МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, професор	доктор економічних наук, професор
_____ С.В. Легомінова	_____ С.В. Легомінова
«_____» _____2022 р.	«_____» _____2022 р.

ДИПЛОМНА РОБОТА (МАГІСТЕРСЬКА)

на тему:

«ЗАБЕЗПЕЧЕННЯ НЕОБХІДНИХ УМОВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ БЕЗПРОВОДОВОЇ МЕРЕЖІ ДЛЯ УПРАВЛІННЯ РОБОТАМИ»

СТУДЕНТ: Грабчук Артем Ярославович

КЕРІВНИК: кандидат технічних наук, доцент Дзюба Тарас Михайлович

НОРМОКОНТРОЛЕР:

(підпис)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Освітньо-кваліфікаційних рівень – магістр
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
(підпис)
“___”_____ 2021 р.

ЗАВДАННЯ
на дипломну роботу
студенту Грабчуку Артему Ярославовичу

1. Тема роботи «ЗАБЕЗПЕЧЕННЯ НЕОБХІДНИХ УМОВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ БЕЗПРОВОДОВОЇ МЕРЕЖІ ДЛЯ УПРАВЛІННЯ РОБОТАМИ», затверджена наказом по університету від «11» жовтня 2021 р. № 170.

2. Термін здачі студентом оформленої роботи « 10 » січня 2022 р.

3. Об’єкт дослідження: безпроводова мережа управління роботами.

4. Предмет дослідження: захист інформації в безпроводовій мережі управління роботами.

5. Мета дослідження: обґрунтування доцільних шляхів захисту інформації в безпроводовій мережі управління роботами.

6. Перелік питань, які мають бути розроблені:

6.1. Дослідити особливості розвитку систем управління мобільними робототехнічними комплексами.

6.2. Провести аналіз комплексу методів і засобів захисту інформації у радіоканалах систем управління робототехнічними комплексами.

6.3. Обґрунтувати доцільні шляхи захисту інформації в безпроводовій мережі управління роботами.

7. Дата видачі завдання «14» жовтня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: « 14 » жовтня 2021 р

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження	**21.10.2021**	
2.	Збір та аналіз літератури	**15.11.2021**	
3.	Дослідження особливостей розвитку систем управління мобільними робототехнічними комплексами	**25.11.2021**	
4.	Аналіз комплексу методів і засобів захисту інформації у радіоканалах систем управління робототехнічними комплексами	**07.12.2021**	
5.	Обґрунтування доцільних шляхів захисту інформації в безпроводовій мережі управління роботами	**24.12.2021**	
6.	Формулювання висновків за результатами проведеного дослідження	**25.12.2021**	
7.	Оформлення роботи	**10.01.2022**	
8.	Оформлення презентації	**11.01.2022**	
9.	Отримання рецензії на роботу	**12.01.2022**	
10.	Захист в ДЕК	**18.01.2022**	

Студент **А.Я. Грабчук**

підпис

Науковий керівник **Т.М. Дзюба**

підпис

РЕФЕРАТ

Текстова частина магістерської роботи : 75 сторінок, 45 рисунків, 4 таблиці, 22 джерела.

Об'єкт дослідження – безпроводові канали зв'язку.

Предмет дослідження - методи та засоби захисту інформації в безпроводових каналах зв'язку.

Мета роботи - дослідження та реалізація комплексу методів та засобів захисту інформації в безпроводових каналах зв'язку, що застосовуються у мобільних робототехнічних комплексах.

Методи дослідження – у магістерській роботі використані методи захисту інформації в радіоканалі із застосуванням криптографії та стійких алгоритмів захищеного обміну ключами. Використано наукові положення теорії обчислення дискретних логарифмів та операцій на мультиплікативних групах цілих чисел.

Виконуючи поставлені завдання у магістерській роботі проаналізовано сучасний стан та перспективи розвитку робототехніки. Проаналізовано технічні особливості та структуру системи управління мобільним робототехнічним комплексом. Розглянуто особливості структури бездротових мереж стандарту IEEE 802.11 з погляду захисту інформації. Проаналізовано стандартні засоби та методи захисту інформації в радіоканалі. У практичній частині, запропоновано методи покращення стандартної системи безпеки заснованої на алгоритмі WEP. На основі експериментальних даних досліджено технологію, що дозволяє здійснювати ефективний пошук та локалізацію неавторизованої станції у захищеній мережі.

Галузь використання – безпроводова мережа зв'язку.

РОБОТОТЕХНІЧНІ КОМПЛЕКСИ, МЕРЕЖЕВА АТАКА, ТРАФІК, ВІРТУАЛЬНА МЕРЕЖА, МАРШРУТИЗАЦІЯ, ПЛАТФОРМА, ЕФЕКТИВНІСТЬ, АУТЕНТИФІКАЦІЇ, БЕЗПЕКА, РАДІОКАНАЛ.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АА – активні атаки

АС – автоматизована система

БД – база даних

БПЛА - безпілотні літальні апарати

ДККР - дистанційно керований комплекс розмінування

ПА - пасивні атаки

ПК - персональний комп’ютер

ПМО -програмно-математичне забезпечення

ППП - пакетно-прикладні програми

СЗІ - системи захисту інформації

СРД - системи розділеного доступу

ОС - операційна система

КМ - комп’ютерна мережа

МРК - мобільних робототехнічних комплексів

НСД - несанкціонований доступ

РТК - робототехнічні комплекси

AP (Access Point) - точка доступу

SSL (Secure Socket Layers) - протокол передачі шифрованих даних

RSSI (Received Signal Strength Indicator) - значення рівня прийнятого сигналу

NAT (Network Address Translation) - служба трансляції мережевих адрес

WEP (Wired Equivalent Privacy) - алгоритм забезпечення безпеки мереж

ВСТУП

Актуальність дослідження. У сучасному світі, як в нашій країні, так і за її межами, проводяться активні дослідження зі створення і застосуванні мобільних робототехнічних комплексів (МРК). Активний розвиток нових інформаційних технологій та концепції створення базових елементів штучного інтелекту, а також значний технологічний прогрес у галузі створення надміцних матеріалів і малогабаритних енергоємних джерел електроживлення дозволяють вже сьогодні створювати робототехнічні комплекси (РТК) широкого спектру застосування. При цьому завдання, що покладаються на РТК, з кожним роком дедалі більше розширюються, проникаючи у всі сфери інтересів людства, і ускладнюються, що часто вимагає групового застосування роботів у різних фізичних середовищах. Сфера застосування роботів є досить великою, першочерговими якого є завдання, під час яких робот діє в умовах, які є небезпечними для людини. Перспективним є використання автоматизованих робототехнічних комплексів у бойових умовах, коли є пряма загроза життю людини. У складі пошукової групи МРК можуть здійснювати дії віддаленої розвідки, вони діють автономно та передають інформацію безпроводовим каналом.

Слід зазначити що під час створення МРК одним з важливих завдань є можливість забезпечити необхідної захищеності інформацію. Аналіз показав, що найбільш уразливими є дані, які транслюються по радіоканалу. Команди керування, які надаються роботу через радіоканал, можуть бути виявлені і модифіковані. Інформація, що передаються від робота до пункту керування, також можуть бути виявлені і модифіковані.

Окремим важливим завданням є знаходження станції-порушника в межах бездротової мережі яка захищається, тому дана кваліфікаційна робота присвячена дослідженню захисту інформації в радіоканалах мобільних роботів, із застосування заходів щодо захисту від можливих атак спрямованих на перехоплення та заміну переданих даних.

Ступінь наукової розробки. Досліджено та запропоновано методику створення комплексної удосконаленої системи безпеки даних у радіоканалах стандарту 802.11, що поєднує в собі шифрування даних, автентифікацію сторін та обмін ключами, застосування якої значно підвищує рівень захисту даних порівняно зі стандартними засобами.

Практичне значення одержаних результатів. Отримані теоретичні та практичні результати доцільно застосовувати в організаціях, які використовують радіоканали для передачі конфіденційної інформації з підвищеними вимогами до безпеки.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ РОЗВИТКУ, ТЕХНІЧНИХ ХАРАКТЕРИСТИК ТА СТРУКТУРИ СИСТЕМИ УПРАВЛІННЯ МОБІЛЬНИМ РОБОТОТЕХНІЧНИМ КОМПЛЕКСОМ

1.1 Світовий ринок та тренди розвитку робототехніки

Останніми роками зростання промисловості робототехніки було надзвичайно високим. Але наступні кілька років будуть сповнені грандіозних досягнень у галузі робототехніки.

Завдяки технологічним досягненням зростання промисловості робототехніки значно прискорилося. Раніше взаємодія машини та людини була нудною та обмеженою. Але останні тенденції свідчать, що світ, сповнений роботів, може бути дуже цікавим. Сьогодні роботи можуть усно спілкуватися, простягати руку допомоги, а також рятувати життя, що, ймовірно, з кожним днем робить роботів все більш схожими на людей.

Крім того, роль роботів у різних сферах бізнесу та суспільства постійно збільшується. Наприклад, у галузі промислової автоматизації коботи сьогодні простягають руку допомоги. У сфері охорони здоров'я роботи допомагають лікарям виконувати складні операції. Крім того, спостерігати, як роботи беруть на себе відповідальність за вашу розвагу в торгових центрах, парках розваг та на ярмарках, сьогодні теж не рідкість. П'ять факторів, що підтримують таке стрімке зростання робототехніки представлено на рис.1.1.

Поняття «робот» не має однозначного визначення. Це породжує в тому числі неузгодженість оцінок ринку, до складу якого найчастіше включаються різні сегменти. Так, згідно з стандартом ISO 8373 під роботом розуміється «програмований механізм, здатний переміщатися з двома і більш ступенями свободи, що володіє певним ступенем автономності і здійснює рух до виконання певних завдань». Очевидно, що подібне формулювання не є достатнім для визначення меж ринку.

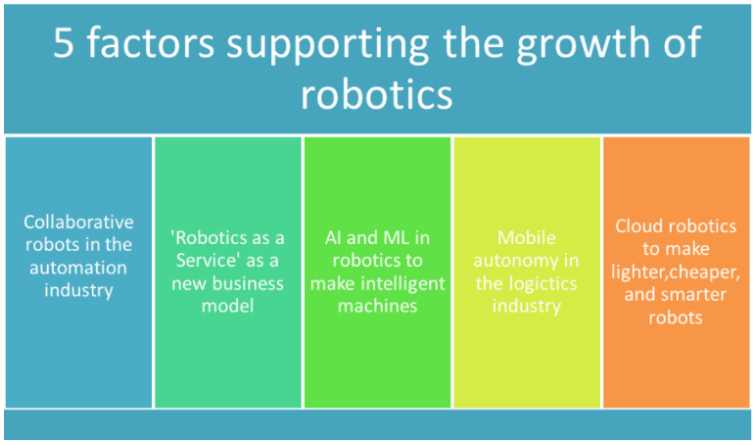


Рис.1.1. Фактори підтримки зростання робототехныки

Наприклад, сучасні літаки мають високий рівень автономності і здатні переміщатися в просторі, проте їх не прийнято включати. на ринок робототехніки. Щоб уникнути неоднозначності при обговоренні об'єкта дослідження нами запропонована класифікація пристроїв, найбільш часто належать до робототехніки.

Обсяг світового ринку робототехніки (включаючи промислову та сервісну сфери) оцінюється в діапазоні від 14,5 до 29 млрд. доларів США. Різниця в оцінках обумовлена різницею у підходах до визначення меж цього ринку. Так, згідно зі статистикою Міжнародної федерації робототехніки (International Federation of Robotics, IFR), яка враховує виключно продаж роботизованих пристроїв, обсяг ринку у 2020 році становив 14,5 млрд доларів США. За даними міжнародної некомерційної асоціації euRobotics, поточний обсяг ринку роботів становить 29 млрд доларів США, включаючи послуги з розробки програмного забезпечення, інжинірингу та системної інтеграції. У цьому звіті (якщо не зазначено інше) ми спиратимемося на статистику IFR як найавторитетнішої галузевої організації у світі, яка аналізує цей ринок з 1991 року [1].

1.1.1 Особливості розвитку промислової робототехніки

Ринок промислових роботів є невеликою частиною більш загального ринку систем автоматизації та промислової робототехніки, сукупний обсяг якого у 2019 році, за оцінками дослідницької компанії Transparency Market Research, становив

102 млрд. доларів США. Згідно зі статистикою IFR, продаж власне промислових роботів у 2019 році становив лише 8,7 млрд доларів США, або 8,5% від обсягу всього ринку систем автоматизації.

Ринок промислових роботів, що виник понад 50 років тому, є досить зрілим. Незважаючи на це, він продовжує зростати із середнім темпом 8,4% на рік у грошах. Швидше зростання спостерігається у країнах, які активно створюють або оновлюють промисловість. Подібно до інших ринків капітальних товарів, цей сегмент значною мірою схильний до впливу економічних циклів та активності промисловості: у кризовому 2015 році падіння попиту на промислову робототехніку склало майже 50%. Але вже у 2018-2019 роках ринок вийшов на рекордні обсяги продажу.

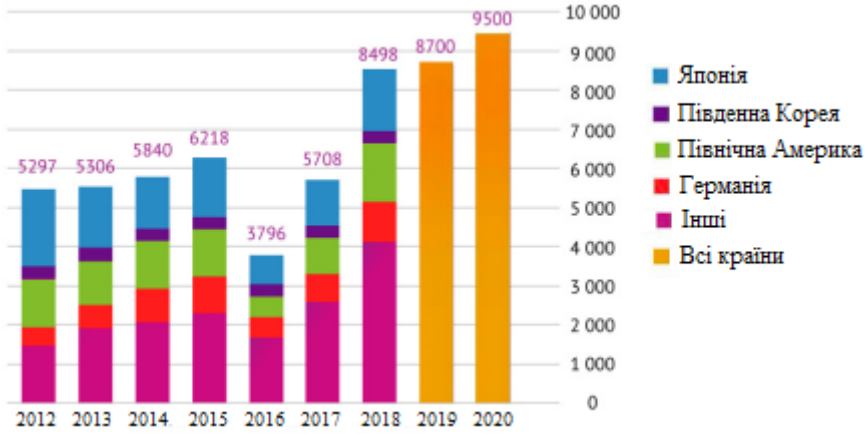


Рис.1.2. Обсяги продажів промислових роботів у світі, млн доларів США

Обсяг та динаміка ринку. У 2020 році продаж промислових роботів зріс зі 159 тис. до 178 тис. штук, досягнувши рекордної кількості за всю історію галузі. За даними, наведеними у звіті «Промислові роботи для світової та китайської автомобільної промисловості» компанії Research and Markets, у 2020 році обсяг ринку промислових роботів становив 9,5 млрд доларів США. Середня ціна нового промислового робота без послуг інтеграції становила приблизно 55 тис. доларів США [2].

Наведені показники не включають вартість програмного забезпечення, периферійного обладнання та послуг системної інтеграції, які в сукупності

становлять 2/3 вартості проекту для кінцевого замовника. Тому сукупний обсяг ринку промислової робототехніки та супутніх послуг, за оцінками IFR, становив у 2013 році становитиме понад 29 млрд доларів США.

Статистика IFR не враховує постачання роботизованого обладнання для монтажу друкованих плат. Згідно з даними дослідження «Тренди ринку робототехніки у 2019 році» Міністерства економіки, торгівлі та промисловості Японії (Ministry of Economy, Trade and Industry, METI), обсяг продажу цього обладнання для електронної індустрії у 2019 році становив 4,9 млрд. доларів США. Таким чином, якщо включити до розгляду зазначений сегмент, то оцінка сукупного ринку промислових роботів у 2020 році становитиме понад 14,5 млрд. доларів США.

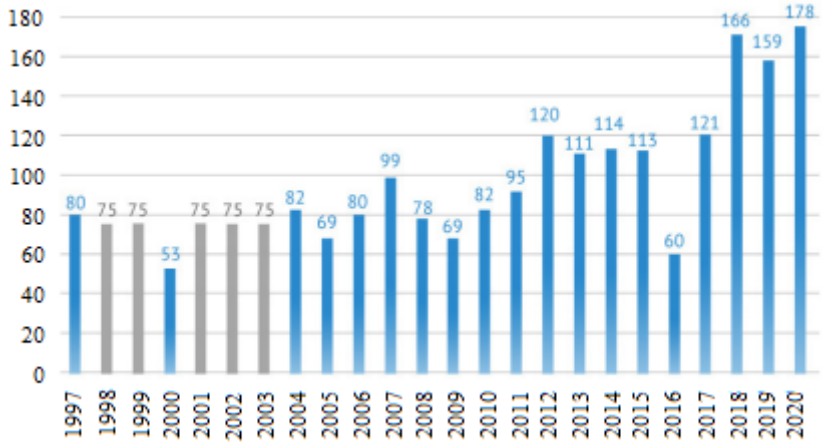


Рис.1.3. Обсяги продажів промислових роботів у світі, тис. шт

За статистикою IFR, починаючи з 1960-х років було продано близько 2,5 млн. промислових роботів. Середній термін служби таких пристроїв становить від 12 до 15 років. З урахуванням старіння сукупний обсяг промислових роботів, що діють, на початок 2013 року становив від 1,235 до 1,5 млн штук. У період з 1997 по 2020 рік попит на промислові роботи залишався стабільним у діапазоні 70-80 тис. штук на рік, відчуваючи незначні циклічні коливання. З 2010 по 2020 рік ринок промислової робототехніки демонстрував у середньому зростання як у натуральному (з темпом 7,6% на рік), так і у вартісному вираженні (8,4% на рік).

При цьому попит на промислові роботи схильний до сильних циклічних коливань. У 2016 році на тлі світової фінансової кризи галузь зазнала падіння продажів на 47%, що вперше призвело до зниження оцінок кількості встановлених промислових роботів за рахунок їхнього природного вибуття. Причинами зростання ринку у 2018-2019 роках став відкладений попит, а також відновлення промисловості після спаду [3].

Експерти дуже оптимістично оцінюють подальші перспективи розвитку ринку промислової робототехніки. Так, дослідницька компанія Markets and Markets прогнозує зростання ринку промислових роботів та супутніх послуг із середнім темпом 5% з 2019 по 2024 рік до 32,8 млрд доларів США наприкінці цього періоду. Американська дослідницька компанія Allied Market Research оцінює зростання цього ринку з темпом 5,4% до 41,2 млрд. доларів США в 2020 році.

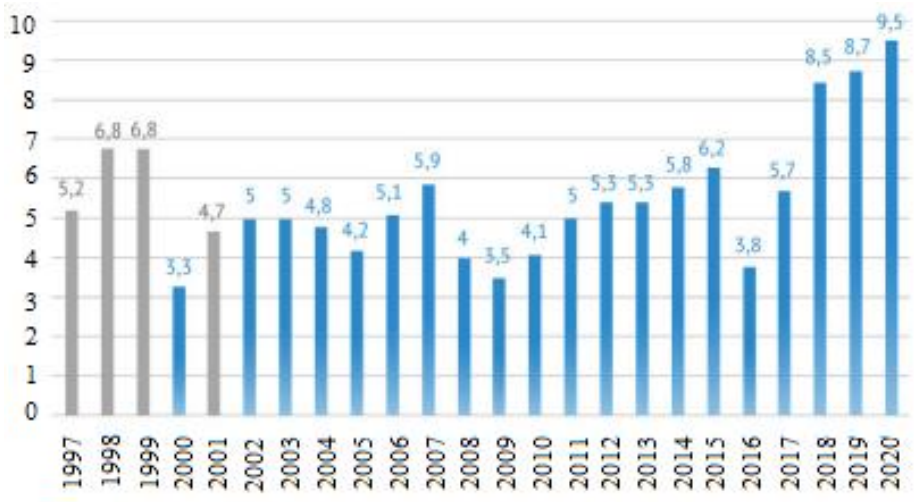


Рис.1.4. Обсяг світового ринку промислових роботів, млрд доларів США

При використанні цих прогнозів важливо пам'ятати про вираженому циклічному характері галузі, що уможливлює лише приблизну оцінку тренда, тоді як реальний рівень продажів може на десятки відсотків відрізнятися від очікуваного.

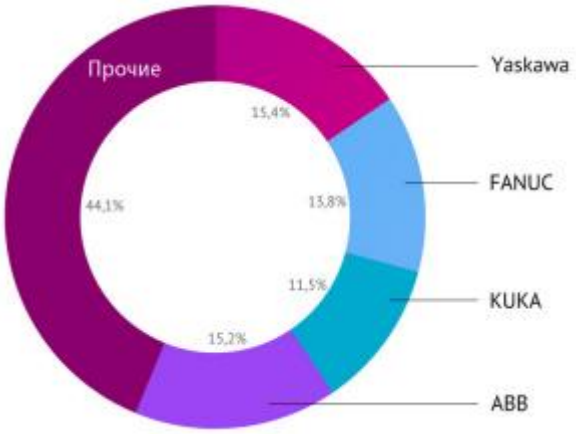


Рис.1.5. Частки основних гравців на ринку промислової робототехніки, %

Регіональна та галузева структура ринку. Попит на промислову робототехніку має нерівномірний географічний розподіл. Ключовими покупцями є країни, де йде активний процес створення нових чи модернізації діючих промислових підприємств.

Найбільший попит роботи користуються в Японії, Південній Кореї, Китаї, США, Німеччині [4].

У 2019 році лідерами за кількістю роботів на 10 тис. співробітників стали: Південна Корея (396), Японія (332) та Німеччина (273). Промисловість США не належить до лідерів з автоматизації виробництва, маючи лише 76 роботів на 10 тис. виробничих працівників, що перевищує середньосвітовий рівень (58). Китай у відносних показниках показує суттєве відставання від лідерів, маючи лише 11 роботів на 10 тис. осіб, зайнятих у промисловості. Проте з огляду на масштаб економіки Китай вже сьогодні є найбільшим покупцем промислових роботів і зберігає великий потенціал для розвитку.

Європа посідає друге місце після Азії за обсягом закупівлі нових промислових роботів. З придбаних у Європі у 2019 році 43,3 тис. роботів на Німеччину припадало 18,3 тис., на Італію – 4,7 тис., на Францію – 2,2 тис., на Велику Британію – 2,5 тис., на Іспанію — 2,8 тис., на Чехію — 1,0 тис. Серед країн, що розвиваються, можна відзначити Таїланд (3,2 тис. роботів на рік), Мексику (2,7 тис.), Бразилію (1,4 тис.) , Туреччину (1,1 тис.) та Росію (0,4 тис.).

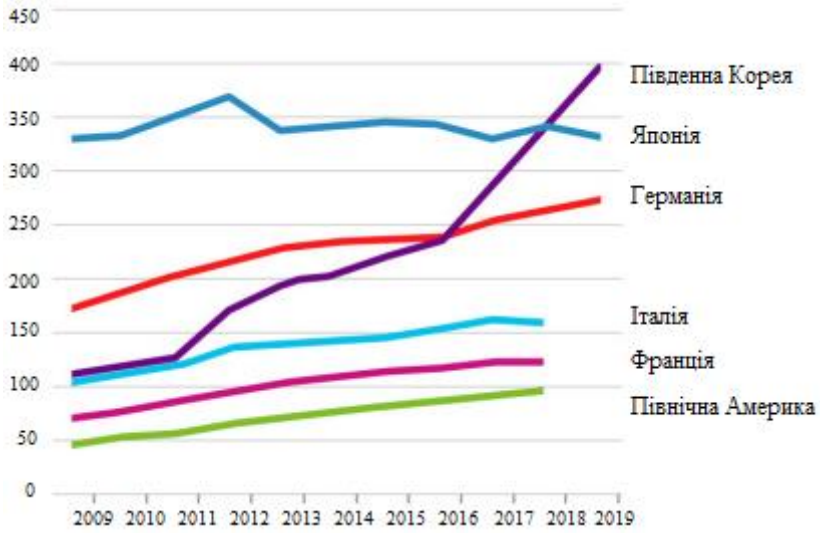


Рис.1.6. Динаміка кількості промислових роботів на 10 тис. робітників по країнах, шт

Японія залишається лідером у виробництві промислових роботів, посівши 52% ринку у 2019 році, тоді як німецькі компанії утримують друге місце з часткою 21,7%. На думку Альберта Єфімова, директора IT-проектів Фонду «Сколково», важливою причиною лідерства Японії у сфері промислових роботів є відсутність попиту з боку військових: «У Японії сталася дивовижна історія. Оскільки сили національної оборони ніколи не були зацікавлені в робототехніці, а галузь бурхливо розвивалася, японські вчені-робототехніки сфокусувалися на промисловому секторі». Японські компанії обслуговують внутрішній ринок, а також домінують на світовому ринку в таких галузях, як виробництво електроніки, конвеєрне складання, металообробка, виробництво пластмас та харчових продуктів. Європейські виробники переважають в автомобілебудуванні, займаючи більшу частину китайського, американського та європейського ринків. Крім того, вони лідирують у сфері створення роботів для високотехнологічних виробництв, штампування, фарбування та герметизації [5].

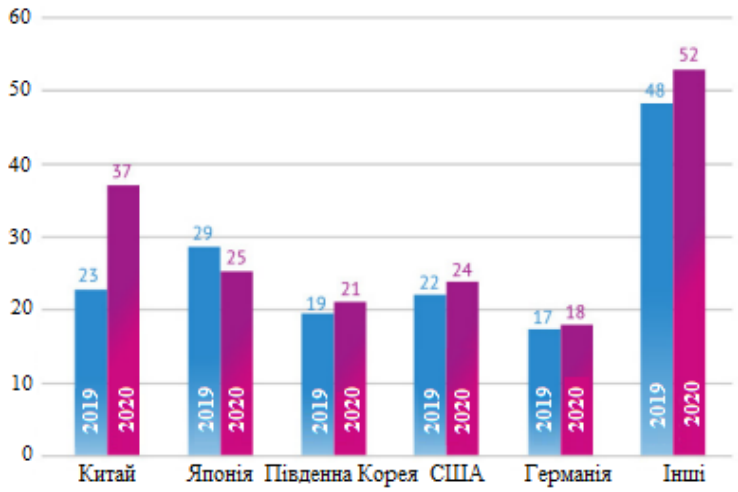


Рис.1.7. Обсяг продажів промислових роботів країнами, тис. прим.

Основними сферами застосування промислових роботів, як і раніше, залишаються автомобілебудування та виробництво автомобільних комплектуючих. Важливими напрямами з погляду потенціалу зростання продажів є металургія та машинобудування, а також харчова промисловість, фармацевтика та електроніка.

Таблиця 1.1.

Обсяг продажів промислових роботів по галузях, шт.

Галузь	Продажі
Автомобілебудівництво	59705
Електроніка та електротехніка	37751
Металургія і машинобудівництво	14125
Хімічна промисловість	11825
Виробництво скла і кераміки	828
Освіта	699
Паперова промисловість	484
Продукти харчування	465
Деревообробка	297
Будівництво	256
Легка промиловість	213
Сільське господарство	133
Житло-комунальне господарство	40
Видобуток корисних копалин	20
Інші галузі	35002
Загальне світове споживання	166028

Ключові фактори зростання. Підвищення попиту на промислову робототехніку зумовлено такими факторами:

- Зростання вартості праці. За даними Бюро статистики праці США, заробітна плата у міських районах у Китаї з 2009 по 2016 рік зросла з 0,95 до 2,85 долара США на годину. Зростання вартості праці змушує підприємства автоматизувати виробничі операції, заміняючи працівників роботизованими маніпуляторами;

- Збільшення числа високоточних виробництв. Застосування роботів дозволяє досягати стабільно високої якості виконання операцій.

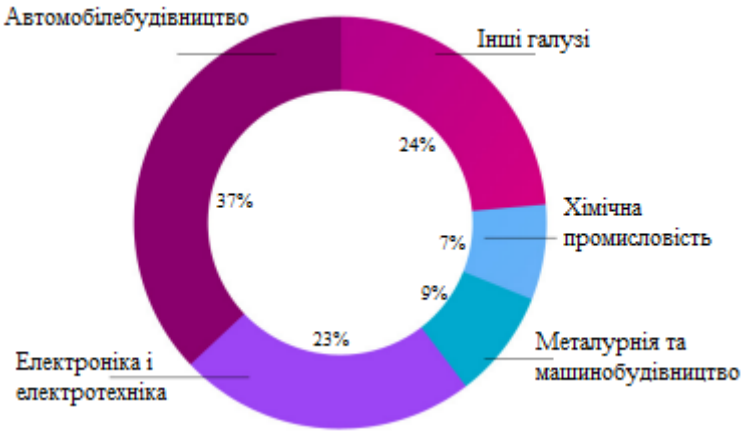


Рис.1.8. Структура світового попиту на промислові роботи з галузей застосування

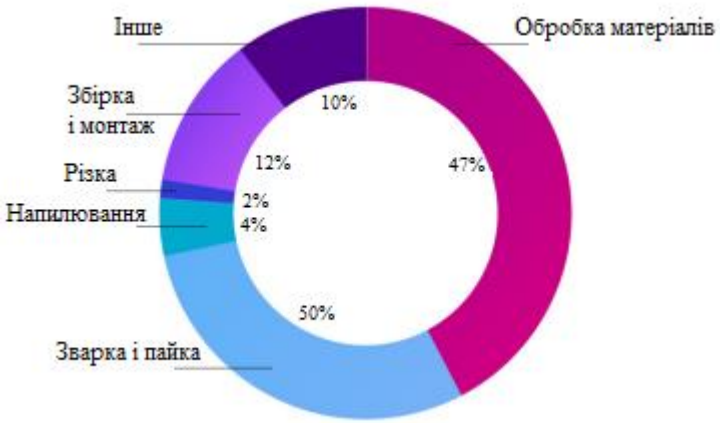


Рис.1.9. Структура світового попиту на промислові роботи з функціонального використання

1.1.2 Огляд ринку сервісної робототехніки

Ринок сервісних роботів виник на початку 1990-х років. Від ринку промислової робототехніки його відрізняє нижчий рівень консолідації, причиною чого є наявність значної частини сегментів, кожен із яких потребує специфічних компетенцій. Технологічний прогрес у сервісній робототехніці багато в чому забезпечується за рахунок військових розробок, що знаходять цивільне застосування.

Цикл розробки відрізняється більшою тривалістю, ніж інших напрямах IT.

У 2000-х роках ринок робототехніки зазнало стрімкого зростання, яке базувалося на технологіях, створених у 1990-х роках. Збільшення обсягів досліджень і розробок у цій галузі, що зазначається в даний час, дозволяє сподіватися на збереження позитивної динаміки до 2025 року.

Обсяг світового ринку. Обсяг світового ринку сервісних роботів перевищує 5,3 млрд. доларів США.

Ця консервативна оцінка відповідає офіційним даним Світової федерації робототехніки (IFR) за 2020 рік. У своїх розрахунках IFR спирається в основному на відкриті джерела, тому є ймовірність, що деякі ніші, наприклад, військова робототехніка, залишилися недооціненими. Згідно з іншим дослідженням, виконаним компанією Markets and Markets, обсяг ринку сервісної робототехніки в 2018 році склав 17,6 млрд доларів США.

Відмінності в оцінках пояснюються тим, що IFR не включає статистику витрати на дослідження, програмне забезпечення, впровадження і системну інтеграцію роботизованих пристроїв. Крім того, у статистиці відсутні військові витрати, які становлять значну частину цього ринку. Згідно з дослідженням компанії Global Industry Analysts, обсяг сегменту військових роботів у 2019 році склав 5,6 млрд доларів США. При цьому експерти прогнозують зростання цього сегмента до 8,5 млрд. доларів США до 2025 року. Абсолютне лідерство у цій ніші утримують США: на закупівлю автономних повітряних, наземних та морських транспортних засобів [6].

Міністерство оборони США в 2019 році планувало виділити 4,8 млрд доларів США. Проте й інші держави мають попит на військових роботів: наприклад, витрати Міністерства оборони Великобританії на розробку та виробництво безпілотних літальних апаратів за 2015–2019 роки становили 3,3 млрд доларів США.

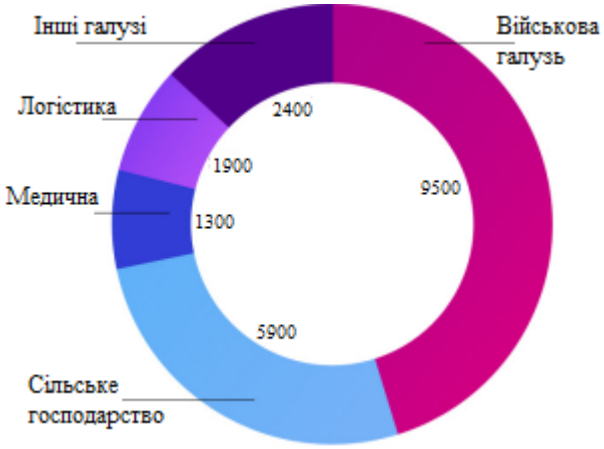


Рис.1.10. Структура ринку професійних сервісних роботів у 2020 році, шт

За оцінкою IFR у 2020 році обсяг ринку професійних сервісних роботів склав 3,57 млрд. доларів США. У натуральному вираженні сегмент зріс із 20,2 тис. пристроїв у 2019 році до 21 тис. у 2020-му. Понад 9,5 тис. з них належать до військових робіт, що становить майже 45% від числа всіх проданих професійних роботів у 2019 році. Найбільш затребуваними з військових роботів виявилися безпілотні літальні апарати (БПЛА): їх продаж у натуральному вираженні зріс на 8% і склав 8,5 тис. одиниць. При цьому експерти визнають, що пов'язана інформація з військовими роботами, не є повністю відкритою, тому дійсні обсяги ринку можуть бути суттєво вищими. Обсяг продажів сільськогосподарських роботів у 2020 році склав 883 млн. доларів США або близько 25% ринку професійних роботів у грошовому вираженні.

Загальна кількість проданих роботів у цьому сегменті становить близько 5,9 тис. штук, або 28% від усіх врахованих IFR професійних роботів. Більшість сільськогосподарських роботів (5,1 тис. штук) становлять автоматизовані доїльні

системи. Серед інших пристроїв переважають роботи для збирання приміщень та автоматичної подачі кормів.

Основну частину ринку професійних сервісних роботів у вартісному вираженні займають медичні пристрої. До цього сегменту відносяться роботизовані хірургічні комплекси, апарати для променевої терапії та пристрої для реабілітації пацієнтів. Обсяг продажів подібних пристроїв становив 1,45 млрд доларів США, або 41% вартості всіх професійних роботів, проданих у 2020 році, без урахування військових систем. Фактично було продано близько 1300 медичних роботизованих приладів, 546 з яких було вироблено американською компанією Intuitive Surgical. Медичні роботи є найдорожчими: базова ціна одного комплексу da Vinchi Surgical System в середньому становить 1,5 млн. доларів США, а в залежності від конфігурації може доходити до 2,3 млн. доларів США.

Ще одним активно розвивається є логістика. 2020 року було продано майже 1,9 тис. роботизованих пристроїв для роботи у виробничих приміщеннях, що на 37% перевищило аналогічні показники 2019 року. Враховуючи велику кількість учасників ринку, експерти вважають, що реальна кількість подібних пристроїв може суттєво перевищувати зроблені оцінки. Загальний обсяг цієї ніші у грошовому вираженні за 2020 рік становив 216 млн доларів США.

Обсяг продажів інших пристроїв із сегменту професійної сервісної робототехніки становив близько 2,4 тис. штук. У цю категорію потрапляють різні пристрої: машини для прибирання комерційної нерухомості, офісні роботи телеприсутності, пристрої для внутрішньотрубної діагностики і підводні роботи вартістю понад 3,1 млн доларів США.

У сегменті споживчої робототехніки в 2020 році було продано близько 4 млн. пристроїв на загальну суму близько 1,7 млрд. доларів США. Майже 2,7 млн із цієї кількості — це роботи для виконання роботи по будинку: пилососи, газонокосарки та інші побутові пристрої. Обсяг ніші побутових роботів склав 799 млн. доларів США. У сегменті роботів для розваг у 2020 році було продано 1,2 млн. пристроїв.

У грошах цей ринок склав 911 млн доларів США.

1.2 Оцінка обсягів інвестицій у робототехніку

Складність оцінки обсягів венчурного інвестування у сфері сервісної робототехніки пов'язана з нестачею інформації про угоди. Згідно з даними порталу про робототехніку hyzook.com, у 2020 році розробники роботів залучили щонайменше 235 млн. доларів США венчурного капіталу. Для порівняння: 2019 року ця цифра становила 196 млн доларів США, а 2018-го — 157 млн. доларів.

В рамках цього дослідження було здійснено аналіз сегменту венчурних інвестицій у робототехніку на основі відкритих джерел. У таблиці нижче наведено дані про обсяг венчурних інвестицій у цілому, а також робототехнічну галузь.

Таблиця 1.2.

Загальний об’єм венчурних інвестицій в світі, млн.дол. США

	2018 рік	**2019 рік**	**2020 рік**
Венчурні інвестиції	54700	47600	48500
В тому числі в робототехніку	157	196	235

В США позитивна динаміка інвестування спостерігається також в окремих сегментах ринку робототехніки. Цю тенденцію можна простежити з прикладу інвестицій у проекти безпілотних літальних апаратів. Так, аналітичний ресурс CB Insight опублікував дані про інвестиції у цьому напрямі з 2017 року. Згідно з проведеним ним аналізом, ринок безпілотних літальних апаратів в даний час знаходиться у фазі швидкого зростання.

Найбільшу активність у поглинанні розробників роботів демонструють лідери ринку IT: Google, Aethon та ін.

Інвестиційна активність починає приносити свої плоди і з погляду виходів. Якщо 2011 року виходи були поодинокими, то 2019-го було здійснено 12 угод зі стратегічними інвесторами, а 2020-го — вже шістнадцять. Крім того, у березні 2021 року японський виробник екзоскелетів Cyberdyne успішно вийшов на токійську біржу і залучив 86 млн. доларів США [2].

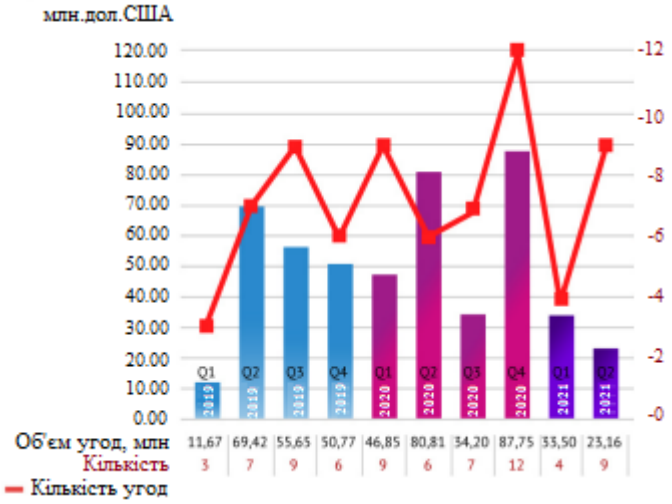


Рис.1.11. Обсяг інвестицій та кількість угод у робототехнічній галузі

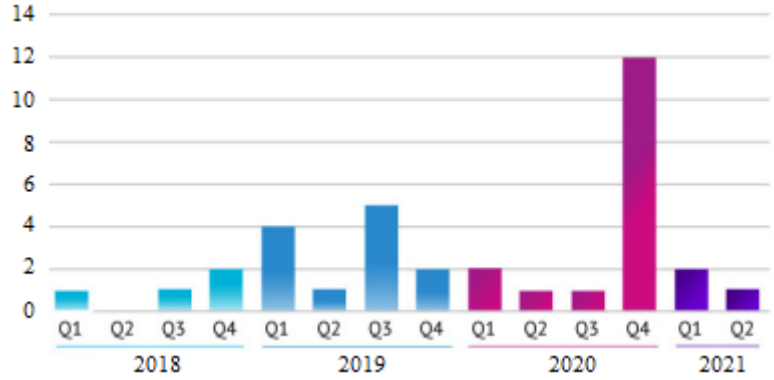


Рис.1.12. Число угод з купівлі компаній у галузі робототехніки, шт.

Кількість спеціалізованих робототехнічних венчурних фондів невелика. Найбільш типовими прикладами є Drone.VC Syndicate, Grishin Robotics та інші.

Drone.VC Syndicate - венчурний фонд, який орієнтований на компанії, що розробляють дрони комерційного призначення, у тому числі для сільського господарства, нафто- та газовидобутку, нерухомості, у сферах логістики та безпеки. Drone.VC Syndicate планує протягом найближчих трьох п'яти років інвестувати в 30 компаній, що знаходяться на різних стадіях зрілості.

Robert Bosch Venture Capital – корпоративний венчурний фонд німецького виробника автокомпонентів, промислового обладнання та побутової техніки Bosch.

Фонд орієнтований проекти ранніх стадій. Серед пріоритетів — автоматизація та робототехніка. Розмір перших раундів становить від 1,5 до 4 млн. євро. В разі

Участь фонду в наступних раундах інвестиції може досягати 6-10 млн євро за частку в 10-20% у капіталі компанії.

У квітні 2021 року Robert Bosch Venture Capital спільно з венчурними фондами Innovacom та SEB Alliance інвестував 3 млн. євро в робототехнічну компанію Robart, яка займається системами навігації для автономних роботизованих побутових приладів.

1.3 Підтримка розвитку робототехніки у Європі

Європейські виробники займають міцні позиції ринку промислової робототехніки з допомогою ємного місцевого ринку. Основними викликами для Європи є утримання технологічного лідерства та освоєння нових ніш на ринку сервісних роботів.

Промислова робототехніка. Історія європейської промислової робототехніки налічує понад 40 років. Перший виробничий маніпулятор Famulus із шістьма ступенями свободи був створений німецькою компанією KUKA у 1973 році.

У 2019 році Європа займала 27% ринку промислової робототехніки за обсягами закупівлі нових промислових роботів. Їх використання є одним із ключових факторів, що дозволяють зберігати конкурентоспроможність європейської промислової продукції в умовах високої вартості праці.

2019 року в Європі було продано 41,2 тис. промислових роботів. 2018-го цей показник становив 43,8 тис. одиниць. Середнє річне зростання галузі за кількістю проданих одиниць з 2014 по 2019 рік становило 3%. Основними споживачами кількості куплених роботів на ринку європейської промислової робототехніки є Німеччина, Італія, Франція, Великобританія та Іспанія.

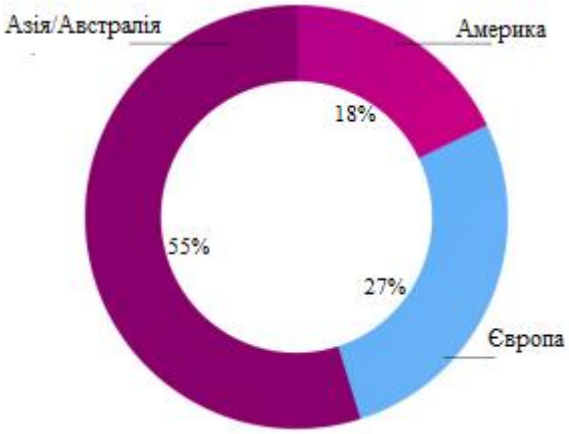


Рис.1.13. Структура продажів промислових роботів у натуральному вираженні по регіонах, 2019 рік

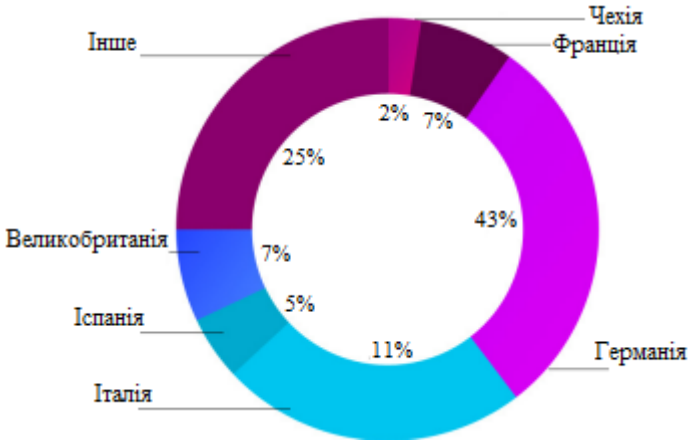


Рис.1.14. Структура продажів промислових роботів країнами Європи, 2019 рік

Найбільші гравці на ринку промислової робототехніки у Європі: KUKA (Німеччина), Schunk (Німеччина), ABB (Швеція), Stäubli (Швейцарія), Comau (Італія).

Основними галузями застосування промислової робототехніки у Європі є автомобільна, металургійна, хімічна та електронна промисловість. Потенціал у розвиток робототехніки також представляє харчова галузь [5].

Сервісна робототехніка. Європа є лідером у виробництві професійних сервісних роботів, якщо не брати до уваги пристрій військового призначення. Найбільш сильні напрямки: мобільні роботи (сільськогосподарські, шахтні роботи,

пошукові), транспортно-логістичні (транспортування, складські роботи), медичні (хірургічні, діагностичні, роботи-помічники для пацієнтів).

Європейська спрямованість зниження енергоємності економіки створює потенціал у розвиток автоматизованих енергоефективних технологій, застосовуваних у побуті. Найбільші гравці на ринку сервісної робототехніки: Amazonen Werke (Німеччина),

In Mach (Німеччина), BA Systèmes (Франція), DeLaval (Швеція), Fullwood (Великобританія), Insentec (Нідерланди), Lely (Нідерланди), GEA Farm Technologies (Німеччина), Thales (Франція), Eca-Robotics (Франція) , QinetiQ (Велика Британія).

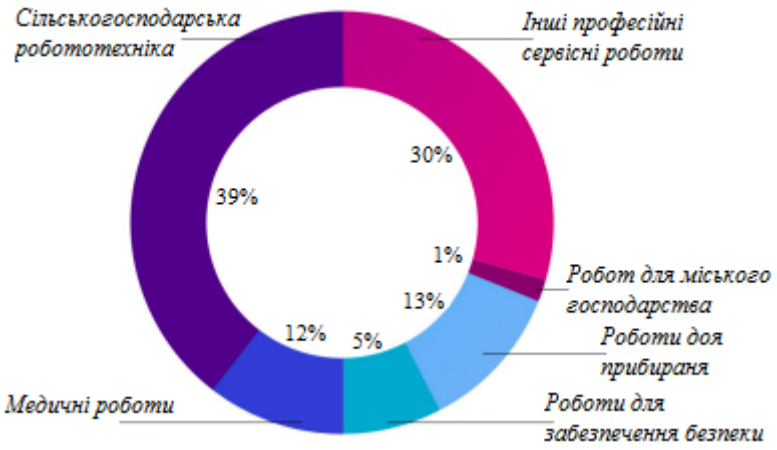


Рис.1.15. Області застосування професійних сервісних роботів у Європі, 2016 рік

Незважаючи на певні успіхи, європейська робототехніка має вразливі місця, які перешкоджають подальшому розвитку:

- Компанії-стартапи стикаються зі складністю переходу від етапу створення прототипу до стадії продажу готового продукту. У Європі недостатньо розвинена підтримка ранніх стадій інноваційних проектів, зокрема й у галузі робототехніки;

- дефіцит венчурного капіталу: європейські стартапи зазнають складнощів із залученням фінансування на посівній стадії;

- відсутність поінформованості потенційних споживачів про робототехніку та можливості її використання;

- слабка взаємодія між академічними колами та бізнес-сектором.

Робототехнічні кластери поки що перебувають у стадії формування;

- Залежність від імпортних базових компонентів для робототехніки. Зокрема, датчики та силові приводи імпортуються до Європи з інших країн;

- Використання робототехніки в суспільстві викликає багато етичних, правових та соціальних проблем (ELS). Європа очолює всесвітню дискусію на цю тему [7].

1.4 Перспективи та прогнози розвитку робототехніки

У міру свого розвитку інформаційні технології охоплюють нові галузі. В результаті динамічно розвиваються такі ринкові сегменти, як «розумний дім», цифрове виробництво, електроніка, що «носиться» і робототехніка. Найважливішими технологічними трендами, здатними забезпечити розвиток нових ринків у короткостроковій перспективі, є:

- Зростання обчислювальних потужностей. Це найважливіший тренд, який впливає на робототехніку. Згідно з деякими оцінками, основний внесок у зростання продуктивності праці в США з 1973 по 2011 рік зробив розвиток інформаційних технологій. Збільшення продуктивності комп'ютерів уможливлює появу нових ніш на ринку сервісних роботів;

- Зниження вартості компонентів. Стрімке розширення ринку сервісних роботів призводить до збільшення обсягів виробництва ключових комплектуючих: електродвигунів, редукторів та ін, що веде до зниження цін. Також впливає ринок поява нових гравців і поступове зростання якості комплектуючих китайських виробників;

- Стандартизація платформ у робототехніці. Це додатковий фактор зниження вартості розробки та виробництва нових продуктів. Подібно до того, як створення IBM PC призвело до розвитку ринку доступних персональних комп'ютерів, нові, у тому числі відкриті платформи роботів дозволять радикально знизити ціну на масові продукти, наприклад, на персональні коптери, медичні маніпулятори,

мобільні платформи. Це призведе до швидкого розвитку сервісів та інтегрованих рішень, що надаються на їх основі.

Розвиток робототехніки залежить від прогресу базових технологій, наприклад, машинного зору або навігації. На підставі опитування російських експертів та аналізу тематик зарубіжних досліджень нами були виділені технологічні обмеження розвитку робототехніки у світі, а також можливі шляхи їх подолання, які впливатимуть на створення нових продуктів та ринкових ніш [8].

Як найбільш значущі в економічному та соціальному відношенні були виділені такі сфери застосування робототехніки:

- логістика є перспективним напрямом для використання роботів, оскільки оперує з добре структурованими даними та об'єктами.

Нині вже відбувається автоматизація складської логістики. Істотного економічного ефекту може бути досягнуто у сфері транспортної логістики, особливо для вирішення проблеми доставки у великих мегаполісах, а також за рахунок використання безпілотних автомобілів;

- медицина та охорона здоров'я зазвичай пред'являють високий попит на передові технології. Хірургічні маніпулятори та технології неінвазивної променевої терапії поступово стають стандартом лікування. Розвиток технологій протезів та медичних екзоскелетів є скоріше соціальною, ніж комерційною сферою, проте прогрес у цій галузі призведе до суттєвого підвищення якості життя інвалідів;

- оборонні відомства та спеціальні служби є основними споживачами сервісних роботів, а також важливим джерелом інновацій у цій сфері. Робототехніка знижує ризики для особового складу у бою або під час несення служби в екстремальних умовах. Розвиток робототехніки дозволить досягти радикальних змін у тактиці військових операцій;

- Видобуток природних копалин. Основні перспективи в автоматизації цієї галузі пов'язані із заміною людини роботизованими машинами на небезпечних та шкідливих виробництвах, наприклад у кар'єрах. Переміщення видобутку нафти та газу на шельфи та прокладання трубопроводів по дну акваторій створюють попит

на підводних роботів, здатних контролювати інфраструктуру та проводити ремонт. Ще одним напрямком є використання БПЛА для моніторингу територіально розподілених систем, наприклад трубопроводів чи доріг;

- логістика є перспективним напрямом для використання роботів, оскільки оперує з добре структурованими даними та об'єктами.

Нині вже відбувається автоматизація складської логістики. Суттєвого економічного ефекту може бути досягнуто у сфері транспортної логістики, особливо для вирішення проблеми доставки у великих мегаполісах, а також за рахунок використання безпілотних автомобілів;

- медицина та охорона здоров'я зазвичай пред'являють високий попит на передові технології. Хірургічні маніпулятори та технології неінвазивної лучової терапії поступово стають стандартом лікування. Розвиток технологій протезів та медичних екзоскелетів є скоріше соціальною, ніж комерційною сферою, проте прогрес у цій галузі призведе до суттєвого підвищення якості життя інвалідів;

- оборонні ведомства та спеціальні служби є основними споживачами сервісних роботів, а також важливим джерелом інновацій у цій сфері. Робототехніка знижує ризики для особового складу біля бою або під час несення служби в екстремальних умовах. Розвиток робототехніки дозволить досягти радикальних змін у тактиці військових операцій;

- Добування природних іскопаючих. Основні перспективи в автоматизації цієї галузі пов'язані із заміною людини роботизованими машинами на небезпечних та шкідливих виробництвах, наприклад у кар'єрах. Переміщення видобутку нафти та газу на шельфі та прокладання трубопроводів по дну акваторій створюють попит на підводних роботів, здатних контролювати інфраструктуру та проводити ремонт. Ще одним напрямком є використання БПЛА для моніторингу територіально розподілених систем, наприклад трубопроводів чи доріг;

- догляд за людьми похилого віку та інвалідами є серйозною економічною та соціальною проблемою для суспільств зі зростаючою часткою літнього населення.

Впровадження роботизованих пристроїв для пересування, моніторингу стану та допомоги інвалідам дасть величезний економічний ефект для Японії та країн

Західної Європи, оскільки в майбутньому дозволить відмовитися від послуг доглядальниць та звільнить значні трудові ресурси, задіяні у цій роботі;

- сільське господарство. Нині найбільшою нішою сільськогосподарських роботів є доїльні апарати. Зростання попиту спостерігається в сегменті БПЛА для моніторингу та обробки посівних площ. Крім того, у майбутньому будуть затребувані роботи для заміщення людини в операціях, які вимагають ручної праці: вибіркова обробка посівів, збирання та сортування плодів тощо;

- будівництво - галузь, у якій використання роботів може дати значний економічний ефект у середньостроковій перспективі. Її особливістю є добре структуроване середовище, що має чіткий план та прив'язку до місцевості, а також використання стандартизованих матеріалів. Ефект від впровадження роботів може бути досягнутий за рахунок скорочення термінів, зниження потреби у некваліфікованій робочій силі та підвищення якості будівництва;

- автоматизація домашньої роботи є актуальним завданням робототехніки, хоча поки що знаходиться на початку свого розвитку. Зростання вартості праці буде призводити до збільшення попиту на роботів, здатних займатися роботою по дому. З іншого боку, люди з певним матеріальним статком прагнутимуть відмовитися від праці покоївок, кухарів та інших працівників [8].

Рис.1.16. Прогнози розвитку робототехніки

1.5 Загальна характеристика та принципи побудови системи управління робототехнічними комплексами

Роботи, які використовуються в критично важливих процесах, до прикладу, пошук та знешкодження вибухонебезпечних пристроїв, пошук радіоактивних зон, ліквідація наслідків аварій в складних ландшафтних місцях, потребують особливої уваги при проектуванні та експлуатації, оскільки від них залежать життя людей. При цьому, дуже часто, використання роботів в таких критичних умовах є єдиним реальним рішенням проблеми.

Рішення, які використовують при проектуванні сучасних роботів, основані на використанні МРК, принцип роботи яких передбачає дистанційне керування оператором за визначеними командами. Такий МРК має в своєму складі мобільного робота з маніпулятором та апаратною частиною, та дистанційне керування (пульт, який з'єднується з роботом по каналах зв'язку). [9].

На рис. 1.17. представлено структурну схему, яка демонструє систему управління та обробки даних МРК

Рис. 1.17. Система управління та обробки даних МРК

Принцип роботи наступний. Для зручності інформування оператора про стан робота, на робочому комп'ютері реалізовано графічний інтерфейс. Він забезпечує інформаційну підтримку роботи оператора за допомогою графічного системи Photon, з ОС реального часу QNX.

Для обміну інформацією та взаємодії між обчислювальними завданнями на бортових ПК та пультах, реалізовано системне мережеве середовище:

- передача даних по кабельним системам між пультовим ПК управління та пультовим ПК, який займається обробкою даних пошукової апаратури. Цей же принцип, між бортовою ЕОМ управління та бортовою ЕОМ обробки даних пошукової апаратур

- передача даних по радіомережах між пультовим та бортовим комп'ютером, який відповідає за управління. Цей же принцип між між пультовою та бортовою ЕОМ обробки даних пошукової апаратури.

Математичне та ПЗ. Прикладне програмно-математичне забезпечення (ПМЗ) комплексу пультового комп'ютера оператора-водія включає наступні програми:

- пультову програму, яка забезпечує диспетчеризацію процесів, координацію функціонування пультових завдань з обчислення та обмін інформації між різними завданнями;

- графічний інтерфейс (програма), який полегшує сприйняття та підвищує продуктивність діяльності оператора;

- пультові програми управління компонентами дистанційно керованого комплексу розмінування (ДККР), який надає можливість реалізації функцій та сценаріїв автоматизованого управління;

- програму для систематизації та подальшої обробки інформації щодо функціонування компонентів ДККР, що забезпечує ведення протоколу виконання робіт.

До складу прикладного ПЗ пультового комп'ютера обробки даних пошукової апаратури включає входять наступні програми:

- графічний інтерфейс (програма) оператора-пошуковика, який забезпечує візуалізацію інформації, яка надсилається з пошукової апаратури, та інформаційну підтримку його діяльності;

- програми вторинної обробки інформації, що надходить із пошукової апаратури та надає ідентифікацію виявлених об'єктів з інформації, яка надходить з камер.

Прикладне програмне забезпечення бортового комп’ютера управління складається з наступних програми:

- бортову програму диспетчеризації, яка необхідна для координації бортових обчислювальних завдань та задля обміну інформацією між цими завданнями;

- бортові програми управління, що забезпечують обробку інформації з датчиків компонентів ДККР, які забезпечують виконання розрахунків, , у вигляді послідовностей команд виконавчим механізмам компонентів ДККР;

- програму обробки та збору інформації про функціонування компонентів ДККР, яка необхідна для ведення протоколу виконання робіт.

Прикладне програмне забезпечення бортового ПК для обробки даних пошукової апаратури складається з наступних програм [9]:

- програму первинної обробки даних пошукової апаратури, яка забезпечує алгоритми виявлення об'єктів, за якими здійснюється пошук;

- програму для первинної обробки інформації, яка передається із телекамер.

2 ДОСЛІДЖЕННЯ КОМПЛЕКСУ МЕТОДІВ І ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ У РАДІОКАНАЛАХ

2.1 Огляд особливостей безпроводової мережі стандарту IEEE 802.11

Особливості протоколу 802.11, а саме структура реалізованого в ньому механізму для захисту інформації, надають йому чимало уразливостей. Наприклад, слабким місцем з точки зору захисту інформації, є протокол WEP, який для шифрування інформації використовує секретний ключ [10]. Також, 802.11 не не враховує можливість аутентифікації та поділ секретних ключів між окремими станціями мережі.

Принцип захисту в бездротових мережах багато в чому відрізняється від забезпечення безпеки проводових мереж. Для захисту звичайної дротової мережі від зовнішніх атак достатньо створити безпечний периметр з мережевих екранів на мережевих інтерфейсах, через які здійснюється підключення внутрішньої захищеної мережі до зовнішніх відкритих сегментів. У разі бездротової інфраструктури цього підходу явно недостатньо. За відсутності надійної системи аутентифікації зловмисник може увійти у внутрішню мережу, опинившись у зоні із достатнім рівнем сигналу. Навіть якщо неможливо зареєструватись в мережі атакуюча сторона має велику можливість здійснення перехоплення всього трафіку внутрішньої мережі.

У 2001 році група з Каліфорнійського університету в Берклі представила документ, в якому описуються слабкі сторони механізму безпеки 802.11 WEP (дротова еквівалентна конфіденційність), визначеного в оригінальному стандарті; за ними була робота Флюрера, Мантіна та Шаміра під назвою «Слабкі сторони в алгоритмі планування ключа RC4». Невдовзі Адам Стабблфілд і AT&T публічно оголосили про першу перевірку атаки. Під час атаки вони змогли перехопити передачу та отримати несанкціонований доступ до бездротових мереж.

IEEE створив спеціальну групу завдань для створення замінного рішення безпеки під назвою 802.11i, яке раніше використовувалося як частина ширшої роботи 802.11e для покращення рівня MAC. Wi-Fi Alliance оголосив про проміжну специфікацію під назвою Wi-Fi Protected Access (WPA) на основі підмножини поточного проекту IEEE 802.11i. Вони почали з'являтися в продуктах у середині 2003 року, а WPA2 був ратифікований в червні 2004 року і використовує розширений стандарт шифрування замість RC4, який використовувався в WEP і WPA.

Визначення сумісності Wi-Fi Alliance виходить далеко за межі можливості працювати в мережі Wi-Fi. Щоб отримати сертифікацію за певною програмою, продукти повинні демонструвати задовільний рівень продуктивності в типових мережевих конфігураціях і підтримувати як встановлені, так і нові програми. Наприклад, користувач, який купує ноутбук із підтримкою Wi-Fi, не буде задоволений, якщо ноутбук встановить з'єднання з домашньою мережею, лише щоб отримати пропускну здатність комутованого з'єднання. Аналогічно, абоненти, які використовують мобільний телефон із підтримкою Wi-Fi, будуть розчаровані, якби голосовий дзвінок не проходив або був перерваний.

Процес сертифікації Wi-Fi Alliance включає три типи тестів для забезпечення сумісності. Сертифіковані продукти Wi-Fi перевірені на:

1. Сумісність: сертифіковане обладнання перевірено на підключення до іншого сертифікованого обладнання. Тестування на сумісність завжди було і залишається переважаючим компонентом тестування інтероперабельності, і це елемент, який більшість людей асоціює зі «сумісністю». Він включає тести з кількома пристроями від різних постачальників обладнання. Тестування на сумісність – це програмний компонент, який допомагає переконатися, що пристрої, придбані сьогодні, працюватимуть із сертифікованими пристроями Wi-Fi, які вже є у власності чи придбані в майбутньому.

2. Відповідність: обладнання відповідає певним критичним елементам стандарту IEEE 802.11. Тестування відповідності зазвичай включає окремий аналіз окремих продуктів і встановлює, чи реагує обладнання на вхідні дані, як

очікувалося та зазначено. Наприклад, тестування на відповідність використовується, щоб переконатися, що обладнання Wi-Fi захищає себе та мережу, коли обладнання виявляє ознаки мережевих атак.

3. Продуктивність: обладнання відповідає рівням продуктивності, необхідним для задоволення очікувань кінцевих користувачів щодо підтримки ключових додатків. Тести продуктивності призначені не для вимірювання та порівняння продуктивності між продуктами, а просто для того, щоб переконатися, що продукт відповідає мінімальним вимогам до продуктивності для хорошого користування, встановленим Wi-Fi Alliance. Конкретні результати тестів продуктивності Wi-Fi Alliance не оприлюднює.

IEEE 802.11 має два фундаментальних архітектурних компонента:

Станція (STA). STA — це бездротовий кінцевий пристрій. Типовими прикладами STA є портативні комп’ютери, КПК, мобільні телефони та інші користувальницькі електронні пристрої з можливостями IEEE 802.11.

Точка доступу (ТД). ТД логічно з’єднує STA з системою розподілу (СР), яка зазвичай є дротовою інфраструктурою організації. Точки доступу також можуть логічно з’єднувати бездротові STA один з одним без доступу до СР. Крім того, точки доступу можуть функціонувати в мостовому режимі, що дозволяє точкам доступу створювати з’єднання «точка-точка» для приєднання двох окремих мереж.

Стандарт IEEE 802.11 визначає дві основні топології мережі. Перший, спеціальний режим, не використовується АР — лише STA задіяні в комунікації. Другий, інфраструктурний режим, має точку доступу з’єднує бездротові STA один з одним або з СР, як правило, дротовою мережею. Інфраструктурний режим – це найбільш часто використовуваний режим для WLAN.

Режим ad hoc концептуально зображений на рисунку 2.1. Цей режим роботи, також відомий як режим однорангового зв’язку, можливий, коли два або більше STA можуть спілкуватися безпосередньо один з одним. Рисунок 2-1 показує три пристрої, які спілкуються один з одним у режимі однорангового зв'язку без будь-яких бездротових з'єднань інфраструктури або дротових з'єднань. Набір STA,

налаштований таким чином, відомий як незалежний базовий сервісний набір (IBSS).

Рис. 2.1. Режим ad hoc

Однією з ключових переваг ad hoc WLAN є те, що теоретично їх можна сформувати в будь-який час і в будь-якому місці, дозволяючи кільком користувачам створювати бездротові з’єднання дешево, швидко та легко з мінімальним обслуговуванням обладнання та користувача. На практиці можлива низка різних типів спеціальних мереж, і специфікація IEEE 802.11 дозволяє багато з них. Можна створити спеціальну мережу для різні причини, наприклад, підтримка обміну файлами між двома клієнтськими пристроями. Однак клієнтські пристрої, що працюють виключно в режимі ad hoc, не можуть спілкуватися із зовнішніми бездротовими мережами. Ще одна складність полягає в тому, що спеціальна мережа може заважати роботі мережі в режимі інфраструктури на основі точки доступу, яка існує в тому самому бездротовому просторі.

У режимі інфраструктури WLAN IEEE 802.11 містить один або кілька базових наборів послуг (BSS), основних будівельних блоків WLAN. BSS включає ТД і одну або більше станцій. AP в BSS з'єднує станції з системою розподілу (CP). CP — це засіб, за допомогою якого станція можуть спілкуватися з дротовими локальними мережами організації та зовнішніми мережами, такими як Інтернет. Режим інфраструктури IEEE 802.11 показаний на рисунку 2.2 двома BSS, підключеними до CP.

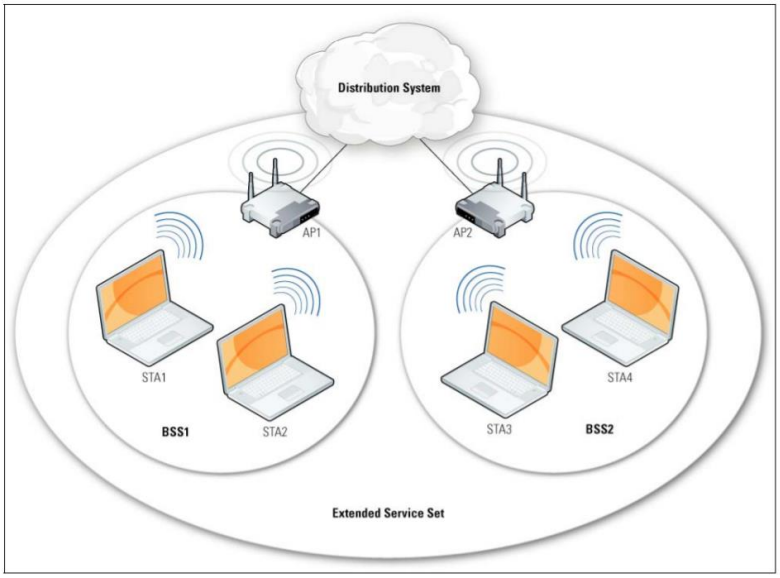


Рис. 2.2. Режим інфраструктури IEEE 802.11

2.2 Класифікація типів атак на радіоканал

Одними з ключових ризиків при використанні безпроводової мережевої інфраструктури стандарту 802.11 є атаки на конфіденційність інформації, а також на цілісність, доступність мережевих ресурсів.

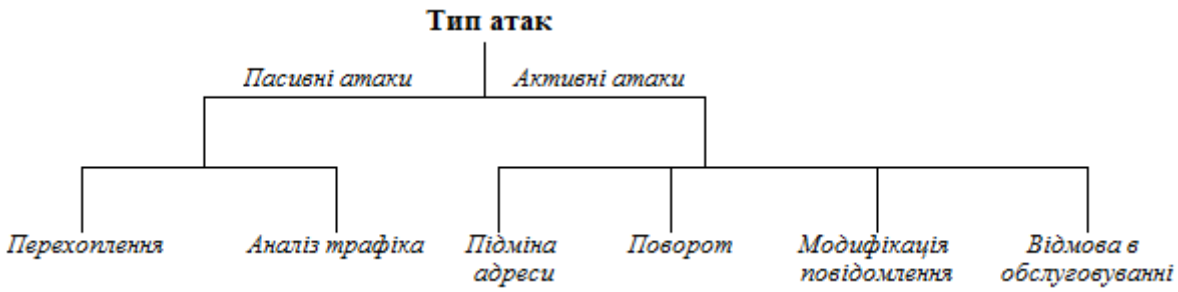


Рис. 2.3 Типи атак на бездротову мережу стандарту 802.11

На рис. 2.3 показано, що атаки можна поділити на два основних класи: на активні та на пасивні. Класифікація виділяє ще підкласи в цих основних класах.

Якщо говорять про пасивні атаки, то вважають, що неавторизована сторона отримує доступ до даних, при цьому не відбувається їх модифікація. До цього типу атак відносять перехоплення даних та використання аналізатора трафіку. Такий тип атаки системний адміністратор не може встановити.

Під перехопленням трафіку розуміють можливість третьою стороною переглядати зміст повідомлень, пересланих по бездротовій мережі. Це може відбуватися між станцією та точкою доступу, чи між окремими станціями в мережі.

Аналіз трафіку передбачає застосування фільтрації трафіку за визначеними критеріями.

Активні атаки передбачають можливість модифікації перехвачених повідомлень. Цьому типі атак виділяють чотири підкласи:

1. Модифікація повідомлення, яка можлива шляхом додавання, вилучення або зміни передаваємих даних.

2. Повтор – перехоплення третьою стороною даних та їх подальша передача під виглядом авторизованого користувача.

3. Зміна адреси. Третя сторона при зміні адреси отримує частину можливостей авторизованого користувача.

4. Відмова в обслуговуванні – третьою стороною, яка формує повідомлення певного виду, стає неможливою повноцінне користування безпроводовою мережею.

2.3 Огляд методів захисту інформації на базі протоколу WEP

Протокол WEP призначений для бездротової локальної мережі та є частиною стандарту безпеки IEEE 802.11. У WEP для забезпечення безпеки та цілісності даних використовується циклічний код надмірності (CRC-32), а для забезпечення конфіденційності використовується потоковий шифр RC4. Стандартна специфікація WEP підтримує довжину ключа 40 біт, а нестандартна специфікація забезпечує довжину ключа 128 та 256 біт при шифруванні даних.

Процес шифрування WEP для передачі даних складається з 5 кроків. В процесі ініціалізації 24-бітний вектор послідовно зв'язується разом з 40-бітним ключом WEP. Алгоритм цілісності виконується для простого тексту, тому може бути згенеровано значення перевірки цілісності, яке потім пов'язується з простим текстом. Щоб згенерувати зашифрований текст, алгоритм RC4 застосовується до

звичайного тексту на додаток до та послідовності ключів. Кадр корисної навантаження управління доступом до бездротового середовища (MAC) генерується шляхом приміщення вектора ініціалізації перед зашифрованими даними, що поєднують перевірку цілісності разом з іншими полями.

Як правило, у 802.11 відбувається взаємодія між клієнтською станцією та ТД, використовуючи радіохвилі. Якщо перешкоди (до них відносять несучі стіни, різного типу перешкоди на шляху розповсюдження сигналу) між ТД та клієнтською станцією не забивають радіосигнал, в такому випадку немає необхідності у прямій видимості. Поряд зі специфікаціями передачі даних стандарт визначає протокол WEP (Wired Equivalent Privacy), що є механізмом захисту даних при передачі по радіоканалу від перехоплення. Захист інформації здійснюється за допомогою зовнішнього сервісу управління ключами, створеними для процесів шифрування та розшифрування повідомлень, що передаються мережею. WEP це необов’язковий компонентом стандарту IEEE 802.11 і може реалізовуватися у пристроях бездротового зв'язку, а не у самій мережі.

Серед основних особливостей та характеристик алгоритму WEP можна назвати:

- Висока стійкість до підбору ключів. Ця характеристика на пряму залежить від того, якою буде довжина секретного ключа, та як часто він буде змінюватися.

- Самосинхронізація. Під цією характеритсикою розуміється, що алгоритм WEP дає змогу синхронізувати кожне з послань. Це стає вкрай актуальним для шифрування інформації на канальному рівні, для мереж з надвисокою вимогою до надійності передачі та при високих ймовірностях втрати інформаційних пакетів.

- Ефективність для реалізації. Оосбливості алгоритму WEP дозволяють його реалізації як на програмному так і на апаратному рівнях.

Розглянемо принцип його функціонування. Стандартний процес захисту від перехоплення під час передачі інформації по радіоканалу зводиться до шифрування даних [12]. Нехай:

-P (plaintext) – незашифровані дані, які підлягають передачі;

- C (ciphertext) – зашифровані дані.

Криптографічний алгоритм представляє собою реалізацію математичної функції для шифрування чи дешифрування даних. Функція шифрування E перетворює P в C:

$$E_k(P) = C$$

Для зворотнього перетворення використовують функцію D, яка здійснює дешифрування:

$$D_k(C) = P$$

На рис. 2.4 бачимо, що один і той самий ключ може використовуватися для шифрування, і для дешифрування даних:

$$D_k\big(E_k(P)\big) = P$$

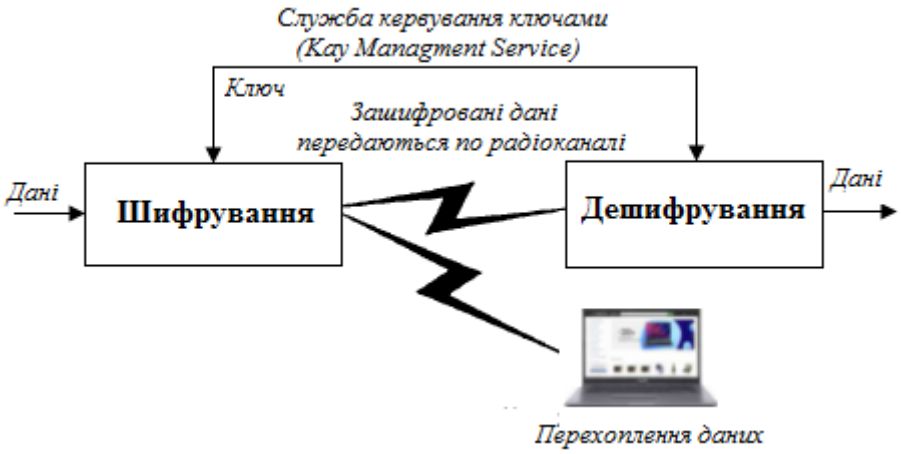


Рис. 2.4. зображено процес шифрування даних.

Для шифрування використовують секретний ключ, який мають обидві сторони передачі інформації. Він доставляється зовнішньою службою керування ключами.

Секретний ключ з використанням операції конкатенації об’єднується з вектором ініціалізації (IV). Результат цієї операції надходить на вхід генератора псевдовипадкових чисел (PRNG RC4). Вихід генератора - ключова послідовність, яка складається з псевдовипадкових октетів, та, в свою чергу, дорівнює довжині переданих даних + 4, так як послання включає значення контролю цілісності (integrity check value - ICV):

$$k = RC4(IV, K)$$

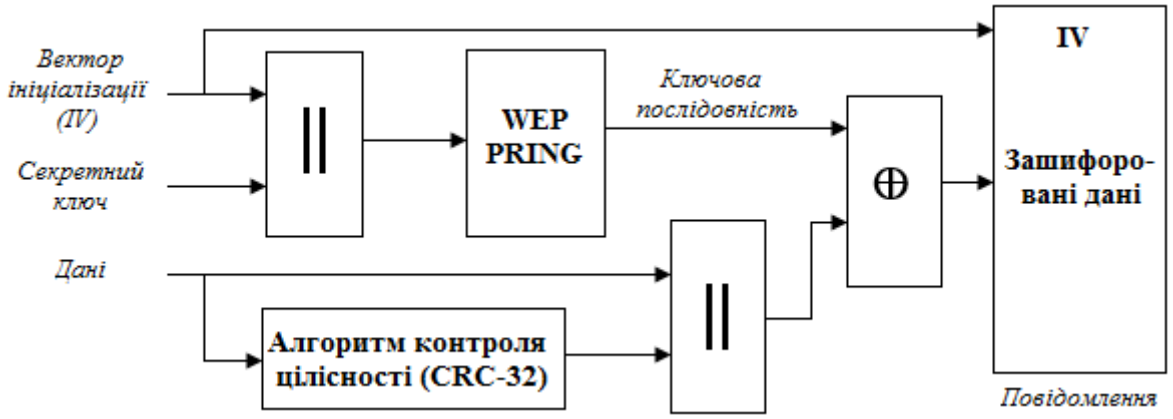


Рис.2.5. Шифрування даних

Для захисту від неавторизованої зміни даних алгоритм контролю цілісності (CRC-32) визначає c(P) - значення ICV від P. Дані P поєднуються зі значення контролю цілісності:

$$M = P||c(P)$$

Закішчення процесу шифрування - комбінування (операція «що виключає АБО» - XOR) ключової послідовності і даних, об'єднаних зі значенням ICV (M):

$$C = M \oplus RC4(IV, K)$$

Вихідним значенням процесу є повідомлення, яке має IV і зашифрований текст, яке готове до передачі по радіолінії.

Символічно перетворення можна записати у такій формі:

$$A \rightarrow B: IV, (M \oplus RC4(IV, K) \text{де } M = P||c(P)$$

Найбільш критичним компонентом є генератор псевдовипадкових чисел. Він трансформує достатньо короткий секретний ключ. Оскільки необхідна передача тільки одного секретного ключа між станціями взаємодії, це значно полегшує розподіл ключів.

Вектор ініціалізації (BI) забезпечує продовження ефективного часу використання секретного ключа та надає можливість самосинхронізації алгоритму. Секретний ключ залишається незмінним (постійним), тоді як BI періодично підлягає зміні. Кожен новий вектор ініціалізації породжує нову ключову

послідовність, саме так відбувається створення однозначної відповідності між вектором ініціалізації та таким чином створюється однозначна відповідність між IV і До.

На рисунку 2.6 представлено процес дешифрування повідомлення.

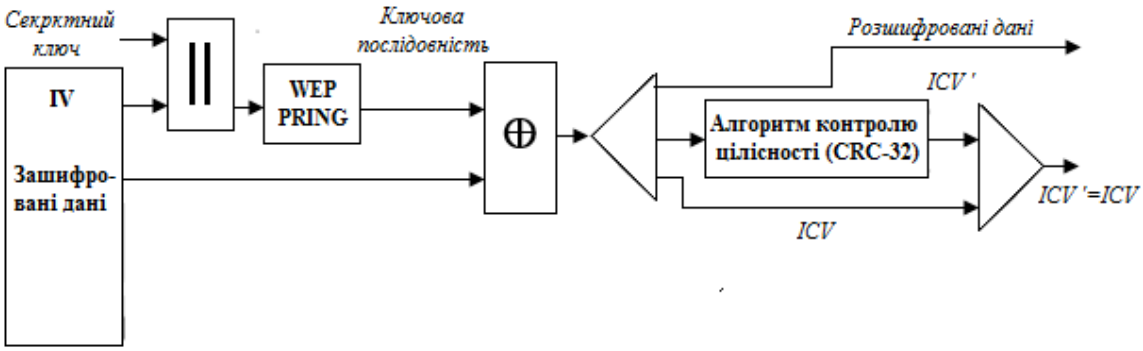


Рис. 2.6. Процес дешифрування повідомлення

Завдяки вектору ініціалізації, який є частиною повідомлення, стає можливою генерація ключової послідовності, яка необхідна для дешифрування даних. Використання операцію XOR до зашифрованих даних та певної ключової послідовності дозволяє отримати вихідні розшифровані дані та значення ICV:

$$M' = \text{C} \oplus RC4(IV, K) = (\text{M} \oplus RC4(IV, K)) \oplus RC4(IV, K) = M$$

де $M = P||c(P)$

Щоб перевірити коректність шифрування даних можна використовувати порівняння отриманого ICV і подальшого обчислення значення ICV' = c(P') над даними, які відновлено. Якщо знайдений ICV' не відповідає ICV, отриманий з повідомленням, розуміємо, що виникає помилка.

2.4 Огляд можливостей захисту із застосуванням методу аутентифікації EAP

Шаблонна система аутентифікації має ряд недоліків, найголовніші з них наступні:

1. Необхідність доставки загального секретного ключа WEP, неможливість постійної заміни ключа;

2. Заміна MAO адреси;

3. Захват пакетів та подальше отримання значення SSID;

4. Одностороння автентифікація на базі запиту-відповіді із використанням загального криптографічного ключа.

Система аутентифікації радіоканалу стандарту 802.11 побудована на основі стандарту IEEE 802.1x. 802.1x визначає, як використовувати розширений Протокол Аутентифікації (Extensible Authentication Protocol-EAP) на канальному рівні. EAP є транспортним протоколом, який працює з різними типами аутентифікації, які називаються EAP методами. EAP стандартизовано організацією IETF 1998 року.

Серед EAP методів, які спеціалізовані під безпроводові мережі, слід окремо виділяти ряд із них, принцип роботи яких передбачає використання стійких паролей.

З метою подолання проблеми низького ступеню безпеки та надскладною реалізації аутенифікації для методів з сертифікатами, було створено алгоритм SPEKE. Дослідження призвели до розробки нового сімейства алгоритмів аутентифікації на основі паролів, причому були усунені недоліки, що присутні у традиційних алгоритмах, які використовують паролі. Тоді ж було введено термін «стійкий пароль», що показує належність алгоритму даного сімейства. Головна перевага алгоритмів на основі стійких паролів у тому, що обидві сторони можуть довести один одному, що їм відомо секретні паролі, та не викриваючи його при третій стороні, яка може перехоплювати повідомлення. Ще одна важлива переваа – застосування для аутентифікації коротких поролів, що значно полегшує їх запам'ятовування користувачами.

В основі таких алгоритмів лежить метод обміну Діффі-Хелмана (Diffie-Hcllman), принцип роботи якого дозволяє двом сторонам передачі створювати ключ шифрування. У цьому методі третя сторона, яка потенційно може перехопити повідомлення, не може отримати цей ключ.

2.5 Дослідження і порівняння алгоритмів аутентифікації SPEKE та DH-EKE

Характеристики алгоритмів, що базуються на стійких паролях. Алгоритм SPEKE (strong password-only remote authentication) і DH-EKE маютть наступні основні характеристики:

1. При реалізації вже закладено вбудовану систему обміну ключів.

2. Протистоять атакам у режимі реального часу.

1. Запобігають можливості відкладеної (off-line) атаки за словником на пароль.

3. Надають можливість взаємної автентифікації

5. Відкидається потреба у довгострокових (persistent recorded secret data) секретних чи специфічних (sensitive host specific data) даних.

Здійснення атак за словником у реальному часі (On-line dictionary attacks) може бути легко виявлена та їй можливо запобігти, наприклад, простим знаходженням того, скільки разів було невдало виконано спробу зайти до системи. При цьому сама проблема відкладеної атаки за словником на пароль несе Сама сторона, яка атакую, має змогу маскуватися під другого учасника автентифікації та взаємодії, або навіть перехоплювати повідомлення, які передаються між учасниками взаємодії. Навіть невеликий витік інформації під час обміну може надати ефект успішної атаки. Алгоритм захисту повинен бути стійким до атак даного типу, навіть, якщо ми використовуємо короткі пролі.

Взаємна автентифікація є бажаною для того, щоб кожна з двох сторін була впевнена, що інша знає пароль.

Можливо два підходи до генерації ключа сесії для забезпечення безпеки обміну даними між передаючою та приймаючою стороною.

Сама необхідність у вбудованій системі обміну ключів під час аутентифікації пердставлено у [13]. Якщо розділити процес аутентифікації та процес обміну ключами, створює можливість третій стороні створити атаку, при цьому

перехопити передане повідомлення. Захищений обмін ключами вимагає обов’язкової участі обох сторін взаємодії і має є невід'ємною частиною процесу.

Прибравши необхідність зберігати довгострокові секретні дані прибирає необхідність користувачеві використовувати додаткові приватні, симетричні чи відкриті ключі. Для створення захищеного каналу розроблено цілий ряд способів. Ті методи, які використовують лише паролі, використовують його як незалежний фактор і тим самим спрощують частину системи користувача. Додаткові проблеми створює необхідність згенерувати, зберігти та поширити довгострокові дані. В той же час, секретні дані не підлягають розкриттю, зашифровані дані необхідно зберігати від можливого втручання ззовні.

Таким чином, є необхідність використання певних захищених областей пам'яті. Це, в свою чергу, робить слабкою систему безпеки та надає додаткові можливості для порушення захисту. Ті системи, в яких безпека пароля на пряму залежить від збереженого ключа набагато простіші в розробці. Їх недолік в тому, що вони лише переміщують основу безпеки з пароля на ключ. При цьому, у випадку, коли ключ викрадено, пароль також може бути скомпрометований. Якщо користувач відмовиться від ключів, ця проблема зникає. Так само, як зникає і необхідніст у захищеному середовищі.

Нище розглянемо алгоритми SPEKH та DH-EKE, які обладають усіма перерахованими перевагами та рядом додаткових бажаних характеристик.

Опис алгоритмів SPEKE та DH-EKE. Алгоритми SPEKE та DH-EKE базуються на методі обміну ключів Діффі-Хелмана. Класичний обмін алгоритмом DH дозволяє двом сторонам без попередньої домовленості створити загальний секретний ключ сесії.

По своїй суті алгоритм DH не передбачає аутентифікації тому є можливість атак типу «людина в середині».

Розглядаємі алгоритми входять до складу одного з типів протоколів автентифікованого обміну ключами. Використання DH робить захист паролю від відкладеної атаки за словником, в той час, як механізм використання пароля в розглядаємих алгоритмах робить неможливою атаки «людина у середині». В статті

[14] описано як збільшення ключа сесії сприяє захисту загального секретного пароля. Передавальні сторони, спільно використовуючі паролі малої довжини (S), використовують аутентифікацію (при цьому передача відбувається по незахищеному каналу), щоб повыдомити один одному знання S і згенерувати при цьому новий великий ключ сесії (K).

Для прикладу розглянемо Z_m^* , де m є великим простим числом.

При описі використовуємо позначення «сторона А» (А) та «сторона В» (В) як сторони обміну. Під час взаємодії типу користувач-хост А є користувачем, а В - хостом (аутентифікатором). В табл.2.1. представлено інші терміни

Таблиця 2.1.

Таблиця термінів

S	Секретний загальний пароль для сторін А та В невеликого розміру
m	Велика проста кількість, придатні для використання в алгоритмі Діффі-Хелмана
q	Великий простий множник числа m -1
g	Прохідний генератор порядку великого простого числа
G_x	Підгрупа Z_m^* порядку x. Де x- множник m-1
$f(S)$	Функція яка конвертує S у відповідний базис DH
R_A, R_B	Випадкові числа, обрані сторонами А і В
Q_A, Q_B	Значення, відіслані сторонами А і В
$E_k(t)$	Симетрична функція шифрування від t, використ. ключ k
$h(t)$	Стійка одностороння хеш-функція від t
$A \rightarrow B:t$	Сторона А відсилає t стороні В
K	Породжений ключ сесії

SPEKE використовує серію повідомлень, які мають вигляд випадкового набору чисел. В SPEKE реалізовано модуль, який може провести обчислення та визначити коректність пароля, який надходить з іншого боку. При рівності паролів створюються індивідуальні ключі у кожного пристроя. В цей час третя сторона, яка здійснює атаку, бачить повідомлення як довільні числа. Це робить неможливим обчислення чи підбір паролю.

SPEKE використвує метод обчислення відкритого ключа, при якому знімається потреба у спеціальній секретній інформаціїї, наприклад у використанні

довгострокового відкритого ключа чи індивідуальних ключів. В алгоритмі SPEKE реалузує метод аутентифікації ZKPP (Zero Knowledge Password Proof) для захисту паролів.

Серед особливих характеристик безпеки алгоритму SPEKE слід зазначити:

- Процес аутентифікації у клієнта та у сервера проходить одночасно.
- Відпадає необхідність у реалізації додаткових механізмів безпеки.
- Можливість встановлення ключа необмеженої довжини.
- Сучасна криптографія, яка застосовується у алгоритмі, дозволяє використовувати звичайні короткі паролі.
- Для клієнта та для сервера не потрібна наявність сертифікатів безпеки.

Принципів роботи алгоритмів. Алгоритм SPEKE базується на операції зведення у ступінь, яка є великим випадковим числом по модулю великого простого числа. При цьому, операцію зведення в ступінь, вважають односторонньою функцією. Все це через складність у проведенні обчислення дискретного логарифму (зворотна операція відведення в ступінь). І користувач і аутентифікатор обчислюють за допомогою пароля S загальний основний ключ сесії *K*. Для цього кожна зі сторін генерує велике випадкове число. Користувач генерує значення R_A, а аутентифікатор значення R_B. При цьому, кожній зі сторін відомо лише своє значення. А сам пароль S, відомий обом сторонам, може бути коротким.

Розглянемо взаємодію двох сторін - користувача пристрою та автентифікатора. По суті, у безпроводовій мережі у ролі автентифікатора виступає точка доступу (AP). Бувають випадки, коли задіяна третя сторона – сервер аутентифікації, який відповідає за централізовану аутентифікацію. В такій взаємодії сервер аутентифікації грає роль аутентифікатора, а AP займається пересилкою запитів. AP запускає ЄAP переговорів з надсилання запиту ідентифікації (EAP-Identity Request) користувачеві. В свою чергу, користувач отримує повідомлення та відповідає повідомленням EAP-Identity Response рис. 2.7. У разі застосування сервера аутентифікації AP достатньо лише надіслати відповідь користувачу. Після цього сервер автентифікації здійснює процес переговорів EAP-SPEKE, який, в свою чергу, складається ще з двох кроків.

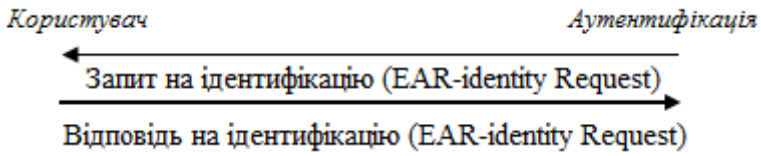


Рис. 2.7. Запит/відповідь EAR автентифікація

Коли аутентифікатор отримав відповідь від користувача, він починає шукати користувача в репозиторії та витягує пароль S.

Наступний крок - рис.2.8. автентифікатор створює велике випадкове число R_B і обчислює:

$$Q_B = f(S)_B^R mod\ m, B \to A: Q_B$$

m - велике просте число, що використовується як модуль

Аутентифікатор пересилає т і Q_B користувачеві в тілі запиту (EAP-SPEKE Request). Після цього станція користувача генерує ще одне велике випадкове число R_A та розраховує:

$$Q_A = f(S)_A^R mod\ m, A \to B: Q_A$$

Далі на боці користувача відбувається обчислення:

$$K = h(Q_B^R{}_A\ mod\ m)$$

де K- обчислений користувачем основний ключ сесії;

Q_B – значення, яке було отримано від автентифікатора.

На останньому кроці користувач обчислює:

$$Proof_{AK} = h(Q_A|K)$$

де h-одностороння хеш-функція

Далі користувач надсилає відповідь автентифікатору, яка складається з Q_A та $Proof_{AK}$.

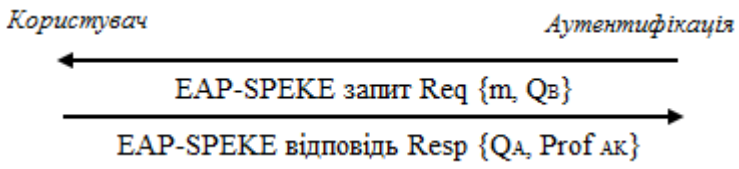


Рис. 2.8. Перша фаза EAP-SPEKE

Коли автентифікатор отримує відповідь по першому запиту EAP-SPEKE, він обчислює:

$$K = h(Q_A^{R}{}_{B} \; mod \; m)$$

Де:

K-обчислений автентифікатором основний ключ сесії;

Q_A – отримане від користувача значення.

Структура даного показаний на рис. 2.9.

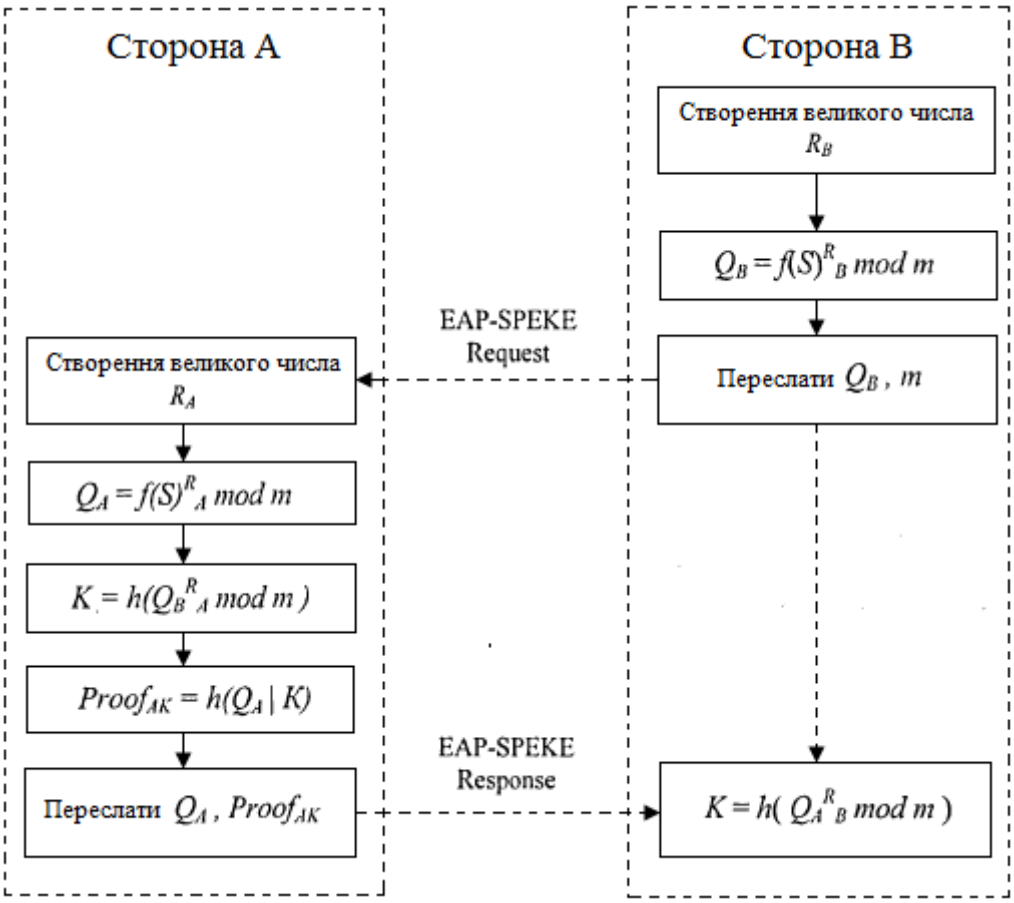


Рис.. 2.9. Алгоритм першої фази SPEKE

Наступним кроком автентифікатор обчислює рис. 2.11:

$$Test_{AK} = h(Q_A|K)$$

$$Proof_{BK} h(Q_B|K)$$

Далі автентифікатор порівнює розраховане значення $Test_{AK}$ з значенням $Proof_{AK}$, отриманим від користувача. Якщо значення-збігаються, автентифікатор посилає другий запит користувача EAP-SPEKE рис.2.10.

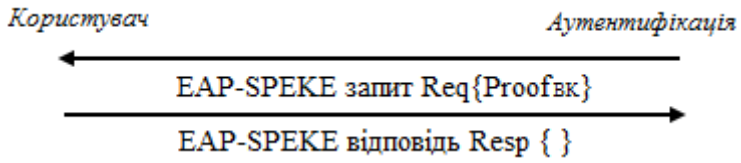


Рис. 2.10. Друга фаза EAP-SPEKE

Коли користувач отримує другий EAP-SPEKE запит, він обчислює, використовуючи значення, обчислені або отримані раніше:

$$Test_{BK} = h(Q_B|K)$$

Користувач порівнює TestBK та значення ProofBKy отримане від автентифікатора. Якщо вони виявляються рівні, він надсилає порожній EAP-SPEKE відповідь автентифікатору, тим самим показує, що результат автентифікації вірний. Коли відповідь порожня, аутентифікатор повертає повідомлення «EAP Success» користувачеві як завершальний сигнал, тим самим підтверджує успішну аутентифікацію рис. 2.11.

Кожна зі сторін незалежно одна від одної генерує ключ сесії K, що стає можливим завдяки асоціативним властивостям операції зведення в ступінь. Через складність обчислення дискретного логарифму, обчислення S за значеннями Q_A або $\underline{Q_B}$ технічно неможлива за релевантний проміжок часу. У випадку коли третій стороні стає відомо S, їй все одно неможливо обчислити значення K, оскільки їй потрібно для цього знати значення R_A і R_B, а вони є величезними випадковими числами. Неможливим є і обчислення K значень $Proof_{AK}$ або $Proof_{BK}$, оскільки h - одностороння хеш-функція.

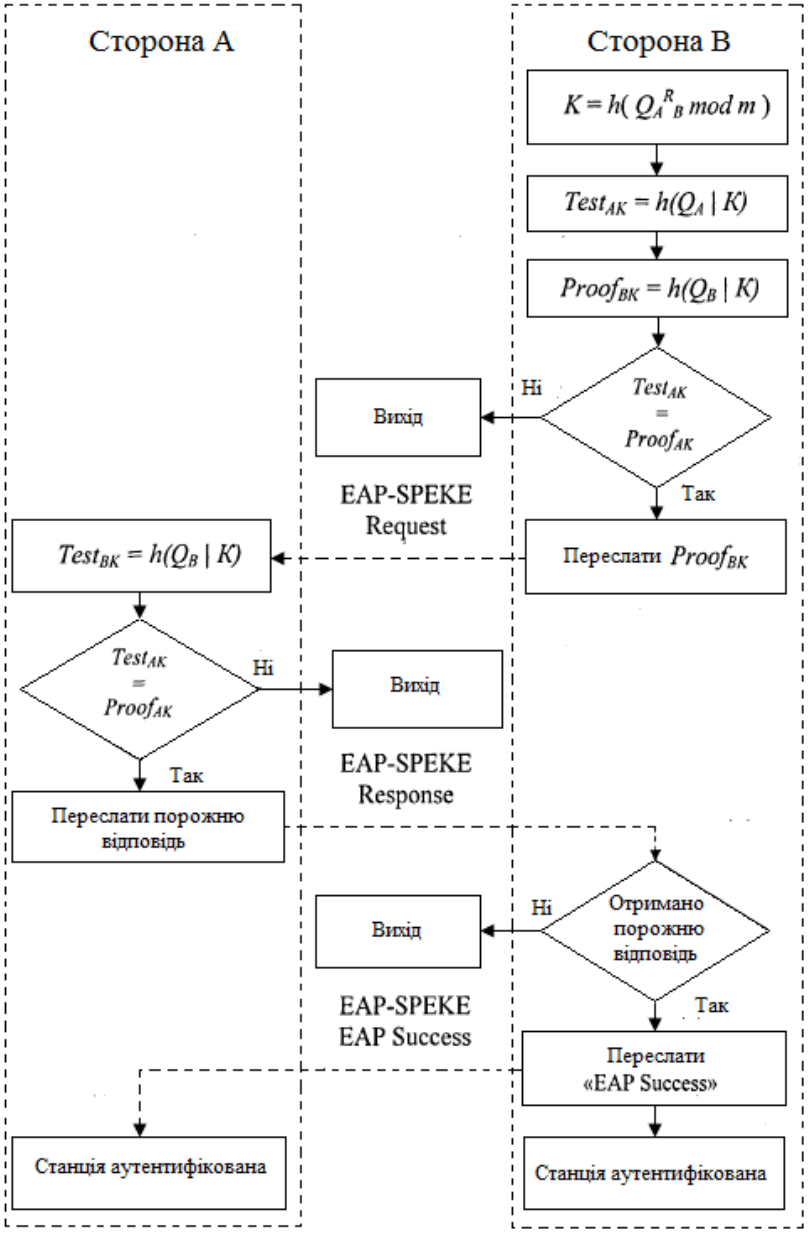


Рис. 2.11. Алгоритм другої фази SPEKE

Існує ще один спосіб доказати сторонами володіння ключем K:

$A \rightarrow B: E_k(C_A)$, де C_A – випадкове число, яке обирає сторона А

$B \rightarrow A: E_k(C_B, C_A)$, де C_B – випадкове число, яке обирає сторона В

Сторона В перевіряє, що C_B збігається

$$A \rightarrow B: E_k(C_B)$$

Для запобігання можливості обчислення дискретного логарифмування, значення m-1 повинно мати великий простий дільник q.

Можна розділити на дві станції алгоритм роботи DH-EKE (Diffie-Hellman Encrypted Key Exchange). На першому кроці використовується DH обмін, для генерації загального ключа K, причому обидві або одна з двох сторін зашифровують значення експоненти, які передаються, використовуючи при цьому пароль S. Знаючи S, сторони здатні дешифрувати повідомлення, використовуючи E_S і визначити єдиний ключ K.

Сторона А обчислює: $Q_A = g^R{}_A mod\ m, A \rightarrow B: E_S(Q_A)$

Сторона В обчислює: $Q_B = g^R{}_B mod\ m, B \rightarrow A: E_S(Q_B)$

Сторона А обчислює: $K = h(Q_B^R{}_A mod\ m)$

Сторона В обчислює: $K = h(Q_A^R{}_B mod\ m)$

В літературі [29, 31] припускають, що можливо пропустити один з кроків шифрування, але це може надати змогу третій стороні робити успішну атаку. Розглянемо чому.

Значення m, g, як і E_S (симетричної функції шифрування) необхідно вибирати, керуючись при цьому вимогами безпеки до алгоритму DH-EKE, що детально описано у [33].

На другому кроці DH-EKE, обидві сторони підтверджують, що знають своє знання K, перед тим, як вони почнуть використовувати його в якості ключа сесії. Слід зазначити, що в алгоритмі DH-EKE вкрай важливим є і порядок повідомлень, які надсилаються при перевірці[15].

2.6 Виявлення спроби несанкціонованого доступу в безпроводову мережу

Стандарт 802.11 передбачає роботу в спектрі мікрохвильових частот. Як правило, використовують від 2412 МГц до 2462 МГц, який розподіляють на 11 каналів. При цьому використовується технологія широкосмугової передачі (Spread spectrum) [16].

Радіо комунікації, засновані на технології широкосмугової передачі, дуже активно застосовується у військових цілях. Вона має ряд переваг:

1. Стійкість до перешкод;

2. Підвищена складність перехоплення.

Це досягається за рахунок того, що широкосмуговий сигнал розподіляється по великому діапазону частот, а потім збирається на приймачі. Таким чином, можлива прихована передача даних, що створює підвищену складність для сторони, що перехоплює.

Широкосмугова передача даних робить складною задачу відділення сигналів з даними від шуму і в той же час служить додатковим захистом протоколу 802.11 від перешкод в ефірі. На жаль, незважаючи на застосування широкосмугової передачі, можливості захисту даних обмежені, так як алгоритм розподілу частот заздалегідь відомий і застосований в кожному з 802.11 сумісному пристрої. Незважаючи на це, застосування широкосмугової передачі призвело до збільшення зусиль, необхідних для виявлення місця розташування неавторизованих бездротових карт і точок доступу, у зв'язку з тим, що приймальні пристрої, що працюють на фіксованих частотах, не завжди здатні відокремити факт передачі даних пристроями 802.11 від звичайних шумів.

Більшість методів визначення становища біля (тріангуляція) базується на технологіях визначення напрями. При цьому використовується спрямована антена, і проводити сканування з метою визначити напрям на найбільш сильний сигнал. Потім станція переміщається, здійснюється повторне сканування і за результатами визначається місцезнаходження сигналу, використовуючи найпростіші тригонометричні перетворення рис. 2.12.

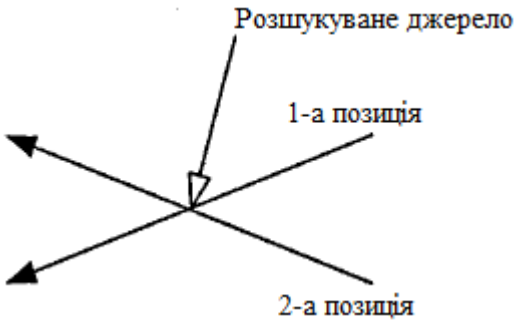


Рис. 2.12. Пошук із використанням тріангуляції

При практичному застосуванні все складніше. Поширення радіосигналу ускладнюється за рахунок наявності різних перешкод, таких як особливості ландшафту, теплове випромінювання, відбиття, рефракція, характеристики конструкції антени та ряд інших факторів ускладнюють поширення радіосигналу. Знайдена зона найпотужнішого сигналу може вказувати на реальне розташування передавача.

Є менш розповсюджена технологія, дозволяє визначити місцезнаходження передаючої сторони, аналізуючи тільки потужність сигналу. Для реалізації такого алгоритму потрібно знати коефіцієнт втрати потужності сигналу від відстані та потужність передавача.

На рисунку 2.13 представлено принцип знаходження положення передавача, якщо відомо потужність передавача, коефіцієнт посилення передавальної та приймаючої антени, залежність падіння потужності від відстані та потужність прийнятого сигналу. У точці А, виходячи з потужності сигналу та рівняння ослаблення сигналу від відстані, ми можемо визначити відстань до передавача. У точці В ми також можемо провести подібні обчислення, таким чином, положення передавача перебуватиме на перетині кіл з радіусами dA і dB.

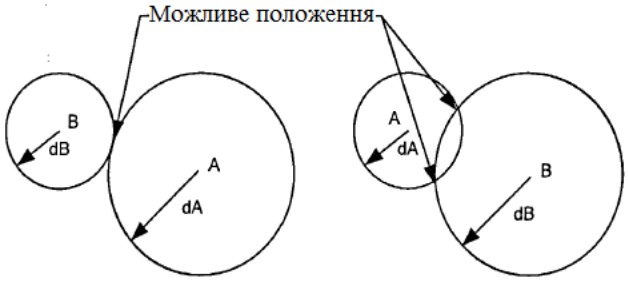


Рис. 2.13. Пошук із вимірюванням сили сигналу

Якщо потужність передавача не відома, або коефіцієнт посилення будь-якої з антен, або є більша кількість невідомих у рівнянні, необхідно зробити більшу кількість вимірів. Якщо положення точок, де вимірюються, обрані вдало, буде отримано одне чи два прийнятних рішення.

3 ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАКИ НА БЕЗПРОВОДОВУ МЕРЕЖУ

3.1 Дослідження методів покращення системи безпеки на базі алгоритму WEP

Класифікація типів атак. На ряду з великою кількістю переваг в алгоритмі WEP є також і недоліки у сфері безпеки. У WEP застосовується відомий симетричний алгоритм генерації псевдовипадкових чисел RC4 PRNG (Ron's Code 4 Pseudo Random Number Generator). Проте реалізація містить низку недоробок у сфері безпеки. Дані недоліки дозволяють здійснювати ряд як активних, так і пасивних атак з перехоплення та заміни повідомлень, що передаються бездротовими мережами.

У протоколі реалізовано стандартний 40 бітний ключ а також 24 бітний IV, але конкретними виробниками зазвичай розробляються розширені версії, що піддержують більшу довжину ключа. Отже чим менша довжина ключа, в такому разі він є більш схильним до атаки шляхом перевірки комбінацій (brute-force attack), що є під силу більшою сучасних комп'ютерів. При збільшенні розрядності секретного ключа, наприклад, до 128 біт, перебір стає неможливим навіть спеціальних обчислювальною частиною комп'ювальних систем. Проте залишаються варіанти для атак, які не використовують метод перебору і зводять спроби нанівець усі переваги довгого ключа.

Усього можливі чотири види атак.

Пасивна атака з метою розшифрування трафіку. Як було сказано вище, IV є 24-розрядним числом, яке використовується спільно з секретним 40 бітним ключем, для генерації ключової послідовності. Таким чином кожна станція, що бере участь у сеансі зв'язку на швидкості 11 Мбіт/с, може вичерпати всі комбінації чисел IV протягом п'яти годин:

$$\frac{1500\ \text{байт}}{\text{пакет}} \times \frac{8\ \text{біт}}{1\ \text{байт}} \times \frac{1\ \text{сек}}{11\ \text{Мбіт}} \times \frac{1\ \text{Мбіт}}{10^8\ \text{біт}} \times 2^{24}\ \text{пакета} \approx 18{,}3\ \text{сек} \approx 5\ \text{год.}$$

11 Мбіт/с це теоретично максимальна швидкість роботи протоколу 802.11b, насправді швидкість передачі виявляється нижчою через перевантаження мережі та можливих колізій пакетів. Цей факт може продовжити час, протягом якого з'являться використані раніше IV. З іншого боку пакети даних не завжди виходять максимального для Ethernet мереж розміру 1500 байт, що зменшує час появи повторних IV. У будь-якому випадку такий малий діапазон значень IV гарантує появу вже використаних IV протягом робочого дня.

В результаті за відносно невеликий проміжок часу можливе перехоплення двох пакетів даних, які зашифровані однією і тією самою ключовою послідовністю. Далі можливий статистичний аналіз відновлення вихідного незашифрованого тесту, що міститься в одному з повідомленні. У разі вдалого підбору, провівши операцію «виключає АБО» (XOR) над зашифрованим повідомленням і розпізнаним текстом зловмисник відновлює відповідну ключову послідовність, що дозволяє йому переглядати всі інші зашифровані повідомлення, зашифровані за допомогою даного IV:

$$M \oplus C = M \oplus \big(M \oplus RC4(IV, K)\big) = RC4(IV, K)$$

Навіть якщо не вдасться розпізнати звістку контекст повідомлення, про нього можна здогадатися, використовуючи передбачувану структуру та надмірність IP трафіку. Надалі знання структури вмісту зашифрованого тексту дозволяє звузити область пошуку можливого контексту. Оскільки зловмисник має два або кілька пакетів зашифрованих тим самим IV, він має можливість застосувати операцію XOR до вмісту і виявити відмінності та збіги в структурі:

$$C_1 = M_1 \oplus RC4(IV, K)$$

$$C_2 = M_2 \oplus RC4(IV, K)$$

Де C_1 і C_2 – сповіщення закодовані за допомогою одного IV, тоді:

$$C_1 \oplus C_2 = \big(M_1 \oplus RC4(IV, K)\big) \oplus = \big(M_2 \oplus RC4(IV, K)\big) = M_1 \oplus M_2$$

Інакше кажучи, використання операції XOR над 2-ма подібними закодованими сповіщеннями дозволяє усунути вплив ключової послідовності та розглянути різницю незакодованих даних (M1 ⊕ M2), що може дати більше шансів у виявленні вмісту пакетів із застосуванням методу статистичного аналізу.

Активна атака з метою заміни трафіку. Якщо зловмиснику вдалося зіставити текст який виходить і зашифрований , тоді він, очевидно, зможе згенерувати ключову послідовність. Володіючи даними відомостями не складно організувати передачу зашифрованого трафіку на станцію жертви, причому приймач повідомлень упізнає пакети, що надходять, як коректні Ця атака має можливість здійснюватися й іншим способом. Якщо навіть зловмисник не зможе досягти повного розкодування вмісту пакета, тоді він може у вільній формі змінювати значення бітів у повідомленні, потім додавати перераховане значення контролю цілісності ICV для отримання версії вдосконаленого пакета. Процедура XOR має властивість дистрибутивності: c(x ⊕ y) = c(x) ⊕ c(y) для будь-яких x і y. Проаналізуємо ситуацію, в якій виконано перехоплення пакета з даними, де C-зашифровані дані:A → (B): $(IV||C)$ відповідає деякому зашифрованому повідомленню P:

$$C = (P||c(P)) \oplus RC4(IV, K) \quad (3.1)$$

яке має значення P' де P' = P + Δ, до того ж Δ може бути обрана стороною що атакує. Далі є можливість замінити пакет з дінформацією:

$$(\text{A}) \rightarrow B\text{: } (IV||C^{"})$$

В даному випадку станція має отримати перероблений пакет даних P' з коректним значенням контролю якості і цілісності.

Проаналізуємо механізм можливого отримання значення C', яке відповідає M'. Так як алгоритм RC4, який застосовується в WEP, застосовує для перетворень лінійні функції, має можливим наступне змінення - застосування XOR (Δ || c(Δ)) до двох частин виразу 3.1, щоб отримати значення C:

$$C^{"} = C \oplus (\Delta||c(\Delta)) = RC4(IV, K) \oplus (P||c(P)) \oplus (\Delta||C(\Delta)) =$$
$$= RC4(IV, K) \oplus ((P \oplus \Delta)||(c(P) \oplus C(\Delta)) = RC4(IV, K) \oplus (P^{"}||c(P \oplus \Delta)) =$$
$$= RC4(IV, K) \oplus (P^{"}||c(P^{"}))$$

В даному випадку ми використовували той факт, що перетворення CRC лінійно і, отже, c(P) ⊕ c(A) = c(P ⊕Δ). В результаті, ставати можливим перетворити

зашифроване повідомлення C в C', яке відповідає відкритому повідомлення $\oplus\Delta$ тобто зміненому атакуючої стороною. Таким чином, можливе порушення цілісності інформаційних пакетів, причому для цього потрібно лише часткове знання вмісту пакета для його модифікації.

Активна атака з двох сторін. Можлива ситуація в якій порушник, намагаючись перехопити трафік у безпроводовій мережі, має інформацію лише про заголовок кадру, а не про сам вміст повідомлення. Як приклад, або заздалегідь відома або обчислена IP адреса жертви. Маючи лише цю інформацію, зловмисник може замінити відповідні біти пакета для заміни IP адреси на адресу станції, яка знаходиться під його контролем, за умови, що мережа, на яку ведеться атака, підключена до мережі Інтернет. Далі пакет потрапляє на крапку доступу, що з'єднує бездротову мережу з Інтернетом, розшифровується, і у відкритому вигляді пересилається на машину зловмисника. До того ж удосконалений пакет прямує з безпроводової мережі до Інтернету, таким чином він не буде затриманий великою кількістю звичайних мережевих екранів.

Для здійснення даної атаки недостатньо просто замінити IP адресу одержувача пакета, необхідно щоб контрольна сума зміненого пакета була коректною. Припустимо, що D_L і D_H - це дві 16-бітові частини IP адреси одержувача їх необхідно замінити на $D_L^{'}$ і $D_H^{'}$. Позначимо значення старої контрольної суми як 5, причому її значення необов'язково відомо. Тоді нове значення обчислюється за такою формулою:

$$S^{"} = S + D_L + D_H - D_L^{"} - D_H^{"}$$

Якщо наперед відомо S, то стає простим визначення S' і модифікувати пакет операцією ХОЯ зі значенням S $\oplus$ S'. Якщо ж не відомо значення S, то обчислення стає складним. Відомо значення E = S”-S, обчислюємо Δ= S $\oplus$ S'. Використовуючи статистичний аналіз та знаючи структуру повідомлення, зростають шанси підібрати потрібне значення.

Атака на основі складання таблиці. Невелика кількість можливих значень IV дають змогу третій стороні будувати таблиці розшифровки. Якщо спроба вдала, стає можливим відновити ключову послідовність, згенеровану при поточному IV.

Ця ключова послідовність потім може бути використана для розшифрування всіх інших пакетів, що використовують те саме значення IV. За досить добре відпрацьованої технології статистичного аналізу зловмисник може побудувати таблицю відповідності IV векторів та відповідних їм ключових послідовностей. Така таблиця міститиме близько 2 (більше 16 мільйонів) записів, що становитиме об'єм близько 24 Гб. Користуючись цією таблицею, зловмисник зможе розшифрувати будь-який пакет без зусиль, достатньо з'ясувати значення ключової послідовності за його IV.

Можливі рішення питання безпеки. Аналітичні данні показують, що на сьогодняшній день 40% безпроводових мереж вайфай мають активований протокол WEP. Такая ситуація відкриває можливість атак на інфраструктуру мережі та також до втрати самої передаваємої інформації. Як виход – часта зміна ключа та використання протоколу WEP. Налаштовуючи конфігурацію слід застосовувати довгі, максимально стійкі до підбору ідентифікатори SSID.

Використовуючи фільтрацію MAC адрес або застосовуючи VLAN ми робимо неможливим доступ до неавторизованих безпроводових карт. Слід закривати доступ до інтерфейсу конфігурування ТД безпроводової мережі. Використання програми антивірусу та мережного екрану усуне можливість появи па клієнтських машинах сторонніх програм-шпигунів та перехоплювачів.

Об'єднуючи захист за допомогою мережевого екрану та технології IPSec, SSH або SSL, можливо з високою ймовірністю виключити можливість перехоплення інформації та запобігши доступу для непізнаних клієнтів.

Користувачі Windows можуть скористатися альтернативою ненадійної Shared Key Authentication (автентифікація на основі ключа, що спільно використовується) - автентифікацією стандарту IEE 802.1x. 802.1.x визначає механізми захищеної аутентифікації та доставки секретного ключа для шифрування трафіку, що покриває серйозну перепустку в безпеці протоколу WEP.

Наразі дослідницька група IEEE (інститут інженерів з електротехніки та радіоелектроніки) розробляють удосконалену версію протоколу WEP2. Основні зусилля докладаються в області розмежування функцій шифрування та

автентифікації для того, щоб не було необхідності спільно використовувати секретний ключ на всіх станціях бездротової мережі. Було прийнято чорновий варіант стандарту попередньо названий Enhanced Security Network (ESN), в якому передбачено посилений варіант захищеної автентифікації та система управління 128-бітними ключами.

Система шифрування ESN заміниться алгоритм генерації псевдовипадкових чисел RC4 PRNG на сучасний стандарт Advanced Encryption Standard (AES). Прийняття WEP2 надає рівень безпеки бездротових мережі, який стане таким самим, як рівень безпеки проводових мереж.

3.2 Аналіз шляхів вдосконалення системи безпеки, для радіоканалу стандарту IEEE 802.11

Недоліки стандартної системи безпеки. Розглянемо механізм роботи системи безпеки [18]. У структурі мережевої моделі OSI протокол 802.11 займає фізичний рівень і частина канального рівня - підрівень управління доступом до середовища (MAC). Додаток стандарту пропонує використання протоколу 802.2 для управління LLC. Протокол TCP/IP у моделі OSI, що описує функціональність мережевих рівнів, розташований вище за рівні, що використовуються протоколом 802.11b, і використовує сервіси, що надаються рівнями, розташованими нижче рис. 3.1.

Слабкості безпеки 802.11 обумовлюються як фізичними чинниками, так і його особливостями реалізації. До недоліків відносять:

- недоліки шифрування;
- низька надійність аутентифікації;
- існує можливість перехоплення пакету інформації.

Проблема перехоплення пакету інформації з’являється через те, що дані передаються через радіоканал. При цьому люба станція, яка входить в зону прийому сигналу, має змогу збирати інформаційні пакети. Якщо не застосовуєтьсяся шифрування, передаваємі дані можна взяти з окремих пакетів і

використовувати третьою стороною. Подібні завдання можуть вирішуватися встановленням звичайного мережевий монітор, що надає змогу переглядати вміст пакетів і здійснювати їх фільтрацію за рядом ознак, наприклад, IP адресою. Складність полягає в тому, що неможливо встановити, прослуховується зараз радіоканал чи ні. А значить перехоплення просто можна не помітити.

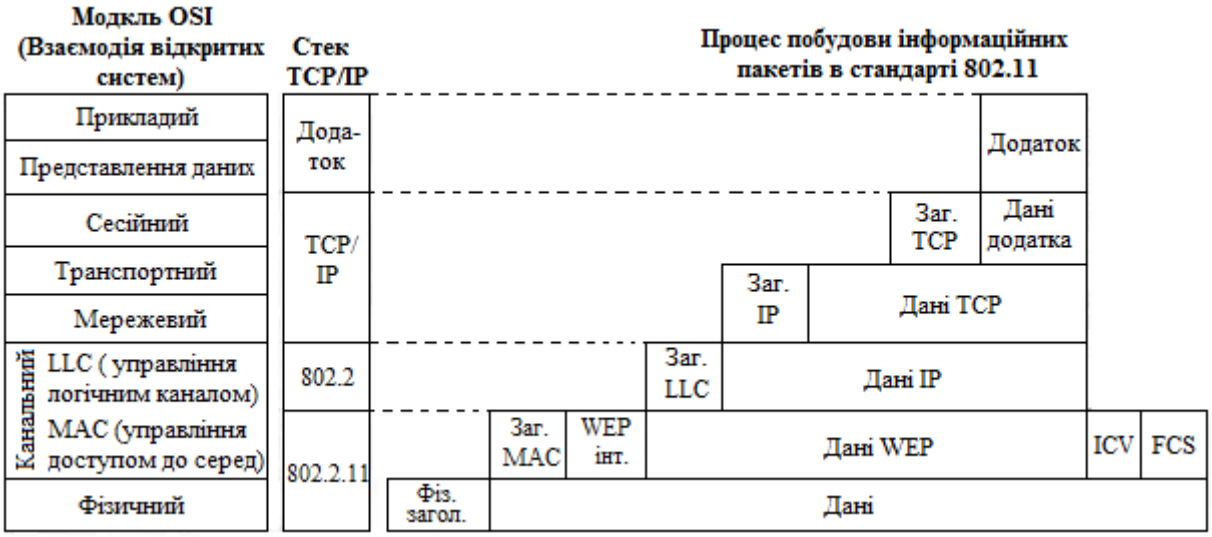


Рис. 3.1. Процес побудови інформаційних пакетів у стандарті 802.11

Аутентифікація має низький рівень надійності. Протокол WEP використовує секретний ключ, який заздалегідь відомий усім станціям мережі. Сам протокол WEP не регламентує спосіб передачі секретного ключа та як часто цей ключ необхідно змінювати. Отже. Ряд виробників обладнання взагалі не реалізують механізми доставки ключа в своєму обладнанні. Отже користувачі самі вимушені конфігурувати пристрої і вручну переносити значення ключа на стації мережі. А отже ключ буде змінюватися рідко, або ніколи.

Ідентифікатор SSID (Service Set Identifier) дозволяє ділити бездротову мережу класу Basic Service Set (BSS) на логічні сегменти, як ідентифікатор підмережі [19]. За допомогою SSID відбувається обмеження доступу для будь-якого клієнтського пристрою, який не має необхідного SSID. Однак найчастіше AP (точка доступу) робить широкомовне розсилання ідентифікатора SSID своєї

підмережі. Навіть у разі відключення функції розсилки SSID, зловмисник може отримати значення SSID, аналізуючи трафік між станціями підмережі.

Крім того, можна заборонити доступ на основі фільтрації MAC адрес. Але не дивлячись на те, що всі стандартні мережні карти повинні мати унікальну MAC адресу, існує програмне забезпечення або часто є апаратна можливість заміни MAC адреси в мережному інтерфейсі.

Протокол WEP має ряд слабких місць в архітектурі, які дозволяють розшифрувати дані третій стороні [3]. Перше - алгоритм шифрування RC4 у поєднанні з 64 або 128 бітним ключем, що складається з секретного ключа і значення вектора ініціалізації IV. Причина, через яку можливий злом WEP у випадку не у недоліках RC4 як і навіть у довжині ключа, а скоріш у невдалої реалізації самого алгоритму.

Враховуючи всі недоліки, система безпеки стандарту IEEE 802.11 потребує ряду покращень. Для цього необхідно застосувати комплексний підхід до цієї проблеми.

Самий простий варіант - застосування NAT маршрутизатора для з'єднань з публічними мережами, але для побудови дійсно захищеної мережі цього недостатньо. У цьому списку наведено основні сфери, які є основою стратегії безпеки безпроводових мереж:

- фільтрація вхідного та вихідного трафіку за допомогою міжмережевого екрану;
- шифрування з'єднань для віддаленого доступу;
- подвійна автентифікація для віддаленого доступу;
- багаторівневі зони безпеки для публічно доступних ресурсів;
- Засоби виявлення спроб несанкціонованого доступу.

Розглянемо систему безпеки протоколу 802.11 з погляду описаної стратегії. Модульний підхід, в основі якого лежать застосування стандартних алгоритмів, і можливість використовувати нові технології без необхідності зміни існуючої структури. Ця система безпеки безпроводової мережі дуже добре вписується в рамки вже існуючої політики безпеки мережі рис.3.2.

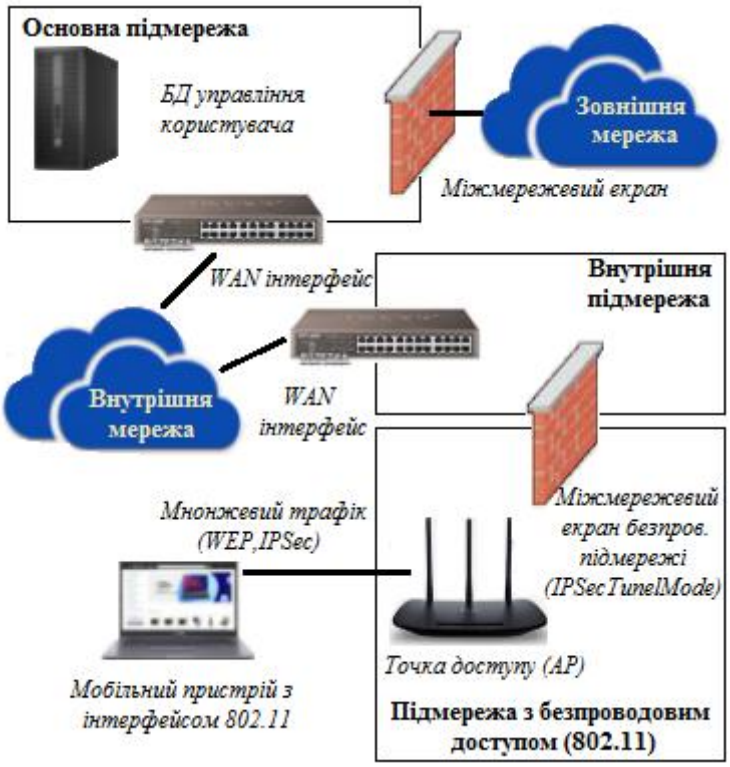


Рис. 3.2. Система безпеки протоколу 802.11 у структурі системи безпеки гетерогенної мережі

Основні елементи, що застосовуються у системі безпеки:

IEE 802.11

- активізація протоколу WEP;
- встановлення довжини ключа 104 біт;
- Увімкнення фільтрації MAC адрес.

Система аутентифікації

- Алгоритм аутентифікації та розподілу ключів SPEKE.

IPSec (Тунельний режим)

- Інкапсуляція зашифрованих даних (ESP) із застосуванням алгоритм DES3.

Міжмережевий екран

- підтримка IPSec;
- Режим заборони всього вхідного трафіку, за винятком тунелювання IPSec.

Зміна значень за умовчанням для обладнання

- ID адміністратора;

- пароль адміністратора;

- секретний ключ WHP;

- SSID.

Управління секретними ключами VVF.P

- Часта зміна секретного ключа;

- Захищена передача ключа на основі SPEKE за розкладом.

Використовуючи ці елементи, побудуємо вдосконалену систему безпеки радіоканалу 802.11 рис. 3.3.

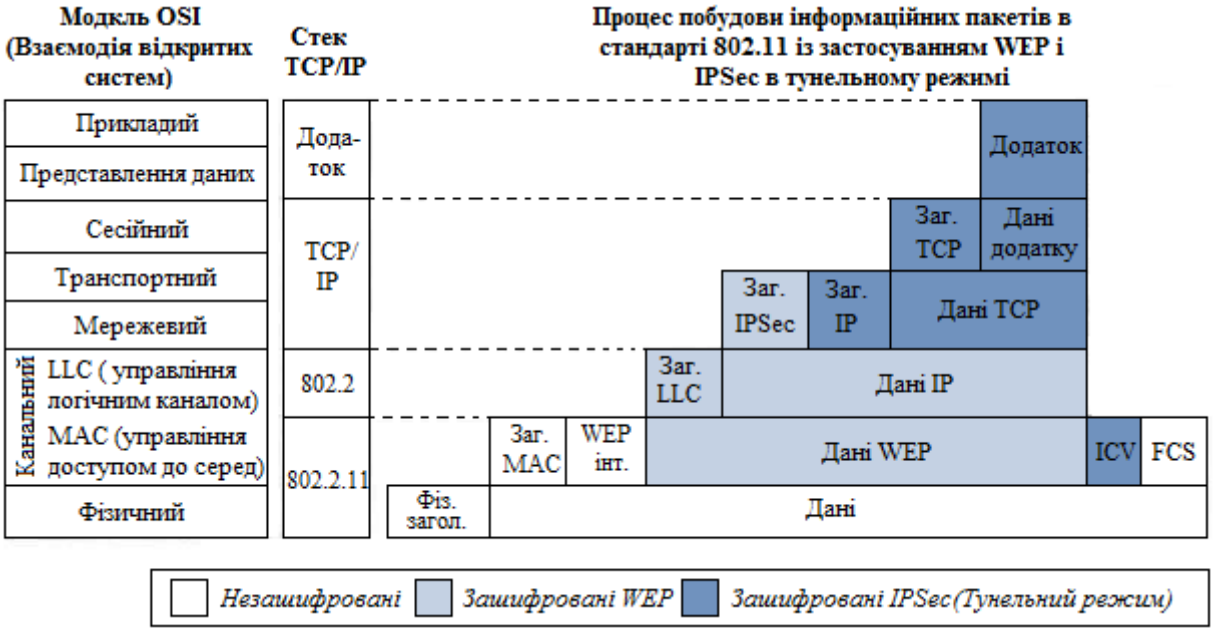


Рис. 3.3. Удосконалена система безпеки радіоканалу 802.11

Процес шифрування даних як на канальному, так і на мережному рівні моделі OSI робить протокол WEP більш стійким до атак, заснованих на спробах дешифрування. Це виходить завдяки тому, що тепер більшість даних, що містяться в пакеті WEP, вже зашифровані за допомогою IPSec, це унеможливлює використання атаки, яка заснована на зіставленні відомого заздалегідь повідомлення та його зашифрованого аналогу. Слід, однак, звернути увагу, що при даному підході заголовок LLC і заголовок IPSec зашифровані лише засобами WAP, що може дещо знизити криптографічну стійкість моделі безпеки.

Також залишаються доступними до можливого перехоплення MAC адресу, Key ID, FCS, SSID, IV. Оскільки ця інформація використовується на фізичному та канальному (підрівень MAC) рівні її неможливо зашифрувати.

У зв'язку з тим, що основні дані захищені за допомогою алгоритмів IPSec (DEC3) і WEP (RC4), інформація, яку можна отримати, використовуючи відкриті значення SSID, IV і Key ID не принесе відчутної користі стороні перехоплення. Значенням FCS є контрольне значення CRC від MAC пакета, яке використовується для контролю, цілісності даних, після того, як вони були передані.

Найбільшою небезпекою з точки зору безпеки є незашифрована передача значення MAC адреси джерела, яке може бути підмінене атакувальною стороною. Тому аутентифікацію за адресою MAC слід сприймати лише як додатковий спосіб захисту від вторгнення.

У запропонованій моделі безпеки автентифікації піддаються як користувач, так і пристрій. Пристрій автентифікується за допомогою ключа WEP. При цьому ключ повинен змінюватися досить часто і розповсюджуватись через захищений канал. Перед тим, як пристрій видасть права на обмін даними через міжмережевий екран, користувач повинен пройти процедуру реєстрації в центральній базі даних управління користувачами мережі, в якій зберігаються облікові записи та політики безпеки.

Міжмережевий екран не тільки запобігає несанкціонованому доступу до мережі, але й блокує широкомовні розсилки, які можуть містити дані про внутрішню структуру мережі. Зашифрований пакет IPSec у тунельному режимі не містить додаткової інформації про структуру, доступну зовнішньому перехопленню, оскільки вона шифрує, а потім замінює заголовок IP пакета, який містить IP адресу пункту призначення, на власний заголовок в якому вказана IP адреса кінцевої точки міжмережевого екрану.

Застосування покращеної системи безпеки на практиці. В першу чергу для успішного застосування розробленої системи, при необхідності у посиленні безпеки вже наявної бездротової мережі стандарту 802.11 або планується

розгортання нової мережі, необхідно переконатися, що протокол VP налаштований належним чином і функціонує. Довжину ключа рекомендується встановити 104 біт.

Наступним кроком необхідно вибрати спосіб розподілу секретного ключа. Одним із можливих рішень є застосування захищених за допомогою SSL каналів за заздалегідь заданим розкладом. У разі непридатності даного підходу у кожному конкретному випадку може бути обраний альтернативний підхід. Найкращий метод з точки зору безпеки - призначити системного адміністратора відповідального за зміну секретних ключів на всіх пристроях, але це може призвести до того, що ключі будуть змінюватися досить часто. Деякі виробники включають власні методи розподілу ключа у свою продукцію, але так як стандарт IEEE 802.11 не визначає, як саме це має бути зроблено, всі подібні рішення є не стандартизованими. В даний час ведуться роботи та стандартизації роботи з ключами в новій версії 802.1x.

Далі необхідно вирішити, який міжмережевий екран найкраще підходить для вирішення завдань із забезпечення безпеки мережі.

Екран є критичним компонентом, що розміщується між бездротовою підмережею та внутрішньою мережею. При виборі слід звернути увагу до основні чинники:

- Міжмережевий екран повинен забезпечувати тунельний режим роботи із зашифрованим трафіком для всіх типів бездротових пристроїв, які використовуватимуться;

- метод аутентифікації має бути сумісним із центральною базою управління користувачами;

- Підтримка аутентифікації віддалених користувачів - Підтримка аутентифікації віддалених користувачів на основі політик безпеки, що зберігаються в базі управління користувачами.

Наступним кроком необхідно визначити, чи застосовується технологія IPSec для наявної інфраструктури. В якості альтернативи може бути використана технологія SSL. Але в цьому підході є недоліки. Так неможлива робота в тунельному режимі між міжмережевим екраном та віддаленим користувачем, це

означає, що можливе перехоплення реальних IP-адрес. Протокол SSL займає більш високий рівень у стеку TCP/IP, ніж IPSec, відповідно більша кількість незашифрованої інформації може бути отримана під час перехоплення та аналізу пакетів. Технологія SSL первинно була розроблена як протокол для роботи в Інтернет, таким чином, деякі програми можуть виявитися непрацездатними в бездротовій мережі.

Проведене дослідження радіоканалу стандарту IEEE 802.11b показало, що, незважаючи на недоліки в галузі захисту даних, використання стандартних методів значно знижує можливість атаки на бездротову мережу. Для забезпечення безпеки даних необхідно створення захищеного каналу зв'язку, який включає наступні компоненти:

1. Протокол WEP, описаний у стандарті ШЕЕ 802.1 lb, що є стандартним методом захисту даних у радіоканалі;

2. Технологія IPSec, що дозволяє здійснити криптографічний захист як самих даних, так і заголовка IP пакета;

3. Міжмережевий екран, за допомогою якого здійснюється організація тунельного режиму проходження даних та здійснюється аутентифікація користувачів бездротової мережі;

4. Система розподілу ключів на основі алгоритму SPEKE, основною функцією якої є безпечна доставка секретного ключа кожному бездротовому пристрої та проводиться їх заміна за заздалегідь складеним розкладом;

5. Система аутентифікації з урахуванням алгоритму SPEKE.

При цьому значно знижується можливість успішного проведення атак на систему захисту інформації радіоканалу.

3.3 Ідентифікація та відстеження спроб несанкціонованого доступу в безпроводову мережу

Використовуване апаратне та програмне забезпечення.

У ході практичного експерименту було використано вільно доступне програмне забезпечення з відкритими кодами.

Використовуємо апаратне забезпечення:

1. Dell Latitude CPH 850 МГц процесор, 256 Мб пам'ять.

2. Cisco Aironet 340 802.11 - карта бездротового доступу.

3. ТД Cisco Aironet 340. Вона потрібна для імітації вторгнення в систему.

4. Карта безпроводового доступу Lucent Orinoco "Silver" 802.11, яка виступає в ролі неавторизованої безпроводової карти.

Програмне забезпечення:

1. ОС SuSE Linux;

2. Бібліотека libpcap (libpcap current-cvs-2001.07.20), аналізатор пакетів, що працює під Linux. Ця версія дозволяє переглядати фрейми формату 802.11;

3. Набір утиліт ethereal (vO.8.19), найбільш повний з доступних інструментарій, що дозволяє аналізувати мережеві протоколи, гідністю є можливість аналізу кадрів протоколу 802.11 у зручному для дослідження людиною форматі;

4. Ядро Linux з повною підтримкою бездротової картки Cisco Aironet 340.

Недоліком більшості безкоштовних пакетів, яких необхідно запускати з командного рядка, є відсутність графічної оболонки, що дозволяє полегшити аналіз даних.

Виявлення. Першим кроком є виявлення факту активності неавторнзованої бездротової карти в межах мережі, яку необхідно захистити. Це може бути зроблено за допомогою вільного програмного забезпечення. Драйвер мережної карти Cisco Aironet, включений в останні версії ядра ОС Linux, підтримує режим «RFMonitor», що дозволяє здійснити моніторинг пакетів стандарту 802.11, у тому числі перегляд вмісту кадрів з метою виявлення широкомовних розсилок з неавторизованих бездротових карт або точок доступу.

Як зазначено у специфікації стандарту 802.11, існують три класи кадрів 802.11. У питанні виявлення неавторизованих карт і точок доступу основний

інтерес представляють кадри 1-го та 2-го класу. Фрейми 1-го класу використовуються станцією, що знаходиться в неавторизованій стадії.

До таких кадрів відносяться керуючі кадри автентифікації, кадри-маяки і пробні кадри (beacons and probe). Фрейми 2-го класу доступні в стадіях I та 2, що використовуються для процесів об'єднання.

Від точок доступу ми очікуємо на велику кількість фреймів маяків (1-го класу). Від неавторизованої мережевої карти, за нашим прогнозом, виходитиме велика кількість пробних фреймів (так само 1-го класу).

Налаштування ПЗ. Для того, щоб перевести бездротову мережну картку в режим моніторингу, необхідно виконати таку команду:

 # echo "Mode: y" > /proc/driver/aironct/ethO/Config

#

Після цього можна розпочинати запис вмісту пакетів за допомогою стандартної утиліти tcpdump, зберігаючи результати у файл, для подальшого аналізу за допомогою ethereal:

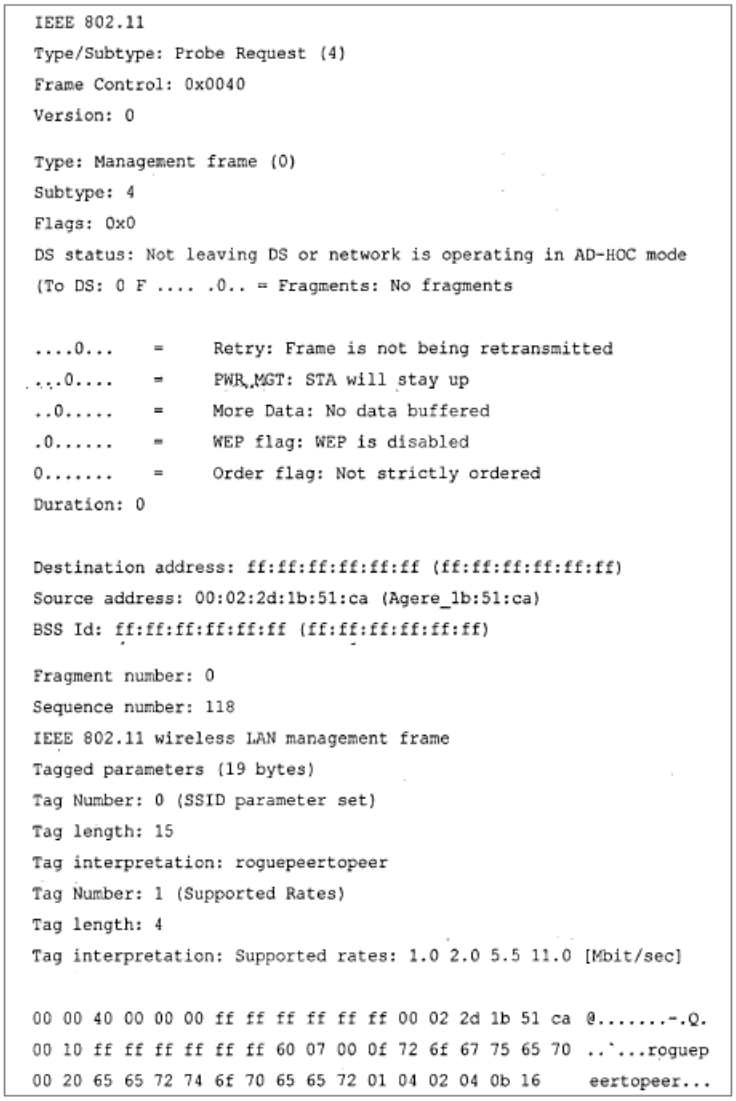
 # tcpdump -i clhO -s 0 -w capturcfile'

#

Виявлення неавторнзіропаної сполуки типу «Ad hoc». Даний тест проводиться з метою переконатися в можливості виявлення активності неавторизованої бездротової карти, що працює в радіусі дії мережної інфраструктури, що захищається. Карта моделі Lucent Orinoco була налаштована для роботи в режимі Ad-hoc на ноутбуці під керуванням ОС Windows і включена, з метою визначити, які характерні кадри будуть надсилатися даною бездротовою картою в процесі встановлення з'єднання в даному режимі.

Після ініціалізації карти утиліта tcpdump було зупинено, запущено пакет ethereal, у якому відкрили файл з результатами моніторингу. Було виявлено велику кількість пробних запитів від бездротової карти Orinoco, що підтвердило нашу гіпотезу про можливість виявлення факту знаходження в мережі, що захищається, неавторизованої бездротової карти в процесі ініціалізації режиму «Ad-hoc».

Приклад одного з виявлених кадрів на рис.3.4.



```
IEEE 802.11
Type/Subtype: Probe Request (4)
Frame Control: 0x0040
Version: 0

Type: Management frame (0)
Subtype: 4
Flags: 0x0
DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0 F .... .0.. = Fragments: No fragments

....0...    =     Retry: Frame is not being retransmitted
...0....    =     PWR_MGT: STA will stay up
..0.....    =     More Data: No data buffered
.0......    =     WEP flag: WEP is disabled
0.......    =     Order flag: Not strictly ordered
Duration: 0

Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Source address: 00:02:2d:1b:51:ca (Agere_1b:51:ca)
BSS Id: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Fragment number: 0
Sequence number: 118
IEEE 802.11 wireless LAN management frame
Tagged parameters (19 bytes)
Tag Number: 0 (SSID parameter set)
Tag length: 15
Tag interpretation: roguepeertopeer
Tag Number: 1 (Supported Rates)
Tag length: 4
Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]

00 00 40 00 00 00 ff ff ff ff ff ff 00 02 2d 1b 51 ca @.......-.Q.
00 10 ff ff ff ff ff ff 60 07 00 0f 72 6f 67 75 65 70 ..`...roguep
00 20 65 65 72 74 6f 70 65 65 72 01 04 02 04 0b 16     eertopeer...
```

Рис.3.4. Приклад виявлення кадрів

Таким чином, можна виявити активність неавторизованої спроби встановлення з'єднання та сканування бездротової мережі: Також можливе отримання корисної інформації з окремих кадрів.

Найбільш корисними є адреси SSID та MAC, оскільки вони можуть бути використані для відстеження конкретного неавторизованого пристрою.

Виявлення неавторизованої точки доступу. Даний тест покликаний підтвердити можливість виявлення неавторизованої точки доступу, що працює в радіусі дії бездротової мережі, що захищається.

Спочатку була запущена сесія tcpdump та активована точка доступу Cisco Aironet 340. Після закінчення процесу завантаження та ініціалізації було проаналізовано файл із результатами моніторингу. Було знайдено велику кількість фреймів-маяків, надісланих точкою доступу. Один із кадрів наведено в прикладі на рис.3.5.

```
IEEE 802.11
Type/Subtype: Beacon frame (8)
Frame Control: 0x0080
Version: 0
Type: Management frame (0)
Subtype: 8
Flags: 0x0
DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0 From DS: 0) (0x00)

.....0.. = Fragments: No fragments
....0... = Retry: Frame is not being retransmitted
...0.... = PWR MGT: STA will stay up
..0..... = More Data: No data buffered
.0...... = WEP flag: WEP is disabled
0....... = Order flag: Not strictly ordered

Duration: 0
Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Source address: 00:40:96:36:88:23 (Telesyst 36:88:23)
BSS Id: 00:40:96:36:88:23 (Telesyst_36:88:23)
Fragment number: 0
Sequence number: 0
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Timestamp: 0x0000000000019274
Beacon Interval: 0.102400 [Seconds]
Capability Information: 0x0021
```

Рис.3.5. Приклад кадрів

Виявлення неавторизованої спроби підключення до мережі. В останньому тесті нами була емульована спроба неавторизованого підключення до мережі.

Цей тест був проведений за двох різних умов:

1. Невідома для порушника адреса SSID;

2. Відома адреса SSID.

У першому випадку мережна карта активно сканувала бездротову мережу пробними кадрами у пошуках точки доступу. По-друге було виявлено лише кілька підозрілих фреймів, решта мережного трафік міг вважатися невідмінним від

нормального. Ця проблема виникла через програмно-апаратні особливості роботи карти Cisco.

Дана карта не змогла приймати пакети одночасно від усіх доступних BSS, особливо працюючих на інших частотах. Докладніше ця проблема та шляхи її вирішення розглядається в наступному розділі.

У ході обох частин експерименту було виявлено характерні пробні кадри, структура одного з них рис.3.6.

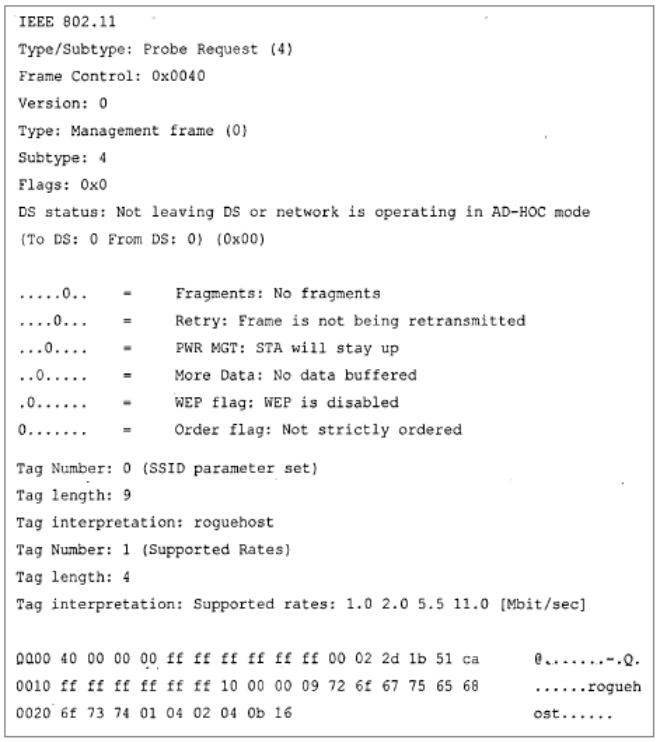


Рис.3.6. Структура пробного кадру

3.4 Експерементальні дослідження

При практичних вимірах буде застосовано підхід, що поєднує експериментальні дані та теорію поширення радіосигналу в приміщенні, викладену в [17].

Умови тестування. Тестування проводилося в офісному приміщенні, розмірами приблизно 30 на 20 м. Структура міжкімнатних перегородок - бетон із включенням металевих конструкцій. Для досвіду було використано три окремі

точки доступу, розставлені у випадкових місцях. Перші дві – Cisco AP350s. На першій було встановлено дві антени, друга не містила антени. Третя модель Orinoco AP-1000 з антеною Lucent.

Збір даних. Першим завданням було збирання значень залежності сили сигналу від дистанції, базуючись на даних, представлених драйвером бездротової карти. Для збору даних використовувалася програма iwspy, налаштована на певну MAC адресу:

 # iwspy eth0:0b:0b:0b:0b:0b:0b

Послідовний виклик *iwspy eth0* повертатиме значення рівня сигналу пакетів, отриманих від даного передавача.

Тестуюча станція переміщається територією, вимірюючи потужність сигналу у випадкових точках. Для обробки представляється файл, що складається з двох колонок, в першій відстані від передавача, в другий рівень сигналу. Графічно значення показано на рис. 3.7 - 3.9

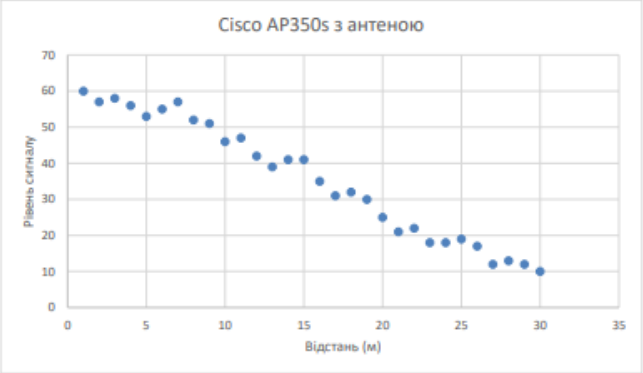


Рис. 3.7. Cisco AP350s з антеною

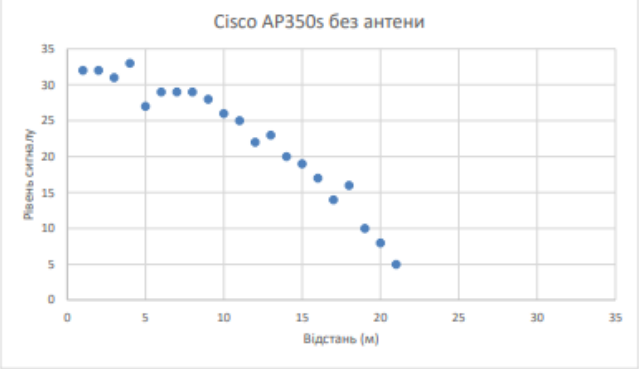


Рис. 3.8. Cisco AP350s без антени

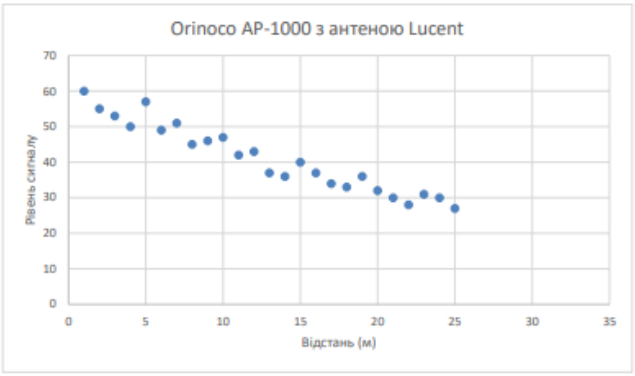


Рис. 3.9. Orinoco AP-1000 з антеною Lucent

Знаходження залежності сили сигналу від дистанції

Наступним кроком необхідно визначити, чи можуть дані, отримані в ході попереднього експерименту, задовольняти співвідношенню.

Для цього необхідно спочатку перевести значення (RSSI - значення рівня прийнятого сигналу), отримані за допомогою утиліти iwspy, в Дб.

Експерементально отримані наступні залежності:

$PdBm$ = 1,205$PRSSI$ − 101,07

$PRSSI$ = 0,83$PdBm$ + 83,891

Де: PdBm - значення рівня сигналу в ДБ, PRSSI - значення, отримане за допомогою утиліти iwspy.

Якщо значення видаються в нормалізованому вигляді (дана опція встановлюється в драйвері бездротової карти), рівняння набувають вигляду:

$PdBm$ = 0,62$NRSSI$ − 101,07

$NRSSI$ = 1,66$PdBm$ + 167,782

В даний час iwspy ioctl для Linux повертає не нормалізовані значення (проте, клієнт Cisco для ОС Windows повертає нормалізовані значення).

Наступним етапом є побудова функції апроксимації кривих, в яку включені наведені вище залежності. В якості базису використовується рівняння, що враховує як загасання при поширенні радіохвиль в приміщенні, так і відображення, рефракцію і інтерференцію.

В результаті експериментів і досліджень було отримано наступне співвідношення для поширення радіосигналу в будівлі на частоті 2,4 ГГц.

Таким чином, на кожні 10 метрів втрати складуть приблизно 75 Дб на 100 метрів 110 Дб. Очікувана похибка перебувати в діапазоні 13 Дб.

Всі невідомі константи, в тому числі значення «40», яке отримано в результаті експериментів, буде об'єднано в одну константу C, де C - невідома константа, що визначає вихідну потужність з урахуванням впливу загасань, конфігурації антени та інших факторів.

$$Rd = C - 35log10$$

Нижче наведено співвідношення, на основі якого проведемо перетворення значення в не нормоване (для відповідності значень вихідним даними утиліти iwspy під Linux):

$$PRSSI = 0{,}83(C - 35log10D) + 83{,}891$$

Розглянемо програму, для побудови апроксимаційної функції в середовищі Gnuplot, використовуючи дані.

```
set view ,,.5
sstodbm(ss) = ss * 1.205 - 101.07
dbmtoss(dbm) = dbm * .83 + 83.891
f(x) = dbmtoss ( a - 35 * (log(x)/log(10)) )
fit f(x) "ld-distance-data/cisco-chan6-antenna.txt" via a
plot [0:25][0:62] "ld-distance-data/cisco-chan6-antenna.txt", f(x)
pause -1 "Hit return to continue"
fit f(x) "ld-distance-data/cisco-chan6-no-antenna.txt" via a
plot [0:25][0:62] "ld-distance-data/cisco-chan6-no-antenna.txt", f(x)
pause -1 "Hit return to continue"
fit f(x) "ld-distance-data/orinoco-chan3-antenna.txt" via a
plot [0:25][0:62] "ld-distance-data/orinoco-chan3-antenna.txt", f(x)
pause -1 "Hit return to continue"
```

Рис.3.10.Приклад кадру

На рис.3.11-3.12. представлено утворену криву апроксимації для кожного з випадків

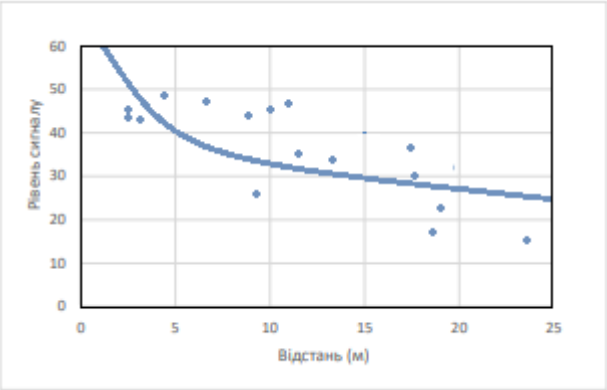


Рис.3.11. Cisco AP350s з антеною

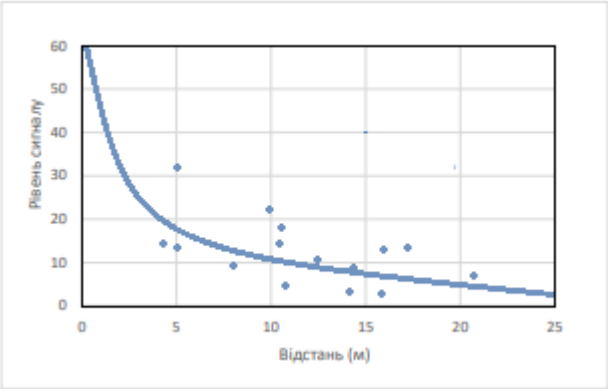


Рис.3.12. Cisco AP350s без антени

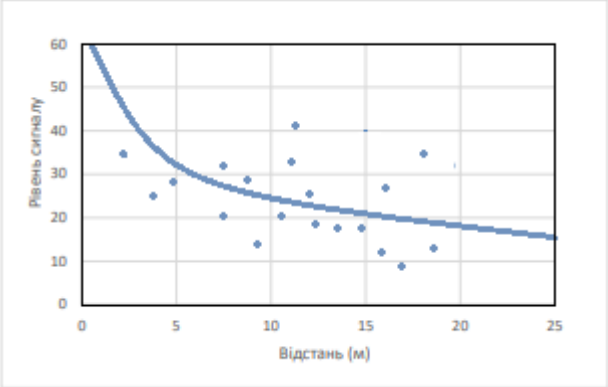


Рис.3.13. Orinoco AP-1000 з антеною Lucent

Інтерполяція рівня сигналу у просторі. Наступний крок – побудова плану приміщення, у якому проводилися експерименти, який нанесені контури, відповідні рівню сигналу. Білою точкою позначено реальне положення точки

доступу, місце якої визначається під час експерименту. Спостерігається пряма залежність точно плану, від кількості зібраних даних.

Останній крок передбачає побудову функціональну залежність рівня сигналу від координат, де R_d - рівень отриманого сигналу (в Дб), N – ненормоване значення рівня отриманого сигналу (%), T_x та T_y – координати передавача, C – константа, що визначає вихідну потужність з урахуванням впливу згасань, конфігурації антени та інших факторів.

$$R_d = C - 35log_{10}\sqrt{(T_x - x)^2 + (T_y - y)^2}$$

$$N = 0?\,83\left(C - 35log_{10}\sqrt{(T_x - x)^2 + \left(T_y - y\right)^2}\right) + 83{,}891$$

Для імітаційногго моделювання використовуємо Gnuplot, яка будує тривимірний графік залежності рівня сигналу від відстані рис. 3.15. Як стартові умови, для алгоритму кращої відповідності (best-fit) обрали такі усереднені значення параметрів T_x = 10, T_y=10 і C=-20.

```
      set isosamples 25
      set hidden3d
      sstodbm(ss) = ss * 1.205 - 101.07

      dbmtoss(dbm) = dbm * .83 + 83.891
      g(x,y) = dbmtoss ( c - 35 * (log( sqrt((a-x)**2 + (b-y)**2) )/log(10)) )
      fit g(x,y) "2d-locate-data/cisco-chan6-antenna.txt" using 1:2:3:(1) via
"2dlocate.
      par"
      splot [0:30][-25:0][0:85] g(x,y)
      pause -1 "Hit return to continue"
      fit g(x,y) "2d-locate-data/cisco-chan6-no-antenna.txt" using 1:2:3:(1)
via
      "2d-locate.par"
      splot [0:30][-25:0][0:85] g(x,y)
      pause -1 "Hit return to continue"
      fit g(x,y) "2d-locate-data/orinoco-chan3-antenna.txt" using 1:2:3:(1)
via "2dlocate.
      par"
      splot [0:30][-25:0][0:85] g(x,y)
      pause -1 "Hit return to continue"
```

Рис.3.14.Приклад усередненого значення

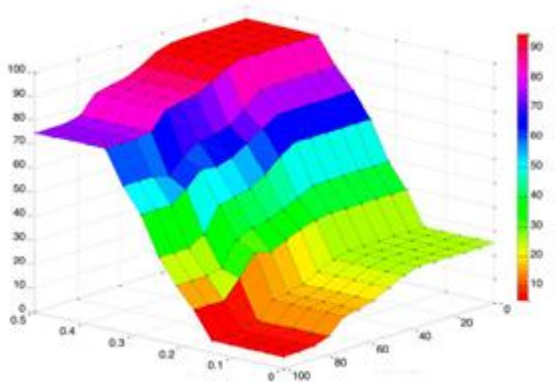


Рис. 3.15. Тривимірний графік залежності рівня сигналу від координат передавача

Отримані результати. Програма для Gnuplot, наведена вище, дозволяє отримати графіки, також виводить знайдене найкраще значення та похибку для кожного з наборів даних. У табл.3.1. наведено реальні значення та найкращі відповідності, отримані з наборів даних.

Таблиця 3.1.

Реальні значення та найкращі відповідності

	Координати передавача (x)	Координати передавача (y)	Знайдене значення (x)	Знайдене значення (y)	Значення константи C (залежить від потужності передавача)
Cisco AP350S з антеною	5,18	-14,94	5,15986 +/- 0,9969	-14,847M 0,7456	-20,1008+/- 1,706
Cisco AP350S без антеною	12,50	-18,29	11,3324 +/- 0,2842	-16,2561+/- 0,55	-50,4432+/- 0,6815
Orinoco AP-1000 з антеною Lucent	14,17	-13,11	14,6243 +/- 1,3	-21,1688+/- 2,547	-34,1176+/- 2,639

Похибка двох результатів не більше 2 метри, тоді як похибка третього результату - 8 метрів.

Розглянемо ряд причин:

1. На шляху сигналу були перешкоди, а значить, згасання сигналу від антени передавача було значним.

2. Не вдалося зібрати достовірну інформацію про рівень загасання сигналу на граничних відстанях, оскільки передавач розташовувався всередині приміщення.

3. У приміщенні було розташовано велику кількіст металевих приладів. Це призвело до послаблення та екранувало сигнал у певних напрямках.

Для більш достовірних результатів слід зібрати більше даних, що призведе до зниження рівня похибки.

ВИСНОВКИ

У процесі виконання поставленого завдання у магістерській кваліфікаційній роботі було впершу досліджено сучасний стан та перспективи подальшого розвитку робототехніки. Аналіз показав, що в результаті розвитку робототехніки людство отримує можливість вирішувати принципово нові наукові та виробничі завдання.

Виконано аналіз технічних особливостей та структури системи управління мобільним робототехнічним комплексом та визначено вимоги і принципи побудови системи управління маніпуляційним роботом, приведено приклад існуючих систем управління та показано можливості і сфери застосування робототехнічних систем.

Як показав аналіз, зазвичай для управління використовують технології безпроводового зв'язку, у нашому випадку за основу дослідження взято технологію IEEE 802.11. В першу чергу розглянуто особливості структури бездротових мереж стандарту IEEE 802.11 з погляду захисту інформації. Проведений аналіз публікацій на тему захисту інформації та специфіка застосування дозволяє виділити перелік вимог, що визначають якість захисту радіоканалів МРК.

Виконуючи друге поставлене завдання, досліджено проблеми захисту інформації в радіоканалі. Також проведено поцінку механізму аутентифікації та досліджено методи захисту інформації у протоколі WEP.

Виконані дослідження показали, що причиною ризиків, пов'язаних з безпекою інформації, при використанні мережевої інфраструктури стандарту 802.11 є атаки на конфіденційність інформації (перехоплення та аналіз трафіку), цілісність (підміна адреси, повтор та модифікація повідомлення). На підставі чого було запропоновано комплекс методів та засобів захисту інформації в радіоканалах, досліджено методи покращення стандартної системи безпеки, заснованої на алгоритмі WEP.

На основі експериментальних даних розглянуто технологію, що дозволяє здійснювати ефективний пошук та локалізацію неавторизованої станції у

захищеній бездротовій мережі. Виявлено причини можливого виникнення помилок, наведено методи підвищення ефективності визначення місцезнаходження станцій-порушника.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ha T., Choi C.-H. An effective trajectory generation method for bipedal walking// Robotics and Autonomous Systems. – 2017. – Т. 55, № 10. – С. 795-810.

2. Kim J.-Y., Kim Y.-S. Human-like gait generation for biped android robot using mo-tion capture and zmp measurement system// International Journal of Humanoid Robotics. – 2016. – Т. 07, № 04. – С. 511-534.

3. Strom J., Slavov G., Chown E. Omnidirectional Walking Using ZMP and Preview Control for the NAO Humanoid Robot// RoboCup 2009: Robot Soccer World Cup XIII / Baltes J. и др. Springer Berlin Heidelberg, 2019. – С. 378-389.

4. Piperakis S., Orfanoudakis E., Lagoudakis M. G. Predictive control for dynamic locomotion of real humanoid robots// 2014 IEEE/RSJ International Conference on Intelligent Robots and Systems –, 2014. – С. 4036-4043.

5. Vukobratović M., Borovac B. Zero-moment point - thirty five years of its life// In-ternational Journal of Humanoid Robotics. – 2014. – Т. 01, № 01. – С. 157-173.

6. Kajita S., Hirukawa H., Harada K., Yokoi K. Introduction to humanoid robotics. Springer, 2018.

7. Angelo J. A. Robotics: A Reference Guide to the New Technology. — Westport, Conn.: Greenwood Press, 2017.

8. Макаров И. М., Топчеев Ю. И. Робототехника: История и перспективы. — М.: Наука; Изд-во МАИ, 2019

9. Зенкевич С. Л., Ющенко А. С. Основы управления манипуляционными роботами. 2-е изд. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2018. — 480 с.

10. Walker, Jesse R. Unsafe at any key size; An analysis of the WEP encapsulation // http://grouper.ieee.org/groups/802/ll/ Documents/ DocumentHolder /0-362.zip - 23 Jan. 2012.

11. Walker R. Unsafe at any key size; an analysis of the WEP encapsulation // Operating Systems Review, vol. 29, Iss. 5. - 2011 - 45-51 p.

12. Успенский А.Ю., Иванов И.П. Анализ проблем защиты информации в радиоканалах стандарта ШЕЕ 802.11 // Вестник МГТУ. Сер. Машиностроение. - 2012. - №. 4 - С. 102-108.

13. National Institute of Standards and Technology, NIST FIPS PUB 186. Digital Signature Standard. // U.S. Department of Commerce. - 2009.-230 p.

14. Bellovin S. M., Merritt M. Encrypted Key Exchange: Password- Based Protocols Secure Against Dictionary Attacks. // Proceedings of the IEEE. Symposium on Research"'in Security and Privacy. Oakland, 2011. -155 p.

15. Jaspan B. Dual-workfactor Encrypted Key Exchange: Efficiently Preventing Password Chaining and Dictionary Attacks. // Proceedings of the Sixth Annual USENIX Security Conference. - 2007.-43-50 p.

16. Donald L., Schilling L., Laurence B. Milstein. Spread Spectrum Goes Commercial. // City College of New York, George Washington University, and UC San Diego. - 2013. -128 p.

17. Rappaport S. Wireless Communications - Principles & Practice. - IEEE Press, 2016 -221 p.

18. Иванов И.П., Успенский АЛО. Модель информационной безопасности радиоканала ШЕЕ 802.11.// Вестник МГТУ. Сер. Машиностроение. - 2013. - №.2(51) - С.89 - 94.

19. Тимофеев А.В. Адаптивные робототехнические комплексы / Машино ведение.2017. – 392 с.

20. Красильникъянц Е. В., Варков А. А., Тютиков В. В. Система управления манипуляционным роботом// Автоматизация в промышленности. - №5. – 2018. – С. 38-44.

21. Mladenova C. Mathematical modeling and control of manipulator systems. Int. J. Robotics and computer-integrated manufacturing, vol. 8, N 4, 2014, pp. 233-242.

22. L. Biagiotti, C. Melchiorri, Trajectory Planning for Automatic Machines and Robots, Springer, 2018.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)