника. Модифікація у режимі виключення порушника з застосуванням трьох каналів має найбільшу ймовірність успішного генерування спільного ключа між кореспондентами. Для реалізації вибирається одна з модифікацій залежно від цілей та доступних ресурсів, виражених у числі доступних каналів зв'язку. Дослідження показують, що при підключенні кореспондентів до кількох операторів зв'язку незалежні двійки та трійки маршрутів є завжди.

Імовірність успішного формування загального ключа в багатоканальній схемі з виявлення порушника зменшується незначно.

У схемі з винятком порушника дана ймовірність збільшується, але при використанні маршрутів великої протяжності можливий збіг вузлів проходження маршрутів, що може знизити ефективність роботи модифікованого протоколу.

3.4 Висновки до розділу 3

Запропонований алгоритм виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана. Алгоритм використовує декілька відкритих каналів зв'язку та опублікований в [50]. Виявлення порушника відрізняється зниженою ймовірністю успішної атаки MITM, а також наявністю механізму визначення активного порушника в каналі зв'язку навіть за відсутності заздалегідь розподіленого загального ключа. Однак, даний алгоритм накладає обмеження на канали зв'язку, що використовуються. Вонополягає в тому, що канали зв'язку повинні бути незалежні.

ВИСНОВКИ

1. Запропонована модель активного зловмисника для захищеної IP-телефонії, яка враховує можливість здійснення цим зловмисником атаки типу man-in-the-middle на протокол розподілу ключів. Це дає змогу розрахувати ймовірність успішної атаки, спрямованої на несанкціонований доступ до інформації.

2. Запропоновано оцінка імовірнісних часових характеристик протоколів розподілу захищених ключів IP-телефонії з урахуванням властивостей протоколу.

3. Запропонований алгоритм виявлення порушника протоколів розподілу ключів, який використовується при роботі за сценарієм клієнт-клієнт для кореспондентів, що не мають попередньо отриманого ключа. Алгоритм дозволяє з більшою ймовірністю встановити безпечне з'єднання між двома кореспондентами порівняно з існуючими алгоритмами, а також достовірно виявити присутність активного зловмисника в каналі зв'язку.

4. Запропоновано модифікацію протоколу ZRTP, яка реалізує запропонований алгоритм ідентифікації порушника. Модифікації порівняно з вихідним протоколом дозволяють ідентифікувати активного зловмисника, який здійснює атаку типу "людина посередині" на протокол розподілу ключів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. RFC 3550 (2003) A Transport Protocol for Real-Time Applications. [Електронний ресурс]. URL: http://www.ietf.org/rfc/rfc3550.txt.

2. RFC 3261(2002) - SIP: Session Initiation Protocol. [Електронний ресурс]. URL: http://www.ietf.org/rfc/rfc3261.txt.

3. Гольдштейн Б.С. IP-телефония. М.: Радио и связь. 2003. 336 с.

4. Гольдштейн, Б. С. Протокол SIP. М.: БХВ, 2005. 456 с.

5. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і безпека. 2011. № 4 (41). С. 107–112

6. Ковцур М.М., Молдовян А.А. Оцінка швидкісних характеристик реалізації атаки типу перебору пароля на IP-АТС при використанні FAIL2BAN. Матеріали конференції SPOISU. 2015. С. 171- 177

7. Рекомендації Y.1291 (05/2004) An architectural framework for support of Quality of Service in packet networks. [Електронний ресурс]. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=43!!PDF-E&type=items.

8. Гольдштейн А.Б. Softswitch. Спб.: БХВ. 2006. 368 с.

9. Росляков А.В. IP-телефонія. Дон.: Еко-тренд. 2003. 256 с.

10. Рекомендації ITU-T Y.1541 Network performance requirements for IP-based services. [Електронний ресурс]. URL: http://www.itu.int/ITU-T/recommendations/rec.

11. Рекомендації ITU-T G.114 One-way transmission time [Електронний ресурс]. URL: https://www.itu.int/rec/T-REC-G.114/en.

12. Comer, D. Internetworking With TCP/IP Vol I:Principles, Protocols, and Architecture. New Jersey: Pearson Education Inc. 2014. 698 p.

13. RFC 2676 (08/1999) – QoS Routing Mechanisms and OSPF Extensions [Електронний ресурс]. URL: http://tools.ietf.org/html/rfc2676.html.

14. Рекомендація ITU-T G.107 (02/2014) The E-model: a computational model for use in transmission planning. [Електронний ресурс]. URL:

http://www.itu.int/rec/T-REC-G.107].

15. Perlicki, K. Simple analysis of the impact of packet loss and delay on voice transmission quality. Journal of telecommunications and information technology. 2002. No. 2. P. 53-56

16. Gelenbe E. Cognitive Packet Networks: QoS and Performance. School of Electrical Engineering and Computer Science. University of Central Florida, Orlando, FL 32816. [Електронний ресурс]. URL: http://pdf.aminer.org/000/339/717/cognitive_routing_in_packet_networks.pdf.

17. Lijing Ding Performance Study of Objective Voice Quality Measures in VoIP. ISCC 2007. [Електронний ресурс]. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4381543&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4381543]

18. Крюков, Ю. С. Безопасность VolP-контента. Текущая ситуация, анализ угроз и тенденции рынка. Защита информации. INSIDE. 2008. №.3. С. 83-99

19. Ковцур, М. М. Протоколы обеспечения безопасности VoIP-телефонии. Защита информации. Инсайд. 2012. №3. С. 74-81.

20. RFC 3261(2002) SIP: Session Initiation Protocol. [Електронний ресурс]. URL: http://www.ietf.org/rfc/rfc3261.txt.

21. RFC 3711 (2004) – The Secure Real-time Transport Protocol (SRTP). [Електронний ресурс]. URL: http://www.ietf.org/rfc/rfc3711.txt.

22. Нікітін В.М., Лагутенко О.І., Ковцур М.М. Забезпечення інформаційної безпеки АТС. Електрозв'язок. 2014. No1. С. 29-31.

23. RFC 3830(08/2004) – MIKEY: Multimedia Internet KEYing. [Електронний ресурс]. URL: http://tools.ietf.org/html/rfc3830.

24. RFC 6309(08/2011) – IANA Rules for MIKEY (Multimedia Internet KEYing). [Електронний ресурс]. URL: http://tools.ietf.org/html/rfc6309.

25. RFC4568 (07/2006) – Session Description Protocol (SDP) Security Descriptions for Media Streams. [Електронний ресурс]. URL: http://tools.ietf.org/html/rfc4568 .

26. RFC 5764. Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP). [Електронний ресурс]. URL: http://tools.ietf.org/html/rfc5764.

27. RFC6189 (04/2011) – ZRTP: Media Path Key Agreement for Unicast Secure RTP. [Електронний ресурс]. URL: http://tools.ietf.org/html/rfc6189.

28. Демедюк С.В. Міжнародний досвід протидії кіберзлочинності. Вісник Харківського національного університету внутрішніх справ: збірник наукових праць. Харків. 2014. № 4 (67). С. 65–75

29. Черкасов Д. Основи технології VoIP та IP-телефонії. Національний Університет «Києво-Могилянська Академія». 2017.

30. Вараксін О.О. Кібербезпека мереж наступного покоління. Навчальний посібник. Одеса. 2013.

31. Чечуй О.В., Комін Д.С., Ревенко В.Д. Формалізована модель оцінки гарантій інформаційної безпеки в системах захищеної IP-телефонії. Збірник наукових праць Харківського національного університету повітряних сил. 2021. 3(69) С.134 – 137

32. Гайворонський М.В. Безпека інформаційно-комунікаційних систем. К.: Вид. группа BHB. 2009. 608 с

33. Нопин, С.В. Передача мультимедийных данных по цифровым каналам в режиме, защищенном от несанкционированого доступа. Дис. канд. техн. наук. ОГТУ. 2008. 233с.

34. Докучаєв В.А., Шведов А.В. Захист інформації в корпоративних VoIP-мережах. Електрозв'язок. 2012. No 4. С. 5–8.

35. Вдовиченко О.О. Методи забезпечення інформаційної безпеки. 2017. [Електронний ресурс]. URL: https://informatika.udpu.edu.ua/?page_id=3405.

36. Комін Д. С. Формалізована модель оцінки гарантій інформаційної безпеки комплексної системи захисту інформації. Системи озброєння і військова техніка. 2018. № 4(56). С. 92-99.

37. Потій А. В. Формальна модель процесу інформаційної безпеки. Радіоелектроніка та комп'ютерні системи. 2006. No 5(17). с. 128–133.

38. Radhika Ranjan Roy. Security Mechanisms in SIP. CRC Press, 2016. 121 p.

39. S. Sabine and oth. Exploiting IP telephony with silence suppression for hidden data transfers. Computers & Security. 2018. Vol. 79. P. 17–32.

40. Mourade Azroura, Yousef Farhaouia, Mohammed Ouanana, Azidine Guezzaz. SPIT Detection in Telephony over IP Using K-Means Algorithm. Procedia Computer Science. 2019. Vol. 148. P. 542–551.

41. Brent Sherman, Mike Borza, Brian Rosenberg, Charles Qi. Security Assurance Guidance for Third-Party IP. Journal of Hardware and Systems Security. 2017. Vol. 1. P. 38–55.

42. Philip R. Zimmermann. PGPfone Pretty Good Privacy Phone Owner's Manual, Version 1.0 [Електронний ресурс]. URL: http://ftp.pgpi.org/pub/pgp/pgpfone/manual/pgpfone10b7.pdf

43. Палагін В. В. Моделювання та аналіз роботи внутрішньої телефонної мережі на базі IP-станції з використанням протоколу SIP. Вісник Черкаського державного технологічного університету. 2020. № 2. С. 29–37. [Електронний ресурс]. URL: https://doi.org/10.24025/ 2306-4412.2.2020.198229.

44. Salnikova O. F., Sivoha I. M., Ivashchenko A. M. Strategic Communication in the Modern Hybrid Warfare. Journal of Scientific Papers "Social Development and Security". 2019. Vol. 9(5). P. 133–142. [Електронний ресурс]. URL: https://doi.org/10.33445/sds.2019 .

45. Potij A., Romin D., Rebriy I. A Method of Evaluating Assurance Requirements. Information & Security. Information & Security: An International Journal. 2012. Vol. 28. No. 1. P. 108–120. [Електронний ресурс]. URL: https://doi.org/10.11610/isij.2809.

46. Радько Н.М. Порівняльна оцінка імовірнісних і часових характеристик подолання захисту паролів. Інформація та безпека. 2007. Т. 10.

No 3. C. 439 - 444.

47. Головко О. О., Новіков В. П. Комплексна система захисту інформації на основі застосування Fuzzy-технологій. Інформаційна безпека України : зб. наук. доп. та тез науково-технічної конф. 12-13 бер. 2015 р. Київ : КНУ ім. Тараса Шевченка, 2015. 156 с.

48. ZRTP Protocol Library [Електронний ресурс]. URL: http://freecode.com/projects/libzrtpcpp.

49. Ковцур М.М. Оптимізація імовірнісних і часових характеристик криптографічного протоколу розподілу ключів IP-телефонії Університет: Технічні науки. 2014. No 2 (3). P. 1-9.

50. Кочій Н.М. Горопаха Н.М. Оцінка імовірнісно-часових характеристик виконання протоколів розподілу ключів. VIII Науково-практична конференція «Інтелектуальні системи та мережі» 5 грудня 2023р. Тернопіль. Україна. с. 82.

51. Березький О.М., Дубчак Л.О., Мельник Г.М. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня “Магістр”. Магістерська програма - Комп’ютерна інженерія". Тернопіль: ЗУНУ, 2022. 32 с.