УДК 621.396.42
DOI https://doi.org/10.32782/2663-5941/2024.6.1/17

Гарист А.В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

ІСТОРІЯ РОЗВИТКУ СТІЛЬНИКОВИХ МЕРЕЖ ЗВ'ЯЗКУ

Стільникова мережа дозволяє сучасним мобільним пристроям не тільки телефонувати, а й відправляти повідомлення та підключатися до всесвітньої мережі Інтернет. Ще не так давно світовій телекомунікаційній галузі були відомі чотири покоління мереж: 1G, 2G, 3G та 4G (LTE). Однак наразі світова телекомунікаційна галузь активно впроваджує технологію 5G. Це найновіший стандарт, розроблений для широкосмугового бездротового цифрового зв'язку.

У статті розглянуто історію розвитку стільникових мереж, як за 40 років змінилося чотири покоління мереж мобільного зв'язку. Якщо мережі першого покоління 1G давно зникли, то мережі 2G, 3G і 4G досі продовжують експлуатуватися. Більше того, кілька успадкованих інфраструктур мереж 3G і 4G органічно увійде до складу мобільних мереж п'ятого покоління 5G.

У статті з'ясовано чим відрізняється технологія 5G від попередніх поколінь, як вона працює, які має переваги та з якими труднощами доводиться стикатися під час її впровадження.

В статті визначено, що попит на доступ до Інтернету у поєднанні з появою нових технологій, таких як штучний інтелект, Інтернет речей (IoT) та автоматизація забезпечує значне збільшення кількості даних, які зростають по експоненті. Сучасна мобільна інфраструктура не призначалася для такого інформаційного навантаження та потребує оновлення.

У статті розкрито, що завдяки високій швидкості, великій пропускній здатності та низькій затримці, технологія 5G може допомогти в підтримці та масштабуванні деяких додатків, наприклад у контролі трафіку підключення до хмарного сховища, доставки за допомогою дронів, використання відеочатів та забезпечення якості потокових ігор. Способи застосування технології 5G не обмежені: вона охоплює сфери від платежів по всьому світу та реагування на екстрені ситуації до дистанційного навчання.

Ключові слова: *стільникова мережа, автентифікація, абонент, комутатор, ідентифікатор, шифрування, базова станція.*

Постановка проблеми. Стільникові мережі зв'язку є однією з основних складових сучасної телекомунікаційної інфраструктури, що забезпечує мобільну комунікацію для мільярдів користувачів у всьому світі. Історія їх розвитку від початкових експериментальних етапів до глобальних високошвидкісних мереж сьогодні є прикладом вражаючого технологічного прогресу та інновацій. Разом із тим, розвиток стільникових мереж супроводжувався численними технічними, соціальними та економічними викликами, які потребували значних зусиль для подолання.

Основна проблема, яку порушує ця стаття, полягає в необхідності комплексного аналізу історії розвитку стільникових мереж, зокрема технічні труднощі, соціальні та економічні наслідки, проблеми приватності та безпеки, а також енергетичні та екологічні проблеми.

Аналіз останніх досліджень і публікацій. Дослідження та публікацій з історії розвитку стільникових мереж зв'язку дозволяють окреслити ключові моменти еволюції цієї технології, а також розглянути новітні дослідження та тенденції, які визначають напрямок розвитку телекомунікаційної інфраструктури.

Серед провідних фахівців у галузі бездротових комунікацій та мобільних мереж можна виділити Андреу Голдсмит [1], яка зробила великий внесок у розвиток теорії мобільних мереж та мультиантенних систем (MIMO), а також у питаннях управління частотами для мереж 4G і 5G, Теодора Раппапорта [2], який одним із перших, хто почав досліджувати питання використання міліметрових хвиль в стільникових мережах нового покоління (5G) та багато інших.

У той же час, незважаючи на значну кількість наукових публікацій, наукові роботи провідних науковців продовжують формувати теоретичні та практичні аспекти сучасних комунікаційних систем.

Постановка завдання. Метою даної статті є дослідження етапів розвитку стільникових мереж зв'язку, починаючи з перших технологій мобільного зв'язку до сучасних та майбутніх інновацій, таких як 5G і 6G. Окрему увагу приділити технологічним, соціальним та економічним змінам, що виникли в результаті розвитку цих мереж,

а також їх впливу на глобальні комунікаційні системи, бізнес та повсякденне життя користувачів.

Виклад основного матеріалу. Перше покоління зв'язку 1G почало розгортатися у 1979 році в Японії. Це був аналоговий низькочастотний сигнал, який був схильний до перешкод і спотворень, тому якість звуку була досить низькою. Було невелике покриття без роумінгу між операторами і тим більше між країнами, тому що в різних країнах були свої стандарти зв'язку. 1G було першим поколінням бездротового зв'язку, в першу чергу, орієнтованим на голосові послуги. Воно працювало на аналогових сигналах, які мали обмеження щодо якості та безпеки. Проте свого часу воно було революційним.

Концепція архітектури мереж залишається незмінною до п'ятого покоління. Розглянемо, які основні компоненти є в мобільних мережах. При здійсненні дзвінка сигнал надходить з мобільного пристрою на базову станцію. Базова станція, перенаправляє сигнал у ядро мережі, яке у першому поколінні називалось Mobile telephone switching office (комутатор мобільного зв'язку). Вона виконувала досить примітивну функцію, а саме комутувала сигнал або на іншу базову станцію, або на телефонні стаціонарні проводові лінії зв'зку.

Розглянемо основні проблеми першого покоління:

– відсутність захисту даних. Мережа не мала шифрування, тобто зловмисник із примітивним перехоплювачем радіоефіру міг почути розмови абонентів на певній частоті. Канал між базовою станцією та мережею оператора також не був захищений, зловмисник міг туди спокійно втрутитись та перехопити сигнал;

– відсутність автентифікації у мережі. Зловмисник міг використовувати ідентифікаційні номери абонента та отримати доступ до послуг оператора мобільного зв'язку. З доступом він міг зробити цільову атаку – телефонувати іншим абонентам з шахрайською метою;

– доступність. Технологія, з допомогою якої виділялися канали абонентів, була примітивна. Весь частотний діапазон поділявся на невеликі піддіапазони, які виділялись абонентам. Цих піддіапазонів була зовсім невелика кількість, і зловмисник, надсилаючи запити на відкриття каналу, міг перевантажити базову станцію так, що офіційним абонентам надати послуги зв'язку вона вже не могла.

На початку 90-х років користувачів мережі 1G було вже близько 20 мільйонів, що обіцяло великий комерційний успіх. Оператори зв'язку почали покращувати технології мобільних мереж. Так виникли мережі другого покоління 2G. Вони почали розгортатися в 1991 році у Фінляндії. Другим поколінням вважаються стандарти GSM/GPRS та EDGE, це вже цифровий зв'язок. З'явились SMS, MMS, а разом із GPRS-стандартом з'явився доступ до мережі Інтернет.

Розглянемо, як змінилась архітектура мережі. По-перше, з'явився контролер базових станцій, який виділяв канали під користувачів та виконував Handover. Handover – це процес передачі обслуговування абонента від однієї базової станції до іншої під час виклику або сеансу передачі даних, наприклад, під час руху абонента.

Потім з'явився Mobile Switching Center (центр комутації мобільного зв'язку). Цей комутатор переправляє сигнали до зовнішніх мереж комутації даних: іншим операторам або на телефонні стаціонарні проводові лінії зв'зку.

Також додали компонент Authentication Center (центр автентифікації). З назви зрозуміло, що у мережі GSM з'явилася автентифікація. Вона ґрунтувалася на тому, що оператор у своєму центрі прописував ідентифікатор абонента та пов'язаний із ним закритий ключ. Ці дані, записувалися на SIM-картки (Subscriber Identification Module – модуль ідентифікації абонента), які також з'явилися у другому поколінні зв'язку.

Незважаючи на велику турботу про безпеку в мережах другого покоління, ризики залишалися. Наприклад, після автентифікації в мережі оператора абонент генерував ключ шифрування за алгоритмом A8, який потім використовувався для шифрування даних в радіоканалі за допомогою алгоритму A5. Проблемою стало те, що шифрування було обмежене лише базовою станцією. Все, що йшло далі від базової станції до мережі оператора, не шифрувалося. Зловмисник все ще міг втрутитися в канал і перехопити всі дані, що передаються.

До початку 2004 року пристроїв, які використовують мережу другого покоління, було більше одного мільярда. Це дало ще один поштовх розвитку мереж мобільного зв'язку. Було створено консорціум 3GPP (3rd Generation Partnership Project) для стандартизації зв'язку мереж третього покоління, які почали розгортатися на початку XXI сторіччя.

Головним принципом у проектуванні мережі третього покоління стала зворотна сумісність з 2G, таким чином опорна мережа була повністю заснована на мережі 2G з деякими покращеннями. У мережі радіодоступу для виділення раді-

оканалів для абонентів почали використовувати технологію Code-Division Multiple Access (множинний доступ із кодовим поділом), яка дозволила мінімізувати атаки на доступність базової станції. При кодовому розділенні зникло обмеження кількості каналів, але виникла інша проблема – зі збільшенням числа абонентів зростала ймовірність помилки декодування. Це призводило до погіршення зв'язку, але не біло відмови в обслуговуванні.

Архітектура мережі мало змінилася. Ще у другому поколінні з'явилася мережа GPRS, яка надала доступ абонентів до інтернету. Лише у підмережі радіодоступу змінилися назви компонентів та її функціональність. Завдяки цьому 3G-мережі змогли надати вищу швидкість підключення абонентів та якісніші послуги зв'язку.

Усі впроваджені концепції безпеки залишаються актуальними й у наступних поколіннях зв'язку, але допрацьовуються і поліпшуються. Так, в алгоритмі автентифікації відбулося доповнення, абонентський пристрій також автентифікував мережу оператора, тобто з'явилась двостороння автентифікація. Автентифікаційний центр вже не за допомогою алгоритмів A3, A5, A8, а за допомогою інших способів шифрування генерував автентифікаційний вектор і направляв його мобільному пристрою. Пристрій, у свою чергу, за допомогою криптофункцій генерував очікуваний автентифікаційний код і порівнював його з кодом, який надійшов від автентифікаційного центру. Якщо код не збігається, то мережа не знає закритий ключ, можливо зловмисник намагається провести атаку Fake BTS. Якщо коди збігаються, мережа знає закритий ключ, і їй можна довіряти.

Шифрування та захист цілісності забезпечувалися алгоритмом KASUMI, який згодом виявився не достатньо «криптостійким». Йому на заміну прийшов алгоритм SNOW3G, який досі використовується в мережах LTE. Внутрішні атаки залишалися актуальними, тому що всередині мережі оператора, на каналах між контролером радіомережі та іншими компонентами захисту не було.

Також консорціум запропонував використовувати IPsec на з'єднанні між GPRS із мережею оператора та зовнішніми інтернет-провайдерами для забезпечення взаємної автентифікації та шифрування даних, але остаточне рішення про використання IPsec залишалося на операторі. IPsec – це набір протоколів для забезпечення захисту даних, що передаються міжмережевим протоколом IP. Він дозволяє здійснювати підтвердження автентичності, перевірку цілісності та/або шифрування IP-пакетів. IPsec також включає протоколи для захищеного обміну ключами в мережі Інтернет. Однак підключення до мереж комутації даних інших операторів продовжувало ґрунтуватися на SS7-протоколах, тому загрози, пов'язані з SS7-мережами, залишилися актуальними і в 3G.

Мережі четвертого покоління почали розгортатися наприкінці 2000-х років. Сьогодні LTE – найпопулярніший стандарт зв'язку. Він повністю побудований на IP-мережах. В них інформація відправляється на інші мережі за допомогою технології Voice-over-LTE. VoLTE має втричі більше голосову ємність та ємність даних, ніж мережі 3G і до шести разів більше, ніж мережі 2G. Протокол SS7 нарешті замінили на протокол Diameter, який забезпечує захист даних у мережі.

Архітектура мережі досить сильно змінилася. З'явився канал між базовими станціями, а також між базовою станцією та мережею оператора. Виключили контролер базових станцій – його функціональність розподілилася між базовою станцією та опорною мережею. Залишився лише один вихід до зовнішніх мереж, тому що тепер вони засновані тільки на IP-пакетах. Так як 4G мережі засновані на пакетній передачі даних, комутаційні канали до інших операторів замінили IP-канали, що дозволило організувати один вихід до всіх зовнішніх мереж.

Відбулися й зміни захисту даних. Тепер між мережею оператора та мобільним пристроєм генерується цілих п'ять ключів: два – для захисту контрольних даних від мережі оператора, два – для захисту контрольних даних від базової станції та один – для шифрування даних між мобільним пристроєм та базовою станцією.

Алгоритми захисту в 4G – SNOW3G, AES та ZUC. Криптоалгоритм AES є світовим стандартом симетричного шифрування та широко використовується для вирішення практичних завдань захисту даних. Його використання підвищило безпеку мобільних мереж четвертого покоління, і зараз це найпоширеніший алгоритм захисту та шифрування трафіку в мобільних мережах.

Також використовується протокол IPsec на з'єднанні між базовими станціями та базовою станцією з мережею оператора для взаємної автентифікації та захисту даних. 3GPP запропонували вимоги для захисту базової станції, так званого захищеного середовища базової станції. Але ці вимоги описані досить загально, і тому реалізація залишається на плечах мобільного оператора, що може додавати певні ризики, вразливості у реалізації кожного їх.

Незважаючи на рівень безпеки, що значно зріс, зловмисники знайшли спосіб експлуатувати вразливості мереж старих поколінь – через даунгрейд. Принцип атаки полягає в тому, що пристрій постійно відправляє на базову станцію measurement reports – звіти про те, яку якість зв'язку вона отримує зараз. Зловмисник може від імені жертви надіслати повідомлення про поганий зв'язок. В такому випадку базова станція автоматично перепідключає абонента до мережі нижчого покоління. Тепер зловмисник може використати вразливість цього покоління для атаки на абонента.

Атаку через даунгрейд важко реалізувати, оскільки вона орієнтована на певного абонента. Вибір жертви – лише початок атаки. Далі потрібно реалізувати загрози того покоління, на яке переключився абонент, при тому, що багато загроз оператори вже можуть контролювати. У зв'зку з цим даунгрейд – це рідкісна та непроста атака.

Мережі п'ятого покоління почали розгортати на початку 2010-х років. Вони засновані на мікросервісній архітектурі, віртуалізації та створені для розгортання у хмарній інфраструктурі.

Ядро мережі змінилося. Кожна функція мережі виконує певну функцію. Наприклад, AMF (Action Message Format – формат обміну даними) управляє функціями доступу абонентів до мережі та їх мобільності, при цьому делегуючи функції керування сеансами користувачів та потоками даних у мережі компоненту SMF (Service Management Facility), функції дотримання мережевих політик та угод про рівень обслуговування – PCF (Policy Control Function), а автентифікацію абонентів покладено на компонент AUSF (Authentication Server Function).

Базову станцію за специфікацією OpenRAN розділили на три складові:

– Radio Unit, який приймає сигнал від мобільних пристроїв,

– Distributed Unit (DU), основний процесорний блок, який обробляє дані у стеку протоколів,

– Central Unit (CU), який керує потоком даних у мережі та визначає, як пакети проходитимуть через інфраструктуру.

Розглянемо найбільш помітні відмінності від 4G-мережі:

Вищі швидкості. 5G забезпечує пікову швидкість передачі даних до 100 разів вище, ніж 4G, що дозволяє транслювати відео надвисокої чіткості та швидше завантажувати файли. Однак для досягнення цих швидкостей потрібні правильні умови (відсутність перешкод). Під час перших тестів Vodafone в Україні було досягнуто пропускну спроможність прийому даних 1508 Мбіт/с, що в 3 рази більше теоретичного максимуму 4G і до 5 разів швидше за його практичні показники.

Низька затримка. Мережі 5G мають значно меншу затримку, скорочуючи затримку передачі майже до реального часу, що має вирішальне значення для таких додатків, як автономні транспортні засоби і віртуальна реальність. Але для цього потрібна велика інфраструктура.

Збільшення пропускної здатності. Завдяки покращеному мобільному широкосмуговому зв'язку 5G підтримує більше пристроїв у заданій області, пристосовуючись до зростаючої кількості підключених пристроїв у розумних містах та будинках. Однак це також залежить від пропускної спроможності мережі.

Розділення мережі. 5G дозволяє створювати приватні мережі з індивідуальними послугами, оптимізуючи пропускну спроможність мережі для конкретних випадків використання, наприклад для аварійно-рятувальних служб або промислової автоматизації.

Хоча мережі 5G пропонують безліч переваг, вони також мають численні проблеми. Розглянемо основні з них:

– деякі люди висловили стурбованість щодо потенційного впливу випромінювання 5G на здоров'я, особливо при використанні високочастотних діапазонів. Хоча дослідження не знайшли переконливих доказів шкоди, необхідні постійні дослідження, щоб гарантувати безпеку мереж 5G. Однак суспільне сприйняття, як і раніше, залишається проблемою;

– розгортання мереж 5G вимагає значних інвестицій в інфраструктуру, що може виснажити бюджети операторів мобільного зв'язку та призвести до вищих витрат споживачів. Крім того, перехід на 5G може порушити роботу галузей, які покладаються на старі технології, що призведе до втрати робочих місць та економічних проблем. Однак зрештою очікується, що довгострокові вигоди переважать ці короткострокові наслідки;

– розширення можливостей підключення та збору даних, що забезпечується 5G, може призвести до проблем конфіденційності, особливо якщо персональні дані не захищені належним чином. Використання 5G у розумних містах та додатках IoT потребуватиме надійних заходів захисту конфіденційності для запобігання неправомірному використанню даних. Однак забезпечення дотримання цих заходів захисту буде складним завданням;

– щоб повною мірою скористатися перевагами 5G для бізнесу, багатьом підприємствам потрібно буде повністю переоснастити свою телекомунікаційну інфраструктуру. Це включає закупівлю нового обладнання, модернізацію технологічних процесів, відкриття нових ліцензій, поповнення команди галузевими фахівцями, надання послуг;

– оскільки специфікація 5G вимагає вищих частот, мережа має обмежений радіус дії. Дерева та високі будівлі перешкоджають поширенню хвиль, тому для досягнення великого покриття потрібно більше вишок стільникового зв'язку. Для збільшення пропускної здатності та покращення сигналу необхідно встановити датчики та додаткові антени на будівлях та вуличних об'єктах;

– при підключенні до 5G акумулятор будь-якого пристрою зношується швидше. Чим потужніша мережа, тим сильніше вона впливає на акумулятор і послаблює пристрій. Оскільки дослідження та розробки в області 5G продовжуються, виробники також шукають нові способи підвищення продуктивності багаторазових джерел живлення.

Висновки. Останні публікації з історії розвитку стільникових мереж зв'язку свідчать про швидкий прогрес у галузі, що охоплює нові технології, підвищену безпеку, зростаючі вимоги до якості послуг і здатність мереж підтримувати мільярди пристроїв в рамках Інтернету речей. Стільникові технології продовжують змінювати наше життя, забезпечуючи нові можливості в комунікаціях, бізнесі та повсякденному житті, одночасно ставлячи нові виклики щодо енергозбереження, безпеки та приватності користувачів. Історія розвитку стільникових мереж є не лише історією технологічних інновацій, але й свідченням їхнього глибокого впливу на соціальну та економічну структуру суспільства. Розуміння цих процесів є важливим для прогнозування майбутніх тенденцій та подальшого вдосконалення мобільних технологій.

Список літератури:

1. Andrea Goldsmith «Wireless Communications», Cambridge University Press, 2005, 644 p.

2. Theodore S. Rappaport «Wireless Communications: Principles And Practice», Pearson Education, 2010, 709 p.

3. David Tse, Pramod Viswanath «Fundamentals of wireless communication», Cambridge University Press, 2005, 564 p.

4. Ke-Lin Du, M. N. S. Swamy «Wireless Communication Systems. From RF Subsystems to 4G Enabling Technologies», Cambridge University Press, 2010, 985 p.

Haryst A.V. HISTORY OF THE DEVELOPMENT OF CELLULAR COMMUNICATION NETWORKS

The cellular network allows modern mobile devices not only to make calls, but also to send messages and connect to the worldwide Internet. Not so long ago, four generations of networks were known to the global telecommunications industry: 1G, 2G, 3G and 4G (LTE). However, the global telecommunications industry is currently actively implementing 5G technology. It is the latest standard developed for broadband wireless digital communications.

The article examines the history of the development of cellular networks, how four generations of mobile communication networks have changed over 40 years. If the networks of the first generation 1G disappeared long ago, then the 2G, 3G and 4G networks are still in use. Moreover, several legacy infrastructures of 3G and 4G networks will organically become part of the fifth generation 5G mobile networks.

The article explains how 5G technology differs from previous generations, how it works, what advantages it has, and what difficulties you have to face during its implementation.

The paper identifies that the demand for Internet access combined with the emergence of new technologies such as artificial intelligence, the Internet of Things (IoT) and automation is driving a significant increase in the amount of data that is growing exponentially. Modern mobile infrastructure was not designed for such an information load and needs to be updated.

The paper reveals that with its high speed, high bandwidth and low latency, 5G technology can help support and scale some applications, such as traffic control of cloud storage connections, drone delivery, video chat and game streaming. The applications of 5G technology are limitless, ranging from global payments and emergency response to distance learning.

Key words: *cellular network, authentication, subscriber, switch, identifier, encryption, base station.*