УДК 004.056
DOI: 10.31673/2409-7292.2022.040003

Мацько О.Й., Гаврилюк І.Ю., Круогла А.В.

АНАЛІЗ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ПОКОЛІННЯ 5G

У статті досліджуються питання захисту в телекомунікаційних мережах нового покоління на основі технологій 5G. Розглянуто моделі безпечного розгортання мереж 5G, Захист абонентів та пристроїв, Захист мережі, Новий стек IT-протоколів, Технології захисту, які застосовуються у 5G. Показано Спадковість безпеки у поколіннях технологій, зроблено Порівняння захисту LTE з захистом 5G.

Ключові слова: мережа 5G, Захист мережі, технологія, безпека телекомунікацій.

Вступ

Технологія 5G – це наступне покоління телекомунікаційних мереж, яке почало виходити на ринок наприкінці 2018 року та продовжує розширюватися в усьому світі. Крім підвищення швидкості, очікується, що ця технологія розкриває величезну екосистему 5G IoT (Інтернет речей), де мережі можуть обслуговувати комунікаційні потреби для мільярдів підключених пристроїв із пошуком компромісу між швидкістю, затримкою та вартістю.

Технологія 5G керується 8 специфікаційними вимогами: швидкість передачі даних до 10 Гбіт/с, що означає 10-100-кратне підвищення швидкості в порівнянні з 4G і 4,5G; затримка до 1 мс; 1000-кратна пропускна здатність на одиницю площі; до 100-кратної кількості підключених пристроїв (порівняно з 4G LTE); доступність 99,999%; 100% покриття; 90% зниження споживання енергії в мережі; термін служби батареї до 10 років для малопотужних пристроїв IoT.

Щоб досягти цього, 5G застосовує багатомережеве розшарування та багаторівневі послуги з багатьма підключеннями. Щоб забезпечити необхідну гнучкість і економію масштабу, ці технології будуть надаватися через віртуальні та контейнерні середовища.

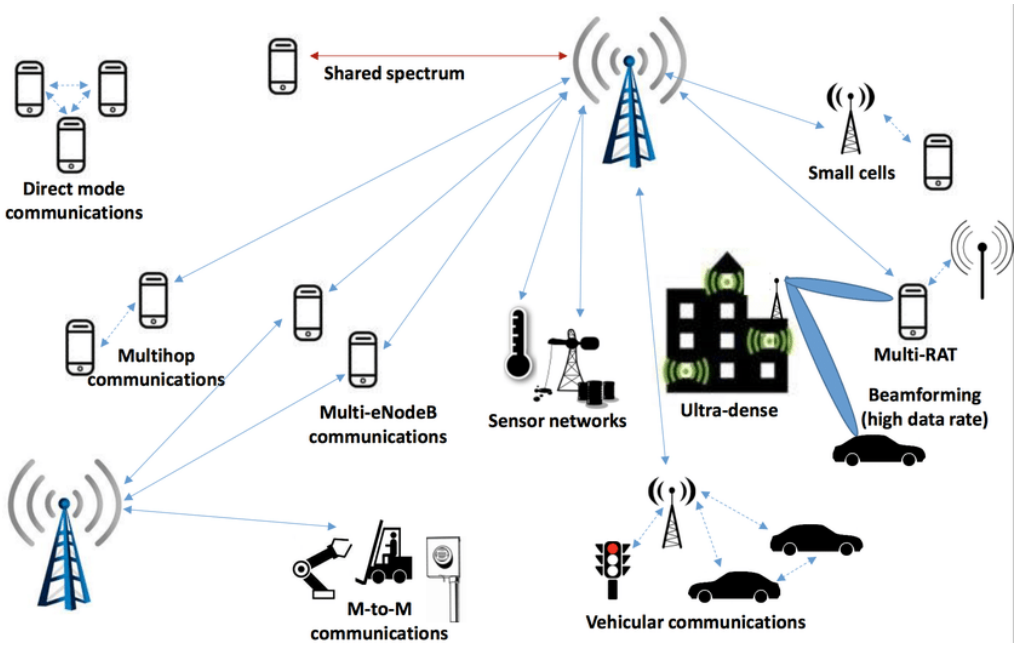

Рис. 1. Структура мережі за технологією 5G [1]

Для 5G розроблено засоби безпеки, щоб усунути загрози, з якими стикаються сучасні мережі 4G/3G/2G. Ці елементи включають нові можливості взаємної аутентифікації, покращений захист ідентичності абонента та додаткові механізми безпеки. 5G пропонує мобільній індустрії безпрецедентну можливість підвищити рівень безпеки мережі та послуг. 5G забезпечує профілактичні заходи для обмеження впливу відомих загроз, але

впровадження нових мережевих технологій створює нові потенційні загрози, з якими галузь має боротися.

Метою статті є розгляд основних заходів безпеки технології 5G, включаючи їх переваги та обмеження.

Моделі безпечного розгортання 5G. Стандарти 5G описують декілька моделей розгортання. Хоча в майбутньому планується запровадити щонайменше 5 додаткових опцій, єдиною опцією, яка зараз застосовується, є неавтономний (NSA) режим, точніше EN-DC. Базові станції 5G інтегруються з існуючою мережею 4G, яка працює в тандемі з базовими станціями LTE і підключається до ядра LTE, спираючись на заходи захисту, які забезпечує ядро LTE. Наступним етапом розгортання 5G, ймовірно, стане автономний режим (SA), точніше SA NR, який складається з нової радіомережі (NR), підключеної до базової мережі 5G (5GC). Перехід на ядро 5G дозволить реалізувати всі функції безпеки специфікацій 5G. Хоча визнається, що нові структури (власна хмара, архітектура на основі послуг) створять і нові проблеми безпеки (рис. 2).

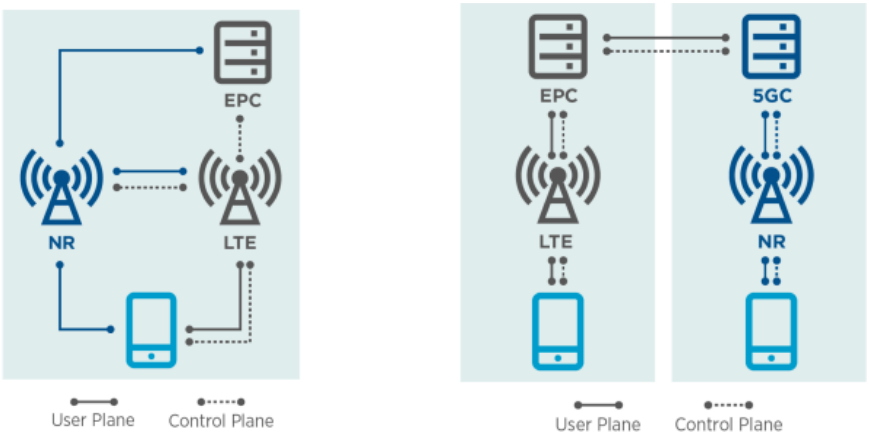

Рис. 2. Неавтономне (NSA) та автономне (SA) розгортання [2]

Захист абонентів та пристроїв. 5G покращує конфіденційність і цілісність даних користувачів і пристроїв на відміну від попередніх поколінь мобільних систем 5G:

захищає конфіденційність початкових повідомлень про відсутність доступу (NAS) між пристроєм і мережею. Як результат, більше неможливо відстежити обладнання користувача (UE) за допомогою поточних методів атак через радіоінтерфейс; захист від атак людини посередині (MITM) і фальшивих базових станцій (Stingray/IMSI catcher);

впроваджує механізм захисту, який називається домашнім контролем. Це означає, що остаточна автентифікація пристрою у відвіданій мережі завершується після того, як домашня мережа перевірить статус автентифікації пристрою в зовнішній мережі. Це вдосконалення запобігатиме різним типам шахрайства у роумінгу, які історично заважали операторам, і підтримуватиме вимогу оператора щодо правильної автентифікації пристроїв для послуг;

підтримує уніфіковану автентифікацію в інших типах мереж доступу, наприклад WLAN, що дозволяє мережам 5G керувати раніше некерованими та незахищеними з'єднаннями. Це включає в себе можливість виконання повторної автентифікації UE, коли вони переміщуються між різними мережами доступу або обслуговування;

запроваджено перевірку цілісності площини користувача, гарантуючи, що трафік користувача не змінюється під час транзиту;

покращує захист конфіденційності за допомогою пар відкритих/приватних ключів (ключів прив'язки), щоб приховати особу абонента та отримати ключі, які використовуються в усій архітектурі служби.

Захист мережі. Контроль цілісності даних. 5G представляє новий елемент мережевої архітектури: Security Edge Protection Proxy (SEPP). SEPP захищає периметр домашньої мережі, діючи як шлюз для з'єднань між домашньою та зовнішніми мережами (рис. 3).

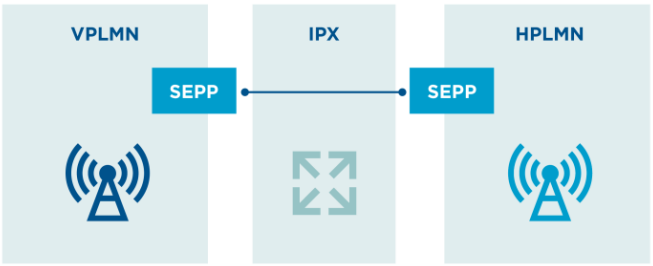

Рис. 3. Security Edge Protection Proxy [2]

SEPP призначений для:

забезпечення безпеки прикладного рівня та захисту від атак підслуховування;

забезпечення наскрізної автентифікації, захисту цілісності та конфіденційності за допомогою підписів і шифрування всіх повідомлень у роумінгу HTTP/2;

реалізації механізмів керування ключами для встановлення необхідних криптографічних ключів і виконання процедур узгодження можливостей безпеки;

фільтрації повідомлень і контроль, приховування топології та перевірку об'єктів JSON, включаючи міжрівневу перевірку інформації з адресною інформацією на рівні IP.

Крім того, для подолання існуючих ризиків безпеки, пов'язаних із використанням SS7 і Diameter, запроваджено посилений захист послуг міжнародного роумінгу. Це впровадження виділеного вузла безпеки в рамках стандартів 5G є суттєвим покращенням у порівнянні з існуючою практикою в мережах 4G/3G/2G з використанням SS7 і Diameter.

Новий стек IT-протоколів. Історично операторські мережі в основному використовували власні протоколи для керування мережею. 5GC переходить на стек протоколів на основі IP, що забезпечує взаємодію з більшою кількістю послуг і технологій у майбутньому. Наступні протоколи, схеми та процеси будуть прийняті в 5GC: HTTP/2 через N32, заміна Diameter на опорну точку S6a; TLS як додатковий рівень захисту, що забезпечує зашифрований зв'язок між усіма мережевими функціями (NF) у наземній мобільній мережі загального користування (PLMN); TCP як протокол транспортного рівня як заміна транспортного протоколу SCTP; RESTful framework з OpenAPI 3.0.0 як мовою визначення інтерфейсу (IDL).

Рис. 3. Порівняння протоколів безпеки в 4G та 5G [3]

Оскільки ці протоколи використовуються в ширшій IT-індустрії, їх використання, ймовірно, буде:

призводити до короткого терміну використання вразливості та більшого впливу вразливостей, розташованих у цих протоколах;

розширювати коло потенційних зловмисників. Основні мережі 4G і особливо 3G виграють від того, що зловмисники мають невеликий досвід роботи зі стандартами, які використовуються в них.

Схеми звітування про вразливості, такі як програма GSMA Coordinated Vulnerability Disclosure (CVD), повинні будуть керувати розширеним обсягом цих протоколів. Після локалізації час для виправлення відповідних вразливостей має бути коротким.

Технології захисту, які застосовуються у 5G

Віртуалізація. Архітектура мережі 5GC буде заснована на послугах, тобто операції з базовою мережею можуть виконуватися за допомогою функцій за межами мережі оператора, наприклад у хмарі. Це суттєвий перехід від усталених засобів контролю безпеки ядра мережі, однак надає оператору можливість використовувати технології віртуалізації. З цією можливістю з'являються нові вектори загроз, з якими потрібно боротися. Слід розглянути традиційні засоби керування віртуалізацією, включаючи ізоляцію орендарів і ресурсів. Відповідні засоби контролю ізоляції зменшують ризик витоку даних і вплив спалахів зловмисного програмного забезпечення з підтримкою віртуалізації. Уразливості на рівні мікропроцесора, наприклад Spectre і Meltdown підкреслили, що ізоляція оренди у віртуальному середовищі не гарантується, оскільки такі орендарі повинні розміщуватися разом відповідно до вимог безпеки, наприклад, не можна розміщувати орендарів нижчого рівня безпеки з орендарями високого рівня безпеки.

Контейнерізація – це технологія віртуалізації на рівні ОС, яка набуває популярності. ОС хоста обмежує доступ контейнера до фізичних ресурсів, таких як ЦП, сховище та пам'ять, тому один контейнер не може використовувати всі фізичні ресурси хоста. Таким чином, зменшується вплив атак доступності на платформу. Контейнери часто запускаються від імені root, тому можлива можливість вийти з контейнера та отримати доступ до базової файлової системи. Програмно-визначена мережа (SDN) надає операторам можливість віртуалізувати свої мережеві потоки, що призводить до спрощення апаратного забезпечення. Усі технології віртуалізації дозволяють сегментувати мережу та ізолювати ресурси, забезпечуючи безпеку та зменшуючи вплив успішних атак. Конфігурація цих служб повинна здійснюватися з безпечним дизайном, щоб гарантувати, що пропонований захист не буде зведено нанівець через погані процеси управління та оркестровки (MANO). Центральна система керування, часто гіпервізор, діє як мозок віртуалізованих технологій. Таким чином, захист цієї базової технології має бути високим. Має бути завершено моделювання конкретних загроз для атак і вразливостей у віртуалізації.

Хмарні служби. Базуючись на віртуалізованих службах, хмара є ключовим фактором 5G. Архітектура 5G була розроблена для хмари, оскільки забезпечує еластичність і масштабованість. Використання хмарних технологій може ускладнити ланцюг поставок і ланцюжок відповідальності. Відповідно до Mobile World Live, 5G дозволяє операторам надавати широкий спектр послуг через Cloud і Restful API. Необхідно дотримуватися методів безпечного кодування, щоб гарантувати, що дані не витікають, а код не можна використовувати для використання хмарної мережі постачальника або оператора.

Перерозподіл мережі. Перерозподіл мережі дозволяє оператору налаштовувати поведінку мережі, адаптуючи (розподіляючи) мережу для обслуговування конкретних випадків використання з використанням того самого апаратного забезпечення. GSMA визначив 35 атрибутів, які характеризують зріз мережі в постійному довідковому документі (PRD) NG.116. Модель безпеки для кожного фрагмента повинна бути адаптована до випадку використання. Можна передбачити різні рівні ізоляції, що охоплюють від одного вузла базової мережі до повністю виділеного радіодоступу. Кожен тип ізоляції повинен бути інтегрований на етапі проектування. Наприклад, фрагмент мережі для віддаленої операції повинен враховувати постійну взаємну ідентифікацію та авторизацію, щоб зупинити загрози MITM, але фрагмент для керування вмістом AR/VR не потребуватиме такого ж рівня безпеки.

Мобільний IoT. Незважаючи на те, що IoT вже переважає в мережах 2G/3G/4G, кількість підключень IoT має експоненціально зрости в 5G. Це не означає, що елементи керування безпекою мають суттєво змінитися, однак їх потрібно масштабувати. Інтернет речей має бути безпечно закодований, розгорнутий і керований протягом усього життєвого циклу. Більшість служб Інтернету речей мають спільну архітектуру, тому атаки, яким піддаватиметься кожна служба, ймовірно, підпадають під три поширені сценарії атак: атаки на пристрої (кінцеві точки) через програми, запущені на пристрої, віддалені атаки з

Інтернету та через фізичну атаку; атаки на сервісні платформи (наприклад, хмара); атаки на канали зв'язку (наприклад, стільниковий зв'язок, WLAN, повітряний інтерфейс BLE тощо).

Пристрої IoT дедалі частіше використовують для запуску DDoS-атак, оскільки кожен пристрій створює певну форму даних, що, зважаючи на кількість пристроїв, призводить до значних атак на основі обсягу трафіку.

eSIM. eSIM усуває потребу в змінній SIM-картці на мобільному пристрої, а дані на цій картці готуються на платформі віддаленої підтримки SIM-картки (SM-DP+), а потім завантажуються у формі профілю eSIM через HTTPS у безпечний елемент. (eUICC), постійно вбудований у мобільний пристрій. Цей eUICC, ідентифікований глобально унікальним EID, може зберігати багато профілів, і коли профіль увімкнено, дані в цьому профілі використовуються для ідентифікації та автентифікації абонента в мобільній мережі так само, як знімна SIM-карта. Система використовує сертифікати інфраструктури відкритих ключів (PKI), що дозволяє SM-DP+ і eUICC взаємно автентифікувати один одного. Усі ключі генеруються за допомогою Perfect Forward Secrecy (PFS). Управління профілями eSIM в eUICC здійснюється Кінцевим користувачем у варіанті споживчого використання або віддаленою платформою надання SIM-карти у випадку використання M2M/IoT.

Штучний інтелект (AI). Хоча це загальний термін для багатьох технологій, очікується, що штучний інтелект буде широко використовуватися в мережах 5G і повинен сприяти безпеці. Оператори повинні використовувати машинне навчання (ML) і глибоке навчання (DL) для автоматизації виявлення загроз і шахрайства. Використання штучного інтелекту є особливо актуальним з огляду на обсяги даних, які генеруватимуть мережі 5G. ШІ може бути більш здійсненним способом пом'якшити попередні невідомі атаки в режимі реального часу. Штучний інтелект також може використовуватися для живлення мереж самовідновлення, де система здатна виявляти проблеми та вживати автоматизованих дій для доставки виправлення. Однак ця технологія також доступна для зловмисника, і очікуються атаки, керовані ШІ.

Спадковість безпеки у поколіннях технологій. 5G – це можливість для мобільної індустрії підвищити безпеку мережі та послуг. Нові можливості автентифікації, покращений захист ідентичності абонента та додаткові механізми безпеки призведуть до значних покращень безпеки порівняно зі старими поколіннями. Досвід показує, що мережі 2G/3G використовують незахищені, некеровані протоколи та регулярно піддаються шахрайству та загрозам. Багато з цих атак вдалося пом'якшити за допомогою 4G і 5G. Однак через зворотну сумісність 4G з 3G/2G вони не зникнуть, доки не буде припинено використання застарілої технології. Визначаючи розгортання 5G, операторам доведеться враховувати, як ці застарілі мережі вплинуть на них з часом, розглядаючи те, як можна запобігти нападам, якщо успадковані покоління ізольовано або видалено з екосистеми (рис. 4).

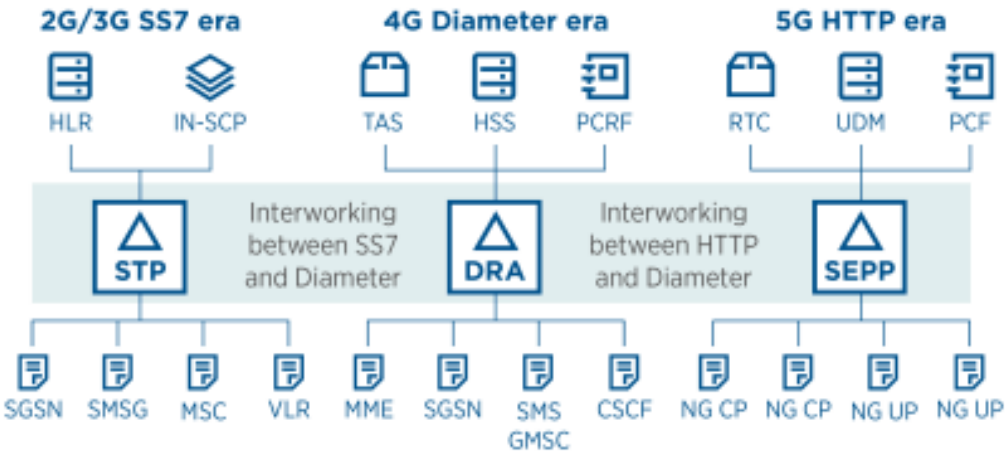

Рис. 4. Спадковість технологій захисту між поколіннями технологій зв'язку [4]

Таблиця 1

Порівняння захисту LTE з захистом 5G

Функція	LTE	5G
Шифр конфіденційності та цілісності	Шифрування на радіоканалі між мобільною станцією та eNodeB (базова станція LTE)	На додаток до LTE
Угода про ключ автентифікації (AKA)	Шифрування площини управління та цілісність між UE та Mobility Management Entity (MME)	Поточна підтримка 256-розрядних алгоритмів, запропонована для майбутнього випуску
Функція кріплення безпеки (SEAF) або ключ кріплення	Підтримуються 128-розрядні алгоритми	Реалізовано цілісність, що запобігає несанкціонованій зміні даних користувача.
Постійний ідентифікатор абонента (SUPI)	Спільний ключ, наданий в UICC і AUSF (серверна функція автентифікації) у мережі.	Прихований ідентифікатор підписки (SUCI) забезпечує механізм використання відкритого ключа домашньої мережі для шифрування частини MSIN ідентифікатора абонента (IMSI). Захист конфіденційності початкових повідомлень про відсутність доступу (NAS) між пристроєм і мережею.
Домашній контроль	Немає	HPMN може підтвердити, що UE присутній і запитує послугу від VPMN – корисно в сценаріях роумінгу та запобігання шахрайству.
Функція мережевої експозиції (NEF)	Немає	Мережеві функції безпечно передають можливості та події стороннім додатковим функціям (AF) через NEF.
Захист проксі-сервера Security Edge	Немає	Забезпечує безпечне надання інформації в мережі 3GPP за допомогою автентифікованих і авторизованих функцій програми.

Висновок

Мета технологій 5G полягає в тому, щоб відкрити мережу для більш широкого набору послуг і дозволити мобільним операторам підтримувати ці послуги. Це можливість захистити послуги та споживачів від багатьох сучасних загроз. 5G поставляється з багатьма вбудованими елементами керування безпекою, розробленими для покращення захисту як окремих споживачів, так і мобільних мереж; це ефективніше, ніж доповнення або додаткові компоненти після розгортання.

Разом з тим, удосконалення технологій і використання нових архітектур і функцій, таких як розподіл мережі, віртуалізація та хмара, створять нові загрози, які вимагають впровадження нових типів контролю.

Перелік посилань

1. Eniola Elizabeth Fase. 5G network. https://techthoroughfare.com/technology/5g-network/
2. Key Elements for 5G Networks. https://www.sdxcentral.com/5g/definitions/key-elements-5g-network/
3. Securing the 5G Era. Security. https://www.gsma.com/security/securing-the-5g-era/
4. William Malik. Private Network 5G Security Risks & Vulnerabilities. https://www.trendmicro.com/en_us/research/22/f/5g-security-risks-vulnerabilities.html

Надійшла: 28.10.2022 Рецензент: д.т.н., професор Гайдур Г.І.