НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

До захисту допущено:

Завідувач кафедри

_____ Сергій КРАВЧУК

«___»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інженерія та програмування інфокомунікацій»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Розвиток безпеки Інтернету речей в середовищі 5G»

Виконав:
студент IV курсу, групи ТЗ-01
Гаєв Іван Олександрович _____

Керівник:
Доцент кафедри ТК НН ІТС, к.т.н.
Міночкін Дмитро Анатолійович _____

Рецензент:
Доцент кафедри ІТТ НН ІТС, к.т.н., доцент,
Новогрудська Ріна Леонідівна _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2024 р.

ЗАВДАННЯ
на дипломну роботу студенту
Гаєву Івану Олександровичу

1. Тема роботи «Розвиток безпеки Інтернету речей в середовищі 5G», керівник роботи Міночкін Дмитро Анатолійович, к.т.н., с.н.с, затверджені наказом по університету від «22» травня 2024 р. № 2064-с.

2. Термін подання студентом роботи 10 червня 2024 р.

3. Вихідні дані до роботи: інформаційні матеріали про архітектури та функціонування безпеки мереж інтернету речей.

4. Зміст роботи: Провести огляд наявних архітектур та принципів безпеки мережі. Проаналізувати аспекти безпеки мережі IoT на основі технологій 5G. Розглянути основні методи захисту, які використовуються в мережах 5G. Розглянути можливості забезпечення безпеки в мережах 5G. Дослідити основні переваги протоколів захисту.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): слайди презентації за матеріалами проведеного дослідження безпеки мереж інтернету речей на базі технологій 5G:

1. Тема
2. Вступ. Актуальність. Мета

3. Загальні відомості про IoT
4. Загальні відомості про 5G
5. Безпека багаторіневої архітектури IoT
6. Безпека багаторіневої архітектури IoT (продовження)
7. Виклики безпеки мережі 5G
8. Потенційні рішення викликів
9. Висновок

6. Дата видачі завдання «20» лютого 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Розробка, оформлення, узгодження та затвердження технічного завдання на роботу. Аналітичний огляд інформаційних матеріалів. Підбір та опрацювання необхідної науковотехнічної літератури.	20.02.2024-09.03.2024	Виконано
2	Вивчення та розбір основних відомостей про безпеку мереж: основні складові захисту, рівні захисту. Ознайомлення з архітектурою інтернету речей: Існуючі в літературі архітектури безпеки мереж; Порівняльний аналіз існуючих архітектур і типів протоколів захисту. Розглянути можливості безпеки мереж 5G.	10.03.2024-24.03.2024	Виконано
3	Ознайомлення з основними протоколами безпеки 5G: архітектури та їх компоненти. Ознайомлення з найпопулярнішими протоколами захисту мереж 5G. Розробка власної захищеної мережі інтернету речей на базі 5G. Проведення порівняння критеріїв безпеки мереж та їх архітектур.	25.04.2024-01.06.2024	Виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	01.06.2024-10.06.2024	Виконано
5	Підготовка та оформлення презентації для доповіді	10.06.2024-15.06.2024	Виконано

Студент Іван ГАЄВ

Керівник Дмитро МІНОЧКІН

РЕФЕРАТ

Дипломна робота містить 54 сторінки, 4 риснуки. Було використано 7 джерел інформації.

Метою роботи є дослідження стану розвитку безпеки Інтернету речей в середовищі 5G. Основними методами були аналітичний огляд літератури та моделювання.

У результаті роботи було детально розглянуто архітектуру IoT та 5G мережі, основні виклики та загрози, можливі атаки. А також огляд методів та засобів уникнення і протистоянню загроз. Отримані результати включають огляд основних методів уникнення загроз для технології IoT в мережі 5G, що підвищує імовірність успішного конструювання розумних мереж.

Рекомендації щодо використання результатів дипломної роботи включають впровадження методів запобігання загрозам при створенні IoT мереж. Результати роботи можуть бути використані для подальшого аналізу розвитку безпеки Інтернету речей на базі технології 5G

Ключові слова: Безпека мереж, засоби уникнення загроз в технологіях IoT.

ABSTRACT

The thesis comprises 54 pages and includes 4 figures. Nine sources of information were utilized.

The aim of the work is to study the state of Internet of Things (IoT) security development in a 5G environment. The primary methods used were a literature review and modeling.

As a result of the work, the architecture of IoT and 5G networks, the main challenges and threats, and possible attacks were examined in detail. Additionally, an overview of methods and means to avoid and counter threats was provided. The obtained results include a review of the main threat avoidance methods for IoT technology in 5G networks, which increases the likelihood of successfully constructing smart networks.

Recommendations for the application of the thesis results include the implementation of threat prevention methods when creating IoT networks. The results of the work can be used for further analysis of IoT security development based on 5G technology.

Keywords: Network Security, Threat Avoidance Methods in IoT Technologies.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

DDoS	Distributed Denial of Service
DNS	Domain Name System
GNSS	Global Navigation Satellite System
IoT	Internet of Things
M2M	Machine to Machine
NGMN	Next Generation Mobile Networks
NFV	Network Functions Virtualization
RFID	Radio-Frequency Identification
SBA	Service-Based Architecture
SDN	Software-Defined Networking
UE	User Equipment
WSN	Wireless Sensor Network
3GPP	Third Generation Partnership Project

ВСТУП

У нашому світі, де Інтернет речей стає все більш розповсюдженим, а технологія 5G набирає обертів, безпека цих мереж стає крайньою важливістю. IoT відкриває необмежені можливості для спілкування та взаємодії пристроїв з веб-сервісами, а технологія 5G, завдяки своїм характеристикам, дозволяє забезпечити ще більше підключень та використання можливостей IoT.

Проте, зі зростанням розмірів і складності мереж IoT, що базуються на технології 5G, збільшується ймовірність вразливостей і кібератак на них. Злоумисники можуть використовувати ці вразливості для незаконного доступу до пристроїв, крадіжки конфіденційної інформації або навіть атак на критичну інфраструктуру.

Метою дипломної роботи є проведення аналізу проблем безпеки, пов'язаних з мережами IoT в середовищі 5G. Деякі аспекти цієї роботи:

1. Аналіз архітектури мереж IoT на базі технологій 5G та ідентифікація основних загроз безпеці.
2. Аналіз вразливостей мереж IoT в середовищі 5G та існуючих методів атак.
3. Аналіз наявних рішень проблем

Ця робота спрямована на розуміння основних викликів, що стоять перед безпекою мереж IoT на базі технологій 5G.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ ТА 5G МЕРЕЖІ

1.1. Огляд технології 5G

Наступне покоління телекомунікаційних мереж (п'яте покоління або 5G) з'явилося на ринку наприкінці 2018 року і досі розширюється по всьому світу. Очікується, що ця технологія створить величезну екосистему 5G IoT (Інтернет речей), в мережі якої зможуть обслуговувати комунікаційні потреби мільярдів підключених пристроїв із правильним компромісом між швидкістю, затримкою та вартістю. Станом на жовтень 2023 року, за даними останнього звіту Ericsson Mobility Report, у світі налічувалося близько 1,9 мільярда підписок на 5G[6].

Основні особливості технології 5G:

- висока швидкість передачі даних: технологія 5G забезпечує швидкість передачі даних до 10 Гбіт/с, що в 100 разів перевищує швидкість 4G мереж. Це дозволяє завантажувати великі файли, такі як фільми у форматі 4K, за лічені секунди. З точки зору граничних значень швидкості передачі інформації, які характерні для різних поколінь мобільного зв’язку, технологія 5G приблизно у 10 разів швидша за діючу 4G. Максимальне значення швидкості для 5G - 10 Гбіт/с.

- низька затримка: затримка в мережах 5G дорівнює 1 мілісекунді, що є основною перевагою для додатків, що потребують реального часу, таких як автономні транспортні засоби та дистанційна хірургія.

- висока ємність мережі: 5G може підтримувати до мільйона пристроїв на квадратний кілометр, що робить її ідеальною для Інтернету речей (IoT).

Треба заначити що всі ці переваги з’явилися через використання широкосмугового спектру (міліметрові хвилі між 30 ГГц та 300 ГГц).

Переваги технології 5G:

- покращена взаємодія пристроїв IoT: завдяки високій ємності та низькій затримці, 5G забезпечує надійну взаємодію між численними IoT-пристроями, що є критичним для смарт-міст, розумних будинків та промислових додатків.

- підтримка нових технологій та додатків: 5G відкриває можливості для розвитку нових технологій, таких як доповнена реальність (AR) та віртуальна реальність (VR), автономні транспортні засоби, дистанційна медицина тощо.

- енергоефективність: пристрої, підключені до мережі 5G, можуть працювати довше без зарядки завдяки більш ефективному використанню енергії.

Виклики впровадження 5G:

- інфраструктурні вимоги: для забезпечення повного покриття 5G необхідно встановити велику кількість базових станцій, що потребує значних інвестицій та часу.

- безпека та конфіденційність: зі збільшенням кількості підключених пристроїв виникають нові виклики у забезпеченні безпеки та конфіденційності даних.

- регуляторні та юридичні питання: впровадження 5G потребує врегулювання численних юридичних та регуляторних аспектів, включаючи розподіл частотного спектру.

1.2. Розробка та планування 5G

Телекомунікаційні мережі надають споживачам послуги зв'язку, які розвивалися з фіксованої телефонії до мобільного зв'язку, який спочатку пропонував аналоговий голос і мобільність у 1980-х роках - це було 1-е покоління мобільного зв'язку. У 1990-х роках з'явилося 2-ге покоління, яке впровадило цифрові голосові дзвінки, послуги коротких повідомлень (SMS) та базові послуги передачі даних. Мобільний зв'язок продовжив розвиватися з введенням 3-го покоління мереж з мобільним широкосмуговим зв'язком та смартфонами, додавши нові функції до існуючих послуг. Дослідження та

розробки в області мобільного широкосмугового зв'язку сприяли впровадженню мережі 4-го покоління, яка використовує швидкий мобільний широкосмуговий зв'язок та інтернет-протоколи цього покоління, також відомі як мережі LTE (Long Term Evolution - довгострокова еволюція). Організації, такі як 3GPP, продовжують досліджувати та вдосконалювати мобільні мережі, щоб відповідати потребам зв'язку у різних секторах. Результатом цих зусиль є мережа 5-го покоління, яка відзначається подальшими поліпшеннями у мобільному широкосмуговому зв'язку та призначена для обслуговування зв'язку для промислових цілей.

Розробка архітектури мережі 5G, яка підтримує дуже вимогливі програми, є складною. Наприклад, не існує універсального підходу; діапазон програм потребує даних для подорожі на відстані, великих обсягів даних або певної комбінації. Таким чином, архітектура 5G повинна підтримувати низький, середній і високий діапазон частот – з ліцензованих, спільних і приватних джерел – щоб забезпечити повне бачення 5G. З цієї причини 5G розроблено для роботи на радіочастотах у діапазоні від нижче за 1 ГГц до надзвичайно високих частот, які називаються «міліметровими хвилями» (або mmWave). Чим нижча частота, тим далі може поширюватися сигнал. Чим вища частота, тим більше даних він може передавати.

Як показано на Рис.1.1., в основі мереж 5G є три діапазони частот:

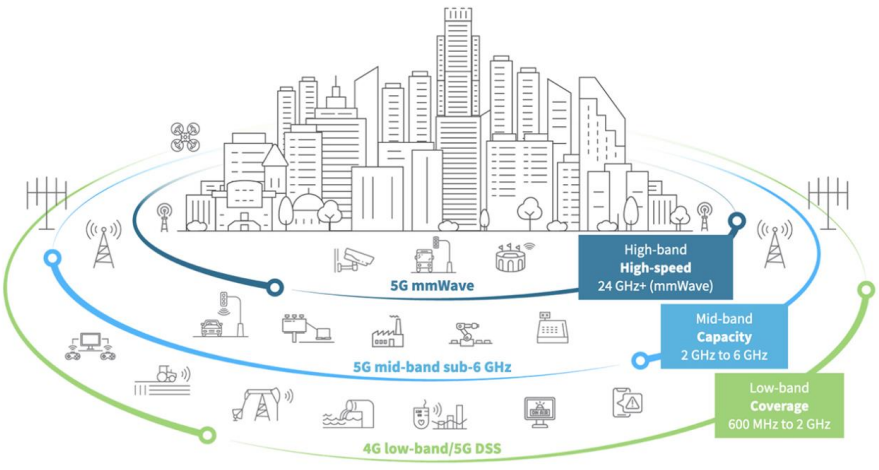

Рис.1.1. Смуги частот в основі мереж 5G [1]

- високочастотний діапазон (High-band) 5G (mmWave) забезпечує найвищі частоти 5G. Вони варіюються від 24 ГГц до приблизно 100 ГГц. Високочастотний 5G за своєю природою має малий радіус дії, оскільки високі частоти не можуть легко проходити крізь перешкоди. Крім того, покриття mmWave обмежене і вимагає більшої стільникової інфраструктури.

- 5G середнього діапазону (Mid-band) працює в діапазоні 2-6 ГГц і забезпечує рівень пропускної здатності для міських і приміських районів. Цей діапазон частот має пікові швидкості в сотні Мбіт/с.

- низькочастотний діапазон (Low-band) 5G працює на частотах нижче 2 ГГц і забезпечує широке покриття. Цей діапазон використовує спектр, який доступний і використовується сьогодні для 4G LTE, по суті, забезпечуючи архітектуру LTE 5g для пристроїв 5G, які вже готові. Таким чином, продуктивність низькочастотного зв'язку 5G подібна до 4G LTE і підтримує використання для пристроїв 5G, які є на сьогоднішньому ринку.

1.3. Базова Мережа 5G (5G Core Network)

Базова мережа 5G, яка забезпечує розширену функціональність мереж 5G, є одним із трьох основних компонентів системи 5G, також відомої як 5GS. Двома іншими компонентами є мережа доступу 5G (5G-AN) і обладнання користувача (UE). Ядро 5G використовує архітектуру на основі хмарних послуг (SBA) для підтримки автентифікації, безпеки, керування сеансами та агрегації трафіку від підключених пристроїв, і все це вимагає складного взаємозв'язку функцій мережі, як показано на схемі ядра 5G.

Архітектура ядра 5G складається з ряду важливих компонентів, які взаємодіють для забезпечення ефективної роботи мережі:

- користувацьке обладнання (User Equipment, UE): включає всі пристрої, які підключаються до мережі 5G, такі як смартфони, планшети, датчики та інші IoT-пристрої

- базова станція наступного покоління (Next Gen Node Basestation, gNB): відповідає за забезпечення радіозв'язку між користувацьким обладнанням та мережею

- функція користувацької площини (User Plane Function, UPF): елемент і функція 5G мережі, яка працює з трафіком користувача і забезпечує його передачу назовні з мобільної мережі. Відповідно, UPF розташований на стику мобільної мережі оператора та зовнішніх мереж

- функція управління доступом і мобільністю (Access and Mobility Management Function, AMF): відповідає за термінацію інтерфейсу контрольної площини RAN (NG2), аутентифікацію доступу, управління мобільністю та захист даних.Core Access and Mobility Management Function (AMF)

- функція управління сесіями (Session Management Function, SMF): відповідає за управління сесіями, виділення IP-адрес для UE, контроль функції користувацької площини та інтерфейси політичного контролю та тарифікації.

- функція аутентифікації серверу (Authentication Server Function, AUSF): виконує процеси аутентифікації з UE

- уніфіковане управління даними (Unified Data Management, UDM): підтримує функцію збереження облікових даних аутентифікації та зберігання інформації про підписку

- функція політичного контролю (Policy Control Function, PCF): забезпечує підтримку єдиної політичної рамки для управління поведінкою мережі та надання політичних правил функціям контрольної площини

- функція додатків (Application Function, AF): запитує динамічні політики та/або контроль тарифікації

Схема архітектури мережі 5G, наведена на Рис.1.2., ілюструє, як пов’язані ці компоненти.

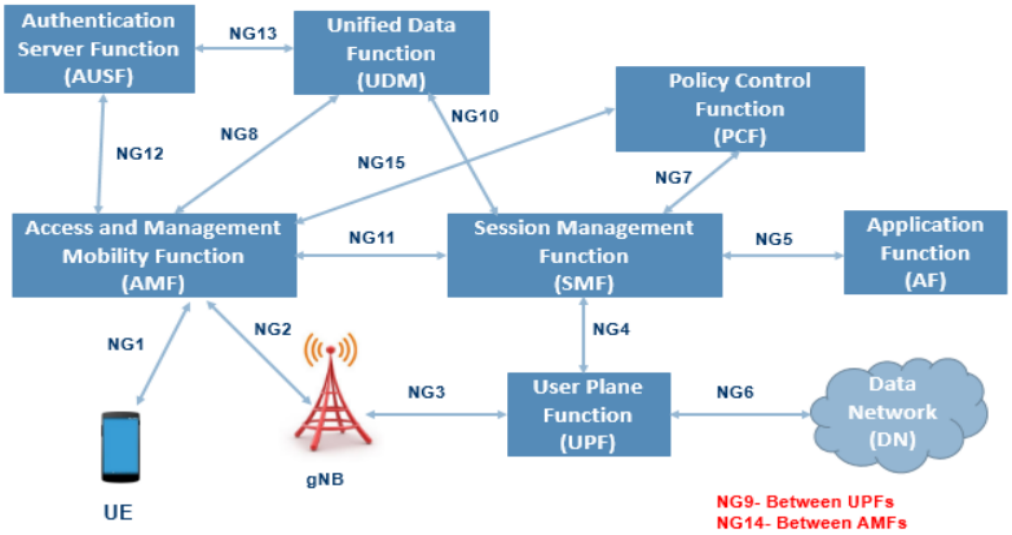

Рис.1.2. Еталонна мережева архітектура [2]

1.4. Основи Інтернету речей

Інтернет речей (IoT) - це концепція, яка передбачає взаємозв'язок фізичних пристроїв, сенсорів, ідентифікаторів та інших об'єктів через Інтернет для збору і обміну даними. IoT дозволяє створювати "розумні" середовища, де об'єкти можуть автономно спілкуватися між собою та приймати рішення на основі отриманих даних. Цей огляд розглядає основні особливості, переваги, виклики та сфери застосування IoT.

Основні особливості IoT:

- взаємозв'язок: об'єкти IoT можуть спілкуватися між собою та обмінюватися даними через мережу, що дозволяє створювати інтегровані системи.

- автоматизація та управління: пристрої IoT можуть автоматично виконувати певні завдання без участі людини, що підвищує ефективність і зручність.

- дані та аналітика: збирання великих обсягів даних з різних джерел дозволяє проводити глибокий аналіз і отримувати цінну інформацію для прийняття рішень.

- віддалене управління: користувачі можуть контролювати та керувати IoT-пристроями з будь-якого місця через інтернет-з'єднання.

Переваги IoT:

- підвищення ефективності: автоматизація процесів і оптимізація ресурсів сприяє підвищенню продуктивності в різних галузях.

- економія часу і коштів: використання IoT дозволяє знижувати витрати на обслуговування і управління системами, а також економити час.

- покращення якості життя: розумні будинки, розумні міста та інші IoT-застосування сприяють підвищенню комфорту і безпеки для людей.

- нові можливості для бізнесу: IoT відкриває нові можливості для розвитку бізнесу, створення нових продуктів і послуг, а також для підвищення конкурентоспроможності.

1.5. Об’єднання технологій IoT і 5G

Інтеграція технології 5G з Інтернетом речей (IoT) відкриває нові горизонти для розвитку сучасних технологій, наприклад, завдяки можливості 5G підтримувати велику кількість підключених пристроїв без погіршення продуктивності, організації можуть розгортати більше сенсорів і пристроїв IoT по всій своїй інфраструктурі, що дозволяє здійснювати моніторинг у режимі реального часу та приймати рішення на основі даних.[7] Цей підрозділ розгляне ключові аспекти та переваги, які надає 5G для IoT. Злиття технологій має значні переваги:

- підвищення швидкості передачі даних:

Технологія 5G забезпечує значно вищу швидкість передачі даних, порівняно з попередніми поколіннями мобільного зв’язку. Це дозволяє IoT-пристроям швидко обробляти та передавати великі обсяги даних. Наприклад, у сфері охорони здоров'я, де використовуються носимі IoT-пристрої для постійного моніторингу життєво важливих показників, швидка передача даних дозволяє лікарям отримувати інформацію в реальному часі, що підвищує оперативність реагування в екстрених ситуаціях.

- покращення енергетичної ефективності:

Енергетична ефективність є критичним фактором для IoT-пристроїв, які часто працюють від батарей. Завдяки 5G, пристрої можуть передавати дані швидше, що зменшує їх активний час роботи і, відповідно, споживання енергії. Це дозволяє збільшити термін служби батарей і знизити частоту їх заміни, що важливо для пристроїв, розташованих у важкодоступних місцях, таких як сільськогосподарські сенсори або датчики для моніторингу довкілля.

- зниження затримок:

Затримка передачі даних (латентність) у мережах 5G знижена до кількох мілісекунд, що є критично важливим для застосувань, які вимагають миттєвої обробки інформації. Наприклад, у промисловому Інтернеті речей (IIoT), де машини повинні реагувати на дані сенсорів негайно, низька латентність дозволяє уникнути збоїв у роботі та підвищує безпеку виробничих процесів

- підвищення надійності мережі:

5G забезпечує більш надійне з'єднання, здатне обробляти велику кількість підключених пристроїв одночасно. Це гарантує стабільність і безперервність передачі даних, що особливо важливо для таких сфер, як охорона здоров'я та управління інфраструктурою, де переривання зв’язку можуть мати серйозні наслідки. Крім того, 5G забезпечує стабільне з'єднання навіть у важкодоступних місцях, таких як віддалені або сільські райони, що сприяє розширенню застосувань IoT у цих регіонах.

Висновки

Цей розділ мав на меті ознайомити читача з ключовими аспектами та концепціями, що стосуються Інтернету речей (IoT) та технологій 5G. У ході дослідження було встановлено, що IoT охоплює мережі, в яких фізичні та віртуальні об'єкти, оснащені датчиками, здатні обмінюватися даними через мережу. Технологія 5G, в свою чергу, представляє нове покоління мобільного зв'язку, що забезпечує вищу швидкість передачі даних, масштабованість та надійність. Детально розглянуто еталонну архітектуру IoT та 5G.

На завершення, розділ надає загальний огляд мереж IoT, заснованих на технологіях 5G, висвітлюючи основні концепції, пов'язані з цими технологіями. Ця інформація слугує основою для подальших розділів дипломної роботи, де будуть розглядатися питання безпеки та її впровадження в мережах IoT на базі технологій 5G.

РОЗДІЛ 2
ЗАГРОЗИ ТА ВИКЛИКИ БЕЗПЕКИ

2.1. Дослідження та статистика

У 2023 році в світі налічується понад 15,14 мільярда підключених IoT-пристроїв. Очікується, що до 2030 року ця кількість зросте до 29,42 мільярда[5]. Дослідження виявило процвітання тіньової економіки у темному інтернеті, спрямованої на послуги, пов'язані з Інтернетом речей (IoT). Особливо великий попит серед хакерів викликають розподілені атаки відмови у послугах (DDoS), які організовуються за допомогою мереж ботів IoT. Протягом першої половини 2023 року аналітики виявили понад 700 оголошень про послуги DDoS-атак на різних форумах темної мережі.

Вартість цих послуг залежить від таких факторів, як захист від DDoS, CAPTCHA та перевірка JavaScript на боці жертви, і коливається від 20 доларів США на день до 10 000 доларів США на місяць. У середньому оголошення пропонувало ці послуги за 63,5 доларів США на день або 1350 доларів США на місяць.

Крім того, на темному ринку мережі пропонуються експлойти для вразливостей нульового дня в пристроях IoT, а також IoT-віруси, які поєднуються з інфраструктурою та супутніми програмами.

Щодо вірусів IoT, існує ряд сімей, багато з яких виникли з Mirai 2016 року. Спрагла конкуренція серед кіберзлочинців підштовхнула розвиток функцій, спрямованих на блокування конкурентних вірусів. Ці тактики включають впровадження правил брандмауера, вимкнення віддаленого керування пристроями та припинення процесів, пов'язаних з конкуруючими вірусами.

Основний спосіб зараження пристроїв IoT залишається перебором слабких паролів, за яким слідує використання вразливостей мережевих служб. Перебор паролів на пристроях, як правило, спрямований на Telnet, широко використовуваний незашифрований протокол. Хакери використовують цей

метод для отримання несанкціонованого доступу, розгадуючи паролі, що дозволяє їм виконувати довільні команди та віруси. Хоча SSH, більш безпечний протокол, також вразливий, він створює більші виклики з точки зору ресурсів для атакуючих.

Протягом першої половини 2023 року горшини Касперського зафіксували, що 97,91% спроб перебору паролів спрямовані на Telnet, тоді як лише 2,09% - на SSH. Ці атаки переважно асоціюються з Китаєм, Індією та Сполученими Штатами, тоді як Китай, Пакистан та Росія виявилися найактивнішими атакувальниками. Крім того, пристрої IoT стикаються з вразливостями через експлойти використовуваних ними служб. Ці атаки часто включають виконання зловмисних команд за допомогою експлойтів веб-інтерфейсів IoT, що призводить до серйозних наслідків, таких як поширення вірусів, таких як Mirai.

Компанії закликають виробників віддавати перевагу кібербезпеці як для споживачів, так і для промислових пристроїв IoT. Повинні обов'язково змінювати стандартні паролі на пристроях IoT та регулярно випускати патчі для усунення вразливостей. Загалом, світ IoT наповнений кіберзагрозами, включаючи атаки DDoS, вимагання викупу та проблеми з безпекою як в домашніх, так і в промислових пристроях. Звіт Касперського підкреслює необхідність відповідального підходу до кібербезпеки IoT, що зобов'язує виробників посилювати безпеку продуктів з самого початку та активно захищати користувачів.

Пристрої IoT вразливі до різних типів вірусів, кожен з яких має власні цілі:

- DDoS-ботнети: Ці зловмисні програми захоплюють контроль над пристроями IoT, щоб запускати розподілені атаки відмови у послугах на широкий спектр сервісів.

- вимагання викупу: Направлені на пристрої IoT, особливо ті, що містять користувацькі дані, такі як NAS-бокси, вимагання викупу шифрують файли і вимагають викупу за розшифрування.

- майнери: Незважаючи на їх обмежену обчислювальну потужність, деякі кіберзлочинці намагаються використовувати пристрої IoT для майнінгу криптовалют.

- змінники DNS: Деякі віруси змінюють налаштування DNS на Wi-Fi маршрутизаторах, перенаправляючи користувачів на зловмисні веб-сайти.

- проксі-боти: Заражені пристрої IoT використовуються як проксі-сервери для перенаправлення зловмисного трафіку, що ускладнює виявлення і мінімізацію таких атак.

Для захисту промислових та споживчих пристроїв IoT експерти рекомендують:

- проводити регулярні аудити безпеки систем OT для ідентифікації та усунення можливих вразливостей.

- використовувати рішення моніторингу, аналізу та виявлення мережевого трафіку ICS для кращого захисту від атак, які можуть загрожувати технологічним процесам та основним активам підприємства.

- переконайтеся, що ви захищаєте індустріальні кінцеві точки, а також корпоративні. Рішення Касперського з кібербезпеки для промислових підприємств включає в себе відповідний захист для кінцевих точок та моніторинг мережі для виявлення будь-якої підозрілої та потенційно зловмисної діяльності в індустріальних мережах.

- при впровадженні IoT оцінюйте статус безпеки пристрою до його впровадження. Перевагу слід надавати пристроям з сертифікатами кібербезпеки та продуктам від виробників, які надають більше уваги інформаці

2.2. Безбека архітектури IoT

Швидке поширення Інтернету речей (IoT) в різних галузях, таких як автоматизація будівель, носимі технології для охорони здоров'я та промисловий контроль процесів, змінює спосіб сприйняття та управління фізичним світом. Прогнозується, що до 2020 року кількість пристроїв IoT

сягне близько 30 мільярдів, більшість з них будуть недорогими та бездротовими з обмеженими обчислювальними та зберігаючими можливостями. Оскільки системи IoT все більше відповідають за виявлення та управління складними екосистемами, питання безпеки та надійності даних, що передаються до та від цих пристроїв, стають все більш актуальними.

Дослідження виявили проблеми безпеки в мережах IoT, зокрема з автентифікацією, авторизацією, витоком інформації, конфіденційністю, перевіркою, підробкою, глушінням та підслуховуванням. IoT забезпечує мережеву інфраструктуру для підключення різних пристроїв, але це створює серйозні проблеми безпеки. Кібератаки, такі як Mirai на Dyn у 2016 році та на українську енергомережу у 2015 році, показують потенційні загрози IoT. Причини проблем безпеки включають небезпечну підключеність до Інтернету та відсутність контролю доступу. Вразливості в системах IoT виникають через обмежені ресурси пристроїв, відсутність стандартів у протоколах безпеки та використання стороннього обладнання та програмного забезпечення.

Безпека полягає в захисті ресурсів від ушкоджень, несанкціонованого доступу та крадіжки, забезпечуючи конфіденційність, цілісність та доступність інформації. У контексті Інтернету речей (IoT) безпека стосується захисту підключених пристроїв та мереж, що використовуються в різних сферах, включаючи розумні міста, домашні автоматизаційні системи, медичні технології та промислові застосування. Впровадження IoT в такі сфери створює нові виклики для безпеки, збільшуючи ймовірність атак та потенційну кількість потенційних жертв. Атаки на IoT, хоча подібні до атак на інформаційні технології, відрізняються масштабом та простотою виконання.

Дослідження показало, що серед найпоширеніших пристроїв IoT для розважальних цілей, таких як смарт-телевізори, веб-камери та принтери, близько 13% з 156 680 мають різні рівні вразливостей. Серед них - виявлення MiniUPnP, NAT-PMP, незашифрованого telnet, наявність SNMP-агентів, слабкі алгоритми SSH та уразливості FTP. Розділ представляє результати дослідження цих вразливостей та заходів захисту, проведеного в контексті IoT

та його сучасних методів безпеки, зокрема за допомогою аналізу атак на трьох рівнях: сприйняття, мережі та застосування. На рисунку 3.1 показана типова архітектура IoT та елементи, які розглядаються на кожному рівні. Далі будуть детально розглянуті ці рівні, можливі проблеми та відповідні їм рішення.

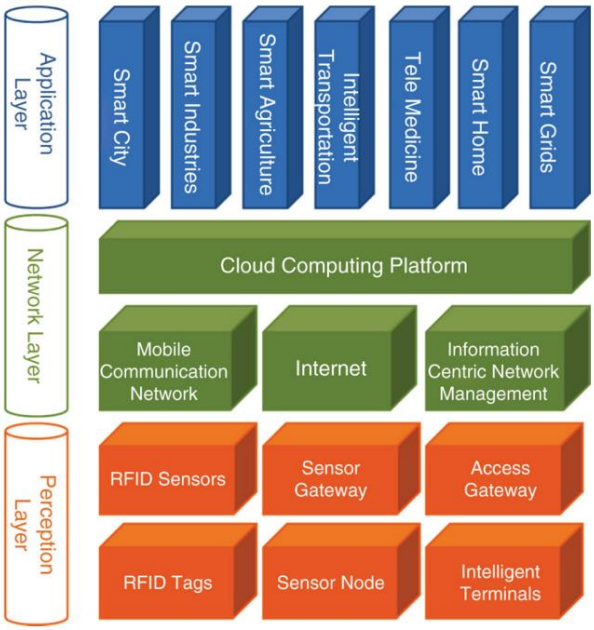

Рис.2.1. Архітектура IoT [3]

2.2.1. Рівень сприйняття

Рівень сприйняття включає збір інформації та управління об'єктами. Він складається з вузлів сприйняття (наприклад, датчики) та мережі сприйняття, що взаємодіє з транспортною мережею. Вузли сприйняття збирають та управляють даними, а мережа сприйняття передає дані на шлюз або надсилає інструкції контролерам. Технології цього рівня включають RFID, WSNs, RSN, GPS.

2.2.1.1. Питання безпеки технології RFID та рішення

RFID (радіочастотна ідентифікація) - це технологія автоматичної ідентифікації без контакту, яка дозволяє автоматично визначати цільовий сигнал мітки та отримувати відповідні дані без необхідності ручного втручання, працюючи навіть в суворих умовах. Попри широке застосування RFID, вона має низку проблем, які наведені нижче:

- єдине кодування: Наразі не існує єдиного міжнародного стандарту кодування для RFID-міток. Найбільш впливовими є стандарти UID (універсальна ідентифікація), підтримувані Японією, і EPC (електронний код продукту), які підтримуються Європою. Через відсутність єдиного стандарту можуть виникати проблеми, коли зчитувач не може отримати доступ до інформації мітки, або ж можуть траплятися помилки під час процесу зчитування.

- конфлікт зіткнення: Коли кілька RFID-міток одночасно передають дані до зчитувача, це може призвести до того, що зчитувач не зможе правильно отримати інформацію. Використання технології антизіткнення може запобігти одночасній передачі даних від декількох міток до зчитувача. Конфлікти RFID можна розділити на дві категорії: зіткнення міток і зіткнення зчитувачів. Коли велика кількість міток знаходиться в зоні дії зчитувача і зчитувач не може правильно отримати дані, це називається зіткненням міток. Інтернет речей (IoT) потребує широкого покриття RFID-датчиків, і кооперативна робота декількох зчитувачів є особливо важливою, але їхні робочі зони можуть перекриватися. Це може призвести до надлишкової інформації, що збільшує навантаження на передачу даних у мережі. Це називається зіткненням зчитувачів. Різні типи зіткнень потребують різних рішень. Наразі алгоритми антизіткнення для міток досліджені достатньо, але для зчитувачів досліджень недостатньо. Алгоритми антизіткнення зчитувачів здебільшого поділяються на рішення, засновані на просторі, та на часі. Основна ідея алгоритму антизіткнення на основі простору полягає в уникненні перекриття робочих зон зчитувачів для зменшення зони конфлікту, але це рішення вимагає додаткової центральної контрольної області для розрахунку робочих зон між зчитувачами, що підвищує складність і вартість.

- захист конфіденційності за допомогою RFID: Низька вартість міток призвела до обмежених ресурсів RFID, таких як мала ємність зберігання і слабкі обчислювальні можливості, що вимагає легких рішень для захисту

конфіденційності, включаючи конфіденційність даних і місцезнаходження. Детальніше:

1) Конфіденційність даних: Технології безпеки та конфіденційності RFID можна розділити на дві категорії: фізичні схеми і схеми на основі паролів. Перші використовують команди деактивації, блокування міток, кліпси для міток, псевдоніми для міток, мережі Фарадея, сигналізаційні перешкоди, аналіз енергії антени тощо. Другі включають такі методи, як хеш-замки, випадкові хеш-замки, хеш-ланцюги, анонімні ідентифікатори, повторне шифрування. Різні стилі організації IoT вимагають різних способів укладання угод щодо захисту конфіденційності. Наприклад, архітектура T2TIT французького національного дослідницького агентства використовує протокол HIP для вирішення питань конфіденційності даних. Компромісним рішенням для проблем конфіденційності даних є зберігання менш важливої інформації на RFID-мітці, а важливої інформації – на вищому рівні обслуговування.

2) Конфіденційність місцезнаходження: Хоча RFID-мітки не зберігають важливої інформації, хакери все ж можуть отримати інформацію про ідентифікатор мітки з метою відстеження її місцезнаходження. Наприклад, коли зчитувач, оснащений інформацією GNSS для транспортних засобів, зчитує інформацію з мітки, він може легко визначити приблизне місцезнаходження мітки відповідно до її діапазону дії.

- управління довірою. В IoT слід більш серйозно ставитися до конфіденційності вузлів. Тому потрібно запровадити управління довірою в систему RFID IoT. Управління довірою має існувати не тільки між рідерами та RFID-мітками, але також між рідерами та базовими станціями. У сфері управління довірою велике значення має технологія цифрового підпису. Вона вже давно використовується для автентифікації даних, автентифікації пристроїв і обміну даними між різними додатками. Криптографічні алгоритми та протоколи відіграють важливу роль у технології цифрового підпису. Проте стандартні криптографічні алгоритми та протоколи потребують більше пам'яті

та обчислювальних ресурсів, ніж доступно на RFID-мітках. Тому алгоритми автентифікації RFID повинні враховувати не тільки питання безпеки та конфіденційності, але й обмеження пам'яті та обчислювальної потужності міток. Складність забезпечення безпеки та обмежені ресурси RFID-міток будуть основними напрямками подальших досліджень. Загалом, уніфіковане кодування, вирішення конфліктів зіткнення, захист конфіденційності та управління довірою є чотирма типовими технологіями для вирішення питань безпеки RFID. Завдяки уніфікованому стандарту кодування ми кодуємо інформацію міток однаково, що максимізує обмін інформацією. За допомогою хорошої технології вирішення конфліктів зіткнення ми можемо забезпечити правильне зчитування інформації RFID-рідерами та мінімізувати потенційні перешкоди даних. Завдяки ефективному легковаговому захисту конфіденційності даних ми допомагаємо захистити конфіденційність даних і місцезнаходження. Нарешті, за допомогою відповідних алгоритмів управління довірою ми можемо забезпечити управління довірою для рідерів/RFID-міток, рідерів і базових станцій.

2.2.1.2. Проблеми безпеки та технічні рішення в WSN

WSN - саморганізовані бездротові мережі з обмеженими ресурсами, що включають обсяг пам'яті, обчислювальну здатність та сенсорний охоплення. Шар сприйняття збирає дані, але може бути підданий підробці, підслуховуванню та зловмисній маршрутизації. Проблеми безпеки даних включають конфіденційність, автентичність, цілісність та свіжість, які можна вирішити за допомогою криптографічних алгоритмів, управління ключами, безпечної маршрутизації та довіри до вузлів. Детальніше:

- криптографічні алгоритми в безпровідних сенсорних мережах: Безпровідні сенсорні мережі (WSN) вимагають високого рівня безпеки даних, зокрема конфіденційності та цілісності, яку можна забезпечити за допомогою шифрування. Шифрувальні алгоритми поділяються на симетричні та асиметричні, проте обчислювальна складність останніх робить їх

неідеальними для застосування в обмежених за ресурсами сенсорних мережах. Симетричні алгоритми шифрування широко використовуються в таких мережах через їх простоту і невеликий обсяг обчислень. Симетричні алгоритми шифрування мають такі проблеми:

1) Протокол обміну ключами: заснований на симетричній криптосистемі, є занадто складним, що призводить до поганої масштабованості симетричних алгоритмів шифрування для безпровідних сенсорних мереж.

2) Проблема конфіденційності ключа: У WSN вузли знаходяться в неконтрольованому середовищі. Якщо вузол буде скомпрометовано, це створить велику загрозу безпеці для всієї мережі.

3) Незручність цифрових підписів та автентифікації повідомлень: У симетричних алгоритмах шифрування для автентифікації зазвичай використовується код автентифікації повідомлень, що збільшує навантаження на комунікації, вимагає більше пам'яті та спричиняє додаткове споживання енергії.

З огляду на ці проблеми, розглядається можливість застосування алгоритмів шифрування з відкритим ключем у безпровідних сенсорних мережах. Кожен вузол має свій власний закритий ключ, а базові станції зберігають відкриті ключі всіх вузлів. Алгоритми з відкритим ключем мають добру масштабованість та забезпечують безпеку мережі. Триває дослідження трьох алгоритмів шифрування з відкритим ключем для безпровідних сенсорних мереж: схеми Рабіна, NtruEncrypt та криптографії на еліптичних кривих. Вони вже тестувалися на платформі безпровідних сенсорів серії Mica2, що демонструє їх ефективність. Щоб подолати труднощі використання цих алгоритмів у WSN, потрібно зосередитися на апаратному та програмному забезпеченні. Хоча обидва типи алгоритмів мають свої переваги, жоден не вирішує проблеми безпеки повністю. Технологія симетричного шифрування вже зріла для додатків WSN, але має обмежену безпеку. Асиметричні алгоритми можуть забезпечити високий рівень безпеки, але наразі їх

ефективність експериментальна. Використання асиметричного шифрування у WSN є ключовим питанням, яке потребує подальших досліджень. Споживання енергії, спричинене алгоритмами шифрування з відкритим ключем і протоколами безпеки, має бути головною темою майбутніх досліджень.

- управління ключами в бездротових сенсорних мережах: Проблема управління ключами є важливою для безпеки бездротових сенсорних мереж (WSN) і є фундаментальною основою для вирішення інших питань безпеки. Це включає процеси створення, розподілу, зберігання, оновлення та знищення ключів, де розподіл ключів має вирішальне значення. Розподіл ключів, як публічних, так і секретних, має забезпечити їх безпечну передачу та розподіл серед легітимних користувачів. Головне завдання полягає у розробці легкої схеми розподілу секретних ключів для сенсорних вузлів з обмеженими ресурсами, що підтримує всі рівні протоколів, додатків та сервісів безпеки. Схеми розподілу ключів у WSN можна поділити на чотири форми, залежно від ролі ключів:

1) Широкомовний розподіл ключів у всій мережі: Ключ використовується для захисту інформації, що передається станцією до всіх вузлів. Широкомовні ключі можуть бути публічними або приватними. Через високе енергоспоживання публічних ключів у всій мережі зазвичай використовується симетричний розподіл ключів. Розподіл широкомовного ключа вирішує проблему оновлення ключів.

2) Груповий розподіл ключів: У деяких випадках сенсорна мережа формує внутрішню групу, що складається з кількох вузлів. Груповий ключ використовується для забезпечення безпеки зв'язку між вузлами в межах однієї групи та може розглядатися як широкомовний ключ для членів групи.

3) Розподіл головного ключа вузла: Головний ключ вузла - це ключ, який розділяється між вузлом і базовою станцією і зазвичай зберігається у вузлі до його розгортання у формі передрозподілу.

4) Розподіл ключа, спільного між вузлами: Ключ, спільний між вузлами, захищає зв'язок між будь-якою парою вузлів. Через енергоспоживання та інші

фактори такі ключі використовуються для забезпечення безпеки зв'язку між сусідніми вузлами, досягнення безпеки всієї мережі або забезпечення заданого рівня безпеки.

5) Сучасні методи розподілу ключів у бездротових сенсорних мережах (WSN) використовують симетричні алгоритми, такі як централізована схема SPINS, випадковий передрозподіл ключів та інші, що базуються на теорії випадкових графів. Ці схеми забезпечують високу безпеку мережі, але їхня складність може призводити до великого енергоспоживання.

- управління ключами в бездротових сенсорних мережах (WSN): Управління ключами є важливою аспектом безпеки бездротових сенсорних мереж. Це включає генерацію, розподіл, зберігання, оновлення та знищення ключів, при цьому розподіл ключів є найбільш важливим. Головна мета - розробка ефективної схеми розподілу секретних ключів для сенсорних вузлів з обмеженими ресурсами, що забезпечує безпеку на всіх рівнях протоколів та додатків. Відповідно до ролі ключів, схему розподілу ключів у WSN можна розділити на чотири форми:

1) Розподіл ключів для мовлення по всій мережі: Ключ використовується для захисту інформації, що транслюється станцією до всіх вузлів. У цій ситуації для зниження енергоспоживання зазвичай використовується симетричний розподіл ключів. Розподіл мовних ключів вирішує проблему оновлення ключів.

2) Розподіл групових ключів: У деяких випадках сенсорна мережа формує внутрішню групу, яка складається з кількох вузлів. Груповий ключ використовується для забезпечення безпеки комунікацій між вузлами в одній групі. Груповий ключ можна розглядати як мовний ключ для членів групи.

3) Розподіл основного ключа вузла: Основний ключ вузла є ключем, який ділиться між вузлом і базовою станцією та зазвичай зберігається у вузлі до розгортання у вигляді попереднього розподілу.

4) Розподіл ключа, спільного між вузлами: Ключ, спільний між вузлами, використовується для захисту комунікацій між будь-якою парою вузлів. Через

енергоспоживання та інші фактори ключ, спільний між вузлами, зазвичай використовується для забезпечення безпеки комунікацій між сусідніми вузлами для досягнення безпеки підключення всієї мережі або досягнення певного рівня безпеки комунікацій.

- безпечні маршрутизаційні протоколи для WSN: Маршрутизація на мережевому рівні є важливою для бездротових сенсорних мереж (WSN). Атаки на маршрутизаційні протоколи можуть призвести до краху мережі, тому безпека маршрутизації завжди була пріоритетом у дослідженнях WSN. Обмеження енергії, обчислювальних можливостей та обсягу зберігання ускладнюють застосування традиційних маршрутизаційних протоколів в WSN. Криптографічні алгоритми та управління ключами можуть забезпечити безпеку даних на мережевому рівні, проте автентифікація маршрутизації потребує розробки безпечних протоколів. У WSN, сертифікація здійснюється між вузлами, відмінно від традиційних схем "кінець-кінець". Дослідження в цій області можна поділити на дві категорії:

1) Безпечні маршрутизаційні протоколи, розроблені спеціально для бездротових сенсорних мереж. Ці протоколи автентифікації повинні детально обговорювати та перевіряти свою безпеку, а також ретельно враховувати питання енергозбереження в бездротових сенсорних мережах, щоб досягти кращих результатів у практичних застосуваннях.

2) Аналіз потенційних вразливостей маршрутизаційних протоколів. Основна ідея полягає в аналізі вразливостей маршрутизаційних протоколів з точки зору зловмисника та розробці відповідних рішень для захисту від потенційних атак.

- управління довірою вузлів у бездротових сенсорних мережах: Бездротові сенсорні мережі (WSN) характеризуються обмеженими ресурсами сенсорних вузлів та унікальним режимом зв'язку, що робить їх вразливими до атак. Крім паролів та криптографічних алгоритмів, необхідно впроваджувати механізми управління довірою для забезпечення безпеки WSN. Такий підхід, вперше запропонований у 1996 році, розглядає чотири напрями дослідження:

вимірювання довіри, оцінка довіри, формалізація довірчих відносин та оновлення довіри. Управління довірою враховує особливості сенсорних мереж, такі як енергоефективність та обмежені ресурси, і має на меті забезпечити ефективну безпеку мережі. Технології, які використовуються для цього, включають легковагові криптографічні алгоритми, управління ключами, безпечні протоколи маршрутизації та управління довірою вузлів. Це важливо для забезпечення захисту даних та стабільності мережі.

2.2.1.3. Проблеми гетерогенної інтеграції

RSN (RFID сенсорна мережа) широко використовується в Інтернеті речей, який поєднує RFID та WSNs. Технологія RSN може вирішити проблему, що виникає через гетерогенні дані.

В IoT накопичується велика кількість розподілених даних, але їх різні формати та протоколи ускладнюють аналіз і можуть призвести до втрати конфіденційності. Проблема безпеки виникає через гетерогенність даних, зокрема у форматах зберігання та доступу. Щоб забезпечити їхню інтеграцію, потрібні стандарти кодування та протоколи обміну інформацією. Різні методи обробки даних вимагають дослідження форматів доступу, зберігання, обробки даних і механізмів безпеки. Існують чотири основні методи інтеграції: мітка, інтегрована з сенсорним вузлом, мітка, інтегрована з бездротовим сенсорним вузлом, зчитувачі, інтегровані з бездротовим сенсорним вузлом і бездротовим пристроєм, комбінація RFID та сенсорного вузла.

В середовищі IoT зустрічаємо багато вузлів з різними обчислювальними можливостями та ресурсами. Сенсорні мережі, розгорнуті у відкритих просторах, стають вразливими до фізичних атак через тривалий період ігнорування. Ненадійність з'єднань та висока щільність мережі ускладнюють транспортування даних в IoT. Існують проблеми, такі як складність сенсорних вузлів та різноманітність обладнання, що взаємодіє в IoT. Ці складності ускладнюють забезпечення безпеки IoT, оскільки всі шари системи є

взаємозалежними, тому безпека одного шару не гарантує безпеку всієї системи.

2.2.2. Транспортний рівень

Транспортний рівень забезпечує повсюдний доступ для шару сприйняття, передачу та зберігання інформації, а також підтримує завантаження інших пов'язаних бізнес-застосунків для прикладного шару. Транспортний рівень можна поділити на три функціональні шари: мережу доступу, ядро мережі та локальну мережу. Він представляє собою комбінацію різних гетерогенних мереж. У цій статті аналізуються питання безпеки транспортного рівня, виходячи з його функціональної структури, а також обговорюються проблеми та рішення, пов'язані з інтеграцією гетерогенних мереж.

2.2.2.1. Функціональна архітектура транспортного рівня з питань безпеки

2.2.2.1.1. Доступ до мережі

Мережа доступу забезпечує доступ до рівня сприйняття, але може стати джерелом проблем безпеки при підключенні до основної мережі. Мережа доступу може включати бездротові мережі, такі як централізовані (наприклад, WiFi) та децентралізовані (наприклад, Ad hoc).

Аналіз питань безпеки:

- аналіз проблем безпеки WiFi: WiFi, або бездротова мережа зв'язку, стандарт IEEE802.11, забезпечує зв'язок між бездротовими терміналами. Використання WiFi в Інтернеті речей включає доступ до інтернету, електронної пошти та відеострімінгу. Проблеми безпеки WiFi включають атаки на доступ, зловмисні точки доступу та DDoS атаки. Контроль доступу та шифрування мережі є ключовими для зменшення ризиків безпеки. Технології,

такі як WPA, TKIP, AES та протоколи аутентифікації, грають важливу роль у забезпеченні безпеки мережі WiFi.

- аналіз проблем безпеки в бездротових Ad-hoc мережах: Бездротова Ad-hoc мережа це мережа без застосування фіксованої інфраструктури, де незалежні вузли співпрацюють для формування, самоорганізації та самокерування. У сфері Інтернету речей вони працюють як мережі peer-to-peer, з метою зниження гетерогенності між вузлами. Такі мережі відкриті для загроз безпеки, включаючи підслуховування, перешкоди та атаки на саму мережу через її децентралізований характер. У контексті Інтернету речей бездротові Ad-hoc мережі зіткнуться з кількома проблемами безпеки:

1) Проблеми безпеки, пов'язані з несанкціонованим доступом до вузлів: Забезпечення можливості кожного вузла аутентифікувати ідентичність спілкуючихся пірів є важливим. Неспроможність аутентифікації залишає вузли вразливими до захоплення зловмисниками, що може призвести до доступу до критичних ресурсів та перешкоджання спілкуванню з іншими вузлами. Впровадження механізмів авторизації та аутентифікації вирішує цю проблему безпеки. Сертифікація підтверджує законність ідентичності вузла, а авторизація вирішує, чи дозволено цій ємності робити певні дії.

2) Проблеми безпеки даних: Спілкування в бездротових адгок мережах є ненаправленим, що робить сенсорні дані вразливими до витоків або підробки з боку зловмисних акторів. Інформація про маршрутизацію мережі також є вразливою до маніпуляцій з боку зловмисних користувачів, що дозволяє незаконний доступ до місць розташування цільових об’єктів. Використання аутентифікації та надійних механізмів управління ключами допомагає вирішити ці проблеми безпеки.

3) Безпека маршрутизації мережі: Загрози, такі як атаки типу "відмова в обслуговуванні" (DoS) або "розподілена відмова в обслуговуванні" (DDoS), можна зменшити за допомогою механізмів шифрування.

- аналіз проблем безпеки мереж 3G: Проблеми безпеки у мережах 3G включають витік інформації, незаконний доступ та атаки. Шляхи вирішення

цих проблем включають конфіденційну інформацію користувача, керування ключами, автентифікацію походження даних та шифрування. У мережах 3G також існують проблеми під час передачі даних, які можна вирішити за допомогою відповідних механізмів керування ключами та автентифікації. Порівняльний аналіз проблем безпеки в мережах 3G та їх ядрі показує важливість автентифікації у доступній мережі та особливості безпеки передачі даних у ядрі. Середня основна увага приділяється безпеці передачі інформації, використовуючи різні методи шифрування. Не існують ефективних рішень для атак типу DDos/Dos, але можна використовувати автентифікацію суб'єктів та інші методи для боротьби з фішинговими атаками на ідентичність.

2.2.2.1.2. Базова мережа

Базова мережа IoT відповідає за передачу даних. Базова мережа здебільшого базується на Інтернеті. Нижче наведено аналіз питань безпеки в Інтернеті. Оскільки велика кількість вузлів потребує доступу до Інтернету, що вимагає великої кількості IP-адрес, традиційний Інтернет на базі IPv4 не може задовольнити потреби в такій кількості сенсорних вузлів. Це питання можна вирішити за допомогою Інтернету наступного покоління на основі IPv6. Для використання сенсорних мереж на базі IPv6 з низьким енергоспоживанням для гетерогенної інтеграції можна використовувати технологію 6LowPAN, яка вирішує проблему з адресами IPv6. Технологія 6LowPAN використовує фізичний (PHY) та канальний (MAC) рівні стандарту IEEE 802.15.4, а транспортний рівень використовує протокол IPv6. Оскільки в IPv6 довжина корисного навантаження MAC може бути значно більшою, ніж у 6LowPAN, для досягнення безперервного з'єднання між канальним і транспортним рівнями, робоча група 6LowPAN рекомендує додати між ними адаптаційний рівень, який забезпечує стиснення заголовків, фрагментацію і збирання даних, а також маршрутизацію в мережі. Адаптаційний рівень є проміжним між мережею IPv6 і канальним рівнем IEEE 802.15.4 MAC. Він забезпечує підтримку IPv6 для середовища доступу IEEE 802.15.4 та контроль за

побудовою мережі LoWPAN, топологією і маршрутизацією на рівні MAC. Основні функції 6LoWPAN включають фрагментацію і збирання даних на канальному рівні, стиснення заголовків, підтримку мультикасту, побудову топології мережі і призначення адрес.

2.2.2.1.3. Локальна мереж

У контексті IoT локальна мережа повинна більш ретельно ставитися до питань витоку даних і забезпечення незалежного захисту серверів. Застосування наступних заходів може посилити управління безпекою в локальній мережі. Контроль доступу до мережі забезпечує легальне використання мережевих ресурсів і є основною стратегією захисту мережі. Інші заходи включають запобігання впровадженню шкідливого коду, вимкнення або видалення непотрібних системних сервісів, постійне оновлення операційної системи, використання надійних паролів. Це все допомагає захистити безпеку локальної мережі в IoT.

2.2.2.2. Загальні питання аналізу транспортного рівня

2.2.2.2.1. Проблеми конвергенції гетерогенних мереж на рівні транспортування

Транспортний рівень IoT складається з різноманітних гетерогенних мереж (таких як Ad hoc мережа, Інтернет, мережі 3G тощо), що створює питання безпеки при їх інтеграції. Для вирішення цих питань безпеки при об'єднанні гетерогенних мереж використовуються такі підходи: тісне з'єднання, слабке з'єднання, ACENET, AN net тощо.

2.2.2.2.2. Аналіз атак на транспортний рівень мережі

DDos-атака є однією з найпоширеніших мережевих атак, особливо в контексті IoT. Через гетерогенність і складність мереж IoT транспортний шар вразливий до атак. Зазвичай рішенням є оновлення системи та використання

механізмів виявлення та запобігання DDos-атакам. Наразі немає ефективного рішення для повного захисту від мережевих DDos-атак. Транспортний рівень IoT також вразливий до троянських програм, вірусів, спаму та інших атак, які призводять до розкриття інформації, паралічу мережі, атак посередника, повторних атак, атак на доступ, фішингових сайтів і комбінованих атак. Хоча такі атаки є досить поширеними, використання необхідних механізмів виявлення вторгнень і механізмів автентифікації може забезпечити своєчасне виявлення загроз. У цьому рівні ми зосереджуємо увагу на питаннях безпеки для доступної мережі, основної мережі та локальної мережі. У доступній мережі ми аналізували питання безпеки для WIFI, Ad hoc та 3G-мереж, а також відповідні технології захисту. В основній мережі ми розглянули питання безпеки великої кількості вузлів і представили технологію 6LowPAN. У локальній мережі ми досліджували технології контролю доступу до мережі для вирішення проблем безпеки, пов'язаних з нелегальним використанням мережевих ресурсів. Також ми розглянули деякі загальні проблеми безпеки всього транспортного рівня, такі як незаконне розкриття інформації та параліч мережі. Оскільки транспортний рівень знаходиться в центрі системи IoT, він має велике значення.

2.1.3. Прикладний рівень

2.1.3.1. Питання безпеки прикладного рівня

Прикладний рівень, що є просунутим шаром над транспортним рівнем, підтримує всі види бізнес-послуг і реалізує інтелектуальні обчислення та розподіл ресурсів для відбору, вибору, виробництва та обробки даних. Під час цього процесу рівень підтримки додатків здатний розпізнавати корисні дані, спам та навіть шкідливі дані, і своєчасно їх фільтрувати. Цей рівень може бути організований по-різному залежно від конкретних послуг і зазвичай включає проміжне програмне забезпечення (middleware), платформи M2M, платформи хмарних обчислень та платформи підтримки послуг.

У контексті IoT проміжне програмне забезпечення (middleware) розроблене на основі певних основних технологій, таких як традиційні сервери проміжного програмного забезпечення як комунікаційний компонент, що дозволяє розгортати програмне забезпечення на різних платформах або операційних системах. Однак дані в IoT є масивними та динамічними, тому проміжне програмне забезпечення IoT повинно мати величезну ємність і можливість лінійного розширення для зберігання зростаючих обсягів даних. Функції, інкапсульовані в проміжне програмне забезпечення IoT, є більш складними, такими як контроль температури навколишнього середовища та підтримка його стану. Воно має обробляти пов'язані запити, що надходять одночасно з різних пристроїв. Ці запити формують контекст, який триває певний час. Різні контексти можуть виконувати різні функції та надавати різні послуги користувачам. Коли є кілька запитів одночасно, справедливо і правильно обробляти їх у порядку їх надходження. Проте IoT включає питання повсякденного життя, події або навіть катастрофи. Більш термінові питання потребують вищого пріоритету обслуговування. Система повинна розпізнавати ступінь терміновості цих питань і присвоювати їм відповідні пріоритети.

Один із найпопулярніших додатків IoT сьогодні, M2M, все ще не може уникнути ризиків безпеки, оскільки передача даних здійснюється через електричний кабель, бездротову мережу або мобільну мережу. Проблеми безпеки, з якими стикається M2M на рівні додатків, можна розділити на три аспекти.

Додатки, що складаються з бекенд системи та проміжного програмного забезпечення, повинні відповідати високим вимогам безпеки, щоб негайно збирати та аналізувати дані та підвищувати інтелект бізнес-процесів. Управління безпекою вихідного коду та IoT також повинно відповідати високим стандартам. Інші питання безпеки включають контроль доступу, захист конфіденційності, авторизацію користувачів, цілісність даних, доступність у реальному часі тощо. Водночас конфіденційність і надійність є

найважливішими питаннями IoT. Останнім часом більшість досліджень зосереджуються на технологіях захисту конфіденційності, таких як k-анонімність, перетворення даних, рандомізація даних, використання терміналів із модулем SIM, прив'язаним до IMEI та IMSI, розробка взаємозалежних карт і машин, надсилання оновлених ключів аутентифікації та сертифікації платформи M2M для запобігання піратству карт і машин, забезпечення безпеки вихідного коду. Ризики безпеки зростають при зміні персоналу адміністраторів операційних служб. Існують загрози неправильної автентифікації користувачів M2M. Обмін даними між операторами може призвести до розкриття торгової інформації та економічних втрат. Тому уряд повинен ухвалити відповідне законодавство для регулювання поведінки операторів, щоб зменшити ризики при зміні провайдерів.

Крім того, оператори повинні забезпечити спеціальний процес для зміни ключів та іншої користувацької інформації під час зміни провайдерів, щоб забезпечити безпеку інформації користувачів. Платформа хмарних обчислень стикається з кількома основними проблемами безпеки, включаючи ризик пріоритетної обробки, ризик управлінських агентств, ризик даних, ризик ізоляції даних, ризик відновлення даних, ризик підтримки розслідування та ризик довгострокового розвитку.

1) Загрози безпеці

Згідно з опитуванням IDC, питання безпеки є найбільш хвилюючим аспектом у хмарних обчисленнях. Усі респонденти мають технічні занепокоєння щодо безпеки. Фактично, платформа хмарних обчислень шифрує дані та робить резервні копії користувацьких даних, які не будуть видалені до певного часу. Тому важливо проводити оцінку ризиків і розробляти план дій на випадок надзвичайних ситуацій перед завантаженням даних у хмару. Хмарні обчислення містять ключову інформацію підприємств, що робить їх і окремих осіб мішенню для хакерів. Хоча це не завжди є поширеною проблемою, безпекові інциденти все ж можуть траплятися. Через

питання безпеки підприємствам, які є чутливими до даних, таким як медичні та фінансові компанії, не рекомендується впроваджувати технології хмарних обчислень.

2) Проблеми з перериванням роботи та атаками

На основі попереднього досвіду використання хмарних обчислювальних сервісів, завжди існують деякі загальні збої в роботі, такі як резервне копіювання даних, вимкнення системи та відключення дата-центрів. На щастя, ці збої можна передбачити. Окрім переривання роботи, існують також атаки типу DDoS. DDoS-атака – це вид атаки, що перешкоджає нормальним користувачам отримувати доступ до хмарних сервісів, змушуючи деякі критичні хмарні сервіси споживати значну кількість системних ресурсів, таких як процеси, пам'ять, дисковий простір і пропускну здатність мережі, що призводить до надзвичайного уповільнення або повної відмови у відповідях хмарного сервера.

2.1.3.2. Проблеми безпеки в додатках Інтернету речe

На рівні додатків Інтернету речей інтегруються або працюють окремі конкретні бізнес-застосунки. Проблеми безпеки, з якими він стикається на цьому рівні, не можуть бути вирішені в інших рівнях Інтернету речей. Наприклад, питання, такі як захист конфіденційності, є унікальними для рівня застосунків і відрізняються від тих, що виникають на рівнях сприйняття або транспортування. Ці проблеми можуть виявитися як спеціалізовані вимоги щодо безпеки в певних контекстах рівня застосунків.

Конкретні контексти в Інтернеті речей, такі як визначення місцезнаходження, вносять проблеми конфіденційності, які включають конфіденційність місцеположення та конфіденційність запиту. Конфіденційність місцеположення стосується захисту минулого або поточного місцезнаходження користувачів, тоді як конфіденційність запиту передбачає захист чутливої інформації, запитаної та аналізованої. Наприклад,

часті пошуки ресторанів або лікарень у певній області можуть потенційно викрити місцезнаходження проживання користувачів, рівні доходів, спосіб життя, поведінку, стан здоров'я та іншу чутливу інформацію зловмисним елементам, що призводить до розкриття особистої інформації.

Існуючі заходи для захисту конфіденційності включають техніки, такі як маскування місцезнаходження, анонімне переглядання та шифрування даних в межах конкретних просторів.

Застосунки Інтернету речей знаходять широке застосування у різних аспектах соціального життя, включаючи управління розумною мережею, інтелектуальні транспортні системи, покращені протоколи безпеки та автоматизацію розумного будинку.

1) Логістика

Системи інтелектуального транспорту все більше використовують технологію IoT в логістичному секторі. Інтегруючи інформаційні технології з управлінням логістикою та моніторингом процесів, логістичні підприємства можуть підвищити ефективність, контролювати витрати та підняти рівень інформаційної інфраструктури. Системи інтелектуальної логістики охоплюють різні підсистеми, такі як отримання, передача, сортування та транспортування товарів, кожна з яких здатна керувати інвентаризацією, полегшувати доставку та автоматизувати процеси розрахунків.

Технологія RFID пропонує можливості в реальному часі та точного відстеження. Використовуючи системи GPS через мережі GSM/CDMA, читачі RFID передають поточні місцезнаходження об'єктів до централізованих дата-центрів. Це дозволяє моніторингу інформаційних та капітальних потоків в реальному часі, сприяючи більшій координації та ефективності в операціях бізнесу.

Однак, подібно до Інтернету, системи RFID вразливі до вірусів та кібератак. Недостатні заходи безпеки на мікросхемах RFID часто створюють вразливості, надаючи хакерам можливість отримати доступ до конфіденційної

інформації. У інтелектуальній логістиці основна проблема з безпекою полягає у витоку даних з систем RFID, що може компрометувати внутрішню або особисту інформацію, вбудовану у електронні мітки. Для зменшення ризиків крадіжки даних можна використовувати заходи шифрування, а чутливі дані слід зберігати окремо від електронних міток, лише зберігаючи незначущу ідентифікаційну інформацію.

Крім того, забезпечення безпеки товарів залишається ключовою проблемою в логістичній галузі, особливо під час пікових періодів, коли випадки втрат вантажів часто збільшуються. У таких випадках проблема безпеки вантажів стає все важливішою. Щодо проблеми зворотного зв'язку в реальному часі стосовно інформації про товари, складно знайти ефективне рішення для широкого спектру питань безпеки. Технологія ZigBee характеризується низькою швидкістю передачі даних, низьким енергоспоживанням, низькими витратами, самоналаштуванням і гнучкою топологією мережі. Тому вона може бути використана для отримання реального зворотного зв'язку щодо інформації про товари.

Кожен вузол зв'язку розраховується на читач RFID для ідентифікації інформації, яку несе мітка RFID. Модуль серійних комунікацій надсилає інформацію електронної мітки, інформацію GPS та іншу інформацію вузла через GPRS. За допомогою архітектури протоколу ZigBee, інтерфейс SPI підключає GPS, GPRS, RFID та інші модулі зв'язку до блоку обробки даних MCU, що дозволяє логістичній системі мати функції позиціонування, антикрадіжкові та антивтратні сигнали. Таким чином, це допомагає відстежувати вантажі, зменшує психологічну тривожність людей та значно знижує витрати енергії системи, що робить можливим промислове впровадження бездротових мереж датчиків.

2) Розумний дім

В епоху підйому Інтернету речей, ринок інтелектуальних будинків виявляє величезний потенціал у всьому світі, пропонуючи великий потенціальний ринок. Ця інноваційна домашня система інтегрує датчики, підключення до Інтернету та розумні контролери, пропонуючи мешканцям ефективне, комфортне, безпечне, зручне та екологічно чисте житло. У Сполучених Штатах "Будинок майбутнього" Гейтса служить орієнтиром для розумних будинків. Кожний елемент, від освітлення до музики, температури та вологості, регулюється за допомогою комп'ютера для задоволення потреб гостей. При вході відвідувачі отримують мікросхемний брош, що дозволяє їм попередньо налаштувати бажані умови навколишнього середовища, незалежно від їхнього місцезнаходження. Ці налаштування, включаючи температуру, вологість, освітлення, музику та мистецтво, передаються за допомогою вбудованих датчиків до центрального комп'ютера, що працює під управлінням системи Windows NT, який автоматично налаштовує оточення відповідно до налаштувань. Наприклад, коли гості прибувають, датчики на підлозі автоматично підсвічуються, а потім вимикаються при їхньому виході. Технологія, що лежить в основі розумних домашніх систем, переважно охоплює технології мережевого управління, зв'язку та мобільних терміналів.

Розумна домашня система, структурована відповідно до трьохрівневої моделі, розгортає датчикові та функціональні вузли в кожній кімнаті. Ці датчикові вузли виявляють зміни в середовищі та передають дані на шлюз за допомогою агрегації маршрутів. Для деяких змін активуються програми заздалегідь визначених реакцій, тоді як функціональні вузли реагують безпосередньо. У випадках, коли потрібне втручання людини, повідомлення відправляються на розумні термінали через Інтернет, що дозволяє користувачам приймати обґрунтовані рішення та видає команди шлюзу. Наприклад, якщо до будинку підійшов незнайомець, коли господарі відсутні, датчики передають сповіщення на розумні пристрої, такі як мобільні телефони. Власник отримує сповіщення про проникнення ззовні, і, якщо він

бажає зупинити незнайомця, він може надати системі вказівку, наприклад, "Закрити всі вікна та двері", яку виконає функціональний вузол керування відповідно до вказівок.

Крім того, технології, що використовуються в інтелектуальних домашніх системах, включають в себе технології мережевого управління, зв'язку та мобільних терміналів:

- технологія мережевого управління: Різні технології, такі як EIB, C-Bus та H-Bus, підключені до міжплатного шини домашнього шлюзу, використовуються. Завдяки складній організації проводових ліній, проводові альтернативи, такі як RF, переносник, Wi-Fi, ZigBee та Bluetooth, вважаються перевагою.

- технологія зв'язку: Технології проводового та бездротового зв'язку, включаючи бездротові мережі на основі ZigBee, використовуються. Бездротові технології мають переваги, такі як низька вартість, низьке споживання енергії, універсальність та широкий охоплення.

- технологія мобільних терміналів: Смартфони, планшети та ноутбуки виступають як мобільні інтелектуальні термінали. Серед проблем безпеки можна відзначити порушення приватності, крадіжки та прослуховування. Крім того, проблеми безпеки виникають від апаратних пристроїв, впливу навколишнього середовища та атак на мережевому рівні, таких як атаки DDOS під час передачі 3G. Проблеми безпеки на рівні застосунків є специфічними для застосунку і вимагають індивідуальних рішень. З різними застосунками IoT виникають різні проблеми безпеки. У цьому рівні ми проаналізували проблеми безпеки на рівні підтримки застосунків, включаючи загрози безпеці, перерви в обслуговуванні та проблеми атак, та вивчили аудит безпеки. Потім ми проаналізували проблеми безпеки застосунків IoT та представили кілька типових застосунків IoT, таких як інтелектуальний транспорт та розумний будинок. Також ми проаналізували відповідні проблеми безпеки та технології.

2.3. Головні виклики безпеки 5G

У епоху 5G підключення важливої інфраструктури вимагає підвищених заходів безпеки, щоб забезпечити не лише захист самої інфраструктури, а й безпеку суспільства в цілому. Наприклад, серйозні наслідки може мати порушення безпеки в онлайн-системах постачання електроенергії, яке може вразити всі електричні та електронні системи, на яких суспільство покладається. Крім того, враховуючи ключову роль даних у процесах прийняття рішень, наслідки, якщо критичні дані будуть пошкоджені під час передачі через мережі 5G, будуть катастрофічні. Таким чином, стає надзвичайно важливим ретельно дослідити і підкреслити значущі виклики безпеки, властиві мережам 5G, а також надати огляд потенційних рішень, спрямованих на зміцнення цілісності систем 5G.

Перелік викликів:

- швидкий потік мережевих даних: Збільшена кількість кінцевих пристроїв користувачів та нові речі (IoT).

- захист радіоінтерфейсів: Передача ключів шифрування радіоінтерфейсів через ненадійні канали.

- забезпечення цілісності користувацького плану: Відсутність криптографічного захисту цілісності для плану даних користувача.

- обов'язкові заходи безпеки в мережі: Обмеження на безпеку, спрямовані на архітектуру безпеки, що призводять до опціонального використання заходів безпеки.

- безпека під час роумінгу: Неоновлення параметрів безпеки користувача при переході з однієї мережі оператора до іншої, що призводить до компрометації безпеки під час роумінгу.

- відмови в обслуговуванні (DoS), атаки на інфраструктуру: Видимий характер елементів керування мережею та відсутність шифрування в каналах управління.

- шторми сигналізації: Складна координація, необхідна для розподілених систем управління, таких як не доступний шар NAS (Non-Access Stratum) протоколів 3GPP (Third Generation Partnership Project).

- Атаки на кінцеві пристрої з відмовою в обслуговуванні: Відсутність заходів безпеки для операційних систем, додатків та конфігураційних даних користувацьких пристроїв.

Робоча група SA WG3 в межах 3GPP активно бере участь у визначенні вимог до безпеки та приватності, а також визначає архітектури та протоколи безпеки для 5G мереж. В той же час, Фонд відкритих мереж (ONF) зосереджений на прискоренні впровадження SDN та NFV та публікує технічні специфікації, включаючи специфікації безпеки цих технологій. NGMN визначив принципи проектування 5G, які виходять за рамки ефективності радіо та акцентують на створенні єдиного, адаптивного ядра та спрощених операційних процесах за допомогою нових обчислювальних та мережевих парадигм. Отже, наш акцент спрямований на зміцнення безпеки технологій, які відповідають принципам проектування NGMN, таких як мобільні хмари, SDN та NFV, а також комунікаційних каналів, які є необхідними або міжзв'язують ці інновації. Додатково, з урахуванням зростаючих збурень щодо конфіденційності користувачів, ми підкреслили потенційні проблеми конфіденційності. Виклики безпеки зображено на Рис.3.1. і деталізовані в Табл.3.1.. Ця таблиця надає огляд різних видів загроз та атак на безпеку, ідентифікує цілі мережевих елементів або служб та позначає технології, які найбільш схильні до цих загроз. У наступних розділах наведено стислий опис цих викликів безпеки.

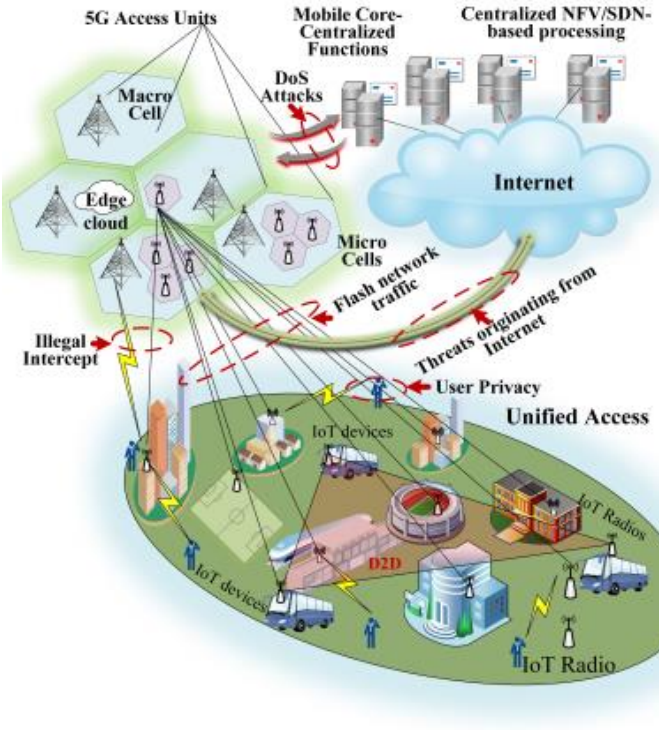

Рис.2.2. Мережа 5G і загрози на ландшафті. [4]

2.3.1. Виклики безпеки в хмарних технологіях

У зв'язку з спільною природою ресурсів у системах хмарного обчислення існує ризик того, що користувач може навмисно або ненавмисно нарушити роботу системи, використовувати надмірні ресурси або отримати доступ до ресурсів інших користувачів без дозволу. У мережах хмарного обчислення з багатьма орендарями, де орендарі керують власною логікою керування, взаємодія може призвести до конфліктів у конфігураціях мережі. Мобільне хмарне обчислення (MCC) розширює концепції хмарного обчислення в екосистеми 5G, вводячи різноманітні вразливості безпеки, переважно пов'язані з архітектурними та інфраструктурними налаштуваннями. Відкрита архітектура MCC, поєднана з гнучкістю мобільних пристроїв, викриває вразливості, які зловмисники можуть використовувати для запуску загроз і порушення конфіденційності в мобільних хмарах.

У цьому дослідженні вразливості MCC класифікуються за цільовими сегментами хмари: фронтенд, бекенд та мережеві загрози безпеки мобільних

пристроїв. Фронтенд, який включає клієнтські платформи, такі як мобільні термінали, стикається з загрозами від фізичних атак на пристрої до загроз, пов'язаних з додатками, таких як шкідливі програми та програми-шпигуни. Бекендова платформа, що включає хмарні сервери, системи зберігання даних та протоколи, переважно стикається з загрозами, спрямованими на хмарні сервери мобільних пристроїв, включаючи реплікацію даних та атаки DoS на HTTP та XML. Мережеві загрози безпеки мобільних пристроїв спрямовані на технології доступу до радіо (RATs), які з'єднують мобільні пристрої з хмарою, такі як прослуховування Wi-Fi, атаки DoS, імітація адрес та захоплення сеансів. Область мережі доступу до радіо (C-RAN) є ще одним ключовим напрямком в аналізі проблем безпеки в мобільних хмарах 5G. Хоча C-RAN пропонує потенційні рішення для потреб розвитку промисловості в галузі високої рухливості в системах мобільного зв'язку 5G, вона також вносить в себе вроджені проблеми безпеки, пов'язані з віртуальними системами та технологією хмарного обчислення, наприклад, централізована архітектура C-RAN піддається загрозі від однієї точки відмови. Інші загрози, такі як вторгнення, коли зловмисники проникають у віртуальне середовище, щоб моніторити, модифікувати або виконувати програмні рутини на платформі, залишаються значними загрозами для системи.

2.3.2. Виклики безпеки в SDN і NFV

Мережі, засновані на програмній визначеності (SDN), централізують контроль над мережевими платформами і сприяють програмованості в комунікаційних мережах. Хоча ці інноваційні функції пропонують значні переваги, вони також вводять уразливості, які можуть бути використані зловмисниками. Наприклад, централізована структура управління є головною метою для атак відмови в обслуговуванні (DoS), а викладення критичних інтерфейсів програмування застосунків (API) для несанкціонованого програмного забезпечення може призвести до перерв у роботі мережі.

Контролер SDN відповідає за модифікацію правил потоку в шляху передачі даних, що робить його трафік легко ідентифікованим. Ця видимість робить контролер вразливим до атак DoS, оскільки він стає важливою сутністю всередині мережі. Крім того, централізація управління мережею може створювати затори, що призводить до атак на перенасиченість і компрометації продуктивності мережі.

Хоча віртуалізація функцій мережі (NFV) має великі перспективи для майбутніх комунікаційних мереж, вона також стикається з основними викликами з питань безпеки, такими як конфіденційність, цілісність, автентичність та відмова в запереченні. У мобільних мережах поточні платформи NFV часто не мають належних заходів безпеки та ізоляції для віртуалізованих телекомунікаційних послуг. Одним із основних викликів у використанні NFV у мобільних мережах є динамічний характер віртуальних функцій мережі (VNF), що може призводити до помилок конфігурації і наступних вразливостей безпеки.

2.3.3. Виклики безпеки в каналах зв'язку

Введення 5G приведе до складного середовища, що включатиме різноманітні елементи, такі як дрони та контроль повітряного руху, хмарно зберігаєму віртуальну реальність, підключені транспортні засоби, розумні заводи, роботи, керовані хмарою, системи транспорту та е-здоров'я. Відтак, існує нагальна потреба у безпечних системах зв'язку, які забезпечують часту аутентифікацію та обмін даними великої чутливості. Крім того, з участю нових учасників, таких як провайдери комунальних послуг, оператори мобільних мереж (MNO) та хмарні оператори, екосистема стане більш різноманітною.

У цій екосистемі необхідні різні шари інкапсульованої аутентифікації як на рівні доступу до мережі, так і на рівні обслуговування, що вимагає частої аутентифікації між різними учасниками. На відміну від мереж попереднього покоління, які мали власні комунікаційні канали, що базуються на тунелях GTP та IPsec, мережі 5G, засновані на мережах з визначенням програмного

забезпечення (SDN), матимуть загальні інтерфейси SDN замість власних. Однак відкритість цих інтерфейсів розширить коло потенційних атак.

Комунікацію в мобільних мережах 5G, заснованих на SDN, можна розділити на три канали: канал даних, канал управління та міжконтролерний канал. Наразі ці канали захищені за допомогою сесій TLS (Transport Layer Security) / SSL (Secure Sockets Layer). Однак сесії TLS / SSL вразливі до атак на рівні IP, атак сканування SDN та відсутність надійних механізмів аутентифікації.

2.3.4. Виклики конфіденційності в 5G

З погляду користувача, основні питання щодо конфіденційності можуть виникнути внаслідок даних, місця розташування та ідентифікації. Більшість додатків для смартфонів вимагають від користувачів надавати особисту інформацію перед встановленням. Однак розробники або компанії рідко вказують, як ці дані будуть зберігатися та для яких цілей вони будуть використовуватися. Загрози, такі як атаки на семантичну інформацію, атаки часу та атаки на межу, переважно спрямовані на конфіденційність місцезнаходження абонентів. На рівні фізичного рівня розташування, конфіденційність місцезнаходження може бути розкрита алгоритмами вибору точок доступу в мобільних мережах 5G. Атаки на перехоплення міжнародного ідентифікатора абонента (IMSI) можуть бути використані для розкриття ідентифікації абонента, перехоплюючи IMSI обладнання користувача. Такі атаки також можуть бути спричинені створенням підробленої базової станції, яка вважається перевагою базової станції користувача, і, таким чином, абоненти відповідатимуть своїм IMSI. Крім того, мережі 5G мають різних акторів, таких як віртуальні оператори мобільного зв'язку (VMNO), постачальники послуг зв'язку (CSP) та постачальники інфраструктури мережі. У всіх цих акторів є різні пріоритети з питань безпеки та конфіденційності. Синхронізація неспівпадаючих політик конфіденційності серед цих акторів буде викликом в мережах 5G. У попередніх поколіннях мобільні оператори

мали прямий доступ та контроль за всіма компонентами системи. Однак мобільні оператори 5G втрачають повний контроль над системами, оскільки вони будуть покладатися на нових акторів, таких як CSP. Таким чином, оператори 5G втратять повне управління безпекою та конфіденційністю. Конфіденційність користувача та даних серйозно викликають питання в спільних середовищах, де одна і та ж інфраструктура використовується різними акторами, наприклад VMNO та іншими конкурентами. Крім того, мережі 5G не мають фізичних меж, оскільки вони використовують зберігання даних в хмарі та функції NFV. Таким чином, оператори 5G не мають прямого контролю над місцем зберігання даних у хмарових середовищах. Оскільки різні країни мають різний рівень механізмів конфіденційності даних в залежності від їхнього контексту, конфіденційність може бути під загрозою, якщо дані користувача зберігаються в хмарі у різних країнах.

2.4. Потенційні рішення безпекових питань

У цьому розділі ми розглядаємо рішення для забезпечення безпеки, які допомагають подолати виклики, описані в попередньому розділі. Проблеми з різкими сплесками мережевого трафіку можна вирішити шляхом додавання нових ресурсів або підвищення ефективності існуючих систем за допомогою новітніх технологій. Ми вважаємо, що нові технології, такі як SDN та NFV, можуть вирішити ці проблеми більш економічно ефективно. SDN має здатність надавати ресурси, наприклад, пропускну здатність, певним частинам мережі в режимі реального часу за потреби. У SDN контролер може збирати статистику мережі через south-bound API від мережевого обладнання, щоб перевірити, чи зростають рівні трафіку. Використовуючи NFV, послуги з хмарного ядра мережі можуть бути перенесені до краю мережі для задоволення потреб користувачів. Аналогічно, віртуальні зрізи мережі можуть бути присвячені лише зонам з високою щільністю UEs для вирішення проблем з різкими сплесками мережевого трафіку.

Безпека ключів радіоінтерфейсу залишається викликом, що вимагає безпечного обміну ключами, зашифрованими за допомогою, наприклад, запропонованої схеми на основі Протоколу Ідентифікації Хоста (HIP). Цілісність користувацького рівня може бути забезпечена за допомогою технологій наскрізного шифрування. Безпеку під час роумінгу та політики безпеки мережі можна реалізувати за допомогою централізованих систем, які мають глобальну видимість активності користувачів і поведінки мережевого трафіку, наприклад, SDN. Сигнальні бурі стануть більш складними через надмірну підключеність UEs, малих базових станцій і високу мобільність користувачів. C-RAN та edge computing можуть вирішити ці проблеми, але дизайн цих технологій має враховувати збільшення сигнального трафіку як важливий аспект майбутніх мереж. Рішення для атак типу DoS або насичення на елементи управління мережею представлені в наступних розділах. Через обмеження простору і для стислості рішення з безпеки для загроз, описаних у попередньому розділі, перераховані в Таблиці II, а методології описані нижче.

2.4.1. Рішення безпекових питань для хмарних технологій

Більшість запропонованих заходів безпеки в мобільних хмарних обчисленнях (MCC) зосереджуються на стратегічному використанні технологій віртуалізації, перегляді методів шифрування та динамічному розподілі точок обробки даних. Віртуалізація є природним вибором для захисту хмарних сервісів, оскільки кожен кінцевий вузол підключається до конкретного віртуального екземпляра в хмарі через віртуальну машину (VM). Це забезпечує безпеку шляхом ізоляції віртуальних з'єднань кожного користувача від інших користувачів. Так само обмеження на рівні сервісів дозволять безпечно використовувати технології хмарних обчислень. Наприклад, автори у своєму дослідженні запропонували "Безпечний обмін і

пошук реального відео в мобільній хмарі", інфраструктуру, яка використовує хмарну платформу та технологію 5G для захисту хмарних сервісів і надає можливість мобільним користувачам ділитися відео в режимі реального часу на хмарах з підтримкою 5G. На відміну від існуючих рішень, де користувачі з спільними посиланнями можуть отримувати доступ до таких онлайн-відео, ця архітектура обмежує доступ тільки для авторизованих глядачів. Для конкретних загроз безпеці, таких як HX-DoS, більш корисними є специфічні рішення, наприклад, системи на основі навчання, які аналізують певну кількість пакетів і виявляють відомі атрибути для виявлення та пом'якшення загроз.

Для забезпечення безпеки мобільних терміналів використання антивірусних програм може значно підвищити стійкість до атак зловмисного програмного забезпечення. Антивірусні рішення можуть бути встановлені на мобільний термінал або розміщені та надані безпосередньо з хмари. В рамках MCC даних і зберігання, система безпеки включатиме енергоефективні механізми перевірки цілісності даних та послуг зберігання в поєднанні з публічною схемою підтвердження володіння даними та деякими легкими механізмами відновлення після компрометації зберігання даних. Для захисту додатків пропонуються деякі структури, які базуються на захисті еластичних додатків на мобільних пристроях для хмарних обчислень, легких динамічних механізмах генерації облікових даних для захисту ідентичності користувача, механізмах просторового затінення в пристрої для захисту конфіденційності, а також MobiCloud - захищена хмарна платформа для мобільних обчислень та зв'язку.

Для безпеки радіодоступу пропонується хмарна структура C-RAN для оптимізації та забезпечення більш безпечних мереж радіодоступу для хмар 5G. Автори описали, як C-RAN може динамічно покращити наскрізну продуктивність сервісів MCC у мережах бездротового зв'язку наступного покоління. Однак для досягнення цих вимог C-RAN повинна забезпечити високий рівень надійності, порівнянний з традиційними оптичними мережами,

такими як Синхронна цифрова ієрархія (SDH), і один із способів досягнення цього - масове впровадження механізмів захисту мережі на основі волоконного кільця, які наразі переважно використовуються в промислових та енергетичних галузях.

2.4.2. Рішення безпекових питань для SDN та NFV

Завдяки логічно централізованій площині керування з глобальним оглядом мережі та програмованістю, SDN полегшує швидку ідентифікацію загроз через цикл збору інформації з мережевих ресурсів, станів та потоків. Таким чином, архітектура SDN підтримує як реактивний, так і проактивний моніторинг безпеки, аналіз трафіку та системи реагування для проведення мережевої криміналістики, зміни політик безпеки та впровадження послуг безпеки. Завдяки глобальній видимості мережі, можна розгорнути послідовні політики мережевої безпеки, тоді як такі системи безпеки, як міжмережеві екрани та системи виявлення вторгнень (IDS), можна використовувати для конкретного трафіку, оновлюючи таблиці потоків комутаторів SDN.

Безпека VNF забезпечується через оркестратор безпеки відповідно до архітектури ETSI NFV. Запропонована архітектура надає захист не лише віртуальним функціям у багатокористувацькому середовищі, але й фізичним елементам телекомунікаційної мережі. Використовуючи довірені обчислення, пропонується віддалена перевірка та перевірка цілісності віртуальних систем і гіпервізорів для забезпечення захисту приватної інформації на апаратному рівні та виявлення пошкодженого програмного забезпечення у віртуалізованих середовищах.

2.4.3. Рішення безпекових питань для комунікаційних каналів

Мережі 5G потребують належного захисту комунікаційних каналів не тільки для запобігання відомим загрозам, але й для збереження додаткових переваг SDN, таких як централізоване управління політиками, програмованість та видимість стану глобальної мережі. Найчастіше

використовуваним протоколом безпеки для захисту комунікаційних каналів у сучасних телекомунікаційних мережах, таких як 4G-LTE, є IPsec. IPsec тунелювання можна адаптувати для захисту комунікаційних каналів 5G з незначними змінами, як показано в деяких дослідженнях.

Крім того, безпека комунікацій у LTE забезпечується інтеграцією різних алгоритмів безпеки, таких як автентифікація, цілісність та шифрування. Проте основними проблемами таких існуючих схем безпеки є високий рівень споживання ресурсів, великий наклад і відсутність координації. Тому ці рішення не є ефективними для критичної інфраструктури зв'язку в мережах 5G.

Вищий рівень безпеки для критичних комунікацій досягається завдяки використанню нових механізмів безпеки, таких як безпека на фізичному рівні з застосуванням радіочастотної (RF) ідентифікації, використання асиметричних схем безпеки та динамічної зміни параметрів безпеки залежно від ситуації. Так само, для забезпечення безпеки комунікацій користувачів від кінця до кінця, можна використовувати криптографічні протоколи, такі як HIP, як зазначено в деяких дослідженнях.

2.4.4. Рішення для забезпечення конфіденційності в мережах 5G

Для мереж 5G необхідно втілювати підхід, що враховує конфіденційність на етапі розробки, де приватність враховується з самого початку, а багато необхідних функцій мають бути вбудованими. Потрібен гібридний підхід на основі хмарних технологій, при якому мобільні оператори можуть зберігати і обробляти високочутливі дані локально, а менш чутливі дані – у публічних хмарах. Таким чином, оператори матимуть більше доступу і контролю над даними і зможуть вирішувати, де їх поширювати. Крім того, орієнтований на послуги підхід до конфіденційності в 5G стане більш життєздатним рішенням для збереження приватності.

Мережі 5G потребуватимуть кращих механізмів для забезпечення підзвітності, мінімізації даних, прозорості, відкритості та контролю доступу.

Тому під час стандартизації 5G слід враховувати суворі правила та законодавство щодо конфіденційності. Регуляторний підхід можна розділити на три типи:

- регулювання на рівні уряду: уряди встановлюють національні норми конфіденційності, а також співпрацюють з міжнародними організаціями, такими як Організація Об'єднаних Націй (ООН) і Європейський Союз (ЄС).

- регулювання на рівні галузі: різні галузі та групи, такі як 3GPP, ETSI і ONF, спільно розробляють найкращі принципи та практики для захисту конфіденційності.

- регулювання на рівні споживачів: забезпечується бажана конфіденційність з урахуванням вимог споживачів.

Для захисту конфіденційності місцезнаходження необхідно застосовувати методи на основі анонімності, де реальна особистість абонента може бути прихована і замінена псевдонімами. Також корисними є методи, засновані на шифруванні, наприклад, повідомлення можуть бути зашифровані перед відправкою постачальнику послуг на основі місцезнаходження (LBS). Методи, такі як обфускація, також є корисними, оскільки знижують якість інформації про місцезнаходження для захисту конфіденційності. Крім того, алгоритми на основі "затемнення місцезнаходження" є досить ефективними для захисту від деяких основних атак на конфіденційність місцезнаходження, таких як атаки з використанням часу і меж.

Висновки

Розвиток мереж 5G і IoT відкриває нові можливості для інновацій та підвищення ефективності в різних сферах. Однак ці технології також приносять з собою численні виклики у сфері безпеки та конфіденційності. Від забезпечення захисту персональних даних та мінімізації вразливостей до впровадження нових регуляторних заходів і технологічних рішень — всі ці аспекти є критичними для безпечного та надійного використання мереж 5G та IoT. Завданням майбутніх досліджень і розробок є створення таких систем, які

б не лише відповідали вимогам часу, але й забезпечували надійний захист від зловмисників і зберігали конфіденційність користувачів.

В цьому розділі було детально досліджено багаторівневу архітектуру IoT, загрози які стосуються кожного рівня та їх рішення. Також було досліджено виклики та потенційні рішення в мережі 5G в контексті IoT.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

Мережа 5G створена для впровадження нових сценаріїв використання, які раніше були недосяжні, і нова стільникова мережа 5G буде корисною не лише для передачі голосу і даних користувачів, але і для багатьох інших галузей та секторів. Забезпечення безпеки є надзвичайно важливим, оскільки незахищена мережа може призвести до катастрофічних наслідків, якщо її зламають. Важко уявити, що станеться, якщо інтелектуальна мережа, пов'язана з 5G, буде скомпрометована. У ході дослідження були виявлені та детально описані функції безпеки 5G.

У цій роботі окреслено основні виклики безпеки в 5G та запропоновані рішення. Враховуючи обмежене впровадження цих технологій, усі загрози ще не повністю зрозумілі. Проблеми безпеки та конфіденційності зростатимуть із підключенням більшої кількості пристроїв і появою нових послуг у 5G. Щоб уникнути потенційних загроз, важливо враховувати ці виклики вже на етапі проєктування та впровадження технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] “What Is 5G Network Architecture?” - https://www.digi.com/blog/post/5g-network-architecture

[2] “5G Reference Network Architecture” - https://www.techplayon.com/5g-reference-network-architecture/

[3] IoT Security: Advances in authentication 2020 / edited by An Braeken, Madhusanka Liyanage, Pardeep Kumar, Mika Ylianttila

[4] Ijaz Ahmad, Tanesh Kumar, Jude Okwuibe, Madhusanka Liyanage 2017 / 5G Security: Analysis of Threats and Solutions

[5] “73 IoT Statistics On Market Growth, Usage & Trends (2024)” - https://www.demandsage.com/internet-of-things-statistics/

[6] “IoT Security in 5G Era” - https://www.rinf.tech/the-iot-security-in-the-5g-era/

[7] “How Does 5G Technology Enhance the Internet of Things?” - https://www.nexusgroup.com/how-does-5g-technology-enhance-the-internet-of-things-nexus-group/#:~:text=5G%20technology%20significantly%20enhances%20data,efficiency%20of%20the%20IoT%20systems.