ВСТУП

Враховуючи поширеність і популярність бездротових мереж як серед звичайних користувачів так і потенційних зловмисників безумовно зростають потреби у захисті бездротових технологій.

Доступність, простота розгортання, доволі легке налаштування і можливість підключити велику кількість пристроїв пояснюють популярність бездротових мереж, але не зважаючи на велику кількість переваг бездротових мереж можна стверджувати, що якщо мережа не захищена, то переваги не матимуть сенсу. Саме тому важливим є розуміння роботи мережі та розуміння необхідності захисту бездротових мереж за допомогою сучасних методів і технологій.

Незважаючи на те, що в сучасних бездротових мережах для забезпечення захисту використовуються складні математичні алгоритми аутентифікації, шифрування інформації та контролю цілісності передавання даних, все ще існує можливість отримання несанкціонованого доступу до окремих корпоративних мереж. У деяких випадках для цього не потрібно застосовувати спеціалізоване обладнання чи програмне забезпечення — достатньо лише перебувати в зоні покриття мережі. Отже, зазначені вище положення свідчать про потребу вдосконалення та створення нових методів захисту інформації під час її передавання в розподілених бездротових мережах за умов протидії навмисним атакам.

Бездротові мережі стали невід’ємною частиною повсякдення як домашніх так корпоративних користувачів надавши свободу пересування під час роботи чи дозвілля. Одними з них є мережі стандарту IEEE 802.11 (Wi-Fi) мережі, не знайдеться жодного мобільного пристрою, який би не був оснащений модулем Wi-Fi. У випадку передавання даних по радіоканалу, ще не винайдено нічого кращого за радіусом дії і швидкості передачі ніж Wi-Fi та у випадку даної технології платити доводиться безпекою. Безпека є надважливим аспектом організації обміну інформації будь-якого підприємства. Якщо доступ до дротових мереж можна отримати лише фізично підключившись до порта комутатора чи до

мережевої розетки, то підключення до бездротової мережі є набагато простішим, необхідно бути лише у зоні її покриття. Бездротові мережі використовують радіохвилі, які розповсюджуються за законами фізики, і контролювати їх поведінку є не тривіальною задачею. Поряд із перевагами, які надають мережі Wi-Fi стоять і виклики пов'язані із інформаційною безпекою. За наявності вузько-направленої антени високої потужності, зловмисник може вторгнутись у бездротову мережу на відстанях 2 км і більше, таким чином ускладнюється задача визначення його місцезнаходження.

Мета роботи – розробка системи адаптивного захисту бездротових мереж на базі технології Wi-Fi з використанням штучного інтелекту та аналізу поведінки.

Об'єкт дослідження – технології та методи захисту бездротової мережі.

Предметом дослідження – методи захисту інформації в бездротовому середовищі.

Завдання, які необхідно вирішити для досягнення поставленої мети:

- проаналізувати особливості бездротового середовища;
- виявити проблематику захисту інформації та вразливості бездротового середовища;
- дослідити існуючі методи захисту інформації при роботі в бездротовому середовищі;
- розробити програмне забезпечення, що дозволить робити моніторинг бездротової мережі та виявляти підозрілий трафік.

Методи дослідження дипломної роботи:

- аналіз технічної літератури;
- аналіз існуючих стандартів бездротових мереж;
- аналіз вразливостей бездротових мереж;
- порівняння методів і технологій захисту бездротових мереж.

1 АНАЛІЗ БЕЗДРОТОВИХ МЕРЕЖ ТА ЇХ ВРАЗЛИВОСТЕЙ

1.1 Сучасні бездротові мережі

У сучасному світі великого поширення набули безпровідні мережі. Вони набули такого поширення, що охоплюють майже всю поверхню землі. Локальні мережі, персональні мережі, глобальні мережі – всі вони являються частиною нашого життя. Тому питання розуміння безпеки у бездротових мережах є дуже важливим для їх користувачів.

Для того щоб поглибитись у питання аналізу і безпеки бездротових мереж спочатку треба розуміти що собою представляє бездротова мережа і як вона працює.

Бездротову мережу можна схарактеризувати як комп'ютерну мережу, яка використовує для підключення до мережевих вузлів і передачі даних бездротове з'єднання.

Бездротові мережі бувають різними. Їх можна поділити за технологіями, за дальністю дії, рис.1.1 та за середовищами в яких вони передаються.

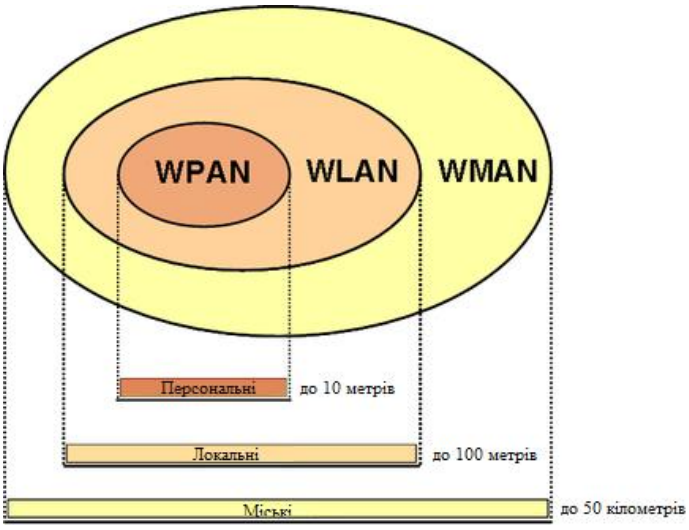


Рис. 1.1 Розділ безпровідних мереж за областю дії

До середовищ передавання даних і технологій, що застосовуються в бездротових мережах, належать радіорелейні комплекси, системи лазерного зв’язку, інфрачервоні технології, мережі з використанням низькоорбітальних супутникових систем, а також рішення на основі радіомодемів і стільникових модемів [1].

Залежно від радіусу покриття бездротові мережі поділяються на кілька груп, показано у табл. 1.1:

- Персональні бездротові мережі (WPAN — Wireless Personal Area Networks), до яких належать, зокрема, технології Bluetooth;
- Локальні бездротові мережі (WLAN — Wireless Local Area Networks), типовим прикладом яких є технологія Wi-Fi;
- Бездротові мережі міського рівня (WMAN — Wireless Metropolitan Area Networks), що реалізуються на основі технології WiMAX;
- Глобальні бездротові мережі (WWAN — Wireless Wide Area Networks), які охоплюють технології CSD, GPRS, EDGE, EV-DO, HSPA та LTE.

З урахуванням застосовуваних технологічних рішень бездротові мережі доцільно класифікувати на три основні види:

- локальні обчислювальні мережі;
- розширені локальні обчислювальні мережі;
- мобільні мережі, що забезпечують роботу переносних комп’ютерів.

Локальними обчислювальними мережами є системи, які можуть містити в собі інтеграцію різних комп’ютерів та пристроїв, розташованих не тільки в межах одного приміщення, а і віддалено. Вони призначені для об’єднання обчислювальної техніки в єдину мережу передачі даних. Локальні мережі можуть бути розширені за допомогою мережевих концентраторів або Ethernet-комутаторів.

Мобільною мережею можна назвати мережу стаціонарних радіостанцій, які обслуговують невелику площу і забезпечують радіозв’язок абонентом у зоні своєї дії.

Розширеними мережами можна назвати мережі в яких поєднані між собою локальні мережі або мобільні мережі з локальними.

Таблиця 1.1

Типи безпровідних мереж

Тип мережі	WLAN – Local area Network	WMAN – Metropolitan area network	WPAN – Personal area network	WWAN – Wide area network
Ціль	Забезпечує доступ до Інтернету в будівлі або на обмеженій території під відкритим небом	Надає доступ за межами офісних та домашніх мереж, як правило, регіональних	Передають сигнали між пристроями на обмежених ділянках, як правило, 100 метрів	Надає доступ за межами діапазону WLAN та WMAN
Підключення	Стільникове	IEEE 802.16 WiMax	Bluetooth, infrared	LTE

Бездротові мережі можуть бути різними, але всі мережі поєднує фізичний момент перенесення даних у вигляді сигналів від однієї точки до іншої по каналу передачі даних. Цей момент називається передачею даних або обміном даних.

У процесі передачі даних у бездротових мережах беруть участь три ключові елементи: радіосигнали, формат даних та структура мережі. З позиції еталонної моделі OSI радіосигнали взаємодіють на фізичному рівні, тоді як формат даних може задіювати декілька верхніх рівнів моделі. Мережна структура включає адаптери інтерфейсів та базові станції, які відповідають за передавання та прийом радіосигналів [5].

У бездротових мережах мережеві адаптери, встановлені на кожному пристрої, виконують перетворення цифрової інформації в радіосигнали, що

передаються іншим елементам мережі. Водночас вони здійснюють зворотне перетворення прийнятих радіосигналів від зовнішніх мережевих компонентів у цифрові дані. Організацією IEEE було створено комплекс стандартів і специфікацій для бездротового зв'язку, відомий як «IEEE 802.11», який регламентує характеристики та структуру цих сигналів.

Початкову версію стандарту IEEE 802.11 було затверджено у 1997 році. Вона передбачала роботу з кількома типами бездротових середовищ, зокрема з двома різновидами радіопередавання та з мережами, що використовують інфрачервоне випромінювання. Станом на сьогодні розроблено значну кількість розширень і модифікацій цього стандарту, які пристосовані до сучасних технологій і підвищених вимог до швидкості передавання даних [2]. Щодо подання інформації, сучасні обчислювальні системи оперують двома можливими станами: наявністю сигналу на вході або його відсутністю. Ці стани прийнято позначати значеннями 1 та 0, які утворюють елементарні одиниці інформації — біти. Окремий біт практично не має прикладного значення, проте об'єднання восьми бітів у байт дозволяє сформувати 256 різних варіантів комбінацій. Цього обсягу комбінацій достатньо для того, щоб закодувати всі літери алфавіту, десять цифр від 0 до 9, пробіли між словами та інші символи, включно зі знаками пунктуації та деякими літерами, що застосовуються в іноземних алфавітах. Сучасні комп'ютери здатні одночасно опрацьовувати кілька 8-бітових байтів. Після завершення обробки інформація знову представлена у бітовому коді та може бути відображена на відеодисплеї, надрукована на принтері або передана через канал зв'язку.

Подібно до процесора комп'ютера, канал передачі даних може обробляти лише один біт за раз — сигнал на лінії або присутній, або відсутній [8]. На невеликих відстанях інформацію можна передавати кабелем, що забезпечує паралельну передачу восьми бітів (або кратного восьми числа) одночасно через окремі проводи. Такий паралельний спосіб дозволяє передавати дані приблизно вісім разів швидше, ніж поодинокий біт через один провід, проте використання восьми проводів підвищує вартість кабелю приблизно у вісім разів. При передачі

інформації на великі відстані витрати на використання багатопровідних ліній можуть стати надто високими. У випадку застосування існуючих каналів, наприклад телефонних ліній, виникає потреба в організації передачі всіх восьми бітів через один і той самий провід або інший доступний носій.

Рішенням цієї проблеми є передача одного біта за раз з додаванням спеціальних бітів та пауз, які позначають початок кожного нового байта. Такий метод отримав назву послідовної передачі даних, оскільки біти відправляються послідовно, один за одним. При цьому не має значення, яка проміжна середа використовується для передавання: це можуть бути електричні імпульси в проводі, два різні аудіосигнали, серії миготливих індикаторів або будь-які інші способи передачі бітів по черзі.

В ідеальному випадку сигнал, що надходить на приймальний кінець мережі, повністю збігається з вихідним. Проте в реальному середовищі практично завжди виникають перешкоди, і майже завжди присутній шум, який накладається на чистий сигнал. Шум визначається як будь-який додатковий сигнал, що додається до вихідного, і може виникати через розряди блискавки, взаємні перешкоди з іншими комунікаційними каналами або ненадійний контакт у ланцюзі.

Незалежно від джерела, шум у каналі може пошкоджувати передавання даних. У сучасних комунікаційних системах біти проходять через канал із дуже високою швидкістю — мільйони бітів за секунду, тому навіть короткочасний вплив шуму може зруйнувати достатню кількість бітів, перетворюючи інформацію на некоректні або непридатні для використання дані [2].

Це свідчить про те, що будь-який потік даних повинен супроводжуватися механізмом контролю помилок. Під час такої перевірки до кожного байта додається спеціальна інформація — контрольна сума. Якщо приймальний пристрій виявляє, що отримана контрольна сума не збігається з очікуваною, він надсилає запит на повторну передачу цього байта.

Поняття сучасних бездротових мереж досить не чітке адже сучасний світ розвивається і технології стрімко змінюють одне одну. Тому для дослідження обрано найбільш популярні бездротові мережі у даний проміжок часу.

Випливаючи з поняття бездротових мереж можна сказати що бездротовою мережею є комп’ютерна мережа, яка використовує бездротові з’єднання даних між вузлами мережі. Бездротові мережі можуть передавати інформацію різними швидкостями, використовувати не однакові технології передачі та мати різну територію покриття.

Є декілька поколінь бездротових мереж: 1G, 2G, 3G, 4G, 5G та інші проміжні варіанти. Певне покоління відповідає за проміжок швидкостей, якими користувач може передавати інформацію, також покоління можуть відрізнятися технологіями передачі даних, які використовуються під час передачі інформації.

До сучасних бездротових мереж, які найбільш поширені у даний проміжок часу можна віднести такі мережі: 4G, LTE та 5G.

4G

До технологій четвертого покоління (4G) відносять ті рішення, що забезпечують передачу даних зі швидкістю понад 100 Мбіт/с. Ще у 2008 році для стандарту 4G були встановлені такі вимоги щодо швидкості:

- 100 Мбіт/с — для користувачів, які рухаються з високою швидкістю (поїзд або автомобіль);
- 1 Гбіт/с — для користувачів, що пересуваються повільно (пішоходи).

До технологій, що претендують на статус 4G, належать:

- LTE
- TD-LTE
- мобільний WiMAX
- UMB
- HSPA +

Найпоширенішими стандартами четвертого покоління є WiMAX та LTE:

- WiMAX (Worldwide Interoperability for Microwave Access) — це розвиток технології Wi-Fi з розширеною зоною покриття;
- LTE (Long Term Evolution) — довгострокове удосконалення або новий етап розвитку GSM.

Мережі 4G працюють виключно з цифровими даними і не використовують окремі канали для голосових викликів, на відміну від мереж 1G, 2G та 3G. Крім того, системи четвертого покоління ґрунтуються на пакетній передачі даних. Для пересилання інформації у мережах 4G застосовується протокол IPv4.

Сьогодні 4G відомий насамперед своїми широкосмуговими можливостями та значно вищою швидкістю, ніж 3G, що забезпечує можливість швидкої передачі даних у просторі.

LTE

LTE (Long Term Evolution) є маркетинговою фразою, яка означає прогресивний рух технології у напрямку справжнього 4G. Тобто кожен раз, коли йдеться річ про 4G LTE – мається на увазі прогрес у розвитку від 3G до 4G.

LTE базується на стандартах, розроблених Проектом партнерства третього покоління - 3GPP, але на даний момент Міжнародний стандарт LTE є слабко визначеним і враховуючи те що він дуже часто оновлюється ускладнюється розуміння дійсного стандарту LTE.

LTE можна сформулювати як модернізований 3G трохи гірший за справжній 4G. Мережі 4G LTE надсилають дані на телефони 4G LTE зі швидкістю нижче 100 Мбіт / с із швидкістю завантаження.

Мережі LTE призначені для подолання розриву функціонального обміну даними між фіксованими бездротовими локальними мережами (LAN) та дуже високою мобільністю стільникових мереж.

Основними цілями LTE є:

- збільшена пікова швидкість передачі даних ніж у 3G по висхідній та висхідній лініях;
- масштабована пропускна здатність;
- покращена спектральна ефективність;
- стандартний інтерфейс, який може підтримувати безліч типів користувачів.

Оскільки для LTE не існує справжнього стандарту, він охоплює весь діапазон мінімальних швидкостей завантаження від 20 Мбіт / с для 3G до 100 Мбіт / с для 4G, надаючи йому величезний діапазон потенційних швидкостей.

Беручи до уваги те що досі LTE використовується дуже поширено і велика кількість операторів використовують його замість справжнього 4G. LTE досі являється лише перехідною ланкою між 3G та 4G.

5G

5G є відносно новим стандартом мобільного зв'язку. У мережах 5G швидкість передачі даних може досягати від 10 до 25 Гбіт/с із мінімальними затримками сигналу — всього 1–2 мс. Цей стандарт здатен радикально змінити спосіб взаємодії між пристроями та революціонізувати швидкість завантаження даних. Впровадження 5G відкриває широкі можливості для нових послуг, сервісів та бізнес-моделей, які раніше були недосяжні у мережах 4G. Для масового споживача вже зараз найбільш популярними технологіями, які можуть використовуввати 5G є віртуальна і доповнена реальність.

Зараз 5G перебуває в процесі розробки, виробники телефонів випускають телефони, сумісні з 5G, але мережі операторів не наближаються до мінімальних 1 Гбіт / с із затримкою в 1 мілісекунду, необхідною для стандарту. Також оператори розраховують досягнути швидкості в 30-50 разів вищої, ніж у LTE.

Наприкінці жовтня 2015 року південнокорейська компанія SK Telecom оголосила про плани стати першим провайдером мереж п'ятого покоління (5G). Під час тестових випробувань компанії вдалося досягти швидкості передачі даних 19,1 Гбіт/с, що у кілька разів перевищує показники сучасних мереж 4G [14].

У квітні 2019 року технології п'ятого покоління (5G) були впроваджені в Південній Кореї (першій країні, що запустила комерційні послуги 5G), а також у Швейцарії та Китаї. Основним виробником обладнання для цих мереж виступає китайська компанія Huawei. За словами представників Huawei, «головним завданням мереж п'ятого покоління стане розширення спектра використовуваних частот та збільшення пропускної здатності мереж. Очікується, що нова технологія

вирішить ключову проблему, над якою працюють оператори в усьому світі, — підвищення ефективності мережевої інфраструктури» [13].

Через обізнаність людей про 5G, компанії вже намагаються продати свої існуючі мережі вгору, при цьому AT&T називає свою мережу 4G "5Ge", незважаючи на те, що вона не наближається до стандартів 5G. T-Mobile заявляє, що пропонує найбільшу мережу 5G в Америці, а Verizon заявляє про найшвидшу швидкість 5G на всіх смугах пропускання. Усі вони не є "справжніми 5G", принаймні, як визначено MCE-R (сектором радіозв'язку Міжнародного союзу радіозв'язку). Проте вони, звичайно, швидші, ніж 4G або 4G LTE.

Також після розгортання мереж стільникового зв'язку 5 покоління 5G у вчених та інженерів посилився інтерес до розробки обладнання наступного покоління стільникового зв'язку. Фахівці сходяться на думці, що в наступному поколінні вони отримають подальший розвиток і вдосконалення недостатньо повно реалізованих підходів в попередньому поколінні. Наступні покоління скоріше всього можуть бути засновані на застосуванні штучного інтелекту, квантових комунікацій, що дозволить досягти швидкості передачі даних від сотень Гбіт / с до 1 Тбіт / с.

1.2 Необхідність захисту бездротових мереж

Бездротові мережі не являються безпечними. Більшу частину часу вони дійсно являються доволі незагрозливими для її користувачів, але вони все ж мають велику кількість вразливостей.

Беручи до уваги те, що бездротова мережа використовує радіосигнали з певним набором характеристик, і при зацікавленості третьої особи, яка може при бажанні виділити велику кількість часу на вивчення мережі, є можливим варіант перехоплення даних у мережі. Навіть якщо конфіденційна інформація пересилається бездротовим з'єднанням, то зловмисник все одно може скопіювати її. Паролі облікових записів, персональні дані, номери кредитних карток являються частиною вразливої інформації.

Шифрування та інші методи захисту можуть трохи ускладнити процес перехвату даних, але вони все одно не в змозі забезпечити повний захист від зловмисника, який володіє досвідом роботи з бездротовими мережами і перехопленням інформації.

Ситуація стає більш небезпечною завдяки недбалому відношенню до безпеки адміністраторів і користувачів мережі, які часто залишають мережі відкритими або не використовують технологій захисту бездротових мереж або найпростішого шифрування, яке б мінімізувало вразливості мереж.

Головна відмінність між дротовими та бездротовими мережами полягає у наявності неконтрольованої зони між кінцевими точками бездротової мережі. Наявність такої зони створює можливість для зловмисників, що перебувають у безпосередній близькості до бездротових компонентів, здійснювати атаки, які неможливі у дротовому середовищі.

Застосування бездротового доступу до локальної мережі значно підвищує рівень загроз безпеці [8]. При проектуванні бездротових мереж особливо гостро постає проблема забезпечення їх надійного захисту.

Обладнання мереж WLAN включає робочі станції для кожного абонента і точки бездротового доступу.

Точки доступу до мережі призначені для забезпечення зв’язку між користувачами та між собою. Вони виконують функцію концентраторів і можуть також слугувати мостами, що забезпечують підключення до кабельної локальної мережі та до мережі Інтернет. Кожна точка доступу здатна обслуговувати одночасно декількох користувачів. Прилеглі точки формують зону покриття Wi-Fi, у межах якої всі абоненти з бездротовими адаптерами можуть підключатися до мережі. Такі зони зазвичай створюють у місцях скупчення великої кількості людей: бізнес-центрах, бібліотеках, аеропортах, торгових центрах та студентських кампусах.

Кожна точка доступу має ідентифікатор набору сервісів (SSID — Service Set Identifier). SSID представляє собою 32-символьний рядок, який використовується як ім’я бездротової мережі і з яким асоціюються всі вузли. Цей ідентифікатор є

необхідним для підключення робочої станції до мережі. Отже, для підключення робочої станції до точки доступу необхідно, щоб на обох пристроях був однаковий SSID. Якщо робоча станція не має відповідного SSID, вона не зможе встановити з'єднання з мережею, оскільки не зможе взаємодіяти з точкою доступу.

Доступ до мережі і підключення також можуть бути вразливою ланкою тому треба також приділяти увагу підключеним робочим станціям до мережі.

Слід зауважити, що бездротові мережі стикаються з кількома ключовими загрозами безпеці. По-перше, існує ризик несанкціонованого підключення сторонніх осіб до мережі без відома або дозволу адміністратора. По-друге, можливе перехоплення даних досвідченими зловмисниками під час їх передачі. Кожна з цих вразливостей є окремою потенційною проблемою і кожна з них потребує окремого спеіцального методу профілактики і захисту. Не дивлячись на правоту ствердження про те що забезпечення повної безпеки бездротової мережі не являється можливим, проте мінімізація ризиків може значно ускладнити життя випадковим злочинцям і зменшити можливості перехоплення інформації досвідченими спеціалістами тим самим покращити життя адміністраторам і користувачам мережі.

1.3 Інформаційні загрози та атаки

Як і в домашній, так і в інших бездротових мережах завжди є ризики реалізування загроз зі сторони порушників.

Типовий діапазон трансляції в приміщенні точки доступу становить 150–300 футів. На відкритому повітрі цей діапазон може сягати до 1000 футів. Отже, якщо зона дії мережі знаходиться у тісному населеному пункті, то відсутність захисту бездротової мережі може відкрити мережеве з'єднання з Інтернетом для багатьох ненавмисних користувачів. Такі користувачі можуть мати можливість здійснювати незаконні дії, відстежувати та фіксувати веб-трафік мережі або красти особисті файли.

Широкий діапазон бездротової точки доступу може відкрити доступ до Інтернету за межами будинку, у якому знаходиться мережа. Розумні користувачі комп’ютерів це знають, і деякі з них проїжджаючи міста і квартали за допомогою бездротового обладнаного комп’ютера - іноді з потужною антеною - у пошуку незахищених бездротових мереж. Подібна практика відома під назвою "охорона праці" [7].

Також багато громадських точок доступу не захищені, а трафік, який вони несуть, не зашифрований. Це може загрожувати конфіденційним комунікаціям або операціям користувачів. Оскільки зв’язок передається „в чистому вигляді”, зловмисні актори можуть використовувати інструменти сніфингу, щоб отримати конфіденційну інформацію, таку як паролі або номери кредитних карток.

Незахищена громадська бездротова мережа в поєднанні з незахищеним спільним використанням файлів може дозволити зловмисному користувачеві отримати доступ до будь-яких каталогів та файлів, які ви ненавмисно надали для спільного використання. Тож підключаючи пристрої до загальнодоступних мереж, краще заборонятиспільний доступ до файлів та папок. Дозволяти використовувати спільний доступ доцільно лише у визнаних домашніх мережах і лише тоді, коли необхідно ділитися елементами.

У громадських місцях зловмисні користувачі можуть просто поглянути через плече людини під час друкування. Просто спостерігаючи, вони можуть викрасти конфіденційну або особисту інформацію. Захисні екрани, які заважають серфінгістам бачити екран вашого пристрою, можна придбати за невеликі гроші.

Не всі зловмисники покладаються на отримання доступу до даних за допомогою бездротового зв’язку. Викравши ваш пристрій фізично, зловмисники могли мати необмежений доступ до всіх його даних, а також до будь-яких підключених хмарних облікових записів. Вжити заходів для захисту пристроїв від втрати або крадіжки є важливим, але якщо трапиться найгірше, невелика підготовка може захистити дані всередині. Більшість мобільних пристроїв, включаючи портативні комп’ютери, тепер мають можливість повністю зашифрувати свої збережені дані, роблячи пристрої марними для зловмисників,

які не можуть надати належний пароль або персональний ідентифікаційний номер (PIN-код). На додаток до шифрування вмісту пристрою, доцільно також налаштувати програми вашого пристрою на запит інформації для входу, перш ніж дозволити доступ до будь-якої хмарної інформації. Нарешті, індивідуально зашифровані або захищені паролем набагато складніше викрасти. Це забезпечить ще один рівень захисту у випадку, якщо зловмисник зможе отримати доступ до пристрою.

До основних вразливостей та загроз бездротових мереж належать:

- сигнали радіомаяків;
- виявлення WLAN;
- підслуховування;
- помилкові точки доступу;
- відмова в обслуговуванні (DoS);
- атаки типу «людина-в-середині» (MITM);
- анонімний доступ до Інтернету.

Сигнали радіомаяка. Бездротова точка доступу працює на визначених частотах і передає широкомовні сигнали радіомаяка, щоб повідомляти навколишні бездротові пристрої про свою присутність. Ці сигнали містять основну інформацію про точку доступу, включаючи її SSID, і запрошують бездротові вузли зареєструватися в зоні дії точки доступу. Після отримання SSID у режимі очікування робоча станція може автоматично додати себе до відповідної мережі. Проте мовлення радіомаяка є потенційною вразливістю бездротових мереж з моменту їх появи. Хоча багато моделей дозволяють приховати видимість SSID, певне вікно вразливості залишається, оскільки SSID все одно передається точці доступу під час підключення до мережі [4].

Виявлення WLAN. Локальні бездротові мережі досить легко виявляти, навіть обстежуючи офісні приміщення за допомогою переносного пристрою, здатного підключатися до мереж Wi-Fi. Крім того, для виявлення бездротових мереж зловмисники та недобросовісні користувачі можуть використовувати спеціалізовані утиліти, наприклад, NetStumber, яка у поєднанні з GPS-навігатором

дозволяє визначати розташування мереж. Таке програмне забезпечення дає змогу зловмисникам ідентифікувати SSID мережі WLAN, а також визначити наявність та тип використаної системи шифрування. Таким чином, можливість виявлення мережі відноситься до категорії вразливостей бездротових мереж.

Підслуховування. Цей тип пасивної атаки застосовується зловмисниками з метою збору інформації про бездротову мережу для подальшого використання. Перехоплені дані часто служать засобом отримання несанкціонованого доступу до мережевих ресурсів. Обладнання, яке застосовується для прослуховування трафіку, може являти собою звичайний клієнтський пристрій, здатний підключатися до даної мережі. Завдяки особливостям бездротових технологій, які дозволяють під'єднувати до фізичної мережі комп'ютери, що перебувають на певній відстані, але в межах зони покриття, такі пристрої можуть функціонувати так, ніби вони знаходяться безпосередньо всередині мережі. Отже, підключитися до бездротової мережі, що розташовується в будівлі, може людина, що знаходиться поза межами будівлі наприклад у сусідньому дворі або у машині поруч. Атаку за допомогою пасивного прослуховування практично неможливо виявити, можна лише відслідкувати за збільшенням активності мережі на певній IP адресі та зменшенням пропускної спроможності мережі.

Помилкові точки доступу в мережу. У сучасномі світі також поширеною є атака підміни точки доступу. Зазвичай подібна атака є наслідком підслуховування мережі. Недобросовісний користувач мережі із досвідом роботи у неї може створити неправдиву точку доступу з імітацією мережевих ресурсів. Нічого не підозрюючі абоненти у той час, звертаються до помилкової точки доступу і повідомляють їй свої реквізити доступу. Цей тип атак може бути застосованим разом з прямим «глушінням» істинної точки доступу в мережу.

Під час здійснення атаки зловмисник спочатку збирає відомості про легітимну точку доступу в публічній мережі, після чого налаштовує власне обладнання для імітації її роботи. При цьому він транслює широкомовний сигнал з більшою потужністю, ніж у справжньої точки доступу, внаслідок чого користувачі, не підозрюючи про загрозу, автоматично підключаються до мережі з

сильнішим сигналом. Оскільки користувач у такій ситуації виходить в Інтернет через систему зловмисника, останній отримує можливість без перешкод застосовувати спеціалізовані засоби для перехоплення інформації, що передається. До перехоплених даних можуть належати номери банківських карток, пари логін–пароль та інші конфіденційні відомості. Тому перед користуванням публічною точкою доступу Wi-Fi необхідно завжди уточнювати її назву та облікові дані для автентифікації, що дозволяє впевнитися у підключенні саме до легітимної і безпечної мережі.

Відмова в обслуговуванні. Атака відмови в обслуговуванні може викликати повну паралізацію. Метою подібної атаки є створення перешкод під час доступу до мережі звичайними користувачами. Під час реалізації атаки включається пристрій, який заповнює весь спектр робочої частоти нелегальним трафіком або перешкодами. Така задача нажаль не викликає особливих труднощів особливо у досвідчених користувачів бездротових мереж. Також сам факт проведення в бездротовій мережі дуже важко довести, тим паче реалізований на фізичному рівні. Бездротові системи все ще є дуже сприйнятливими до таких атак.

Атаки типу «людина-в-середині». Метою виконання атаки типу «людина-в-середині» є руйнування цілісності сеансу зв’язку і порушення конфіденційності сеансів підключення у мережі. Для проведення подібної атаки зловмиснику потрібна детальна інформація про мережу. Зазвичай під час реалізації підміняється ідентифікація одного з мережевих ресурсів та використовується можливість нелегального захоплення потоку даних і прослуховування інформації, що передається мережею з можливим розшифруванням і зламом алгоритмів захисту даних та з метою зміни вмісту пакетів даних.[1].

Анонімний доступ в Інтернет. Незахищені бездротові локальні обчислювальні мережі забезпечують потенційним порушникам анонімний доступ для атак мережею Інтернет. Анонімний доступ може використовуватися наприклад у незахищеній мережі WLAN, і зловмисники можуть у свою чергу анонімний доступ для протиправних дій у мережі. При цьому не залишаються сліди у мережі під час подібної діяльності. Отже організації з незахищеною

локальною обчислювальною мережею формально можуть стати джерелом атакуючого трафіку у наслідок можуть підвищити ризики атак на інші бездротові системи.

Основні способи атак на безпровідні мережі, рис.1.2:

1. Чужаки (Rogue Devices, Rogues, Evil Twin)
2. Нефіксована природа зв'язку:
   - Man-in-The-middle;
   - Мережі Ad-hoc;
   - Hotspot – точки доступу.
3 Вразливості мереж і пристроїв:
   - некоректно конфігуровано точки доступу або клієнти;
   - злом шифрування;
   - підбір пароля.
4. Нові загрози та атаки:
   - прослуховування (розвідка);
   - імперсонація та Identity Theft;
   - відмова в обслуговуванні (Denial of Service, DoS).
5. Особливості функціонування:
   - активність в неробочій час;
   - швидкості;
   - інтерференція;
   - зв‘язок.

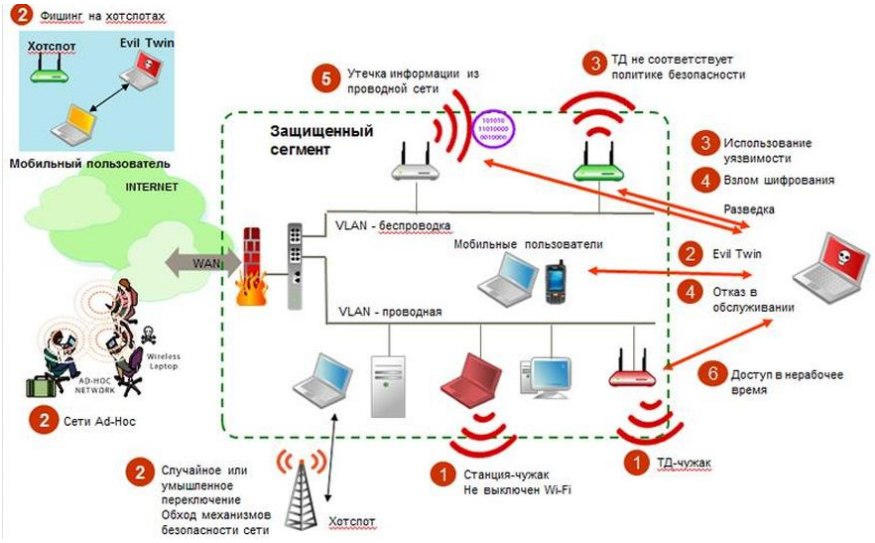


Рис. 1.2 Основні способи атак на безпровідні мережі

Описані вище атаки не є єдиними атаками, використовуваними хакерами для злому бездротових мереж, але є одними з найпоширеніших атак та вразливостей бездротових мереж.

Аналізуючи те, що при передачі інформації бездротовою мережею відправлення і приймання даних здійснюється радіохвилями та приймати їх може хто завгодно при наявній техніці випливає питання необхідності додаткових механізмів захисту.

У процесі передачі даних у бездротових мережах беруть участь три основні складові: радіосигнали, формат даних та структура мережі. З погляду еталонної моделі OSI, радіосигнали взаємодіють на фізичному рівні, тоді як формат даних може охоплювати кілька верхніх рівнів моделі. Мережна структура включає адаптери інтерфейсів і базові станції, які відповідають за передачу та прийом радіосигналів.

Бездротові мережі мають безліч слабких моментів, які можуть стати дуже небезпечними через незахищеність мереж у підключенні, через великий спектр даних які може надати сама мережа для організації подібної і у наслідок її підміни і через не пильне відношення до захисту адміністраторів мережі наприклад у відсутності використання протоколів захисту або шифруванні, або використанні

застарілих методів захисту. Також слабкою ланкою бездротових мереж можуть бути самі користувачі які можуть розповсюджувати паролі до мереж або відкривати інформацію про дані, що пережаються у мережі стороннім особам.

До ключових вразливостей та загроз бездротових мереж належать:

- мовлення радіомаяка;
- виявлення WLAN;
- пасивне підслуховування;
- створення підробних точок доступу;
- атаки відмови в обслуговуванні (DoS);
- атаки типу «людина посередині» (MITM);
- анонімний доступ до Інтернету.

Одними з самих неприємних по наслідкам і по можливостям роботи з мережею є атаки відмови в обслуговуванні та атаки типу людина в середині. У першому випадку створюються перешкоди при доступі користувача. До мережевих ресурсів. Зловмисник може включити пристрій, що заповнює весь спектр на робочій частоті перешкодами і нелегальним трафіком, який звичайно буде заважати вільно користуватися мережею.

Під час реалізації атаки типу «людина посередині» зловмисник попередньо здійснює детальний аналіз мережевого середовища. Як правило, він підміняє ідентифікацію одного з мережевих вузлів або ресурсів, отримуючи можливість перехоплення та несанкціонованого контролю трафіку. Використовуючи перехоплений потік даних, нападник може змінювати його вміст відповідно до власних цілей, зокрема виконувати підміну IP-адрес, змінювати MAC-адреси або імітувати роботу іншого хоста. Подібні атаки зазвичай спрямовані на порушення конфіденційності та цілісності сеансу зв’язку.

Описані вище атаки не є єдиними атаками, використовуваними хакерами для злому бездротових мереж, але є одними з найпоширеніших атак та вразливостей бездротових мереж.

Отже можна зробити висновок що захист бездротових мереж є доволі недосконалим і важливим є розробка нових методик захисту та вдосконалення

існуючих технологій. Також обізнане використання методів і технологій захисту може мінімізувати вплив на слабкі місця бездротових мереж.

2 МЕТОДИКИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ У БЕЗДРОТОВИХ МЕРЕЖАХ

2.1. Стандарти інформаційної безпеки для бездротових мереж

На даний момент існує доволі багато методів і технологій захисту бездротових мереж, таких як обмеження доступу до мережі, фільтрація адрес або захист мережі за допомогою шифрування. Але для проведення досліджень методів захисті необхідно розуміти стандарти які описують процес передачі даних відповідними протоколами та згідно яким вдосконалюються технології захисту бездротових мереж.

Базовим стандартом, який визначає набір протоколів для передачі даних у бездротових мережах, є IEEE 802.11. Цей стандарт постійно розвивається та доповнюється. Його вдосконалені версії були опубліковані у 1999, 2007, 2012 та 2016 роках [2].

Бездротова мережа — це гнучка інфраструктура, що складається з комплексу апаратних і програмних засобів для передавання інформації. Вона може виступати як альтернатива провідним мережам, так і доповнювати їх, надаючи додаткові можливості та функції.

Сучасні бездротові мережі дозволяють вирішувати безліч завдань: за допомогою бездротових мереж можна не тільки організовувати мережі всередині приміщень, а і організовувати мережі масштаблм у ціле місто або державу. Швидке розгортання, відносно низька вартість та широкі функціональні можливості для передавання даних, мультимедійного трафіку та IP-телефонії роблять бездротові технології одними з найдинамічніших напрямків у телекомунікаціях. Подібно до провідних мереж, бездротові мережі класифікують за територіальним охопленням, виділяючи чотири основні типи: WWAN, WMAN, WLAN та WPAN. Для різних зон покриття розроблені спеціальні нормативні документи, які встановлюють правила, рекомендації та технічні характеристики

використання бездротового середовища на певних швидкостях. Такі документи відомі як стандарти бездротових мереж.

На рис. 2.1 показана класіфікація безпровідних стандартів за територіальною ознакою.

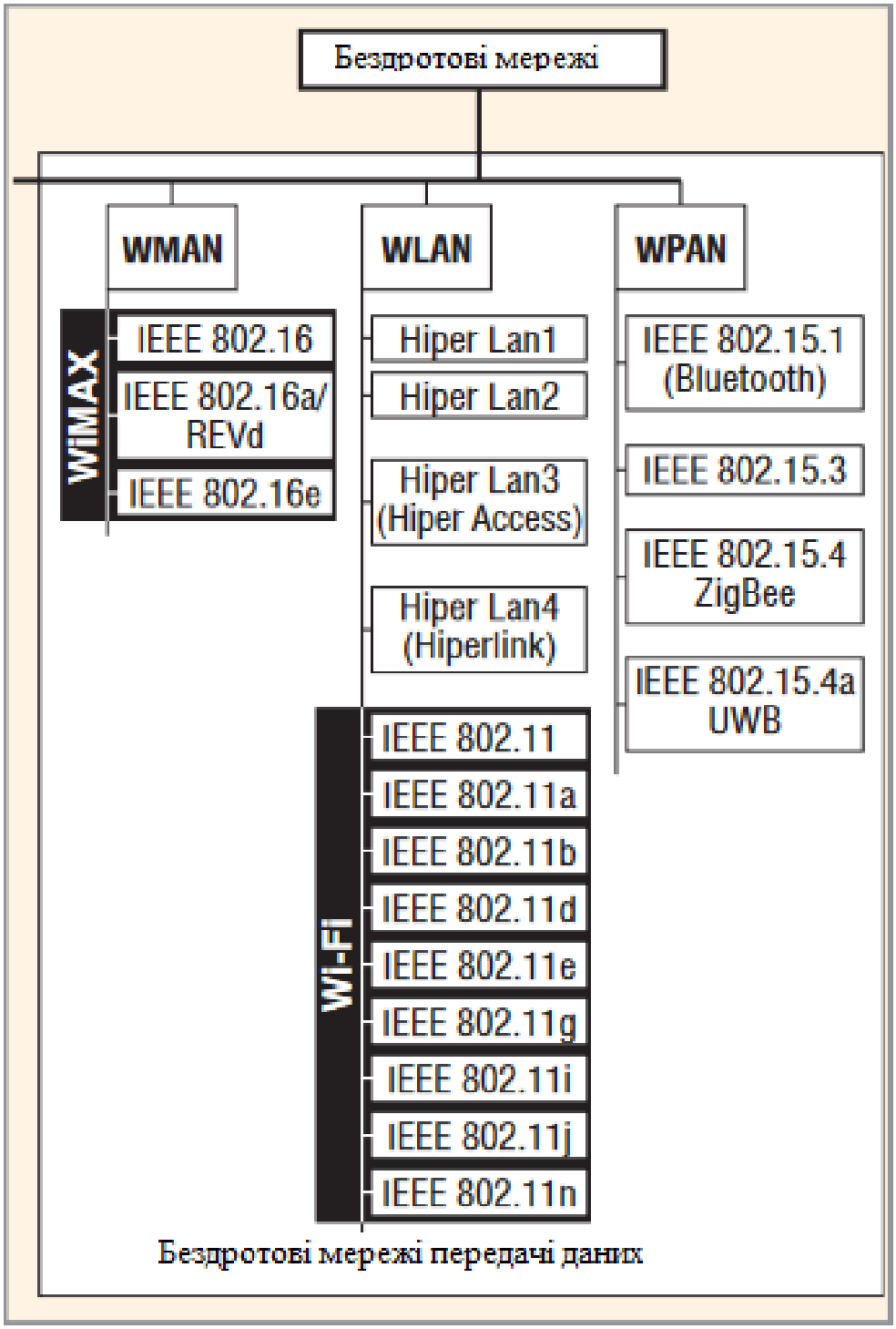


Рис. 2.1 Стандарти передачі даних у бездротових мережах WMAN, WLAN, WPAN

Стандарти для мережі WPAN

IEEE 802.15.1 (Bluetooth)

Технологія Bluetooth була розроблена компанією Ericsson і отримала свою назву на честь датського короля Гарольда Синьозубого, який правив Данією та Норвегією у X столітті. Для комерційного просування технології був створений консорціум, до складу якого увійшли Ericsson, IBM, Intel, Nokia та Toshiba. На сьогодні серед основних членів консорціуму також входять 3Com, Agere Systems, Microsoft та Motorola. Основна мета створення Bluetooth полягала в забезпеченні можливості бездротового зв'язку та обміну даними між різними електронними пристроями — комп'ютерами, мобільними телефонами та побутовою технікою — на відстані до 100 метрів.

Стандарт Bluetooth працює в радіочастотному діапазоні 2400–2483,5 МГц, відомому як ISM (*Industrial, Scientific, Medical* — промисловий, науковий і медичний), який у багатьох країнах використовується для безліцензійного доступу. У Bluetooth цей діапазон розділено на 78 каналів по 1 МГц кожен. У верхній та нижній частинах діапазону передбачені захисні невикористовувані смуги шириною 3,5 МГц і 2 МГц відповідно. У деяких країнах, наприклад у Франції, діапазон ISM значно вужчий [16].

За вихідними потужностями всі пристрої діляться на три класи:

- перший клас - до 100 мВт;
- другий - до 2,5 мВт;
- третій - до 1 мВт.

Для передачі даних у Bluetooth використовується гауссова частотна модуляція (GFSK), при якій частота несучої змінюється у часі відповідно до Гаусової кривої показано на рис. 2.2, що дозволяє обмежити спектр випромінюваного сигналу. Обмін даними відбувається всередині тимчасових інтервалів (слотів) тривалістю 625 мкс. Після передачі кожного слота відбувається перемикання на інший частотний канал. Деякі слоти можуть бути зарезервовані

для синхронних каналів (наприклад, для передачі голосу), причому передбачено до трьох синхронних каналів зі швидкістю 64 Кбіт/с. Паралельно з синхронними даними може передаватися і асинхронна інформація.

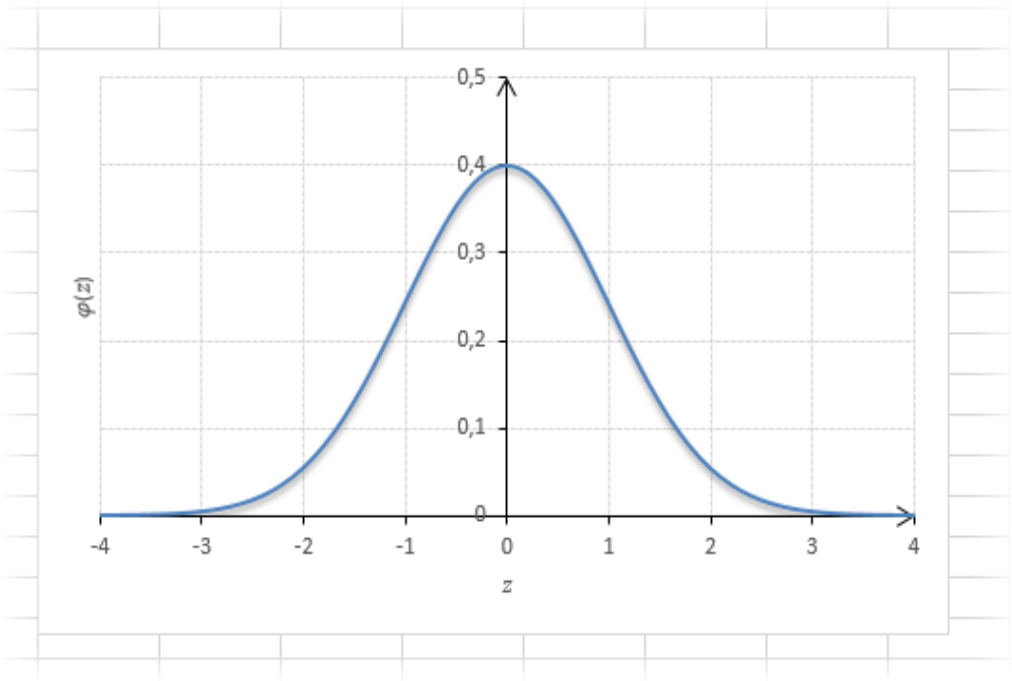


Рис. 2.2 Крива Гаусса

Для забезпечення дуплексного зв’язку застосовується метод **тимчасового мультиплексування**, при якому в одному часовому слоті передає один пристрій, а в наступному — інший. При симетричній передачі асинхронних даних максимальна швидкість складає **433,9 Кбіт/с** в обох напрямках. У разі асиметричного обміну швидкість досягає **723,2 Кбіт/с** в одному напрямку та **57,6 Кбіт/с** у зворотному.

Bluetooth служить головним чином для організації каналів зв’язку типу «точка - точка», однак можлива так само і організація типу «точка - багато - точка». Організацію топологій мереж Bluetooth зображено на Рисунку 2.3.

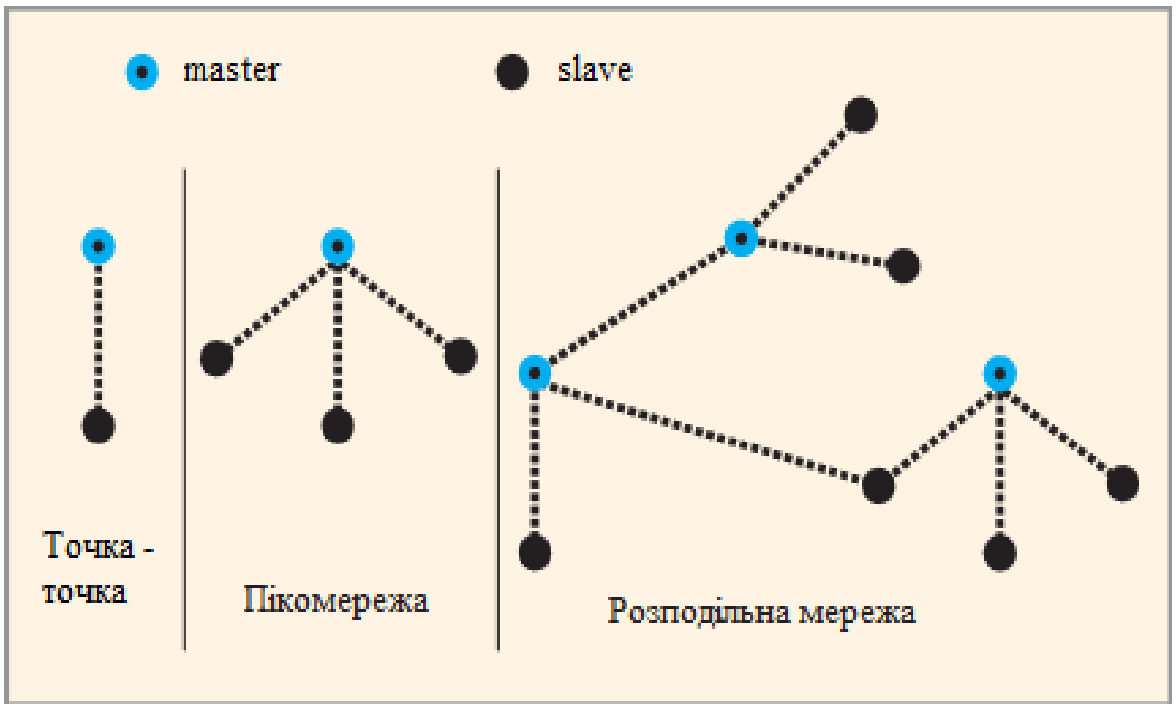


Рисунок 2.3 – Організації топології мереж Bluetooth

У будь-якій конфігурації один із пристроїв виконує роль **провідного (master)**, а решта — **відомих (slave)**. Така організація утворює **пікомережу (piconet)**. У складі однієї пікомережі може бути один провідний пристрій і до семи відомих. Крім того, у пікомережі можуть перебувати інші пристрої, які не беруть участі в обміні даними, але залишаються синхронізованими з провідним — їх називають **блокованими (parked)**.

IEEE 802.15.3

Стандарт IEEE 802.15.3 є прямим спадкоємцем Bluetooth.

Стандарт **IEEE 802.15.3** забезпечує передачу даних зі швидкістю до **55 Мбіт/с** на відстані до 100 м і дозволяє одночасно підключати до мережі до **245 користувачів**. У разі виникнення перешкод від інших побутових пристроїв або мереж, мережі на основі IEEE 802.15.3 можуть **автоматично перемикати канали**. Також підтримуються швидкості передачі **11, 22, 33 та 44 Мбіт/с**. Захист даних у таких мережах може забезпечуватися за допомогою стандарту **AES 128**.

IEEE 802.15.4 (ZigBee)

Стандарт **IEEE 802.15.4 (ZigBee)** призначений переважно для організації зв’язку між автономними пристроями та обладнанням. У корпоративному секторі його застосовують, наприклад, у системах автоматизації виробництва, складських комплексах та різноманітних датчиках і сенсорах. У домашньому середовищі стандарт використовується для систем безпеки, кондиціонування, керування ПК, ігрових приставок, освітлення, радіокерованих іграшок та пультів дистанційного керування.

Стандарт **IEEE 802.15.4** визначає характеристики **фізичного рівня (PHY)** та протокол управління доступом **(MAC)**, забезпечуючи підтримку різних топологій мереж. Основні функції PHY включають

контроль енергоспоживання та якості ліній, а також оцінку каналів для ефективного співіснування з іншими бездротовими мережами. Протокол MAC відповідає за автоматичне підтвердження отримання пакетів, дозволяє передавати дані у визначені часові інтервали та підтримує **128-бітне шифрування AES**. У разі, якщо в зоні досяжності пристроїв ZigBee присутні мережі Wi-Fi або Bluetooth, їх канали можуть використовуватися як тунель для передавання трафіку ZigBee.

Стандарт IEEE 802.15.4 передбачає невелику дальність дії (близько 10 метрів) і пропускну можливість каналу (до 250 Кбіт / с). Передача на цій швидкості ведеться вдіапазоні 2,4 ГГц. Невелика потужність і швидкість обумовлені малою споживаною потужністю пов'язаних пристроїв. Доступні також діапазони 858 МГц (20 Кбіт / с) і902. . .928 МГц (40 Кбіт / с) [12].

IEEE 802.15.4a (UWB)

UWB (Ultra Wideband) — технологія надширокосмугового радіозв'язку, розроблена корпорацією **Intel**, що дозволяє передавати дані зі швидкістю до **500 Мбіт/с** на відстані кількох метрів. Для передачі інформації застосовуються надкороткі радіоімпульси (тривалість менше **1 нс**) у широкому частотному діапазоні **3,1–10,6 ГГц**. Використання технології UWB дозволяє створювати спеціальні мережі, де кілька надширокосмугових пристроїв можуть підтримувати зв'язок між будь-якими вузлами.

Короткі імпульси UWB відносно стійкі до багатопроменевого загасання, що виникає при відображенні сигналу від стін, стелі, будівель чи транспортних засобів. Високошвидкісні пристрої UWB переважно застосовуються для швидкої передачі даних, наприклад відеопотоків та різноманітних додатків. Низькошвидкісне обладнання UWB використовується для відстежування місцеположення користувачів бездротових пристроїв та інших об'єктів на території. Враховуючи, що передача в широкосмуговому спектрі потребує значно менше енергії, ніж у вузькосмуговому через різницю рівнів сигналу, для мобільних пристроїв у широкосмуговому режимі можна застосовувати шумоподібні сигнали з низьким співвідношенням сигнал/шум. Отже, очікується, що **чіпи UWB будуть більш енергоефективними**, ніж, наприклад, чіпи Bluetooth, при цьому забезпечуючи значно вищу пропускну здатність.

2.1.1 Стандарти для мережі WLAN

Технологія **Wi-Fi (Wireless Fidelity)** призначена для створення бездротових локальних мереж та організації публічних точок доступу до Інтернету (*Hot-Spots*). Вона базується на стандартах **IEEE 802.11**, які є основою для WLAN і забезпечують передачу даних зі швидкістю від **1 до 2 Мбіт/с**, функціонуючи на фізичному та канальному рівнях моделі OSI. На **фізичному рівні** визначено один інфрачервоний метод передачі даних у відповідному діапазоні та два широкосмугові радіочастотні методи. Радіочастотні

методи працюють у **ISM-діапазоні 2,4 ГГц** і зазвичай використовують смугу шириною **83 МГц** у межах **2,400–2,483 ГГц**.

Стандарт **IEEE 802.11** застосовує **технологію розширення спектру прямою послідовністю (DSSS, Direct Sequence Spread Spectrum)** та **технологію розширення спектру зі стрибкоподібною перебудовою частоти (FHSS, Frequency Hopping Spread Spectrum)**. Для модуляції сигналу в технології FHSS використовується **Frequency Shift Keying (FSK)**. Приклад застосування цієї технології наведено на рисунку 2.4.

Для передачі даних на швидкості **1 Мбіт/с** застосовується **FSK-модуляція по Гауса другого рівня**, тоді як на швидкості **2 Мбіт/с** використовується модуляція четвертого рівня. Технологія **DSSS** використовує модуляцію **Phase Shift Keying (PSK)**: на швидкості 1 Мбіт/с застосовується **диференціальна двійкова PSK**, а на швидкості 2 Мбіт/с — **диференціальна квадратична PSK**. Заголовки фізичного рівня завжди передаються на швидкості 1 Мбіт/с, тоді як основні дані можуть передаватися як на швидкості 1, так і 2 Мбіт/с.

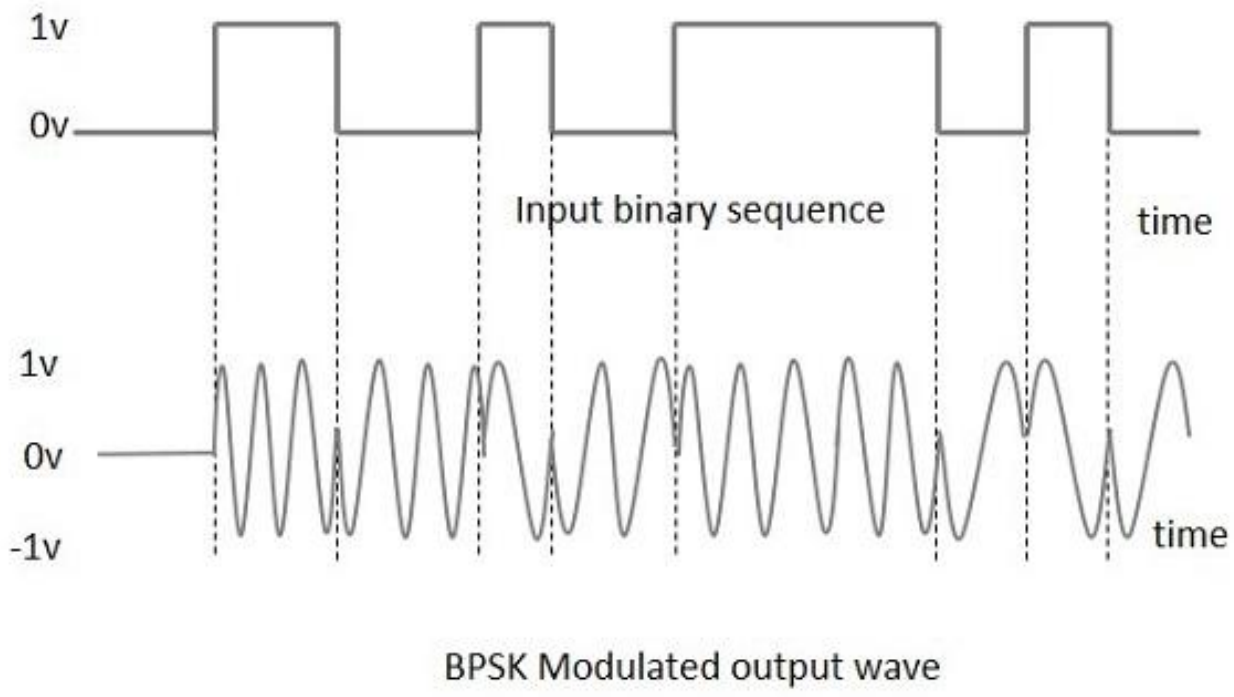


Рисунок 2.4 – Бінарна технологія модуляції PSK із по’єдням DSSS і FHSS.

Спираючись на різноманніття WLAN-мереж, можна сказати, що вони розрізняються швидкостями передачі даних, схемою організації сигналу, радіусом охоплення мережі, а також характеристиками приймальних пристроїв і радіопередавачів.

Найбільш поширеними у використанні користувачами стали бездротові мережі стандарту IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac і інші.

IEEE 802.11a

Стандарт 802.11a був прийнятий в 1999 році, але набув поширення у 2001 році. Він не отримав широкого розповсюдження у Росії і в Європі. Даний стандарт використовується, в основному, в США і Японії.

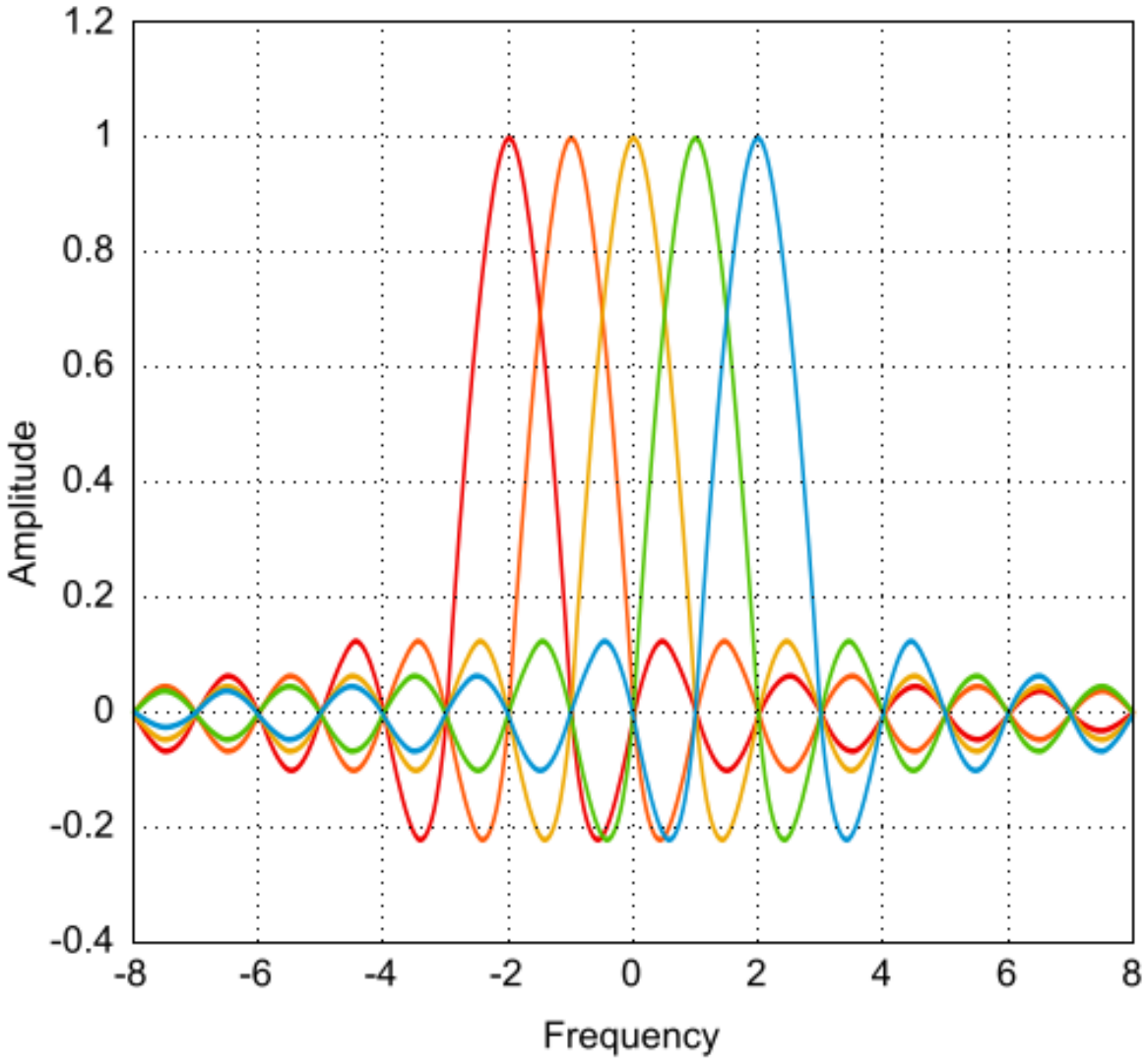


Рисунок 2.5 – Технологія мультиплексування з поділом по ортогональних частотах OFDM

Високошвидкісний стандарт **IEEE 802.11a** забезпечує передачу даних зі швидкістю до **54 Мбіт/с**, переважно на частоті **5 ГГц**. У цьому стандарті використовується **мультиплексування з поділом по ортогональних частотах (OFDM, Orthogonal Frequency Division Multiplexing)**, яке слугує схемою модуляції сигналу під час передачі даних. Технологія OFDM показана на рисунку 2.5. Для модуляції

застосовується певна кількість несучих: основний потік даних розбивається на кілька паралельних субпотоків із відносно низькою швидкістю передачі, які передаються за допомогою несучих хвиль. Стандарт **IEEE 802.11** визначає три обов'язкові швидкості передачі даних: **6, 12 та 24 Мбіт/с**, а також п'ять додаткових: **9, 18, 36, 48 та 54 Мбіт/с**. Крім того, можливо одночасне використання **двох каналів**, що дозволяє подвоїти швидкість передачі даних.

До недоліків 802.11a можна віднести високу споживану потужність радіопередавачів для частот 5 ГГц.

IEEE 802.11b

Стандарт **WLAN** для частоти **2,4 ГГц** було затверджено у 1999 році. Він базується на методі **широкосмугової модуляції з прямим розширенням спектра (DSSS)**, де в якості базової радіотехнології застосовується метод DSSS із **8-бітними послідовностями Уолша**. Усього робочий діапазон розділено на **14 каналів**, віддалених один від одного на **25 МГц** для мінімізації взаємних перешкод. Інформація передається лише через обраний канал без перемикання на інші, причому одночасно можна використовувати до **трьох каналів**. Стандарт також підтримує **швидкість передачі даних до 11 Мбіт/с**. Оскільки обладнання, що працює на максимальній швидкості, має менший радіус дії порівняно з нижчими швидкостями, стандарт **802.11b** передбачає **автоматичне зниження швидкості** при погіршенні якості сигналу. У межах цього стандарту швидкість передачі даних може динамічно змінюватися залежно від відстані між передавачем і приймачем та рівня перешкод [11].

IEEE 802.11ac

Стандарт **IEEE 802.11ac** продовжує розвиток технологій, впроваджених у стандарті **802.11n**. Пристрої, що відповідають **802.11ac**, належать до класу **VHT (Very High Throughput)**, що характеризує їх надзвичайно високою пропускною здатністю. Мережі цього стандарту функціонують виключно у діапазоні **5 ГГц**, а ширина радіоканалу може складати **20, 40, 80 або 160 МГц**. Також передбачена можливість об'єднання двох каналів у конфігурації **80 + 80 МГц**.

IEEE 802.11e

Дозволяє розширити функціональні можливості стандарт IEEE 802.11a, IEEE 802.11b за допомогою використання методів забезпечення якості обслуговування (QoS).

IEEE 802.11f

Стандарт визначає правила взаємодії між рівноправними точками доступу, що є необхідним для побудови розподілених бездротових мереж передачі даних.

IEEE 802.11g

Стандарт 802.11g затверджений в червні 2003р являється удосконаленням специфікації після стандарту IEEE 802.11b та реалізує передачу даних в

аналогічному частотному діапазоні. Стандарт 802.11g встановлює додаткову техніку модуляції для частоти 2,4 ГГц.

Головною перевагою цього стандарту порівняно з іншими є висока пропускна здатність — до **54 Мбіт/с**, тоді як у **802.11b** вона становить лише **11 Мбіт/с**. Стандарт працює у діапазоні **2,4 ГГц**, як і **IEEE 802.11b**, проте для підвищення швидкості передачі даних застосовується та сама схема модуляції сигналу через **ортогональне частотне мультиплексування (OFDM)**, що використовується у **802.11a**.

Стандарт підтримує сумісність із попередньою версією **802.11b**. Адаптери **802.11b** можуть функціонувати у мережах **802.11g**, проте з максимальною швидкістю **11 Мбіт/с**, а адаптери **802.11g** можуть знижувати швидкість до **11 Мбіт/с**, щоб працювати у старих мережах **802.11b**.

Стандарт **802.11g** розрахований на забезпечення швидкості передачі даних до **54 Мбіт/с**.

IEEE 802.11h

У цьому стандарті рівні **MAC** і **PHY** доповнені алгоритмами **оптимального вибору частот**, які базуються на протоколах **DFS (Dynamic Frequency Selection)** та **TPC (Transmit Power Control)**, розроблених ETSI. Процедура динамічного регулювання потужності у **802.11h** передбачає її зміну залежно від рівня перешкод і автоматичний перехід на інший радіоканал у випадку, якщо збільшення потужності не забезпечує необхідне співвідношення сигнал/шум.

IEEE 802.11i

Стандарт який виправляє проблеми безпеки існуючі в областях протоколів шифрування та аутентифікації.

IEEE 802.11n

Стандарт 802.11n був заьверджений 11 вересня 2009 року Він збільшує швидкість передачі даних практично в 4 рази в порівнянні з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт / с), за умови використання в режимі 802.11n з іншими пристроями 802.11n. Максимальна теоретична швидкість передачі даних складає 600 Мбіт / с, застосовуючи передачу даних одразу за чотирма антенами. За однією антеною швидкість може сягати 150 Мбіт / с.

Пристрої 802.11n можуть функціонувати в частотних діапазонах 2,4 - 2,5 або 5,0 ГГц.

У стандарті **IEEE 802.11n**, як і в багатьох попередніх, використовується технологія **OFDM**. Більшість функцій запозичено зі стандарту **802.11a**, проте IEEE 802.11n підтримує застосування

як частотного діапазону стандарту 802.11a, так і діапазону, прийнятого для стандартів **802.11b/g**.

Отже, пристрої, сумісні зі стандартом **IEEE 802.11n**, можуть працювати в частотному діапазоні **5 ГГц** або **2,4 ГГц**, причому вибір конкретного діапазону залежить від регіональних вимог. Для **Росії та України** пристрої IEEE 802.11n повинні підтримувати **діапазон 2,4 ГГц**.

Для збільшення швидкості передачі в стандарті IEEE 802.11n використовується подвоєння ширини каналу з 20 до 40 МГц.

2.1.2 Стандарти для мережі WMAN

Розроблений Інститутом інженерів з електротехніки та електроніки (IEEE) стандарт 802.16 є стандартом розрахованим на впровадження в міських бездротових мережах технологій.

IEEE 802.16

Завданням 802.16 є забезпечення мережевого рівня між локальними мережами (IEEE 802.11) і регіональними мережами (WAN).

Короткі характеристики стандарту 802.16:

- Пропускна здатність до 135 Мбіт / с при смузі несучої 28 МГц. Модуляція OFDM - 64-QAM.
- Доступ до середовища адаптивний, динамічний.
- Управління мережею централізоване.
- Стандарт 802.16e призначений для мобільних систем. Безпека в мережі забезпечується на рівні протоколу 3-DES.

IEEE 802.16a

Технічні характеристики стандарту **802.16a** передбачають роботу обладнання в діапазоні **2–11 ГГц** і є розширеною версією стандарту **IEEE 802.16**, затвердженою в **грудні 2001 року**. Використання цього частотного діапазону дозволяє створювати канали передачі даних із високою пропускною

здатністю за допомогою передавачів, розташованих на щоглах стільникових мереж або високих будівлях. Оборудування, що працює за стандартом 802.16a, може здійснювати прийом і передачу сигналу лише **в зоні прямої видимості**.

Стандарт **802.16** забезпечує високу масштабованість, що дозволяє одній базовій станції обслуговувати сотні тисяч користувачів. Основні характеристики стандартів 802.16 наведено у таблиці 2.1. Крім того, сумісність обладнання, що працює за цим стандартом, дозволяє операторам зменшити витрати на кінцеві пристрої користувачів та одночасно використовувати обладнання різних виробників. Обслуговування клієнтів і управління мережею можуть здійснюватися дистанційно, що додатково знижує поточні витрати.

Таблиця 2.1

Характеристики стандартів 802.16, 802.16a та 802.16e

Назва стандарту	802.16	802.16a	802.16e
Рік впровадження	2001	2003	2004
Швидкодія	10-66 ГГц	2-11 ГГц	2-6 ГГц
Модуляція	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM
Ширина каналу	20, 25 та 28 МГц	1,5 – 20 МГц (Можна регулювати)	1,5 – 20 МГц (Можна регулювати)
Радіус дії	2-5 км	7-10 км	2-5 км
Умови для роботи	Пряма видимість	Робота на відображеннях	Робота на відображеннях

Серед інших переваг стандарту можна відзначити широку зону покриття та високу швидкість передачі даних.

2.2 Методи захисту інформації

Для розглядання методів захисту інформації обрано мережі стандарту 802.11, як найбільш поширені і вразливі до атак. У стандарті **802.11** середовище передавання даних є бездротовим і має певні просторові межі, в яких сигнал може прийматися клієнтським обладнанням. Виходячи з цього, можна стверджувати, що зловмисник отримує можливість несанкціонованого доступу до мережі у разі перебування в зоні покриття її радіосигналу. Аналізуючи потенційні шляхи проникнення, доцільно виділити кілька способів, за допомогою яких можна обмежити зону поширення радіосигналу. У межах зони поширення сигналу можливо застосувати фізичну охорону або огородження, що здатне знизити ризик несанкціонованого доступу до мережі. Такий підхід може ускладнити виявлення мережі сторонніми особами, однак у разі цілеспрямованої атаки використання охоронної зони не забезпечує повного захисту. Додатковим способом є екранування будівлі за допомогою металевої сітки в стінах, що значно послаблює рівень радіосигналу [1]. У такому випадку користувачі можуть безперешкодно працювати з мережевими ресурсами всередині приміщення, не зазнаючи погіршення якості зв'язку.

Також, як один із способів захисту мережі можна виділити приховування імені точки доступу, хоча одним із головних недоліків цього методу захисту є той факт, що мережу приховати можна а її користувачів ні. Тож під час сканування сучасним програмним забезпеченням таку мережу можна буде досить просто ідентифікувати.

Одним із найбільш ефективних способів підвищення безпеки мережі є фільтрація за **MAC-адресами**. Оскільки кожен бездротовий адаптер має унікальний ідентифікатор, під час підключення до точки доступу адміністратор повинен додати відповідну MAC-адресу до спеціального списку дозволених пристроїв. Сформований перелік зберігається безпосередньо на точці доступу та за потреби може редагуватися адміністратором мережі. Під час підключення будь-якого клієнта точка доступу перевіряє унікальний фізичний ідентифікатор пристрою. Якщо ця інформація збігається з записами в таблиці дозволених **MAC-адрес**, пристрою надається доступ до мережі, у протилежному випадку запит на підключення ігнорується. Недоліком такого механізму є те, що на сучасних бездротових адаптерах MAC-адресу можна змінити програмними засобами. Крім того, використовуючи спеціальне програмне забезпечення, зловмисник може аналізувати радіоефір та ідентифікувати окремих користувачів мережі.

Зазначені методи не здатні забезпечити конфіденційність даних, що передаються в мережі, оскільки вони лише обмежують доступ до неї. Для підвищення рівня захисту застосовують використання складних, належним чином налаштованих паролів, а також додаткові технології безпеки та механізми шифрування.

Одним із найважливіших моментів захисту бездротової мережі також являється пильне відношення адміністраторів мережі до методів і технологій захисту мережі, до паролів які встановлюються для підключення користувачів.

2.3 Технології захисту даних

Серед основних технологій захисту бездротових мереж можна виділити шифрування даних. Існує декілька технологій, які використовують алгоритми шифрування для захисту бездротових мереж - WEP, WPA, WPA2, VPN [3]. Опис технологій можна побачити у таблиці 2.2

Технологія WEP (Wired Equivalent Privacy) належить до методів захисту бездротових мереж і базується на застосуванні алгоритму шифрування RC4 із фіксованим секретним ключем та змінним вектором ініціалізації. Під час функціонування мережі частина ключа, що відповідає за ініціалізацію, періодично оновлюється. Основним недоліком WEP є те, що вектор ініціалізації з часом починає повторюватися, а аналіз інтервалів таких повторень дає змогу зловмиснику відновити іншу частину ключа шифрування.

Технологія **WPA (Wi-Fi Protected Access)** також використовує алгоритм **RC4**, але на відміну від WEP ключі змінюються динамічно. Завдяки подовженому вектору ініціалізації та можливості застосування криптографічної контрольної суми для перевірки цілісності пакетів, WPA є значно надійнішою за WEP. Крім того, WPA дозволяє обирати методи шифрування **TKIP** або **AES**, що додатково підвищує безпеку передачі даних.

У WPA виділяють два основні режими роботи: **WPA-PSK** та **WPA-Enterprise**. Режим **WPA-PSK** підходить для персонального використання: на точці доступу задається ключ доступу, який користувач вводить для підключення до мережі. Для адміністрування мережі з великою кількістю користувачів доцільніше застосовувати **WPA-Enterprise**, де аутентифікація здійснюється через зовнішній сервер, незалежний від точки доступу. У цьому випадку кожен користувач під час підключення вводить **унікальну комбінацію логіна та пароля**, що підвищує безпеку мережі.

Технологія WPA2 є протоколом, що входить до стандарту безпеки бездротових мереж **802.11i**. Як і WPA, WPA2 підтримує два режими аутентифікації: **персональний (Personal)** та **корпоративний (Enterprise)**. У персональному режимі з введеної парольної фрази генерується **256-розрядний ключ (Pre-Shared Key, PSK)**. Ідентифікатор ключа (**Service Set Identifier, SSID**) та сам PSK використовуються для формування тимчасових сеансових ключів (**Pairwise Transient Key, PTK**), що забезпечують підключення до мережі та взаємодію між бездротовими пристроями. Недоліком цієї технології є необхідність розподілу та підтримки ключів на всіх бездротових пристроях мережі. У корпоративних мережах оптимальним варіантом є **WPA2-Enterprise**, який працює за схожим принципом із попередніми технологіями, використовуючи віддалений сервер для аутентифікації користувачів мережі.

Технологія WPA3. Wi-Fi Alliance оголосив про закінчення розробки нового стандарту безпеки -WPA3, це сталося 27 червня 2018 року. Нововведенням WPA3 зазначається підтримка PMF (Protected Management Frames) для контролю цілісності трафіку. У майбутньому підтримка PMF повинна стати обов'язковою і для WPA2. WPA3 включає програми Wi-Fi Easy Connect і Wi-Fi Enhanced Open. Wi-Fi Easy Connect і дозволяє реалізувати спрощену настройку пристроїв без екрану. Для цього можна використовувати інший пристрій вже підключений до бездротової мережі.

Ще одна особливість технології полягає у використанні Wi-Fi Easy Connect – тобто у можливості заміни точки доступу без необхідності перенастроювати всі пристрої. Wi-Fi Enhanced Open – ще одна технологія яку пропонує WPA3 має реалізувати шифрування всіх потоків даних між клієнтом і точкою доступу. Ця технологія дозволить захистити приватність користувача в публічних мережах, де не потрібна аутентифікація. Для генерації ключів в таких мережах має бути застосований процес узгодження з'єднання, що реалізовується розширенням Opportunistic Wireless Encryption(OWE).

Подібно до WPA2, **WPA3** підтримує два режими роботи: **Personal** та **Enterprise**. У режимі **WPA3-Personal** передбачено простий вибір пароля, щоб користувачам було легше його запам'ятати, при цьому забезпечується високий рівень безпеки: навіть якщо пароль буде зламано, збережені дані та трафік мережі залишаються захищеними. Режим **WPA3-Enterprise** передбачає шифрування із застосуванням **ключів довжиною не менше 192 біт**, що забезпечує підвищений рівень безпеки для корпоративних мереж.

Таблиця 2.2

Технології захисту даних в бездротових мережах

Технології захисту даних	Шифрування	Ключі
WEP	RC4	Статичний ключ з динамічним вектором ініціалізації
WPA	RC4	Ключі, що динамічно змінюються
WPA2	AES	Ключі, що

		динамічно змінюються
WPA3	WPA3-PSK -128 бітне шифрування і Suite B – 192 бітне OWE	Ключі, що динамічно змінюються
VPN	DES, Triple DES, AES, MD5.	Ключі, що динамічно змінюються

Технологія **VPN (Virtual Private Network)** є ефективним засобом додаткового захисту бездротових мереж. Вона дозволяє створювати віртуальні приватні мережі всередині однієї або декількох існуючих мереж. VPN забезпечує конфіденційність користувачів завдяки шифруванню даних і маскуванню IP-адрес. Деякі сервіси також надають власну систему доменних імен, що дозволяє користувачам вводити зручні назви сайтів замість довгих IP-адрес. Комплекс захисних функцій VPN створює надійний додатковий рівень безпеки для мережі.

Принцип роботи VPN полягає у створенні захищеного «тунелю» між користувачем і сервером. Для шифрування передаваного трафіку VPN застосовує такі протоколи, як **IPSec, PPTP та L2TP**, а також алгоритми шифрування **DES, Triple DES, AES** та хешування **MD5**. Технологія **VPN** зазвичай застосовується у великих корпоративних мережах, проте вона також може бути корисною для домашнього використання. Завдяки високій надійності та сумісності з різними платформами, такими як **Windows, Linux та Mac OS**, VPN може служити додатковим засобом захисту в будь-якій мережі та ефективно поєднуватися з іншими технологіями безпеки бездротових мереж.

Також для того щоб мінімізувати ризики втручання або злому для бездротової мережі у якості захисту можна використовувати:

Заміна паролів за замовчуванням. Більшість мережевих пристроїв, включаючи бездротові точки доступу, постачаються з попередньо встановленими паролями для спрощення налаштування. Однак такі паролі легко знайти в Інтернеті, тому вони забезпечують лише мінімальний рівень захисту. Зміна паролів на складні та їх періодичне оновлення значно ускладнює доступ зловмисників і є першою лінією захисту мережевого пристрою.

Обмеження доступу. Дозвіл доступу до мережі лише авторизованим користувачам є гарною ланкою захисту. Кожна апаратна частина, підключена до мережі, має адресу контролю доступу до медіа (MAC). Можна обмежити доступ до мережі, відфільтрувавши MAC-адреси. Також для надання доступу користувачам у мережі можна використовувати обліковими записами "гість", які

широко використовується у багатьох бездротових маршрутизаторах. Ця функція дозволяє надати гостям бездротовий доступ на окремому бездротовому каналі з окремим паролем, зберігаючи конфіденційність основних даних.

Шифрування даних у бездротовій мережі. Шифрування переданих даних запобігає їх перегляду будь-якими сторонніми особами, які можуть отримати доступ до мережі. Для цього застосовуються різні протоколи шифрування. Наприклад, бездротовий захищений доступ Wi-Fi (WPA) може використовувати протоколи WPA, WPA2 або WPA3. На сьогодні WPA3 вважається найнадійнішим методом шифрування. Хоча WPA і WPA2 досі підтримуються, бажано використовувати обладнання з підтримкою WPA3 або WPA2 у поєднанні з додатковими засобами захисту, наприклад, фаєрволом, оскільки застарілі протоколи можуть залишати мережу вразливою до атак.

Захист ідентифікатору набору послуг (SSID). Щоб сторонні особи не могли легко отримати доступ до мережі, необхідно уникати оприлюднення SSID. Усі маршрутизатори Wi-Fi дозволяють користувачам захищати SSID свого пристрою, що ускладнює пошук зловмисників мережі. Принаймні, можлива заміна SSID на щось унікальне. Залишення за замовчуванням виробника може дозволити потенційному зловмисникові визначити тип маршрутизатора та, можливо, використати будь-які відомі вразливості.

Встановлення брандмауера є ефективним засобом захисту бездротової мережі. Брандмауер може бути встановлений **безпосередньо на пристроях** (хостовий брандмауер) або у **домашній мережі** (брандмауер на маршрутизаторі чи модемі). Якщо зловмиснику вдасться підключитися до мережі, мережевий брандмауер може бути обійдений, тоді як хостовий брандмауер забезпечує додатковий рівень захисту безпосередньо на пристрої, оберігаючи дані користувача.

Підтримка антивірусного програмного забезпечення. Встановлення антивірусного програмне забезпечення та постійно оновлення не тільки допоможе у визначення вірусів, а й у аналізі підозрілих отриманих пакетів по трафіку мережі. Також деякі антивіруси мають функцію попередження про небезпечні веб ресурси, що також корисно. Багато антивірусних програм також мають додаткові функції, які виявляють або захищають від шпигунське та рекламного ПЗ.

Використовування обміну файлами з обережністю. Спільний доступ до файлів між пристроями слід вимкнути, коли це не потрібно. Доступ до файлів

завжди має бути дозволеним лише лише в домашніх або робочих мережах, ніколи в загальнодоступних мережах. Можливим є створення спеціального каталогу для обміну файлами та обмеження доступ до всіх інших каталогів. Крім того треба захищати паролем все що можливо.

Слідкування за оновленням програмного забезпечення точки доступу. Виробник бездротової точки доступу періодично видає оновлення та виправлення програмного забезпечення та мікропрограми пристрою. Обов'язковим є перевірка веб-сайту виробника на наявність оновлень або виправлень для мережевого ристрою.

Для підвищення безпеки бездротової мережі слід звернутися до ресурсів провайдера Інтернету або виробника маршрутизатора. Вони можуть надати рекомендації та інструкції щодо захисту мережі. Крім того, корисно перевіряти **розділи підтримки клієнтів на веб-сайтах**, де можна знайти конкретні поради, пропозиції або детальні керівництва з налаштування безпеки.

Використання віртуальної приватної мережі (VPN) є ефективним методом захисту даних. Багато компаній і організацій застосовують VPN, щоб співробітники могли безпечно підключатися до корпоративної мережі з будь-якого місця поза офісом. VPN шифрує з'єднання на кінцях передачі та отримання даних і захищає трафік, який в іншому випадку міг би бути вразливим. Таким чином, VPN може служити додатковим засобом безпеки для будь-якої мережі.

Висновок за розділом 2

Оцінюючи можливості проникнення до мережі можна виділити декілька способів, якими можна обмежити поширення радіосигналу і захистити мережу – це обмеження території у межах якої діє мережа та екранування стін будівель. Разом із обмеженням поширення радіосигналу є доцільним використання фільтрації по MAC ідентифікаторам.

Зазначені методи обмежують доступ до мережі, але не гарантують конфіденційності передаваних даних. Для підвищення рівня захисту застосовують **складні, правильно налаштовані паролі** та додаткові технології безпеки. Серед алгоритмів шифрування, що використовуються для захисту бездротових мереж, виділяють **WEP, WPA, WPA2 та VPN**, кожен із яких забезпечує різний рівень безпеки та конфіденційності даних.

Аналіз технологій захисту бездротових мереж показав, що найвищу стійкість забезпечує **WPA2**, тоді як **WEP** та **WPA** не гарантують надійного захисту. Оптимальним рішенням для користувачів будь-якої мережі є поєднання протоколу **WPA2** з технологією **Virtual Private Network (VPN)**. Водночас рівень безпеки мережі значною мірою залежить від її адміністрування: надійності та регулярної зміни паролів, а також від відповідальної поведінки користувачів, які не повинні нехтувати заходами безпеки.

Оцінюючи принципи роботи бездротових мереж, аналізуючи їх вразливості та можливості проведення атак на них можна зробити висновок що захист бездротових мереж є доволі недосконалим і важливим є розробка нових методик захисту та вдосконалення існуючих технологій. Також обізнане використання існуючих методів і технологій захисту може мінімізувати вплив на слабкі місця бездротових мереж.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ПРОГРАМНИХ ЗАСТОСУНКІВ ЗАХИСТУ ІНФОРМАЦІЇ ЩО ПЕРЕДАЄТЬСЯ

3.1 Опис ключових характеристик програмного забезпечення

Базуючись на попередніх аналізах вразливостей бездротових середовищ і недосконалості існуючих методів захисту можна стверджувати що бездротові мережі потребують у додаткових механізмах захисту. У наслідок проведеного аналізу було розроблено програмне забезпечення на базі антисніферу для моніторингу стану мережі і пошуку підозрілого трафіку. У процесі розробки програмного забезпечення було використано програмну мову C# та графічну підсистему для створення користувацького інтерфейсу WPF (Windows Presentation Foundation).

Програмне забезпечення зібрало в собі декілька функцій для захисту інформації в бездротових мережах, а саме:

- Збирання інформації про всі доступні точки доступу
- Збирання інформації про підключену точку доступу
- Аналіз трафіку та додавання його до бази програмного забезпечення
- Оповіщення користувача про підозрілий трафік

Ціль програмного забезпечення в покращенні зручності адміністрування мережі за допомогою можливості сканування мережі і дослідження підозрілого або не звичного трафіку у мережі.

Програмне забезпечення працює майже як і більшість аналізаторів мереж Wi-Fi, у ньому як і у звичайних аналізаторах мереж обирається бездротовий спектр для дослідження, наприклад 2,4 ГГц або 5 ГГц і потім досліджується цей спектр, щоб переглянути мережі, їх канали та потужність сигналу.

Простіше кажучи, аналізатор Wi-Fi збирає інформацію про точки доступу та канали у вашій мережі та відображає її легко зрозумілим, візуально доступним способом. У розробленій програмі реалізований зручний користувацький інтерфейс який спрощує процес аналізу мережі (рис.3.1).

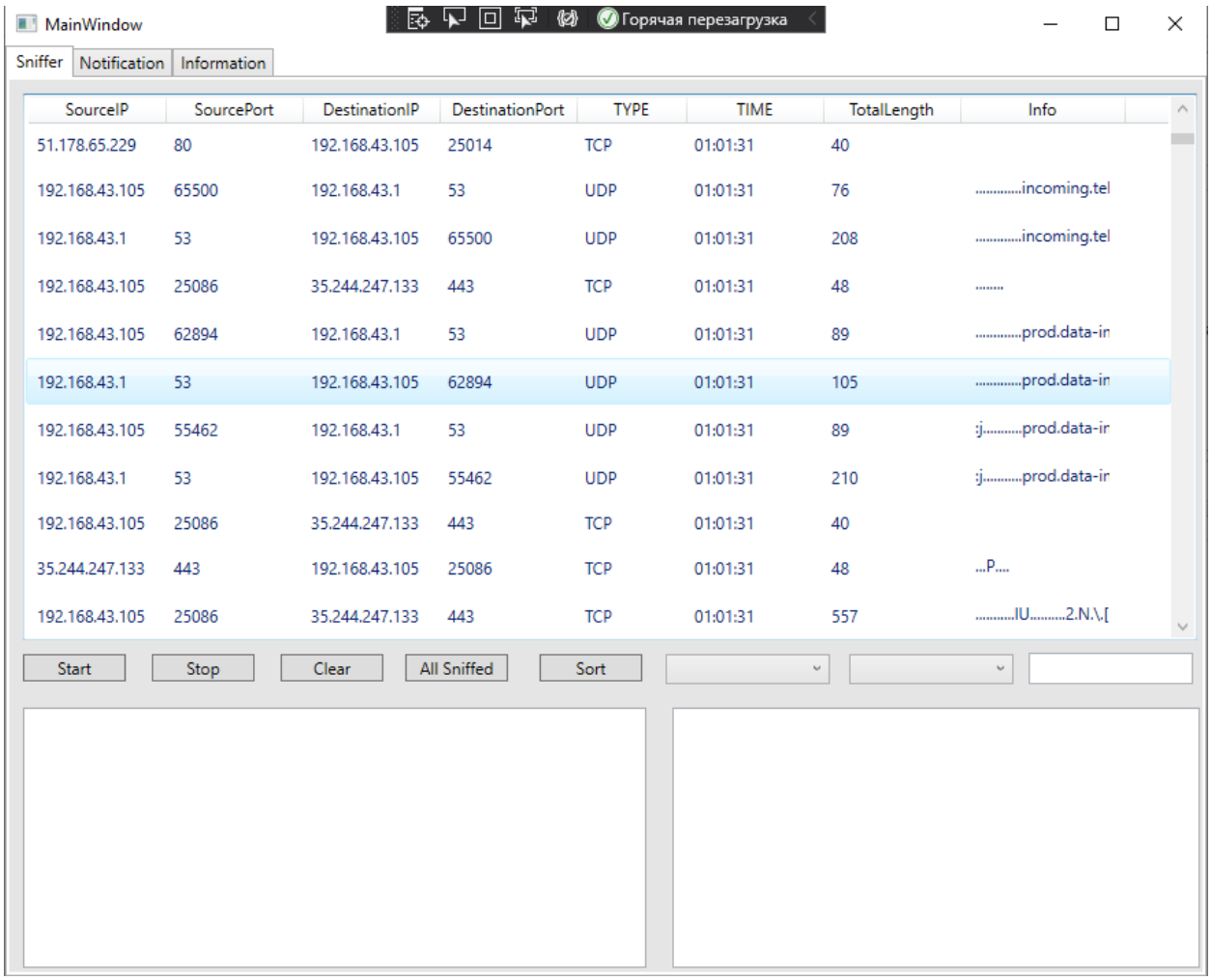


Рисунок 3.1 – Інтерфейс програмного забезпечення

Разом із функціями аналізатору мережі програмне забезпечення підтримує можливість аналізу трафіку, який передається у мережі. За допомогою подібного трафіку можна виділити дані IP адрес, пакети що передаються та порти, якими передано ту чи іншу інформацію.

Аналізатор бездротової мережі може допомогти підтримувати якість з’єднання, що може бути важливим моментом для підняття показників продуктивності у мережі. Сигнали Wi-Fi постійно змінюються, і незначні зміни в мережі можуть мати значний вплив на загальну тривалість роботи з’єднання.

Використання мережевого аналізатора Wi-Fi допомагає збирати дані та виявляти проблеми або вказувати на потенційні рішення, такі як перехід на інший канал для зменшення перевантажень.

3.2 Головні функції програмного забезпечення

Дослідження мережевого трафіку, що проходить через програмні засоби, надає можливість:

- **Виявляти небажаний трафік**, зокрема вірусний, паразитний або зациклений, який призводить до перевантаження мережевого обладнання та каналів передавання даних;
- **Виявляти шкідливе та несанкціоноване програмне забезпечення** у мережі, зокрема мережеві сканери, флуд-утиліти, троянські програми, клієнти p2p-мереж та інші подібні загрози;
- **Здійснювати перехоплення користувацького трафіку**, особливо незашифрованого, а в окремих випадках і зашифрованого, з метою отримання облікових даних, паролів та іншої конфіденційної інформації;
- **Оперативно виявляти й локалізувати проблеми в роботі мережі**, зокрема збої або помилки в налаштуваннях мережних агентів, що часто використовується системними адміністраторами під час діагностики та обслуговування мереж.

Дослідження стану мережі у програмному забезпеченні було розроблено на базі алгоритмів сніферів. До нього входить збір даних про інформацію яка передається у мережі, вивід інформації про всі доступні точки доступу у мережі, вибір протоколу передачі, яким інформація передається та вивід інформації щодо портів і пакетів даних які були відправлені або отримані. Схема роботи програмного забезпечення зображена на Рисунку 3.2.

У програмному забезпеченні реалізовано такі функції:

- вивід кількості отриманих пакетів;
- вивід інформації в середині пакетів;
- можливість сортування пакетів за протоколом, IP адресою та портом;
- можливість отримання інформації всередині переданих пакетів даних;
- вивід інформацію про кількість пакетів надісланих з певної адреси за короткий проміжок часу;
- вивід отриманої інформації щодо реєстрованих даних о власниках мережі за допомогою команди WHOIS;
- вивід інформації про мережі навколо;
- вивід поширеної інформації про мережу, до якої підключено пристрій;
- інформування користувача мережі про не звичний для неї трафік.

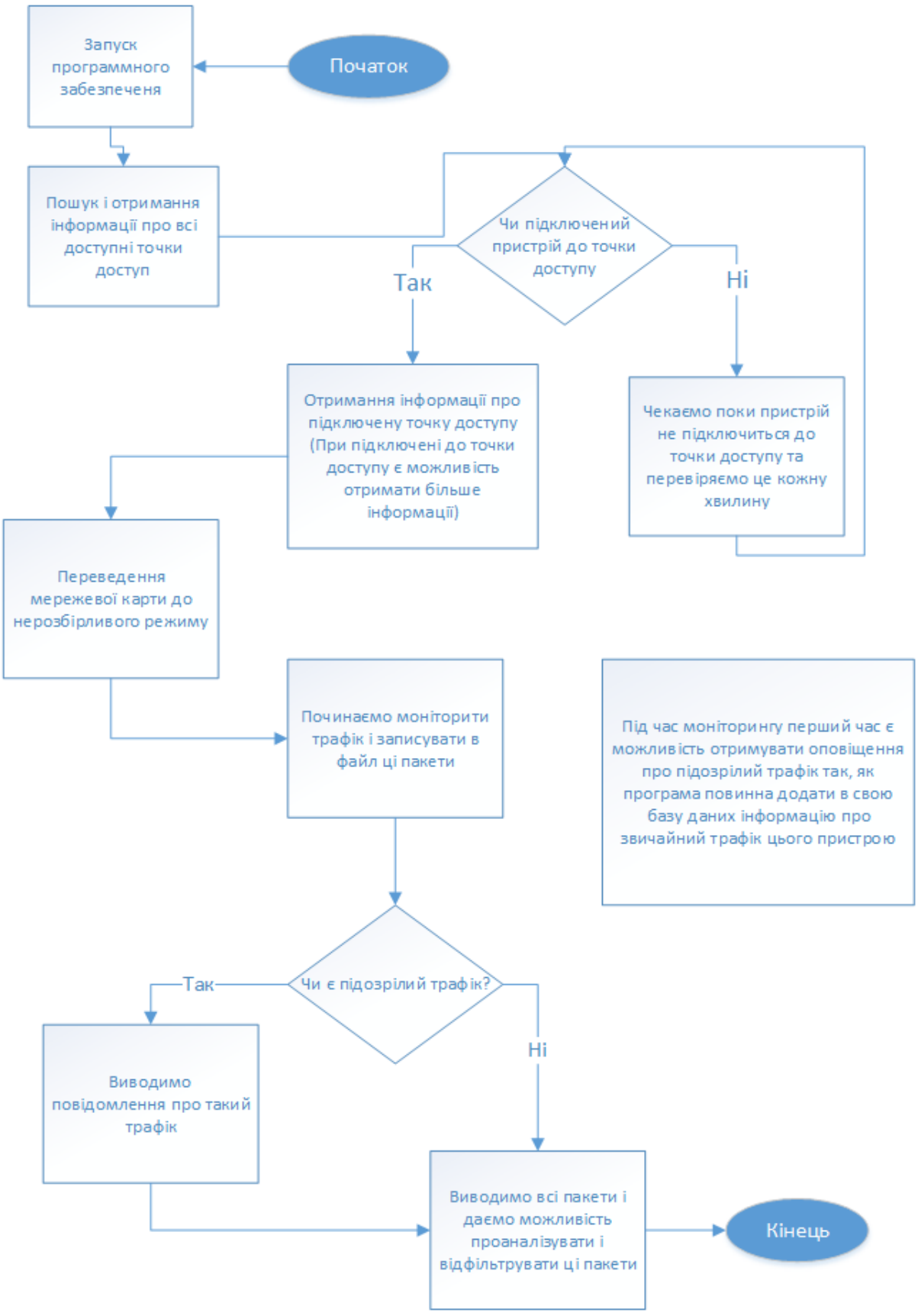


Рисунок 3.2 – Схема роботи програмного забезпечення

Вивід кількості просканованих пакетів вспливає спеціальним повідомленням після закінчення сканування (рис.3.3). Закінчити або тимчасово

зупинити роботу сканування можна за допомогою кнопки «Stop», а розпочати або продовжити роботу програми можна відповідно за допомогою кнопки «Start». Якщо є необхідність очистити список просканованої мережі у програмному забезпеченні то зробити це можна за допомогою кнопки «Clear».

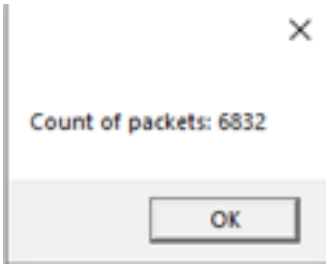


Рисунок 3.3 – Повідомлення про кількість отриманих пакетів за певний проміжок часу

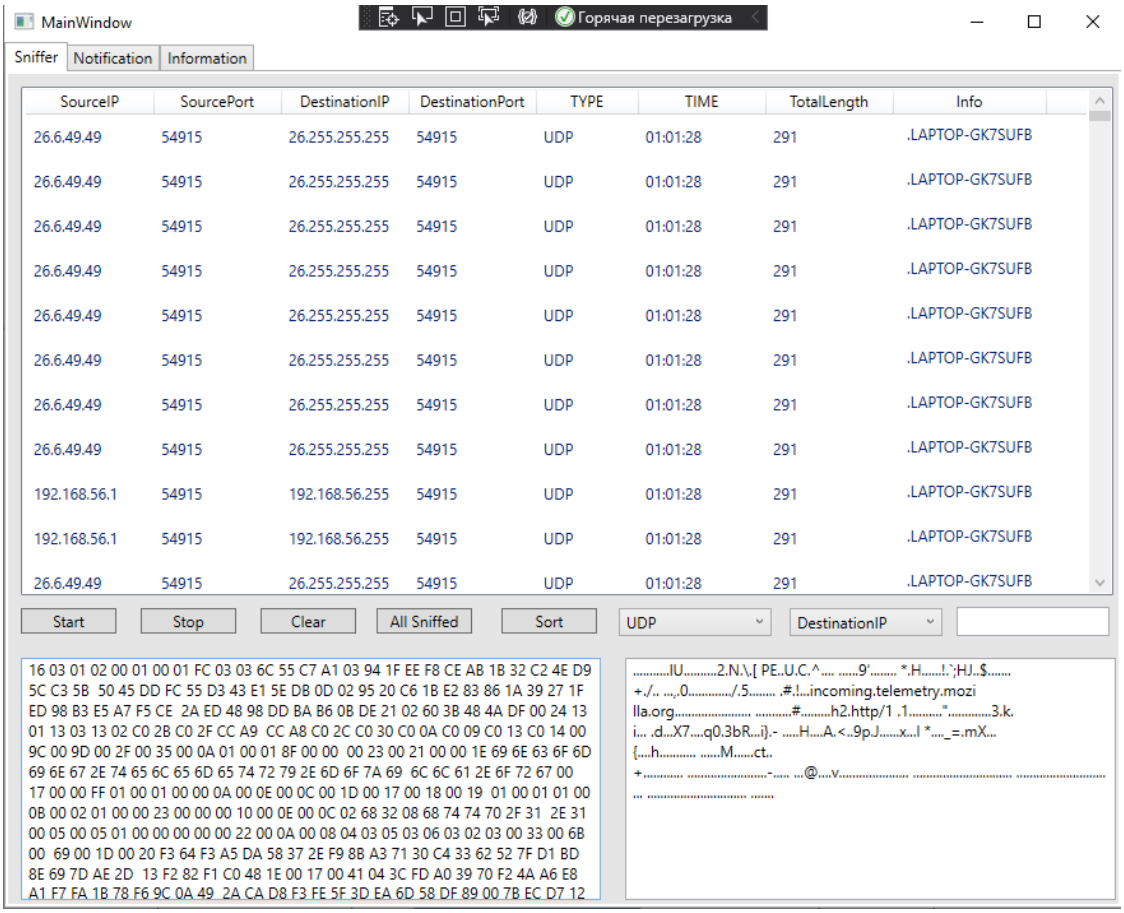


Рисунок 3.4 – Сортування отриманих пакетів за протоколом UDP

Також у програмному забезпеченні реалізована можливість сортування пакетів за протоколами передачі. На рисунку 3.4 зображено відсортировані пакети, які передавались за допомогою UDP.

Програмне забезпечення реалізує механізм сортування за такими протоколами: TCP, UDP, GGP, ICMP, IDP, IGMP, IP, ND, PUP, OTHERS. Механізм сортування зображено на рисунку 3.5.

Також являється можливим сортування за IP адресою та портом. Механізм сортування відбувається при виборі з випливаючого вікна протоколів потрібного для сортування і натисканні кнопки «Sort» або при вводі IP адреси у стрічку вводу, якщо потребується сортування за певною адресою.

Кнопка «All sniffed» повертає назад проаналізований початковий трафік, тож при необхідності можна повернутися до повного списку захопленого програмним забезпеченням трафіку.

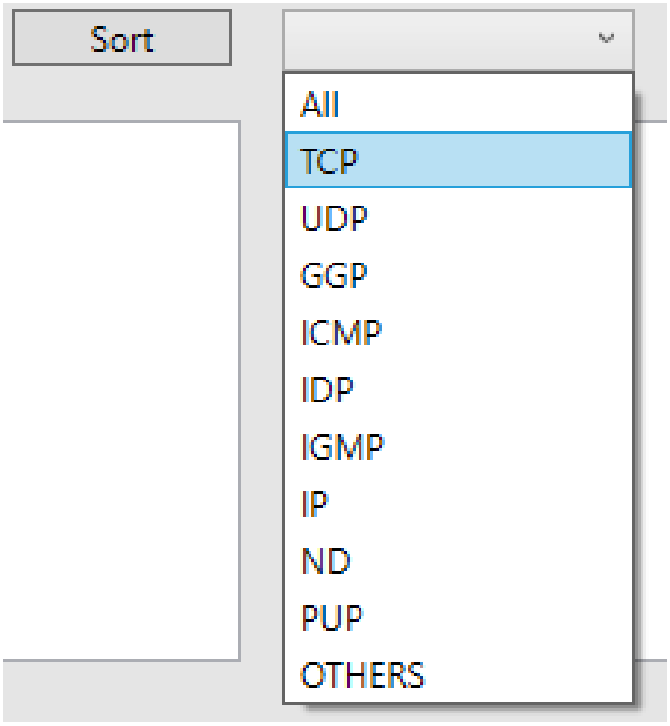


Рисунок 3.5 – Сортування трафіку за протоколами

Програма підтримує функцію отримання інформації щодо реєстрованих даних про власників мережі за допомогою команди WHOIS і реалізується при виборі певної IP адреси і натисканні кнопки «WHOIS» відповідно (рис.3.6.). Дана функція може бути використана для запитів баз даних для визначення доменної

зони, IP адреси або автономного системного номеру у глобальній мережі Інтернет.

У програмному забезпеченні також є функція вираховування кількості пакетів, що були відправлені з певної адреси. Вона допомогає оцінитити небезпечний трафік, який як раз може бути спрямований на перенасичення мережі великою кількістю пакетів у малий проміжок часу. Подібний небезпечний трафік може не тільки сповільнити роботу мережі, а і спровокувати відмову роботи мережі. Отже аналіз кількості отриманих пакетів може попередити адміністратора мережі про можливу загрозу або атаку яка реалізується.

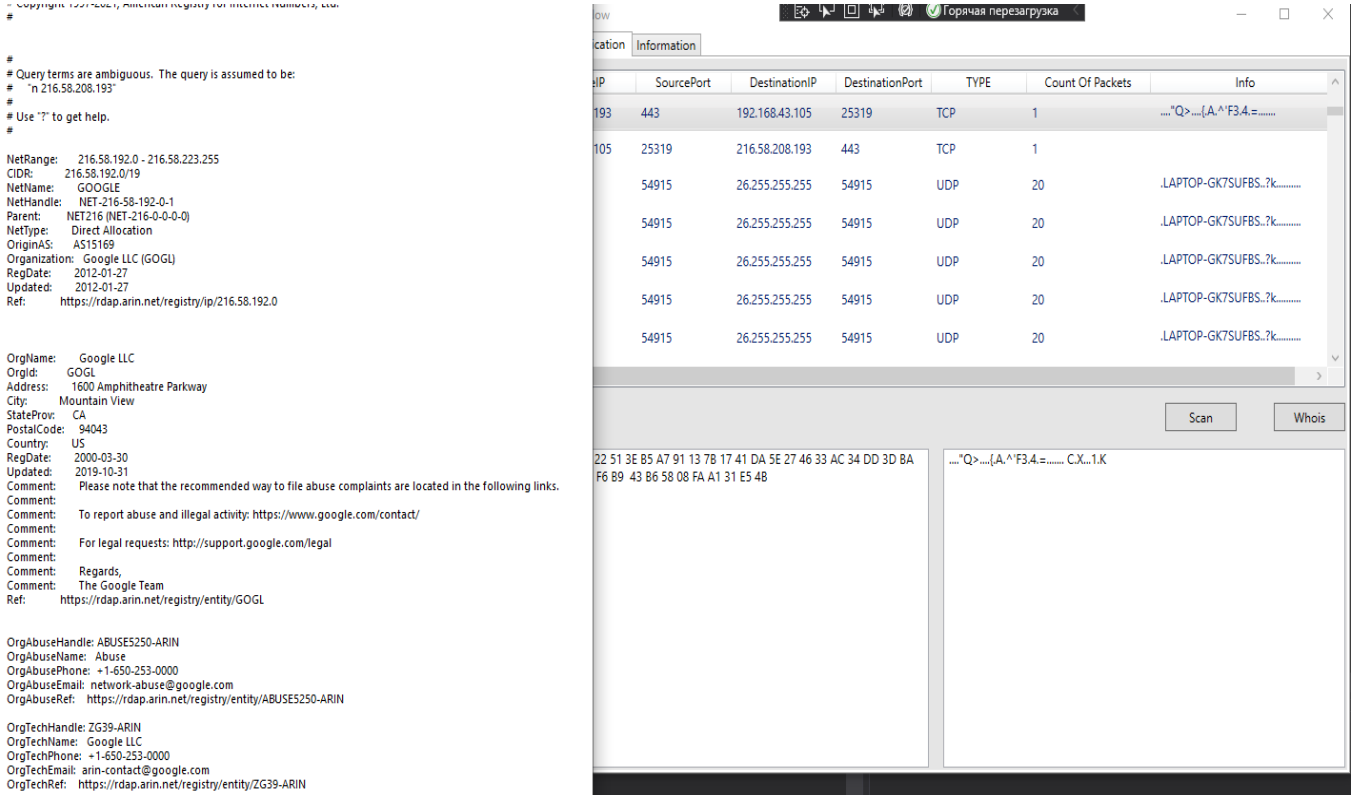


Рисунок 3.6 – Отримання інформації щодо реєстрованих даних про власників мережі за допомогою команди WHOIS

Важливою частиною розробки програмного забезпечення також була можливість аналізу інформації про найближчі точки доступу та про підключену точку доступу. Мережа, яку було просканово мала назву «Weirana». Результат отриманий під час сканування можна побачити на рисунку 3.7.

Сканування мережі дало змогу дізнатися такі характеристики мережі:

- Аутентифікація: RSNA_PSK;
- Шифрування: CCMP;
- Тип мережі: Infrastructure;
- BSSID 1: A:C5:E1:D7:F2:CE;
- Сигнал: 100;
- Частота: 2,462 GHz;
- Тип функції: Wireless80211;
- Канал: 11;
- Базова частота (MBit/s): 11;
- Інші частоти (MBit/s): 1 2 5,5 11 18 24 36 54 6 9 12 48.

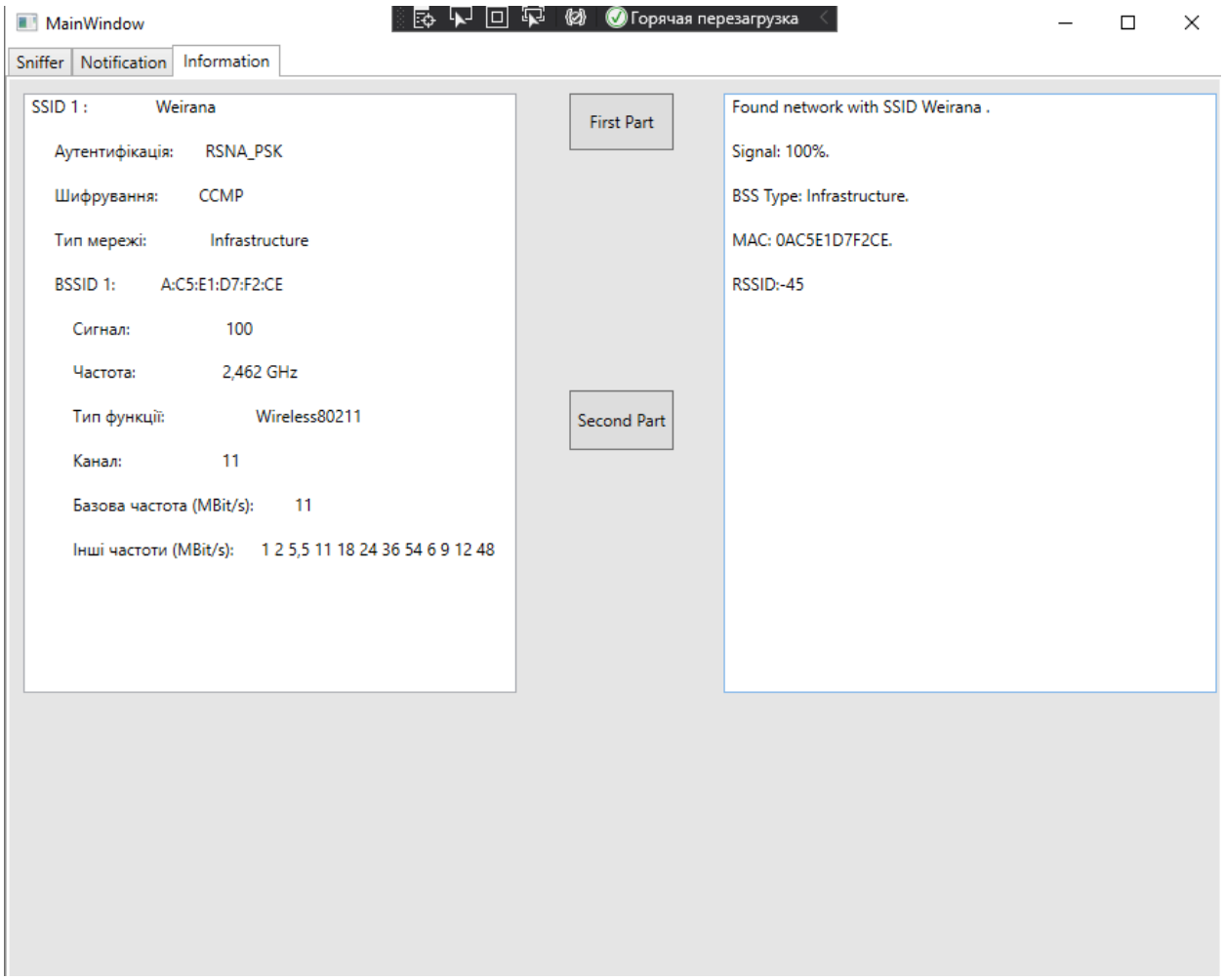


Рисунок 3.7 – Отримання інформації про власну і оточуючі мережі.

Повідомлення про підозрілий трафік у мережі також є невід'ємною частиною програмного забезпечення. При визначенні подібного програмне забезпечення відкриває вікно, щоб повідомити користувача мережі для того щоб він міг приділити увагу до ситуації (рис.3.8).

Підозрілим трафіком програмне забезпечення вважає нові IP адреси і трафік, який з ними пов'язаний. Попередньо програма шукає інформацію у базі даних щодо IP і надісланих з неї пакетів інформації.

На початку старту роботи програми буде дуже багато не звичного трафіку, але з поширенням бази даних програма зможе чіткіше формулювати список підозрілого трафіку. Цю функцію можна вдосконалювати у майбутньому наприклад додавши нейронну мережу, яка буде навчатись розпізнавати такий трафік, порівнювати його з локальною базою даних та відслідковувати загрози мережевого середовища звіряючи отримані данні з мережі з глобальними базами загроз і шкідливого програмного забезпечення.

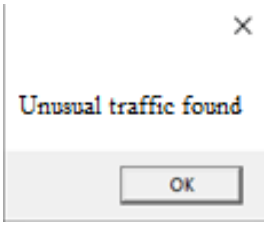


Рисунок 3.8 – Повідомлення про незвичний трафік

Також не звичним трафіком програмне забезпечення вважає велику кількість трафіку що може надсилатися з певних адрес. Тобто якщо програма аналізує те, що більша частина трафіку тобто більше половини трафіку за деякий невеликий проміжок часу була надіслана з одної адреси, то ця адреса потрапить у список підозрілого трафіку. Це може попередити адміністратора мережі про можливість атаки відмови в обслуговуванні. У наслідок адміністратор мережі може не тільки просканувати власну мережу, але й відслідкувати не звичний для цієї мережі трафік і при пильному користуванні програмним забезпеченням у наслідок мінімізувати ризики втручання у мережу при необхідності.

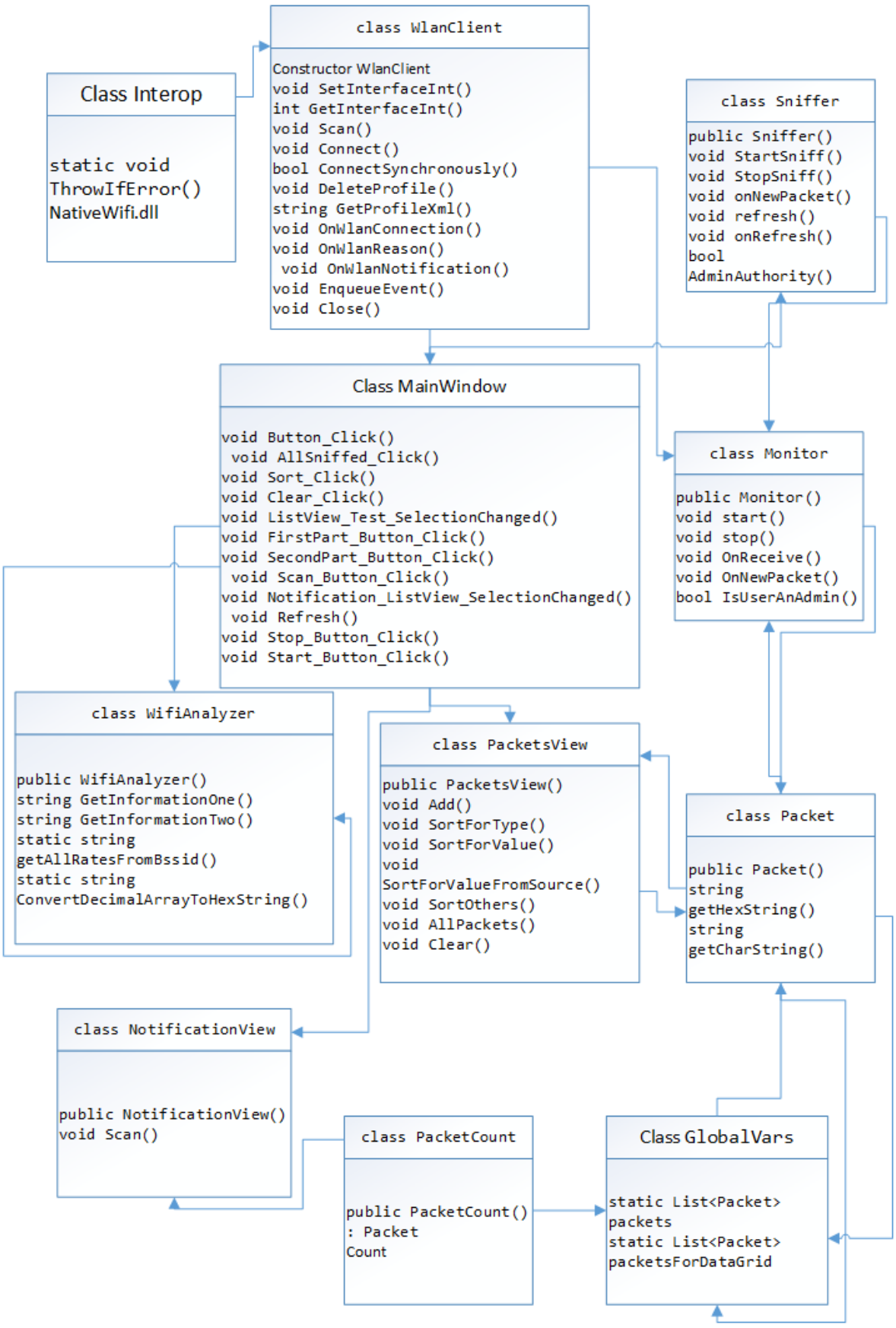


Рисунок 3.9 – Схема класів програмного забезпечення

Програма має 11 основних класів для виконання: Main window, Sniffer, Monitor, Wifi analyzer, Packets View, Packet Count and Global vars (рис.3.9).

Функції сканування мережі, аналіз пакетів і трафіку використовуються завдяки класам Sniffer, Monitor, Packets View, Packet Count аналіз мережі, до якої підключено пристрій реалізовано у класі Wifi analyzer. Інші класи являють собою по більшій частині допоміжну функцію для правильної роботи програми.

Програмне забезпечення на базі антисніферу є корисним застосунком для досвідчених користувачів мережі, які бажають підкращити можливості власної мережі за допомогою аналізатору мереж. Також програмне забезпечення може бути використано в покращенні зручності адміністрування мережі за допомогою можливості сканування мережі і дослідження підозрілого або не звичного трафіку у мережі.

Можливості програмного забезпечення можуть бути використані для наукових цілей. Також можливим є варіант вдосконалення програми у подальшому.

Оцінивши існуючі програми захисту бездротових мереж під час створення програмного забезпечення можна сказати що у програми є майбутне в плані розвитку роботи з нейромережами і машинним навчанням. Ця функція може значно покращити функції аналізатору трафіку за допомогою глобальних баз даних загроз, які можуть використовуватись для пошуку пакетів із зловмисним трафіком і безперечно такий аналіз покращить захищеність бездротових мереж.

Висновок за розділом 3

У результаті аналізу роботи бездротових мереж, їх вразливостей і дослідження методів і технологій захисту бездротових мереж було розроблено програмне забезпечення яке виконує функції моніторингу з аналізом трафіку бездротової мережі, протоколів передачі у мережі. Також програмним забезпеченням виконується аналіз підозрілого трафіку у мережі.

У процесі розробки програмного забезпечення було використано програмну мову C# та графічну підсистему для створення користувацького інтерфейсу WPF (Windows Presentation Foundation).

Розроблене програмне забезпечення зібрало в собі такі функції для захисту інформації в бездротових мережах, а саме

- Збирання інформації про всі доступні точки доступу
- Збирання інформації про підключену точку доступу
- Аналіз трафіку та додавання його до бази програмного забезпечення
- Оповіщення користувача про підозрілий трафік

Програмне забезпечення на базі антисніферу може стати застосунком для досвідчених користувачів мережі, які бажають підкращити можливості власної мережі за допомогою аналізатору мереж. Також програмне забезпечення може бути використано в покращенні зручності адміністрування мережі за допомогою можливості сканування мережі і дослідження підозрілого або не звичного трафіку у мережі.

4. ВДОСКОНАЛЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖАХ IEEE 802.11 ЗА ДОПОМОГОЮ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

4.1. Специфіка MAC адрес в мережах Wi-Fi

У початковій версії стандарту IEEE 802.11 не передбачалося жодних протоколів для забезпечення бездротової безпеки. Одним із способів контролю доступу була фільтрація пристроїв за MAC-адресами. Хоча виробники мережевого обладнання постійно впроваджують нові механізми захисту, на сьогодні немає рішень, які б повністю гарантували безпеку мережі та її користувачів. Кожен пристрій, сумісний зі стандартами сімейства IEEE 802.1x, оснащений унікальним ідентифікатором, який надається виробником.

Такі ідентифікатори зручно застосовувати для контролю доступу клієнтських пристроїв до мережі. Якщо активовано фільтрацію за MAC-адресами, підключення дозволяється лише тим клієнтам, чиї MAC-адреси внесені до переліку дозволених. Разом з тим, зловмисники мають у своєму розпорядженні засоби, що дають змогу обходити механізм MAC-фільтрації, а факт підміни MAC-адреси зазвичай виявляється лише під час проведення розслідувань.

Як зазначалося раніше, за замовчуванням кожен Wi-Fi клієнтський пристрій зберігає інформацію про мережі, до яких він підключався. Це пов’язано з тим, що пристрої автоматично повторно підключаються, щойно опиняються в зоні дії точок доступу. Така функція значно полегшує користування мережею, адже користувачам не потрібно щоразу вводити дані для автентифікації. Однак ключовою загрозою залишається можливість перехоплення значного обсягу метаданих про мережі, до яких раніше підключався клієнтський пристрій. Такі дані передаються у відкритому вигляді на канальному рівні моделі OSI та можуть бути проаналізовані зловмисниками. У разі підключення до будь-якої мережі клієнт постійно обмінюється інформацією з точкою доступу, здійснюючи передачу й прийом даних.

Здебільшого передана інформація перебуває у зашифрованому вигляді, проте окремі службові дані, зокрема MAC-адреси точки доступу та клієнтського пристрою, використовуваний канал, тип бездротового захисту, а також назва мережі (SSID), залишаються відкритими для перегляду за умови переведення мережевої карти в режим моніторингу. У разі відсутності активного підключення клієнтський пристрій може розкривати інформацію про раніше використані SSID, оскільки постійно здійснює пошук знайомих мереж.

Для зловмисника є типовим використання службових та інших метаданих з метою здійснення атак як на клієнтські пристрої, так і на мережеву інфраструктуру загалом. Якщо атакувальнику відома MAC-адреса

клієнта та SSID точки доступу, до якої він підключений, з’являється можливість створити підроблену точку доступу з ідентичними параметрами MAC і SSID, але без застосування протоколів бездротової безпеки, навіть за умови їх використання в легітимній мережі. Підвищення потужності сигналу фальшивої точки доступу разом із проведенням DoS-атаки дозволяє відключити клієнта від справжньої потреби та змусити його під’єднатися до клону. Даний тип атаки відомий під назвою «Evil Twin» («Злий двійник»).

В іншому варіанті описаної атаки зловмисник також розгортає клон точки доступу, однак усі запити від клієнтських пристроїв перенаправляються на фальшиву вебсторінку. На цій сторінці користувача просять ввести пароль нібито з метою повторного підтвердження автентичності. Після введення облікових даних зловмисник миттєво їх перехоплює, а сервер, що забезпечував функціонування атаки типу «злий двійник», негайно припиняє роботу.

Якщо клієнтський пристрій наразі не підключений до жодної точки доступу, він продовжує активно шукати мережі, до яких раніше мав підключення. На канальному рівні моделі OSI цей процес може бути виявлений зловмисником. Використовуючи отримані з клієнтських пристроїв дані, атакуючий здатний створити підроблену точку доступу. Поки легітимний клієнт та зловмисник перебувають в одній і тій же мережі, останній має можливість перехоплювати та/або змінювати трафік першого.

4.2 Проблеми безпеки, пов’язані з MAC-адресами

Швидкий розвиток будь-яких технологій часто супроводжується появою проблем безпеки, які важко помітити на ранніх етапах. Коли базова технологія вже набрала значного функціонального розвитку та широко використовується користувачами, усунення вразливостей може негативно вплинути на її загальну працездатність. Такий процес створює певні труднощі як для виробників, так і для кінцевих користувачів.

Мережі стандарту IEEE 802.11 надають користувачам можливість автоматичного підключення до мереж після попередньої авторизації. Якщо ж цю функцію заборонити задля підвищення безпеки, кожен клієнт буде змушений проходити авторизацію щоразу при спробі підключення до будь-якої точки доступу. У такому випадку механізми на кшталт WDS або інші системи розподіленого доступу втратять ефективність, адже при переміщенні між точками доступу користувачам доведеться постійно проходити процедуру авторизації.

4.3 Розробка методу виявлення атак підміни MAC-адрес та типу «Evil Twin»

Перш ніж сенсори зможуть визначати місцезнаходження та поведінкові характеристики клієнтських пристроїв, їм необхідно встановити взаємне позиціонування між собою. Основна складність полягає в тому, що під час роботи в режимі моніторингу сенсори не здатні розпізнавати один одного, оскільки в

цьому режимі відсутня передача даних. Тому перед активацією режиму моніторингу кожен сенсор має сформувати та надіслати спеціальний кадр сусіднім сенсорам.

При застосуванні моделі WHaaS після розміщення сенсорів у визначених точках здійснюється умовна ініціалізація системи, яка запускає процес обміну службовою інформацією між ними. При цьому зазначені кадри не повинні формуватися за фіксованим шаблоном, оскільки це могло б призвести до створення впізнаваних сигнатур для зловмисників, обізнаних щодо існування відповідної системи захисту та принципів синхронізації сенсорів.

З урахуванням викладеного вище пропонується метод синхронізації, основу якого становить формування синхронізаційних пакетів у командному центрі моделі WHaaS. Після надходження відповідного запиту від користувача командний центр ініціює процес підготовки даних для сенсорних вузлів. Як приклад таких даних можуть використовуватись маячкові кадри, за допомогою яких точки доступу інформують клієнтів про свою наявність, або пошукові пакети, що застосовуються клієнтськими пристроями для виявлення доступних і раніше відомих мереж. На наступному етапі командний центр передає кожному сенсору набір даних, що є індивідуальним для конкретного вузла. Зовнішні елементи отримують перелік команд і, дотримуючись визначеної черговості, здійснюють передачу відповідної інформації в ефір із заданими випадковими інтервалами. Одночасно з передачею власних даних сенсори здійснюють прослуховування ефіру та, використовуючи фільтри й попередньо отриманий перелік даних, виконують ідентифікацію сусідніх сенсорів. Якщо зовнішній елемент приймає дані від сусіднього сенсора, він повинен оперативно передати ідентифікатор цього елемента разом із потужністю отриманого сигналу. По завершенні процесу синхронізації кінцевий користувач отримує карту розташування всіх елементів комплексу та повинен підтвердити або спростувати її коректність.

У разі, якщо ідентифікація зовнішніх елементів реалізується шляхом передавання маячкових кадрів, аналогічно до роботи типової точки доступу, необхідно застосувати додаткові механізми маскування. Це зумовлено тим, що автентичність точки доступу може бути визначена за її MAC-адресою. Зокрема, використання баз даних ідентифікаторів виробників дає змогу зловмиснику встановити походження пристрою та виявити систему, яку планується атакувати. Перші 24 біти MAC-адреси містять інформацію про виробника мережевого обладнання і можуть бути використані для його ідентифікації в ефірі. Крім того, разом із MAC-адресою доцільно застосовувати стандартне значення SSID з метою зменшення рівня підозри.

Для визначення сусідніх елементів достатньо перехоплення лише одного кадру з ефіру, проте така ознака може слугувати сигнальним індикатором для зловмисника. У зв’язку з цим доцільно запровадити ще один параметр, який формуватиметься випадковим чином, а саме кількість кадрів, що передаватимуться в радіоефір.

4. 4 Приклад мережевої інфраструктури з еталонною зоною покриття системи виявлення атак підміни MAC-адрес у мережах стандарту IEEE 802.11

Припустимо, що об’єкт моніторингу розташований у приміщенні, яке має форму ідеального квадрата. Для забезпечення максимально рівномірного покриття сенсори доцільно розмістити на однаковій відстані один від одного. Відповідна схема розміщення за ідеалізованих умов наведена на рис. 3.13.

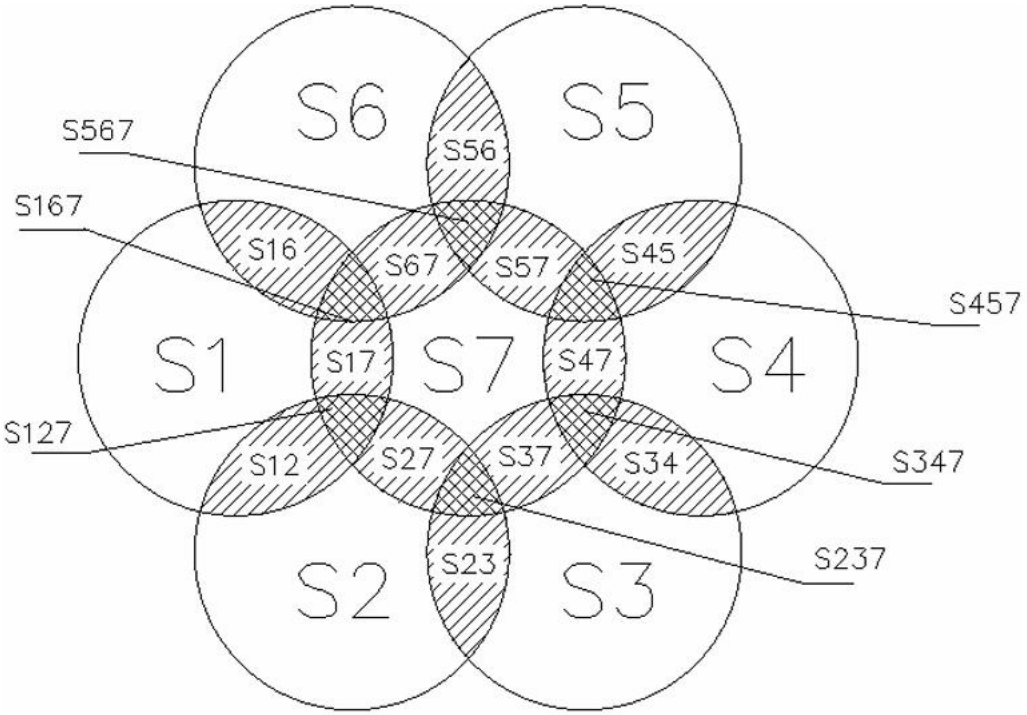


Рис. 3.13. Приклад розташування сенсорів системи виявлення вторгнень у мережах стандарту IEEE 802.11

Для наведеної вище схеми відповідною є таблиця істинності, подана в табл. 3.9.

Таблиця 3.9. Таблиця істинності для схеми, наведеної на рис. 3.10

Ідентифікатор сенсора	*S1*	*S2*	*S3*	*S4*	*S5*	*S6*	*S7*
S1		+	–	–	–	+	+
S2	+		+	–	–	–	+
S3	–	+		+	–	–	+
S4	–	–	+		+	–	+
S5	–	–	–	+		+	+
S6	+	–	–	–	+		+
S7	+	+	+	+	+	+	

Схематичне зображення покриття СВВ, наведене на рис. 16, наочно демонструє, як метод ангуляції може застосовуватись для виявлення вторгнень. Якщо відомо, що користувач повинен перебувати лише

в зоні дії трьох визначених сенсорів і не потрапляти в зону дії інших, цей підхід дозволяє ідентифікувати зловмисника. Наприклад, поява клієнтського пристрою в ефірі, зафіксована сенсорами, що не повинні його охоплювати, сигналізує про можливе порушення. Водночас складною залишається ситуація, за якої зловмисник застосовує, наприклад, вузькоспрямовану антену і рівень сигналу не перевищує межі сенсорів, у зоні дії яких він повинен знаходитися. У такому випадку подібна атака може залишитися непоміченою.

4.5 Застосування методів штучного інтелекту для аналізу поведінки користувачів у мережах IEEE 802.11 та подальшого виявлення вторгнень

На сьогодні не існує універсального методу для ідентифікації атак типу MAC-спуфінг у мережах IEEE 802.11. Проте частково цю проблему можна вирішити шляхом застосування методів штучного інтелекту.

Кожен клієнтський Wi-Fi пристрій характеризується індивідуальною щоденною траєкторією переміщення, яка визначається поведінкою його власника. Водночас окремі пристрої можуть мати фіксоване розташування, наприклад мережеві маршрутизатори. У зв’язку з цим для точок доступу та клієнтських пристроїв доцільно застосовувати відмінні підходи до аналізу та ідентифікації.

Якість та стабільність сигналу залежать від багатьох зовнішніх факторів. На роботу точки доступу можуть негативно впливати, наприклад, сусідні точки доступу, що працюють на тому ж частотному каналі, побутові електроприлади, міжкімнатні стіни або меблі. На рис. 3.14 наведено моделювання потужності сигналу для схеми, представленої на рис. 3.13.



Рис. 3.14. Часова залежність варіації рівня сигналу легітимного Wi-Fi пристрою

На рис. 3.14 видно, що потужність сигналу, зафіксованого сенсором №7, значно перевищує показники інших сенсорів, що може свідчити про знаходження клієнтського пристрою в безпосередній близькості до цього сенсора. У той же час рівень сигналу від спостережуваного пристрою на всіх інших сенсорах залишається стабільним і приблизно однаковим, відповідно до їх відстані від сенсора, біля якого перебуває пристрій.

Під час атаки типу «злий двійник» зловмисник розгортає точку доступу, яка за основними ідентифікаційними параметрами повністю повторює легітимну. Для пересічного користувача така підроблена точка доступу зазвичай не викликає підозр. Водночас навіть у разі ідеального клонування вона, як правило, розміщується в іншому фізичному місці, що призводить до суттєвих відмінностей у рівні сигналу. Сигнатура появи атаки типу «Evil Twin» зображена на рис. 3.15.



Рис. 3.15. Порівняльна варіація рівня сигналу легітимного та нелегітимного Wi-Fi пристроїв

Як видно з рис. 3.15, хоча рівень сигналу від легітимного пристрою на сенсорі №7 залишається стабільним, між десятою та одинадцятою часовими точками на сенсорі №4 спостерігається збільшення потужності сигналу від контрольованого пристрою. Оскільки розташування точок доступу переважно стаціонарне, це свідчить про доцільність застосування методів машинного навчання для аналізу потужності сигналів Wi-Fi точок доступу: нейронні мережі або класифікатори не потребують частого перенавчання.

На відміну від точок доступу, аналіз поведінки клієнтських пристроїв є значно складнішим завданням, оскільки вони з’являються та зникають разом зі своїми власниками. Нижче наведено перелік метаданих, які можуть використовуватися для вивчення поведінки клієнта та запобігання атакам типу MAC-спуфінг та іншим загрозам:

Важливо відстежувати звичайну поведінку клієнтського пристрою, зокрема час його появи та зникнення в зоні покриття. Для наочності розглянемо типовий приклад: працівник умовного підприємства приходить на роботу з понеділка по п’ятницю о 9:00, залишає офіс о 13:00, повертається о 14:00 і перебуває на робочому місці до 18:00, після чого покидає його до наступного ранку. Звичайно, через вплив інших факторів та взаємодію з людьми точний розклад може дещо варіюватися, проте наявність таких даних дозволяє ефективно виявляти аномальні ситуації. Наприклад, аномальною поведінкою можна вважати появу пристрою в зоні покриття у нічний час суботи.

Якщо всі або більшість сенсорів фіксують сигнал від клієнтського пристрою, при цьому максимальна потужність сигналу спостерігається на сенсорах, розташованих на зовнішньому краю інфраструктури, а

далі потужність поступово зменшується в протилежному напрямку, це може свідчити про потенційну атаку. Така ситуація характерна для випадку, коли зловмисник застосовує вузьконаправлену антену (рис. 3.16).

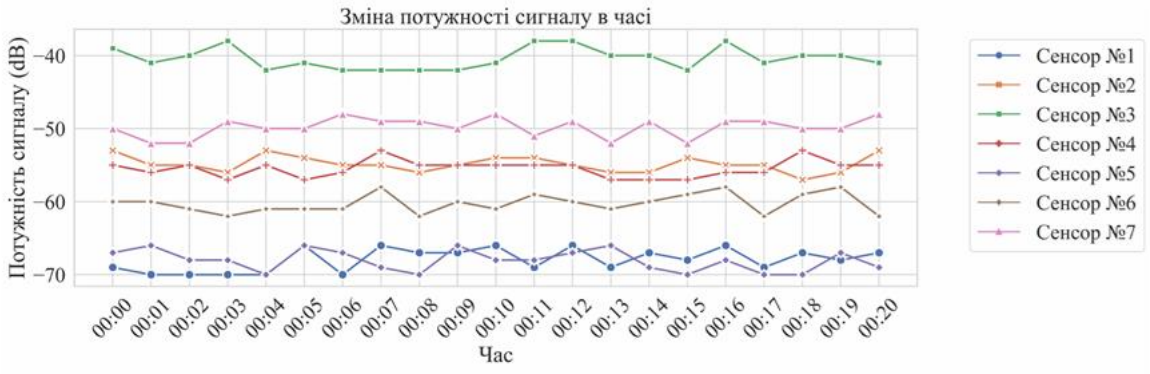


Рис. 3.16. Часова зміна рівня сигналу клієнтського Wi-Fi пристрою зловмисника (із вузькоспрямованою антеною)

На основі описаного сценарію та схеми розташування сенсорів, наведеної на рис. 3.13, на рис. 3.16 представлено часову зміну рівня сигналу потенційного зловмисника, що використовує спрямовану антену. Як видно з рис. 3.16, максимальна потужність сигналу зафіксована сенсором №3, після чого зменшення рівня сигналу спостерігається на сенсорах №7, №2, №4 та №6, що свідчить про наскрізний характер поширення сигналу.

Ідентифікація дубльованої MAC-адреси в зоні покриття. Поява в зоні обслуговування ще одного пристрою з MAC-адресою, яка в певний момент уже зареєстрована в мережі, може свідчити про здійснення атаки. На основі описаного вище сценарію та інфраструктури, наведеної на рис. 3.13, на рис. 3.17 подано варіацію рівня сигналу потенційного зловмисника, який ініціює атаку типу MAC Spoofing поруч з легітимним клієнтом, уже підключеним до мережі.



Рис. 3.17. Виявлення атак підміни MAC-адрес у Wi-Fi мережах із використанням системи виявлення вторгнень моделі WHaaS

Інтерпретація рис. 3.17 може бути такою: першим сенсором, який зафіксував клієнтський пристрій, став сенсор №3, що підтверджується зміною потужності сигналу у часовому проміжку від 0:00 до 0:03. Надалі вектор руху пристрою зміщується в бік сенсора №7, сусіднього до сенсора №3, що свідчить про природний рух у межах зони покриття (часовий проміжок 0:03–0:06). Далі клієнтський пристрій також ідентифікується сенсором №2, при цьому переміщення між сенсорами відображає зміну місцезнаходження пристрою. О 0:17 сенсори №1 та №5, які не є сусідніми, фіксують сигнали від пристроїв із однаковою MAC-адресою, що може свідчити про підозрілу активність, таку як атака типу MAC Spoofing.

Виявлення клієнтського пристрою в неприпустимій зоні

Якщо будівля, яку слід захистити, є великою, зазвичай передбачене розмежування доступу до окремих приміщень. Поява клієнтських пристроїв у незвичних для них зонах — тобто у межах дії сенсорів, які контролюють ці приміщення — може свідчити про присутність зловмисника, що фізично зайняв вигідне для себе місце, або про потенційно небезпечні дії з боку персоналу.

Виявлення атаки MAC Spoofing за допомогою пошукових пакетів клієнтських пристроїв

Кожен Wi-Fi клієнтський пристрій, який раніше підключався до певної кількості бездротових мереж, здійснює їх пошук за допомогою спеціальних пошукових пакетів. Це означає, що кожен пристрій формує власний список точок доступу, активний пошук яких він регулярно виконує. Навіть якщо зловмисник змінить MAC-адресу свого пристрою на адресу легітимного, він надсилатиме пошукові пакети з параметрами, які не відповідають поведінці легітимного пристрою, або взагалі не надсилатиме їх. Подібні аномальні активності можуть слугувати маркером потенційної атаки.

4.6 Використання методів штучного інтелекту для виявлення вторгнень у мережах стандарту IEEE 802.11

У цьому розділі вже наведено приклади сигнатур, які можуть свідчити про різні типи атак із підміни Wi-Fi пристроїв у ефірі шляхом аналізу потужності сигналу. Проте створення системи захисту на основі виключно сигнатурних правил є значним викликом для адміністратора мережі. Будь-які зміни в приміщенні можуть впливати на рівень сигналу від точок доступу до клієнтських пристроїв або сенсорів, що здійснюють моніторинг, що ускладнює точну ідентифікацію атак.

Існує значна кількість підходів до реалізації моделей машинного навчання, зокрема навчання з учителем та без учителя. У випадку навчання з учителем зазвичай потрібні менші обчислювальні ресурси для навчання моделі.

Оскільки дані, зібрані з ефіру, можуть містити шуми — рівень сигналу від точок доступу іноді нестабільний — для їх аналізу в цій роботі було обрано алгоритм класифікації **k-найближчих сусідів**

(KNN). Алгоритм KNN відносить нову точку даних до певного класу на основі її близькості до точок навчального набору. У даному випадку навчання моделі можна проводити, використовуючи максимальні, мінімальні, середні значення потужності сигналу, а також рівень сигналу, який зустрічається найчастіше.

Для обчислення відстані між двома точками даних використовуються різні метрики відстані. Найпоширенішими є **евклідова**, **манхеттенська** та **метрика Мінковського** [86].
На рис. 3.19 представлено компонентну схему програмно-апаратного комплексу, призначеного для виявлення вторгнень у мережах стандарту IEEE 802.11 із застосуванням алгоритмів штучного інтелекту.



Рис. 3.19. Структурно-функціональна схема програмно-апаратного комплексу ідентифікації атаки типу «злий двійник» у мережах IEEE 802.11.

Цілісна система побудована на трьох рівнях. Перший рівень — **збір інформації**. Він включає три компоненти: пристрій збору даних, агрегатор даних та базу даних на основі часових рядів. Основною функцією цього рівня є виключно накопичення та збереження даних.
Другий рівень — **аналіз даних**. Він складається зі сховища даних, підготовлених для навчання, обчислювального середовища для навчання моделей та компонента безперервної інтеграції та доставки моделей штучного інтелекту (CI/CD). Третій рівень — **прикладний**. Він включає балансувальник веб-трафіку, прикладне програмне забезпечення, що працює з натренованою моделлю штучного інтелекту, та базу даних, у якій зберігається інформація про виявлені атаки.

Робота комплексу здійснюється за наступною схемою: на першому етапі сенсори здійснюють збір даних. Після їх агрегації інформація зберігається у базі даних на основі часових рядів. Коли накопичується

достатній обсяг даних, вони передаються у сховище для підготовки та навчання моделі штучного інтелекту. Після завершення тренування натренована модель розгортається на серверному застосунку для подальшого використання.

Після завершення процесів збору даних, навчання та доставки моделей, компоненти першого рівня переводяться у **сторожовий режим**, метою якого є безперервний моніторинг рівня сигналу та порівняння отриманих даних із прогнозами моделі. За потреби можливо активувати режим повторного збору даних та додаткового навчання або перетренування моделі.

У цьому розділі розглянуто приклад інфраструктури з ідеальним покриттям, а також вдосконалено методи виявлення вторгнень у мережах стандарту IEEE 802.11. Було розроблено підхід для ідентифікації атак із підміни MAC-адрес та атаки «злий двійник» (ЗД), а також запропоновано метод визначення атаки ЗД із застосуванням алгоритму штучного інтелекту **KNN**. Для цього рекомендовано використання алгоритму навчання з учителем KNN, який ефективно підходить для аналізу потужності сигналів легітимних точок доступу та подальшого виявлення вторгнень. На відміну від сигнатурних методів виявлення вторгнень, запропонований підхід дозволяє більш точно ідентифікувати атаки типу «злий двійник» навіть у випадку, коли зловмисник створює точну копію точки доступу, дублюючи її ідентифікатор та MAC-адресу. Сигнатурні методи, у свою чергу, здатні виявляти атаки лише шляхом ідентифікації однакових точок доступу з відмінними MAC-адресами. Крім того, було запропоновано концепцію компактного та енергоефективного програмно-апаратного комплексу для моніторингу та аналізу службових мережевих пакетів у ефірі з подальшим збереженням даних у базі на основі часових рядів. З метою зниження навантаження на комп’ютерну мережу та з урахуванням обмежених обчислювальних ресурсів комплексу було запропоновано підхід до агрегації даних, який забезпечує їх оперативну та ефективну передачу. Реалізований програмно-апаратний комплекс дав змогу зібрати та структуровано опрацювати значний обсяг даних як від легітимних, так і від штучно змодельованих нелегітимних точок доступу, які надалі були використані для навчання моделі штучного інтелекту.

ВИСНОВКИ

В дипломній роботі було проведено дослідження щодо захищеності бездротових мереж і проведено оцінку їх вразливостей. Було проаналізовано можливі атаки на бездротове середовище та виділено слабкі місця бездротових мереж. Також були досліджені сучасні методи і технології захисту бездротових мереж і у наслідок написано програмне забезпечення, яке дозволить моніторити стан мережі і виявляти підозрілий трафік.

Під час аналізу особливостей роботи бездротового середовища, передачі даних та під час оцінки поширеності бездротових мереж у сучасному світі було розглянуто існуючі мережі і виділено декілька основних типів бездротових мереж за територіальною ознакою: WLAN, WMAN, WPAN. Також було виявлено проблематику захисту інформації в бездротовому середовищі і зроблено висновок щодо важливості їх захисту.

Не зважаючи на те що сьогодні в захисті бездротових мереж і застосовуються складні алгоритмічні математичні моделі аутентифікації, шифрування даних, контролю цілісності їх передачі, і досі можна сказати, що бездротові мережі являються дуже вразливими.

Результатом дослідження захищеності мережі було отримання даних про те що бездротові мережі вразливі до зламу паролів, перехоплення трафіку, підміни мережі, та затримки роботи мережі або атаки відмови в обслуговуванні. Кожна з цих атак може внести значний вплив на роботу мережі або може відобразитися на користувачах і їх даних, які потрапили у мережу і могли бути скомпроментовані зловмисником. Отже після дослідження захищеності мережі можна сказати, що бездротові мережі потребують у додаткових методах захисту. Також є доцільним використання спеціальних механізмів і технологій захисту.

Аналізуючи методи і технології захисту було описано сучасні технології захисту даних у мережі, які використовують шифрування інформації для безпечної передачі даних. Шифрування та інші методи захисту ускладнюють процес перехвату даних, що у комплексі з іншими методами захисту і пильним

адмініструванням мережі створюють гарну систему захисту бездротової мережі. Також було проаналізовано технологію роботи стандарту Wi-Fi і суміжних протоколів та алгоритмів, що розроблялися для підвищення захищеності мереж.

На основі отриманих даних було розроблено програмне забезпечення яке виконує функції моніторингу з аналізом трафіку бездротової мережі, протоколів передачі у мережі. Також програмним забезпеченням виконується аналіз підозрілого трафіку у мережі.

Виходячи з вищесказаного можна з певністю сказати що була виконана основна мета роботи по розробці аналазатору трафіку на базі отриманих у процесі дослідження даних.

У цьому розділі розглянуто приклад інфраструктури з ідеальним покриттям, а також вдосконалено методи виявлення вторгнень у мережах стандарту IEEE 802.11. Було розроблено підхід для ідентифікації атак із підміни MAC-адрес та атаки «злий двійник» (ЗД), а також запропоновано метод визначення атаки ЗД із застосуванням алгоритму штучного інтелекту **KNN**. Для цього рекомендовано використання алгоритму навчання з учителем KNN, який ефективно підходить для аналізу потужності сигналів легітимних точок доступу та подальшого виявлення вторгнень. На відміну від сигнатурних методів виявлення вторгнень, запропонований підхід дозволяє більш точно ідентифікувати атаки типу «злий двійник» навіть у випадку, коли зловмисник створює точну копію точки доступу, дублюючи її ідентифікатор та MAC-адресу. Сигнатурні методи, у свою чергу, здатні виявляти атаки лише шляхом ідентифікації однакових точок доступу з відмінними MAC-адресами. Крім того, було запропоновано концепцію компактного та енергоефективного програмно-апаратного комплексу для моніторингу та аналізу службових мережевих пакетів у ефірі з подальшим збереженням даних у базі на основі часових рядів. З метою зниження навантаження на комп’ютерну мережу та з урахуванням обмежених обчислювальних ресурсів комплексу було запропоновано підхід до агрегації даних, який забезпечує їх оперативну та ефективну передачу. Реалізований програмно-апаратний комплекс дав змогу зібрати та структуровано опрацювати значний обсяг даних як від легітимних, так і від штучно змодельованих нелегітимних точок доступу, які надалі були використані для навчання моделі штучного інтелекту.