МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра інформаційно-обчислювальних систем і управління

ОЛЕЩУК ВОЛОДИМИР АНДРІЙОВИЧ

Метод безпечної маршрутизації даних для інтернету речей / A secure data routing method for the Internet of Things

спеціальність: 122 - Комп'ютерні науки
освітньо-професійна програма - Комп'ютерні науки

Кваліфікаційна робота

Виконав студент групи КНм-21
В. А. Олещук
_____

Науковий керівник:
к.т.н., доцент Д.І. Загородня
_____

Кваліфікаційну роботу
допущено до захисту:
«___» _____ 20___ р.
В.о. завідувача кафедри
_____ Н.М. Васильків

ТЕРНОПІЛЬ - 2024

Факультет комп'ютерних інформаційних технологій
Кафедра інформаційно-обчислювальних систем і управління
Освітній ступінь «магістр»
спеціальність: 122 – Комп'ютерні науки
освітньо-професійна програма – Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ М.П. Комар
«____» _____20__р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Олещуку Володимиру Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи
Метод безпечної маршрутизації даних для інтернету речей / A secure data routing method for the Internet of Things
керівник роботи к.т.н., доцент Д.І. Загородня
затверджені наказом по університету від 12 грудня 2023 року № 753.

2. Строк подання студентом закінченої кваліфікаційної роботи 4 грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити
- провести аналіз застосування безпечних методів маршрутизації в IoT;
- проаналізувати можливості протоколу маршрутизації RPL та застосування його для безпечної маршрутизації;
- розробити механізм меж рангу та метод безпечної маршрутизації даних для інтернету речей;
- провести тестування системи аналізу безпечної маршрутизації даних для інтернету речей.

5. Перелік графічного матеріалу у роботі
- загальна архітектура моделі;
- схеми алгоритмів фази верифікації та фази оновлення рангу.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1	Затвердження теми кваліфікаційної роботи, ознайомлення з літературними джерелами та складання плану роботи.	до 01.01. 2024 р.	
2	Написання 1 розділу кваліфікаційної роботи	до 01.03. 2024 р.	
3	Написання 2 розділу кваліфікаційної роботи	до 20.05.2024 р.	
4	Написання 3 розділу кваліфікаційної роботи	до 28.10. 2024 р.	
5	Представлення попереднього варіанту кваліфікаційної роботи, перевірка та внесення змін керівником	до 11.11.2024 р.	
6	Опрацювання зауважень та представлення завершеного варіанту кваліфікаційної роботи. Підготовка супроводжуючих документів.	до 25.11.2024 р.	
7	Перевірка кваліфікаційної роботи на оригінальність тексту.	до 30.11.2024 р.	
8	Оформлення кваліфікаційної роботи та отримання допуску до захисту	до 04.12.2024 р.	
9	Подання кваліфікаційної роботи до захисту на засіданні атестаційної комісії.	до 14.12. 2024 р.	

Студент _____ В. А. Олещук
підпис

Керівник роботи _____ к.т.н., доцент Д.І. Загородня
підпис

РЕЗЮМЕ

Кваліфікаційна робота на тему «Метод безпечної маршрутизації даних для інтернету речей» на здобуття освітнього ступеня «Магістр» зі спеціальності 122 «Комп'ютерні науки» освітньої програми «Комп'ютерні науки» написана обсягом в 67 сторінок і містить 25 ілюстрації, 1 таблицю, 4 додатки та 40 використаних джерел.

Метою даної кваліфікаційної роботи є розробка методу безпечної маршрутизації даних для інтернету речей.

Методи досліджень: організація комп'ютерних мереж, системний аналіз, математична статистика, методи комп'ютерного моделювання.

Результати дослідження:

– Запропоновано модель маршрутизації на основі довіри, яка включає формування довіри, ідентифікацію вузлів та виявлення атак.

– Розроблено механізм рангових меж для обмеження незаконної зміни значень рангу у топології мережі.

– Впроваджено механізм автентифікації на основі хеш-ланцюгів, що дозволяє знизити ризики внутрішніх атак.

– Проведено тестування пропускної здатності та енергоспоживання, що підтвердило ефективність запропонованої моделі маршрутизації.

Результати можуть бути застосовані у різних сферах IoT, таких як розумні міста, системи електронної охорони здоров'я, енергоефективні сенсорні мережі, зокрема для захисту даних від атак типу Rank та Blackhole.

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, МАРШРУТИЗАЦІЯ, ДОВІРА, РАНГОВІ МЕЖІ, АВТЕНТИФІКАЦІЯ, ХЕШ-ЛАНЦЮГ, БЕЗПЕКА МЕРЕЖ.

ABSTRACT

The qualification thesis on the topic “ A secure data routing method for the Internet of Things ” for obtaining the degree of Master in specialty 122 “Computer Science” within the educational program “Computer Science” consists of 67 pages and includes 25 illustrations, 1 table, 4 appendices, and 40 references.

The aim of this thesis is to develop a secure data routing method for the Internet of Things (IoT).

Research methods: organization of computer networks, systems analysis, mathematical statistics, and computer modeling methods.

Research results:

– A trust-based routing model has been proposed, including trust formation, node identification, and attack detection.

– A rank boundary mechanism has been developed to restrict unauthorized rank changes in the network topology.

– A hash chain-based authentication mechanism has been implemented to reduce the risks of internal attacks.

– Bandwidth and energy consumption testing was conducted, confirming the efficiency of the proposed routing model.

Practical application: The results can be applied in various IoT domains such as smart cities, e-health systems, and energy-efficient sensor networks, particularly for protecting data from Rank and Blackhole attacks.

Keywords: INTERNET OF THINGS, ROUTING, TRUST, RANK BOUNDARIES, AUTHENTICATION, HASH CHAIN, NETWORK SECURITY.

ЗМІСТ

ВСТУП

Сучасні технології спрощують зв’язок пристроїв і пов’язаних з ними речей навколо нас за допомогою радіочастотної ідентифікації (RFID) і бездротової сенсорної мережі (WSN). Бездротовий зв’язок і плавна поява різних технологій між пристроями призвели до концепції Інтернету речей (IoT), яка дозволяє передавати дані між різними пристроями та їх пов’язаними речами за допомогою мережевих стандартів і протоколів у будь-який час і в будь-якому місці.

Адреса Інтернет-протоколу (IP) призначається унікально для кожного пристрою та речей в IoT. Ці пристрої можуть дистанційно сприймати та збирати необроблені дані зі свого фізичного середовища для обробки даних і прийняття рішень [1,2]. IoT має значний внесок у впровадження кількох додатків для різних секторів, таких як розумні мережі, розумні міста, розумні будівлі, розумний дім та охорона здоров’я, які покращують повсякденне життя людей. Розумні міста вважаються одним із найважливіших секторів IoT. Він складається з різних додатків і сервісів, які мають на меті підвищити якість послуг для громадян і прискорити використання державних ресурсів. У цьому контексті ці служби можуть забезпечувати краще керування дорогами, розумними автомобілями, легким рухом тощо за допомогою розгорнутих датчиків; наприклад, громадяни можуть бути в курсі та уникати інцидентів через активацію різних сигналізацій тощо [3–6]. Крім того, щоб пристрої могли спілкуватися та обмінюватися інформацією в мережі розумних міст, їм потрібен мережевий рівень в архітектурі IoT. Цей рівень використовує різні техніки, стандарти та протоколи для трансляції інформації. Такими стандартами та протоколами є Інтернет-протокол версії 4 (IPv4), Інтернет-протокол версії 6 (IPv6), протокол обмежених додатків (CoAP) і бездротова персональна мережа (WPAN), IPv6 через бездротову персональну бездротову мережу (6LoWPAN), Протокол дейтаграм користувача (UDP) і протокол

керування передачею (TCP). Мережевий рівень сприяє безпечній передачі даних між рівнем сприйняття та рівнем додатків в архітектурі.

Сьогодні дослідницька область Інтернету речей (IoT) приваблює дослідників завдяки великій кількості додатків і простоті розгортання в кількох сферах реального життя, особливо для середовищ, які вважаються критично важливими, такими як електронна охорона здоров'я, розумні будинки, і розумні міста. Ці речі природно розгортаються в розподіленому середовищі бездротовим способом. Вони стають уразливими до різноманітних атак на безпеку, які можуть негативно вплинути на їх належну роботу в будь-який час. Зазначена гострота проблеми стає ще вищою, коли вони розгортаються в розумних містах. Крім того, є велика ймовірність скомпрометувати дані під час передачі з одного джерела в інше до досягнення пункту призначення під час маршрутизації даних. Існуючі протоколи маршрутизації для мереж з низьким енергоспоживанням і мережами з втратами (RPL) вважаються легкими та безпечними протоколами маршрутизації для пристроїв IoT, які пропонують невеликий захист від незліченних форм атак маршрутизації RPL. Виходячи з характеру мережі IoT, будучи обмеженими ресурсами, звичайні методи маршрутизації їм зовсім не підходять. Тому безпека маршрутизації IoT є складним завданням.

Отже розробка методу який би забезпечував безпечну маршрутизацію на основі RPL, є актуальною задачею.

Метою роботи є розробка методу безпечної маршрутизації даних для інтернету речей.

Об'єктом дослідження є процес маршрутизації даних для IoT

Досягнення цієї мети зумовило потребу теоретичних розробок, визначення та послідовного вирішення наступних завдань:

1. Провести аналіз застосування безпечних методів маршрутизації в IoT.
2. Проаналізувати можливості протоколу маршрутизації RPL та застосування його для безпечної маршрутизації.

3. Розробити механізм меж рангу та метод безпечної маршрутизації даних для інтернету речей.

4. Провести тестування системи аналізу безпечної маршрутизації даних для інтернету речей.

Предметом дослідження є методи безпечної маршрутизації даних для інтернету речей та їх протоколи.

Методи дослідження включають аналіз наукових статей та тез конференцій в області маршрутизації з акцентом на використання в IoT.

Практичне значення дослідження полягає в розширені можливостей протоколу RPL для безпечної маршрутизації з використанням механізму рангових мереж.

Структура та обсяг роботи. Кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел.

Апробація результатів дослідження. Основні теоретичні положення роботи й практичні результати дослідження доповідалися й обговорювалися на IV Міжнародній науковій конференції «Період трансформаційних процесів в світовій науці: задачі та виклики» (м. Рівне, Україна) та VIII Міжнародній студентській науковій конференції «Актуальні питання та перспективи проведення наукових досліджень» (м. Дніпро, Україна).

1 БЕЗПЕЧНА МАРШРУТИЗАЦІЯ В IOT

1.1 Огляд протоколу маршрутизації RPL

RPL було розроблено для підтримки бачення бездротових сенсорних мереж (WSN) та доменів Інтернету речей (IoT). RPL також розроблений як взаємосумісний і простий мережевий протокол для задоволення вимог обмежених ресурсів пристроїв і додатків, які з'єднані між собою мережами з кількома стрибками, такими як промислові, домашні, міські та міські середовища [1–4]. Це дозволяє ефективно використовувати енергію інтелектуальних пристроїв, а також дозволяє встановлювати гнучку топологію та маршрутизацію даних.

1.1.1 Ієрархія RPL

RPL — це протокол дистанційної векторної маршрутизації, який побудував свою топологію на основі орієнтованого на призначення ациклічного графа (DODAG). Він призначений для підтримки роботи декількох протоколів канального рівня, включаючи фізичний рівень IEEE 802.15.4 і рівень MAC [5]. Ці рівні зв'язку можуть бути потенційно втраченими, обмеженими або використовуватися з пристроями маршрутизаторів з великими обмеженнями. Подальші відомості про протокол маршрутизації за вектором відстані доступні в [6]. RPL був розроблений і здатний надзвичайно адаптуватися до умов мережі та підтримувати альтернативні маршрути, коли маршрути за замовчуванням недоступні в будь-який час. Він може вибрати оптимальний шлях маршрутизації на основі цільових функцій (OF) спрямованого ациклічного графа (DAG), який визначає вибір сусідніх і батьківських вузлів [7,8]. DODAG — це DAG, який є орієнтованим графом без циклів, без вихідних ребер і з одним коренем призначення. DODAG унікально призначається IP-адресою DODAG та ідентифікатором примірника RPL. Корінь DODAG використовується для збору маршрутів за замовчуванням до Інтернету та розподілу їх в інших

протоколах маршрутизації та встановлення зв’язку між вузлами, такими як Point-to-Point (P2P), Multi Point-to-Point (MP2P) або Point-to-MultiPoint (P2MP). Кожному вузлу в топології присвоюється значення рангу, яке визначає положення вузла відносно кореня DODAG. Значення рангу - це відстань від кореневого вузла, і воно строго зростає в нижчому напрямку та строго зменшується у вищому напрямку на основі цільової функції (OF) [8]. Крім того, відповідно до специфікації RPL, кожен кореневий вузол DODAG містить номер версії. Для повторної перевірки цілісності кореневого вузла DODAG і запуску глобального механізму відновлення нова версія DODAG формується шляхом збільшення номера версії, який визначається лише кореневим вузлом. Створення топології мережі RPL підтримується за допомогою п’яти керуючих повідомлень, таких як:

1. Інформаційний об’єкт DODAG (DIO) дозволяє побудувати висхідну маршрутизацію, за якої інші вузли (некореневі/приймальні вузли) можуть виявити кореневий вузол (екземпляр RPL) і приєднатися до нього як до свого батьківського вузла.

2. DODAG Information Solicitation (DIS) дозволяє побудувати низхідну маршрутизацію для запиту DIO від вузла RPL і для виявлення сусіднього вузла.

3. Цільовий рекламний об’єкт (DAO), який дозволяє транслювати інформацію про призначення вгору вздовж DODAG і дозволяє вузлу приєднуватися як дочірній до кореня DODAG або батьківського DAO.

4. Підтвердження DAO (DAO-ACK), яке є одноадресним повідомленням пакету знань ac, надісланим одержувачем DAO як відповідь на повідомлення DAO.

5. Перевірка узгодженості (CC), яка використовується для перевірки кількості захищених повідомлень і видачі повідомлень виклик-відповідь для безпеки.

Усі ці повідомлення належать до керуючого повідомлення RPL, яке описується як тип інформаційного повідомлення протоколу керуючих

повідомлень Інтернету версії 6 (ICMPv6) зі значенням 155 [9]. На рисунку 1.1 зображено формування графа DODAG, який містить керуючі повідомлення з кількома екземплярами RPL. Крім того, номер версії DODAG пов'язаний з кожним повідомленням DIO та пов'язаний з мережею. Отже, коли номери версій збільшуються коренем DODAG, вузли мережі RPL перевіряють номер версії в кожному вхідному повідомленні DIO, щоб знайти операцію глобального відновлення. Потім він може обмінюватися керуючими повідомленнями RPL і встановлювати новий кореневий номер версії DODAG.

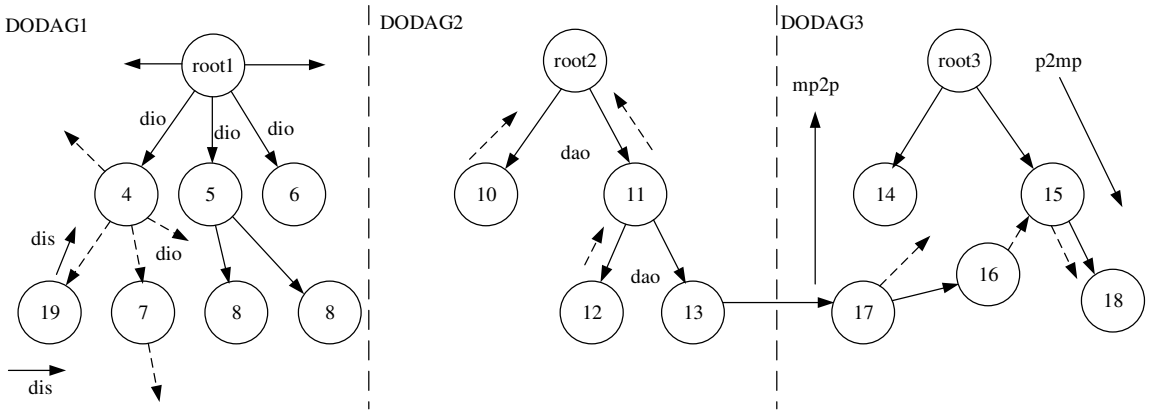


Рисунок 1.1- Формування RPL DODAG

1.2 Безпечна маршрутизація RPL

Щоб приховати інформацію про користувача, використовуються кілька методів криптографії для цілей автентифікації як щит, що може ускладнити доступ неавторизованих сторін до цієї інформації. У своїх специфікаціях протоколи RPL використовують один тип шифрування — симетричне шифрування, відоме як Advanced Encryption Standard (AES) із лічильником із криптографічним блочним шифром — кодом автентифікації повідомлень (лічильник із CBC-MAC (CCM))-(AES/CCM). Оскільки той самий секретний ключ використовується в симетричному шифруванні для обміну між вузлами, це дає зловмисникові простий спосіб отримати доступ до мережі. Однак, якщо зловмисники отримають секретні ключі, шукаючи будь-які можливі доступні

загрози для злому та вставлення своїх вузлів у мережу, це зробить її вразливою для атак безпеки та скомпрометує вузли мережі. Тоді концепція криптографії не може захистити мережу [10,11]. Наприклад, усі вузли спільно використовують один секретний ключ через керування ключами. Таким чином, він стає вразливим до атак, оскільки розкриття ключів може вплинути на всю мережу, і зловмисник може отримати доступ до мережі та прикинутися звичайним вузлом, використовуючи цей ключ, і отримати інформацію за допомогою нього, що ставить під загрозу мережу розумних міст. Отже, через можливість того, що зловмисник може ввести фальшиві дані, функція автентифікації в маршрутизації RPL потребує значного вдосконалення [12,13].

1.2.1 Класифікація атак безпеки RPL

ROLL забезпечує повне розуміння функцій безпеки RPL. Ці атаки класифікуються на основі моделі безпеки, яка включає конфіденційність, цілісність, автентифікацію та доступність (C.I.A.A). Однак доступні звичайні механізми для дротової безпеки, такі як брандмауер, не застосовуються для безпеки RPL через їх динамічну поведінку, і, отже, їхні вузли не мають чітко визначених меж. Крім того, механізми криптографії не можна використовувати для захисту безпеки маршрутизації RPL через відсутність централізованого адміністрування та взаємодії вузлів. Крім того, оскільки пристрої вузлів у мережі не захищені від втручання, стає легше викрити вузли та порушити їхню криптографію. Отже, скомпрометовані вузли можуть знизити продуктивність мережі RPL через маніпуляції з їхнім вихідним кодом [14]. Крім того, на рисунку 1.2 показано таксономію мережевих атак RPL [15]. Безпека на тактах проти протоколів маршрутизації RPL класифікується на три категорії [10,16]:

1. Атаки на ресурси, як правило, змушують вузли виконувати обов’язкові завдання для виснаження їхніх ресурсів. Ці атаки споживають ресурси вузлів, такі як зберігання, енергія та обробка. Отже, на доступність мережі впливає переповненість доступних посилань, а потім впливає на

тривалість життя мережі, яка може бути значно скорочена. Цей тип атак класифікується на дві підкатегорії:

a) Прямі атаки: під час яких зловмисний вузол може погіршити роботу мережі шляхом безпосереднього перевантаження

b) Непрямі атаки: під час яких інші зловмисні вузли, які призведуть до великої кількості накладних витрат трафіку, можуть створити петлю.

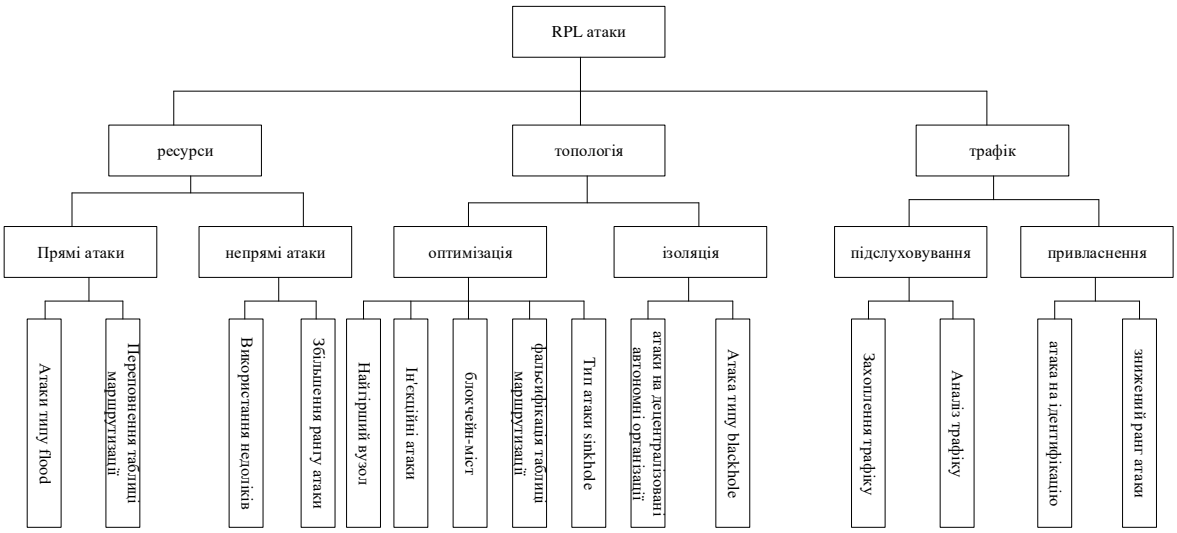


Рисунок 1.2 - Таксономія мережевих атак RPL

2. Атаки на топологію: які завдають шкоди топології мережі та класифікуються на дві підкатегорії:

a) Субоптимізаційні атаки: під час яких зловмисники знижують продуктивність мережі, зменшуючи її оптимальні шляхи.

b) Ізоляційні атаки: під час яких зловмисники ізолюють вузли мережі RPL, через що вони не можуть спілкуватися з батьківським вузлом.

3. Атаки на трафік: стосується впливу на мережевий трафік і поділяються на дві підкатегорії:

a) Пасивні атаки: під час яких зловмисники здійснюють підслуховування ping, наприклад аналіз мережевого трафіку.

b) Атаки обману/незаконного привласнення: під час яких конфіскується ідентифікаційна інформація авторизованого вузла, а його продуктивність завищена. Ці атаки використовуються як перший крок для інших атак.

Виходячи з наведеної вище класифікації атак безпеки RPL, рангова атака є однією з непрямих атак категорії мережевих ресурсів. Виходячи з обчислення рангу, дочірні вузли топології мережі повинні мати найвищі ранги. Рангова атака зі звичайними мережевими шляхами може спричинити втрату пакетів, яка прямо пропорційна атаці. Залежно від рангового розташування сусіднього вузла, батьківський вузол завжди притягує дочірній вузол. Це означає, що батьківський вузол вибирається для конкретного дочірнього вузла, щоб керувати якістю його послуг і надсилати свій пакет даних на основі вузла, який має нижчий ранг [17]. Рангова атака є найбільш руйнівною серед інших для протоколу RPL, оскільки вона породжує інші атаки, такі як чорна діра, воронка тощо. Шкідливий вузол може маніпулювати рангом, щоб навмисно знизити продуктивність. Наприклад, ранг може бути знижений, і шкідливий вузол може бути помилково розташований ближче до батьківського вузла, тоді він може зловмисно маніпулювати величезною кількістю низьких пакетів через нього.

Під час рангової атаки зловмисний вузол рекламує фальшиве місце розташування рангового вузла в керуючих повідомленнях RPL або фальшивий маршрут через кореневий вузол, щоб ввести в оману близькі вузли, щоб вони могли переслати свої пакети через нього [18]. Ранг у прикріпленні працює шляхом порушення глибших рангів дочірніх вузлів у топології мережі RPL. Потім зловмисний вузол може змінити спосіб обробки повідомлень DIO від сусідніх вузлів. Крім того, гірший ранг випадкового шкідливого вузла буде обраний як кращий батьківський вузол під час його операцій, і, як наслідок, OF топології мережі не може бути досягнуто повністю. Крім того, для всіх пакетів даних, які проходять через шкідливий вузол, буде створено неоптимізовану маршрутизацію та більше трафіку [14,18,19]. Наприклад, як показано на рис. 3, певний глибший ранг дочірнього вузла зменшується, і щоб

надіслати певний пакет даних до кореневого вузла, сусідні вузли глибшого дочірнього вузла повинні вибрати його як батьківський вузол. Крім того, коли пакет даних буде направлено від сусідніх вузлів до глибшого дочірнього вузла, він відкине цей пакет. Тому цей глибший дочірній вузол розглядається як шкідливий вузол. Таким чином, рангова атака може бути створена шляхом порушення шляху доставки даних у топології мережі. Це впливає на коефіцієнт доставки пакетів (PDR) мережі, відкидаючи пакети даних на проміжному рівні шкідливих вузлів.

Інша форма рангової атаки полягає в тому, що зловмисник рекламує сусіднім вузлам кращу метрику маршрутизації, але це фальшива маршрутизація, щоб обдурити потоки мережі для передачі через неї. Крім того, залежно від місця розташування зловмисника мережа може постраждати від серйозно збільшеної затримки та зниження пропускної здатності [18]. Існує багато наслідків рангової атаки, які показано в [20,21] як наступне:

1) Неоптимізоване формування шляху.

2) Не розпізнається утворення петлі.

3) Оптимізований маршрут, який ніколи не використовувався в топології мережі RPL.

4) Коефіцієнт доставки пакетів зменшується з невеликою зміною наскрізної затримки зі збільшенням кількості зловмисників.

5) Кількість повідомлень DIO збільшується, оскільки топологія мережі швидко змінюється. Таким чином, рангова атака впливає на деякі обмежені властивості мережі, такі як затримка, пропускна здатність, швидкість передачі даних і споживання енергії [17]. Безпека протоколів PRL є важливою проблемою, яку слід взяти до уваги, оскільки маршрутизовані дані не повинні бути доступні/витоку будь-яким неавторизованим учасником мережі, таким як зловмисник або будь-яка третя сторона [22].

Повний аналіз різних RPL-атак безпеки, включаючи рангову атаку (рисунок 1.3) та інші різні типи атак, був зроблений авторами в [23]. За допомогою симуляційного дослідження вони вивчили вплив цих атак на

продуктивність, наприклад коефіцієнт доставки пакетів, наскрізну затримку та витрати на контрольне повідомлення. Вони змоделювали два сценарії; один з них — це зловмисний сценарій, у якому зловмисні вузли з однаковим розташуванням усувають ефект атаки на місце розташування.

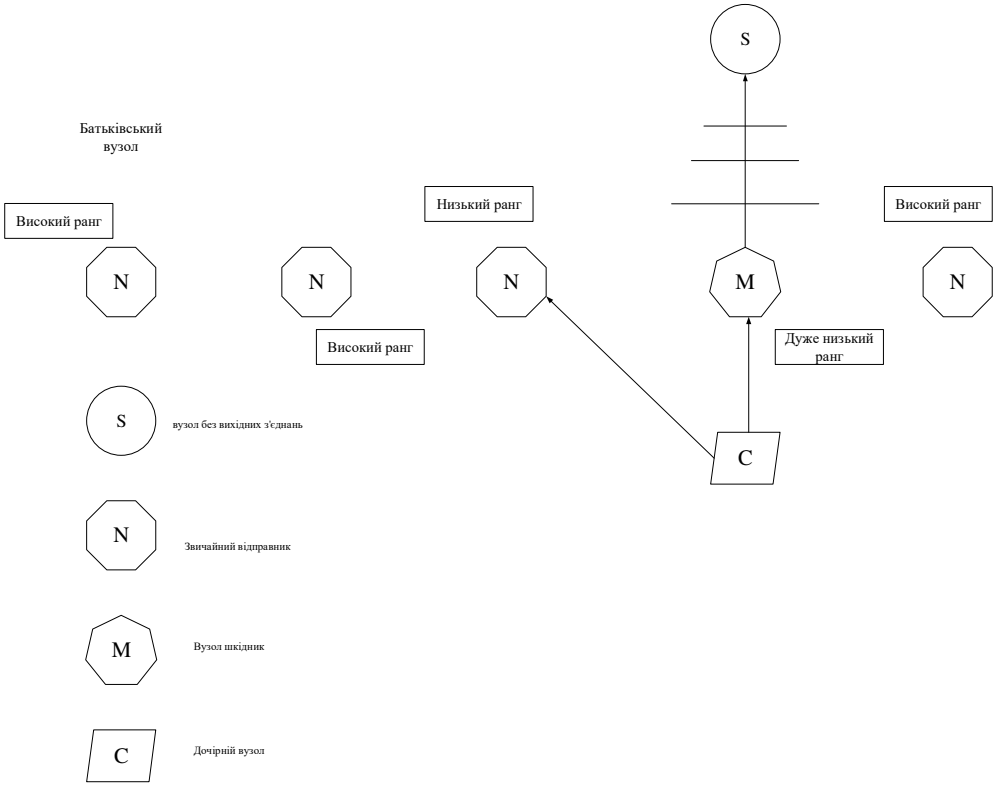


Рисунок 1.3 - Приклад рангової атаки

У той час як другий — це звичайний сценарій без атак для порівняння продуктивності стандартизованих результатів моделювання з продуктивністю шкідливих сценаріїв для виявлення впливу атак.

На рисунку 1.4 показано, що збільшення кількості рангових атак (з 8 до 10) стабільно знижує коефіцієнт доставки до 60%. Це дозволяє вузлам частіше змінювати бажаних точок, що робить топологію мережі нестабільною та нездатною створювати оптимізовані маршрути.

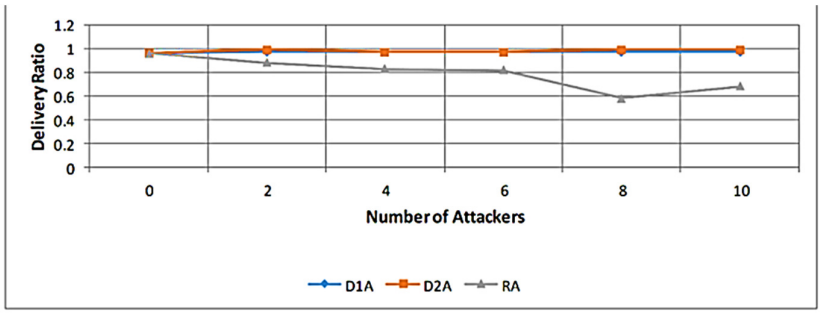


Рисунок 1.4 - Порівняння ефекту кількості зловмисників і коефіцієнта доставки пакетів серед кількох атак

На рисунку 1.5 показано, що збільшення кількості рангових атак може трохи збільшити наскрізну затримку на 15% (до 1 с). Це пов'язано з довшим шляхом (неоптимізованим шляхом) до кореневого вузла, який створюється ранговою атакою.

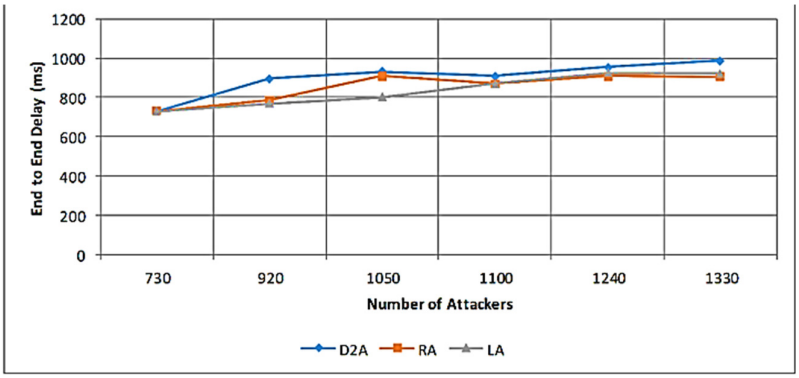


Рисунок 1.5 - Порівняння ефекту кількості зловмисників і наскрізної затримки між кількома атаками

1.3 Вибір перспективного шляху і постановка задачі дослідження

Транспортування та маршрутизація даних в Інтернеті речей (IoT) є складною проблемою, коли збір і збирання великих даних є передбачуваним. Протокол маршрутизації для мереж з низьким енергоспоживанням і втратами (RPL) є одним із найкращих кандидатів для забезпечення маршрутизації в

мережах 6LoWPAN. Однак RPL вразливий до низки атак, пов’язаних із обміном керуючими повідомленнями.

Тому пропонується новий безпечний метод маршрутизації на основі RPL, який називається Secure-RPL (SRPL). Основна мета SRPL — запобігти неправильній роботі вузлів від зловмисної зміни значень контрольних повідомлень, таких як ранг вузла, що може заважати мережі шляхом створення фальшивої топології. Потрібно ввести концепцію порогового значення рангу разом із технікою автентифікації хеш-ланцюга для боротьби з внутрішніми атаками, такими як sinkhole, black hole, атаки вибіркового пересилання тощо.

Метою роботи є розробка методу безпечної маршрутизації даних для інтернету речей. Для досягнення мети роботи необхідно вирішити наступні завдання:

1. Провести аналіз застосування безпечних методів маршрутизації в IoT.

2. Проаналізувати можливості протоколу маршрутизації RPL та застосування його для безпечної маршрутизації.

3. Розробити механізм меж рангу та метод безпечної маршрутизації даних для інтернету речей.

4. Провести тестування системи аналізу безпечної маршрутизації даних для інтернету речей.

Висновки до розділу 1

1. Розробка протоколів маршрутизації в умовах обмежених ресурсів пристроїв є важливою складовою Інтернету речей (IoT). RPL (Routing Protocol for Low-Power and Lossy Networks) став основою для забезпечення ефективної маршрутизації в складних і динамічних топологіях IoT.

2. Незважаючи на ефективність RPL, він залишається вразливим до атак, таких як рангова атака, чорна діра, воронка, та інші. Це зумовлено відсутністю централізованого управління, залежністю від симетричного

шифрування та можливістю маніпулювання контрольними повідомленнями (DIO, DAO).

3. Вразливості RPL класифікуються на три категорії: атаки на ресурси, атаки на топологію та атаки на трафік. Вони призводять до зниження коефіцієнта доставки пакетів, збільшення затримки та підриву загальної стабільності мережі.

4. Рангова атака виділяється серед інших загроз, оскільки вона може спричинити втрату пакетів, створення неоптимізованих шляхів, затримку в передачі даних, що робить мережу непридатною для ефективної роботи.

5. Для протидії цим атакам запропоновано метод, що включає використання порогових значень рангу та хеш-ланцюгів для автентифікації. Це дозволяє захистити мережу від внутрішніх атак, забезпечуючи стабільність і безпеку топології.

Таким чином, забезпечення безпеки маршрутизації в IoT вимагає поєднання технічних реалізацій, таких як криптографічні методи і механізми автентифікації, із впровадженням нових підходів до проектування протоколів. Це гарантує стабільність мереж і підвищує їхню довговічність.

2 МЕХАНІЗМ МЕЖ РАНГУ ТА ОПИС МЕТОДУ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Пропонована модель безпечної маршрутизації

Модель довіри базується на деяких факторах довіри. Основна мета моделі, заснованої на довірі, відіграє важливу роль у розгляді конкретних факторів довіри для розробки ефективного рішення. Дана модель забезпечує безпеку в RPL, і фактори довіри розглядаються відповідно. Фактори довіри формують вимірювані показники довіри. Для запропонованого методу враховується мобільність вузлів, яка становить метрику довіри на основі мобільності.

Запропонований дизайн моделі для безпеки RPL в основному складається з двох етапів: формування довіри та виявлення атак. Формування довіри включає ідентифікацію показників довіри, обчислення показників довіри, розрахунок індексу довіри, рейтинг довіри та моніторинг довіри. Другий етап включає виявлення атак та ізоляцію шкідливих вузлів.

2.1.1 Модель системи

На рисунку 2.1 зображено системну модель, включаючи різні фази та потоки того, як довіра поширюється протягом операції RPL. Фаза формування довіри та фаза виявлення атак були додатково розділені на підетапи.

2.1.2 Створення топології та розгортання атак

Модель дотримується специфікації RPL RFC 6550 для ініціалізації нормальної операції маршрутизації. Подібним чином, топологія створюється відповідно до функціонування та функцій RPL за замовчуванням, що в запропонованій моделі називається створенням топології (рисунок 2.1). Вузли зловмисників розгортаються в мережі для розглянутих прикладів атак Rank і Blackhole. Передбачається, що конкретні вузли зловмисника розташовані випадковим чином серед законних вузлів. Процес зловмисника запускається

шляхом програмування вузлів на дії відповідно до типу атаки. Для рангових вузлів атакуючих вузол запрограмовано на оголошення найнижчого рангу для залучення трафіку. Тоді як вузли зловмисника Blackhole запрограмовані на відкидання всіх отриманих пакетів.

2.1.3 Ідентифікація показників довіри та розрахунок індексу довіри

Вибір відповідних параметрів довіри є фундаментальним для розробки механізму безпеки на основі довіри. Метрики довіри, що використовуються для забезпечення безпеки мереж IoT і маршрутизації, детально досліджуються [24]. Для Моделі розглядаються найбільш відповідні показники довіри, включаючи історичні спостереження, рівень енергії, пряму довіру та рекомендовану довіру. Модель включає мобільність вузлів, враховуючи метрики на основі мобільності в обчисленні довіри.

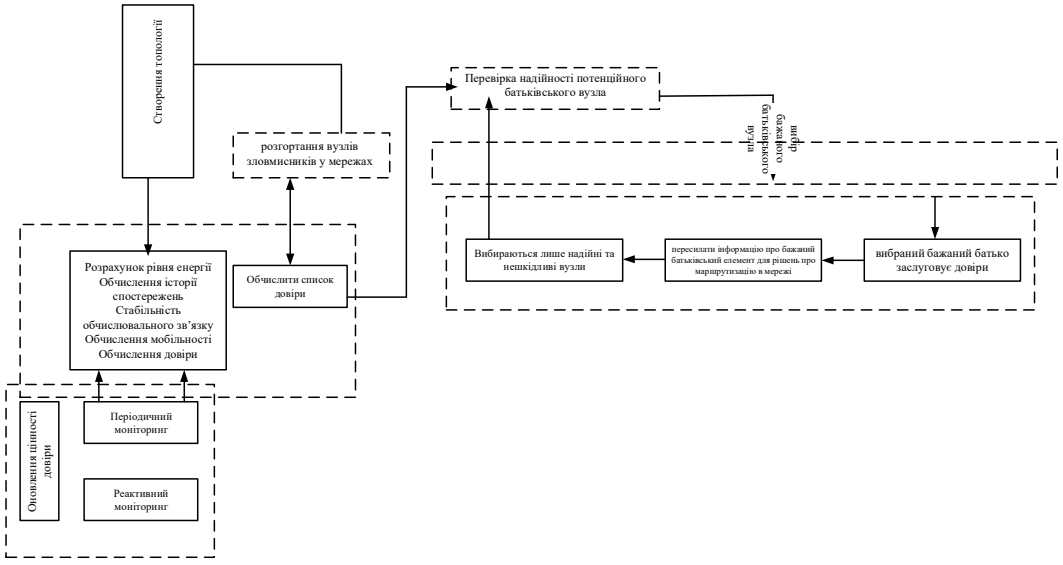


Рисунок 2.1 - Системна модель

У таблиці 2.1 наведено опис застосованих метрик довіри .

Використовуючи розрахунки метрик довіри, розраховується індекс довіри. Обчислене значення довіри підтримується динамічним шляхом

призначення відповідних ваг (w) для розрахунку кожного показника довіри. Таким чином, індекс довіри є зваженою сукупністю показників довіри. Сумарні значення довіри варіюються від 0 до 1.

Таблиця 2.1 - Метрики довіри маршрутизації в мережах IoT

Рівень успіху (TM_{SR})	Відношення кількості переданих пакетів до кількості отриманих пакетів.
Рівень енергії (TM_{EL})	Кількість залишкової енергії вузла.
Історичні спостереження ($TM(H_0)$)	Останнє значення довіри, розраховане для вузла.
Розташування та стабільність зв'язку (TM_{LLS})	Розташування вузла на основі значення індикатора потужності отриманого сигналу (RSSI).
Мобільність ($TM_{Mobility}$)	Відстань, переміщена з раніше зазначеної позиції.
Рекомендована довіра (TM_{RT})	Довіра рекомендаціям сусідів 1-стрибку.

Концепція нечіткого порогового механізму використовується в моделі для оцінки рейтингу довіри [25]. Остаточне значення індексу довіри розраховується за допомогою рівняння.

$$TrustIndex = \omega_1(TM_{SR}) + \omega_2(TM(H_0)) + \omega_3(TM_{EL}) + \omega_4(TM_{LLS}) + \omega_5\left(TM_{Mobility}\right) + \omega_6(TM_{RT}) \quad (1)$$

де $(w_1 + w_2 + w_3 + w_4 + w_5 + w_6) = 1$.

Поточним або прямим значенням довіри надається більша вага, ніж історичним спостереженням. Індекс ступеня довіри, оцінюється за допомогою нечіткого судження, складається з п'яти кортежів, визначених як

$$T = [t_1, t_2, t_3, t_4, t_5], \quad (2)$$

з такими рівнями довіри, відповідно, [«Не довіряю», «Погано довіряю» , «Чесна довіра», «Добра довіра», «Повна довіра»]. Визначені рівні довіри відповідають заданим діапазонам значень довіри, як

$$[0{,}0–0{,}20,\ 0{,}21–0{,}45,\ 0{,}46–0{,}70,\ 0{,}71–0{,}90,\ 0{,}91–1{,}00] \quad (3)$$

Дана модель не враховує вузли, які знаходяться в кортежі t_1 і t_2, для рішень щодо маршрутизації та захисту обміну пакетами. Вузли в кортежі t_4 і t_5 вважаються надійними та заслуговують на довіру для пересилання для прийняття рішень про маршрутизацію. Однак вузли, включені в t_3, знаходяться в середині «Немає довіри» і «Повна довіра». Таким чином, доцільно розглядати вузли в t_3 лише тоді, коли є дефіцит або відсутність вузлів, доступних у діапазоні кортежу t_4 і t_5 для зв'язку, дотримуючись суворого розрахунку індексу довіри. Таким чином, поріг довіри зберігається на рівні 0,46.

2.1.4 Виявлення атак

Бажаний батьківський вузол вибирається зі списку потенційних «батьків» і перевіряється на наявність вузла-атаки за допомогою процедури виявлення атак. Для виявлення атак Blackhole вузол перевіряється на поріг успіху та індекс довіри. Тоді як для виявлення атаки за рангом вузол перевіряється на ранг і DIO_seq порівняно з сусідніми вузлами. Якщо вибраний бажаний батьківський вузол виявлено як зловмисний вузол, він додається до підозрілого списку, а новий батьківський вузол потрібно вибрати зі списку потенційних батьківських вузлів за допомогою процедури вибору батьківського вузла.

2.1.5 Переадресація надійних вузлів для маршрутизації

Якщо вибраний бажаний батьківський вузол не виявлено як вузол-атаку, він пересилається як надійний батьківський вузол для прийняття рішень про

маршрутизацію в мережі. Оскільки дочірній вузол може надсилати пакети лише вибраному батьківському вузлу, а батьківські вузли в моделі перевіряються на надійність за допомогою обчислення показників довіри та порогу довіри для процедури вибору батьківського тому в мережі братимуть участь лише законні вузли.

2.1.6 Оновлення довірчої вартості

Значення довіри потрібно регулярно оновлювати, тобто через певні проміжки часу. Щоб оновлювати довіру через регулярні проміжки часу, модель використовує функціональні можливості трикл-таймера в RPL, що називається періодичним оновленням довіри. Триккл-таймер — це в основному механізм синхронізації, який використовується для оптимізації трансляції повідомлень DIO для збереження ресурсів вузлів. Подібним чином інший механізм приймається з операції маршрутизації RPL для оновлення значення довіри, яке відповідно до зміни поведінки вузла називається реактивним оновленням значення довіри.

Реактивне оновлення відбувається, коли змінюється поведінка вузла та потрібно вибрати новий батьківський елемент зі списку потенційних батьківських вузлів. Наприклад, коли ранг батьківського вузла змінюється, дочірній вузол повинен вирівняти себе в топології і, отже, прагне змінити свій ранг, а також йому потрібно перерахувати довіру батьківського вузла відповідно до його нової позиції та поведінки . Таким чином, дочірній вузол знову виконує обчислення довіри, вибір надійного батьківського елемента та процес виявлення атак, щоб підтримувати надійну топологію.

2.2 Алгоритм потоку процесу моделі

Потік процесу проілюстровано на рисунку 2.2. Після етапів ініціалізації RPL і створення топології разом із розгортанням вузлів зловмисників у мережі, вузол повинен вибрати для себе батьківського вузла, щоб пересилати пакети.

Після чого створюється список потенційних батьківських вузлів, а довіра обчислюється та зберігається в таблиці довіри для всіх сусідніх вузлів.

У процедурі відбору батьківських вузлів потенційний вузол перевіряється на благонадійність. Якщо він заслуговує довіру, відповідно до встановленого порогового значення, він вибирається як бажаний вузол.

В іншому випадку перевіряється інший вузол із потенційного батьківського списку вузлів для вибору бажаного вузла. Після вибору бажаного батьківського вузла його перевіряють на наявність шкідливого вузла.

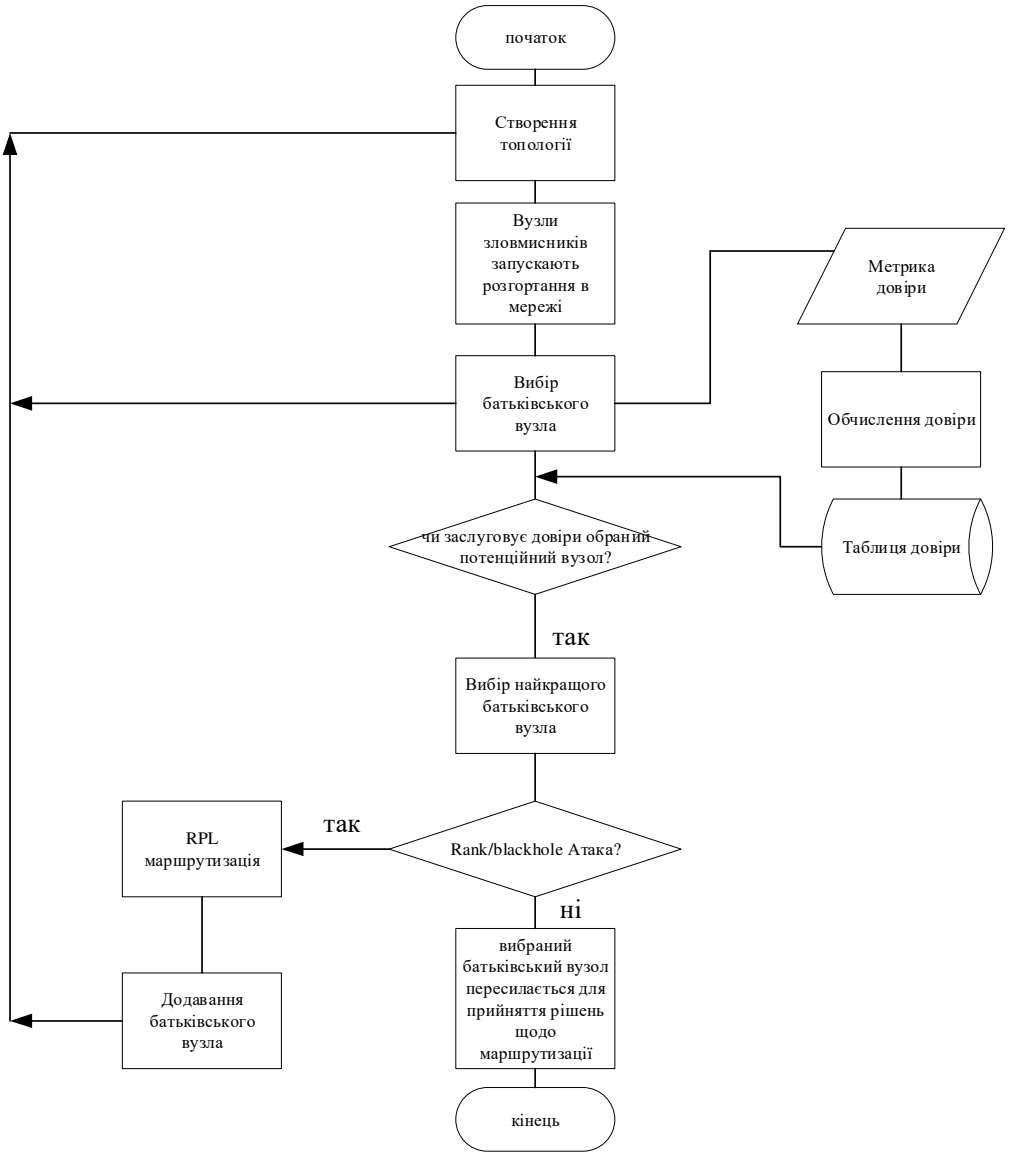


Рисунок 2.2- Алгоритм потоку процесу моделі

Якщо вузол виявлено як зловмисник, він потрапляє в список підозрілих і тоді потрібно вибрати інший вузол. Якщо його виявлено як звичайний і надійний вузол, він пересилається для маршрутизації в мережі.

2.2 Пропонований алгоритм вибору батьківського вузла

Процедуру вибору батьківської системи стандартного RPL змінено для розвитку довірчого зв'язку між DODAG. Нижче наведено запропонований алгоритм вибору надійних батьків.

2.2.1 Обчислення довіри в RPL

Обчислення довіри передбачає, що всі вузли надійні на початку залежно від обміну пакетами ICMPv6 і DIO. Оскільки ContikiRPL припускає, що вузли підслуховують сусідні вузли та їх передачу пакетів [26], В роботі моделі можна використати такий самий підхід. Коли RPL ініціалізується, бажані батьківські вузли та рішення щодо маршрутизації визначаються на основі специфікації в OF для надійного вибору. Ранг обчислюється для вузлів відповідно до звичайних операцій RPL [27]. Після створення топології та створення списку сусідів значення довіри обчислюються відповідно до кількісної оцінки метрик довіри, а індекс довіри обчислюється за формулою (1).

Алгоритм 1 (рисунок 2.3) ілюструє процедуру обчислення довіри та вибору батьківського вузла, що полегшує ізоляцію шкідливих вузлів.

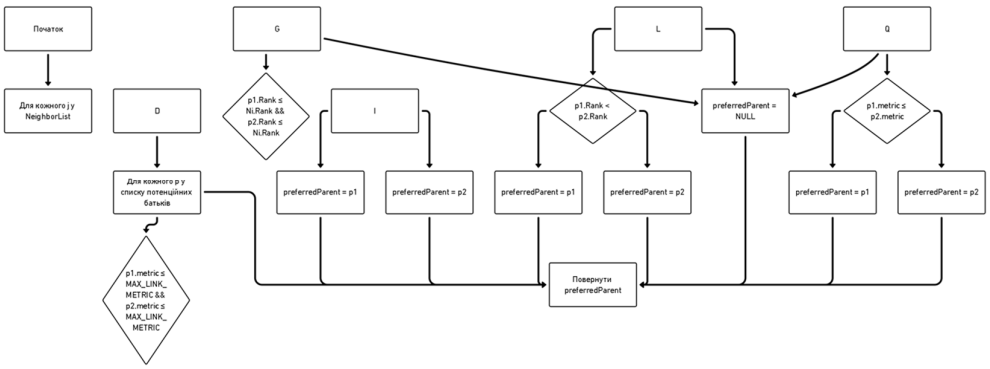


Рисунок 2.3 – Алгоритм процедури обчислення довіри

Коли вузол отримує повідомлення DIO, передана інформація використовується для оновлення таблиці маршрутизації. Вузол обчислює значення довіри для своїх сусідів за допомогою механізму обчислення довіри. Потім вибирається набір довірених потенційних батьківських вузлів для оптимального шляху до кореневого вузла. Вибір надійного бажаного вузла забезпечує надійність маршрутизації трафіку в IoT мережі. Наприкінці, нове повідомлення DIO генерується та транслюється своїм сусідам, яке містить обчислені значення довіри, через метричний контейнер DAG. За цим методом працюють всі сусідні вузли для побудови DODAG. Після цього обслуговування DODAG покладається на таймер Trickle, що обмежує передачу керуючих повідомлень.

Після обчислення індексу довіри який не є статичним, а скоріше продовжує оновлюватися з урахуванням двох умов: періодичного та реактивного моніторингу. У моделі для періодичного оновлення значення довіри використовується алгоритм таймера для надсилання повідомлень DIO у RPL.

Для реактивного оновлення довіри процес моніторингу ініціюється з урахуванням змін у поведінці вузла, наприклад, зміни рангу без зміни DIO-seq (Rank attack). Однак значення довіри не можна часто оновлювати, оскільки це може вплинути на продуктивність протоколу, витрати зв’язку та мережеві ресурси, такі як енергія, пам’ять і цикли ЦП вузла.

Отже, в моделі механізм оновлення старається прийняти реалізацію таблиці маршрутизації в існуючому RPL, як основу для оновлення значення довіри. В моделі не розглядаються відновлення ізольованих вузлів, які класифікуються як шкідливі або підозрілі.

2.2.2 Обчислювальна складність

В моделі цільову функцію стандартного RPL змінено, в основному для вибору батьківського елемента на основі довіри та виявлення атак. Складність

надійного батьківського алгоритму вибору, для алгоритму на рисунку 2.3, становить $O_{(1)}$ у найкращому випадку, за винятком розрахунку довіри для сусідніх вузлів, необхідного, як вхідні дані для вибору батьківського елемента, який дорівнює $O_{(n)}$. Крім того, для певного вузла може бути n кількість потенційних батьківських вузлів, тому для перевірки надійності потенційних вузлів один за одним, складність алгоритму буде становити $O_{(n)}$ у гіршому випадку.

Подібним чином обчислювальна складність для виявлення атак становить $O_{(1)}$ у найкращому випадку та $O_{(n)}$ у гіршому випадку. Таким чином, можна зробити висновок, що загальна складність доданих процедур у модель становить $O_{(n)}$. Отже обчислювальна складність зростає з обчисленням показників довіри та агрегації.

2.2.3 Виявлення рангових і чорних атак та ізоляція вузлів зловмисників

У ранговій атаці фактичне значення рангу змінюється шкідливим вузлом, щоб рекламувати кращий маршрут для залучення трафіку. Однак вузли, які використовують цей зловмисний вузол для маршрутизації свого трафіку, зрештою втрачають пакети так чи інакше.

У мережі RPL зміна рангу відбувається, коли дочірній вузол вибирає нового батьківського вузла з кращим рангом. У ранговій атаці шкідливі вузли рекламують себе за допомогою підроблених рангів і оптимальних маршрутів до своїх сусідів, які, як правило, вибирають його, як новий батьківський вузол. Вузли-жертви вибирають нового «батька» з нижчим рангом, щоб відповідати правилам рангу RPL для топології без петель. Це призводить до відокремлення цих вузлів від ефективного зв’язку в мережі.

В пропонованій моделі використовується підслуховування та моніторинг сусідніх вузлів для виявлення атаки Rank. Атака за рангом має кілька варіантів, включаючи атаку зі зниженим рангом, атаку збільшеного рангу. Для даної моделі конкретно розглядається атака зі зниженим рангом.

Коли повідомлення DIO отримує вузол від сусіднього вузла, він перевіряє, чи змінюється ранг без DIO_seq, тобто новий DIO_seq менше або дорівнює поточному DIO_seq, це означає, що це підозрілий або фальшивий DIO; отже, ідентифікується атака за рангом. Крім того, перевірка невідповідності рангу потенційного «батька» сусіднім вузлам вказує на підроблені значення DIO та Rank [28]. Діаграма послідовності для виявлення рангової атаки зображена на рисунку 2.4.

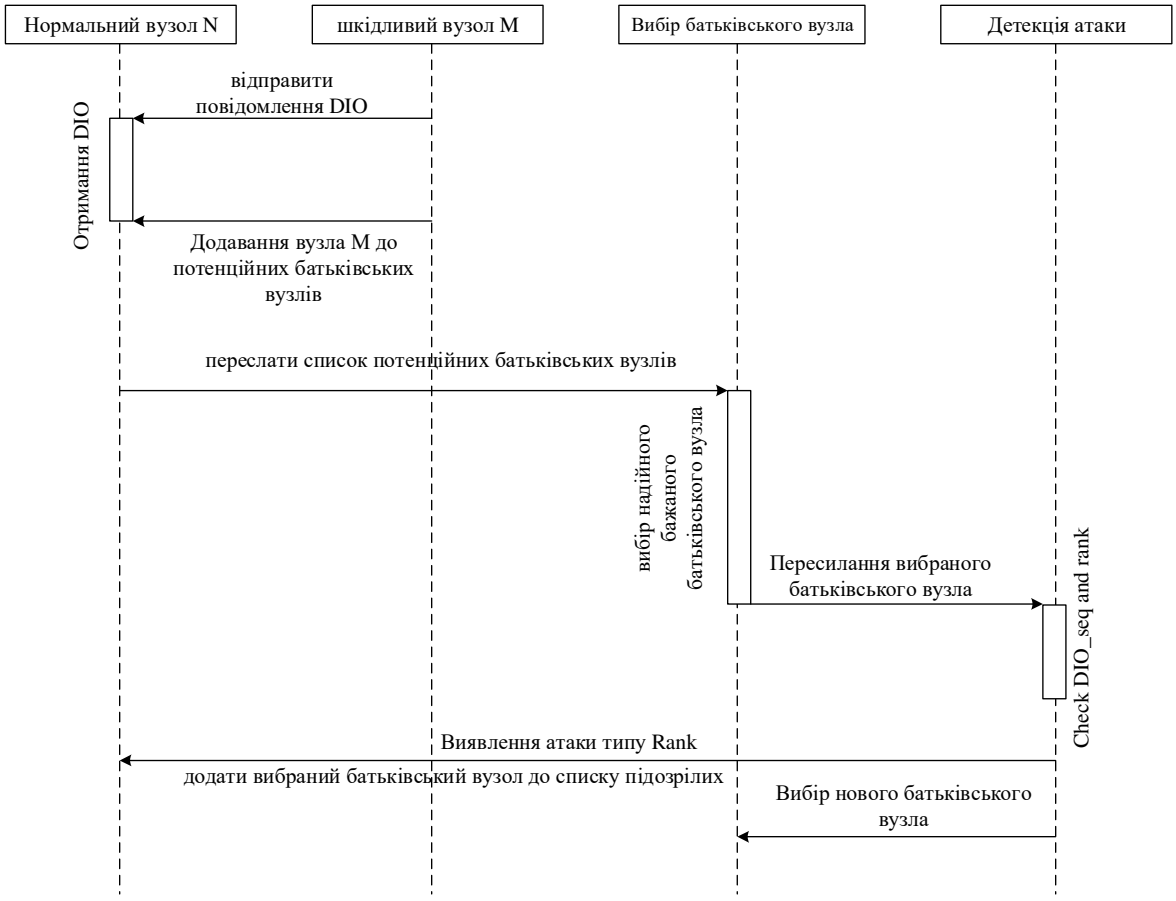


Рисунок 2.4 - Діаграма послідовності для виявлення рангової атаки

Подібним чином, атака Blackhole є одним із видів атак із видаленням пакетів. В моделі реакція на таку атаку досягається шляхом підслуховування та моніторингу сусідніх вузлів, чи пакетів, які пересилаються успішно чи відкидаються довіреним вузлом. Атака Blackhole виявляється за індексом довіри бажаного батьківського вузла. Крім того, проводиться додаткова перевірка рівня успішності, щоб знати, що вузол відкидає пакети, і

підтверджувати атаку з відкиданням пакетів. На рисунку 2.5 зображена діаграма послідовності виявлення атак Blackhole.

Відповідно до визначення та виявлення атак Rank і Blackhole SMTrust додатково використовується метод виявлення та ізоляції атак [29].

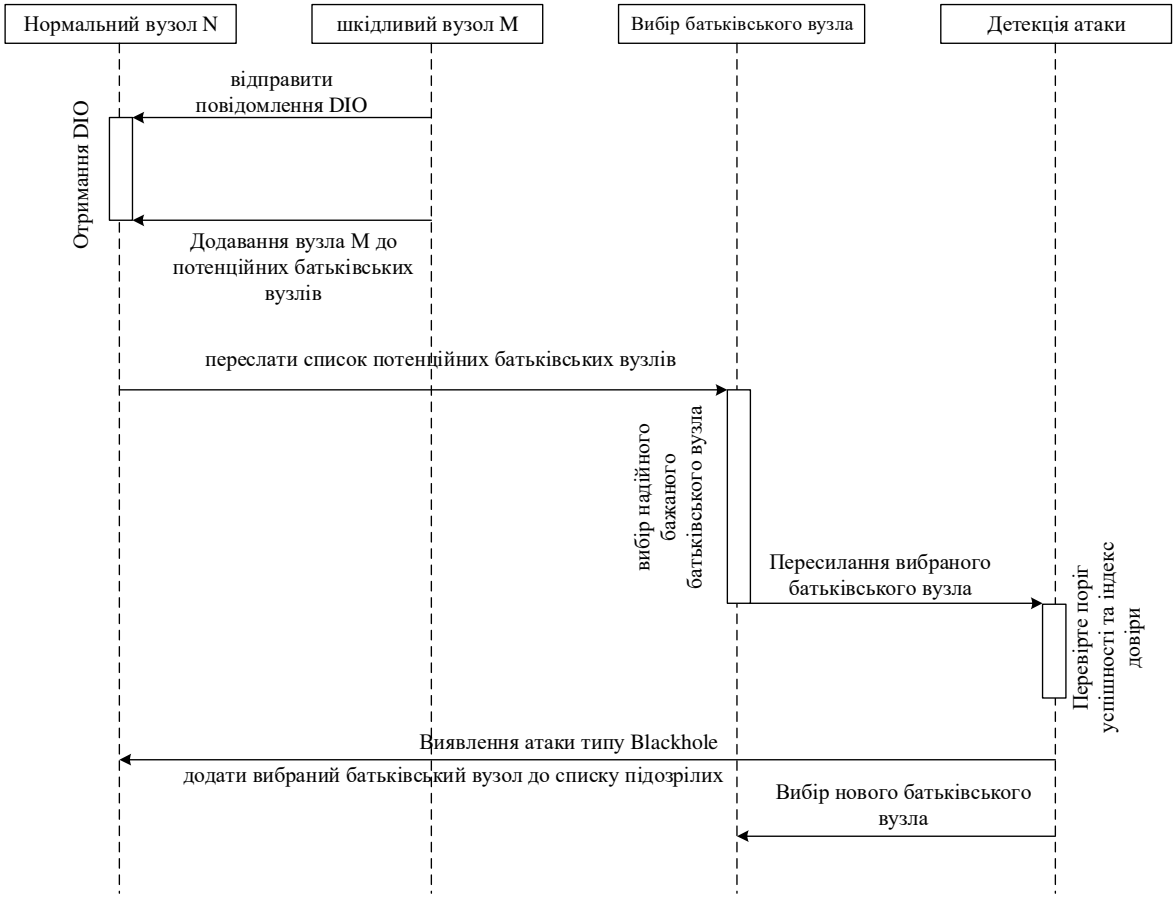


Рисунок 2.5 - Діаграма послідовності виявлення атак типу Blackhole

2.3 Механізм рангових меж

SRPL — це нова схема безпеки, заснована на пороговому значенні рангу та аутентифікації хеш-ланцюжка. Цей підхід застосовується для запобігання внутрішнім атакам, спрямованим на порушення топології DODAG та/або виснаження ресурсів шляхом незаконної зміни значення рангу. Знижуючи свій ранг, неправильно налаштований вузол бажає стати ближчим до кореня DODAG і таким чином отримати повноваження керувати, змінювати або

видаляти більшу частину трафіку, який проходить через нього. SRPL вводить знижений поріг рангу D наступним чином

$$D(r, N_p) = \alpha + \frac{\beta}{(r \cdot N_p)} \quad (2)$$

де, α – ступінь допуску;

β – параметр моделювання, обраний більшим або рівним десяти, що веде до швидшого ослаблення;

D, r – параметр рангу;

Np – номер батьківського набору.

Ця функція, як зображено на рисунку 2.6, має низхідний вигляд у порівнянні зі значенням рангу та доходить до нуля для великого значення рангу.

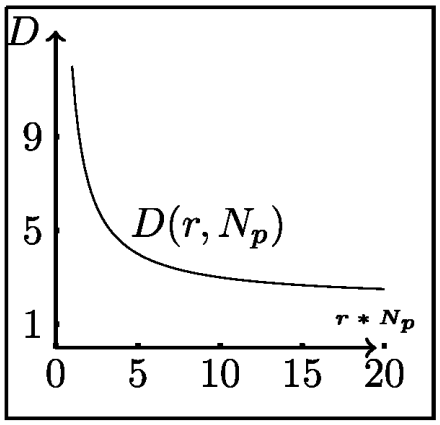


Рисунок 2.6 - Знижений показник рангу

Зниження рангу є неправомірною операцією, яка буде обмежена функцією *D*. Перебування близько до приймача, а потім отримання низького значення рангу під час формування DODAG призводить до сприятливої позиції та надійної посади, що дозволяє вузлам досягати більшого значення D, ніж вузли в глибині DODAG або ті, хто нещодавно приєднався до мережі. .

Таким чином, останні отримують більше можливостей знижувати свій ранг, не порушуючи топологію або перебуваючи в сумнівній поведінці. Крім того, наявність великого батьківського розміру обмежує ймовірність зниження

значення рангу. Це пояснюється тим, що, зменшуючи свій ранг, вузол приваблює інші вузли, які були в його батьківському наборі або їхніх нащадків. Це виправдовує обернено пропорційну еволюцію D від значення Np.

Крім того, внутрішній зловмисник може завдати шкоди топології DODAG, опублікувавши неправомірно підвищений ранг, щоб змусити вузли обмінюватися більшою кількістю керуючих повідомлень і, зрештою, скинути таймер потоку, таким чином виснажуючи ресурси. Щоб пом'якшити цю атаку, SRPL відстежує, скільки разів вузол RPL збільшує своє значення рангу, встановлюючи таке порогове значення:

$$I(r, N_d) = \alpha + \ln\left(\frac{r}{N_d}\right) \tag{3}$$

де, α – це ступінь терпимості;

r – параметр рангу;

N_d – кількість спрямованих нащадків.

Ця функція, як показано на рисунку 2.7, представляє висхідний темп відповідно до параметра рангу.

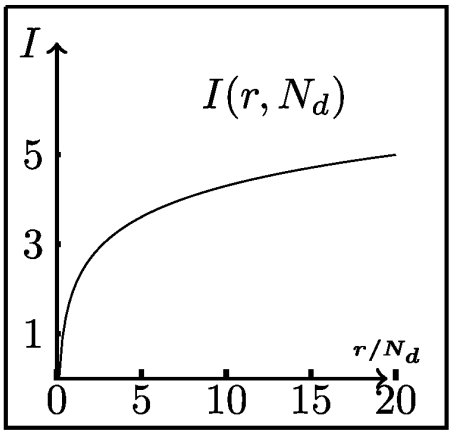


Рисунок 2.7 - Збільшений коефіцієнт рангу

Чим більше збільшується значення рангу, тим більше вузол має шанс зайти глибше в граф DODAG і збільшити свій ранг. Маючи високий ранг, буде менше трафіку для пересилання та, отже, менше приєднаних вузлів. Таким

чином, уражена топологія буде обмежена, а кількість обмінюваних керуючих повідомлень буде обмеженою. Крім того, ця функція залежить від другого параметра, який обернено пропорційний кількості нащадків Nd. Для двох вузлів з однаковим рангом і різним розміром нащадків свобода збільшення рангу призначається вузлу з найменшою кількістю нащадків, щоб зберегти стабільність топології DODAG і вплинути на мінімальні ресурси.

Використовуючи ці дві порогові функції, структурується мережа від атак, заснованих на зміні рангу, перезаписуючи будь-який вузол, який переступає ці пороги. Це також вимагатиме високого рівня безпеки через впровадження концепцій верифікації та автентифікації.

2.4 Опис протоколу

Основною метою протоколу є створення безпечного накладення зв'язку, що охоплює більшість атак внутрішнього рангу, обмежуючи зміну рангу швидкості. Це засновано на концепції порогового значення рангу, яке буде призначено кожному вузлу за допомогою суворих заходів автентифікації. Цей процес автентифікації базується на функції хеш-ланцюга h, яка фактично є криптографічною односторонньою хеш-функцією, наприклад SHA1, визначеною xn+1 = h(xn). Хеш запускається під час присвоєння рангів і порогів, потім він буде виділений під час оновлення рейтингу. Протокол має три основні фази:

– Фаза ініціації: цей крок запускається під час створення DODAG. Кожен вузол зможе обчислити свій ранг, порогові значення та відповідні хешовані значення, які спочатку генеруються коренем.

– Фаза перевірки: ця друга фаза забезпечує довіру до кожного вузла, який повинен контролювати його довірений батьківський вузол. Таким чином, кожен «батько» перевіряє хешований ранг і порогові значення кожного зі своїх нащадків за допомогою процесу моніторингу, заснованого на методах

підслуховування. Реалізація даного алгоритму представлена в псевдокоді нижче.

```
for each node i □ Nd do
 GetDIO(RANK,I,D)
 Calulate:
 x = I − Iparent AND y = D − Dparent
 if Ai == □(Aparent) then
  if Bi = hy(Bparent) AND Ci = hx(Cparent) then
   Accept node
  else
   Discard node
  end if
 end if
end for
```

– Етап оновлення рангу: цей крок виконується під час зміни рангу. Новий батьківський пристрій перевіряє хеш-значення, спочатку обчислені запрошеним вузлом, гарантує, що воно не перевищило порогове значення, а потім вибирає білий або чорний список, які відповідно відповідають прийнятим і відхиленим вузлам. Ця фаза обробляється за алгоритмом представленому псевдокодом нижче

```
GetSolicitationDIO(RANK,I,D)
Authentication
if ORank > NewRank then
    Calulate :
    x = ORank − ORankNewP ι
    y = DNewP ι − D
    if Ai = hx(ANewP ι) and Bi = hy(BNewpι) then
        Accept node
    else
        Discard node
    end if
else
    Calculate
    x = ORankNewP ι − ORank
    y = I − INewP ι
    if Ai = hx(ANewP ι) and Ci = hy(CNewP ι) then
        Accept node
    else
        Discard node
    end if
end if
```

Після ініціалізації корінь DODAG генерує три випадкові числа a, b і c, кожне з яких дає хешоване значення $A0 = h(a)$, $B0 = h(b)$ і $C0 = h(c)$, яке буде транслюватися. Після отримання трьох хешованих значень кожен вузол обчислює свій власний ранг, обчислений за допомогою певної цільової функції, свій коефіцієнт зростання рангу I та коефіцієнт зменшення рангу D. Тоді три хешовані значення отримують шляхом обчислення:

$$A_i = h^{rank} \cdot (A0), B_i = h^D(B0), C_i = h^i(C0) \quad (4)$$

Ці хешовані значення використовуватимуться на етапі автентифікації під час оновлення рейтингу.

Після фази ініціалізації кожен вузол буде перевірено своїм батьківським вузлом, як описано в алгоритмі перевірки. Батьківський вузол обчислює різницю між власним рангом і пороговими значеннями та значеннями вузлів-нащадків. Якщо вузол має підвищене порогове значення або модифіковане значення рангу, його буде негайно видалено. Щоб підтримувати свіжість мережі та оновлювати ранг і порогові значення, фази ініціації та перевірки повторюються щогодини або для кожного оновлення номера версії. Ці три фази доповнюють один одного, і їхня залежність дозволяє захищати DODAG від внутрішніх атак.

За допомогою алгоритму оновлення рангу новий батьківський елемент матиме можливість автентифікувати хешовані значення рангу та порогів I і D, порівнюючи їх зі своїми власними хешованими значеннями. Якщо це успішно завершено, новий батьківський вузол гарантує, що приєднаний вузол не перевищив порогове значення, а потім отримує свою нову позицію в DODAG. В іншому випадку вузол буде вважатися зловмисником і буде негайно виключено.

Висновки до розділу 2

1. Запропоновано модель, яка базується на довірі, що включає формування довіри, виявлення атак та ізоляцію шкідливих вузлів. Основою є визначення та моніторинг факторів довіри, таких як енергоспоживання, мобільність вузлів та рекомендації сусідів.

2. Система враховує історичні дані, поточні метрики та розташування вузлів. Значення довіри обчислюється як зважена сума різних метрик, де кожна метрика отримує відповідну вагу залежно від її важливості.

3. Запропонований метод використовує механізми періодичного та реактивного оновлення довіри. Періодичне оновлення забезпечує

стабільність, тоді як реактивне дозволяє швидко адаптуватися до змін поведінки вузлів. Для протидії атакам, таким як Rank Attack та Blackhole, було впроваджено моніторинг довіри та контроль маршрутів. Шкідливі вузли ізолюються на основі порівняння значень довіри із встановленим порогом.

4. Впроваджено систему рангових порогів, яка обмежує незаконну зміну рангів вузлами. Ця функція забезпечує стабільність мережі та мінімізує ризики маніпуляцій із топологією DODAG.

5. Для запобігання внутрішнім атакам використано механізм автентифікації на основі хеш-ланцюгів. Це дозволяє перевіряти достовірність рангу та інших показників вузлів.

6. Забезпечено обмеження змін рангів шляхом контролю їх частоти та амплітуди. Це дало змогу захистити мережу від виснаження ресурсів через додаткові керуючі повідомлення.

Запропонований метод та модель забезпечують комплексний підхід до безпеки маршрутизації в IoT, зосереджуючись на довірі, рангових межах та автентифікації. В результаті чого можна мінімізувати ризики атак, підтримуючи стабільність мережі та оптимізуючи використання її ресурсів.

3 ТЕСТУВАННЯ СИСТЕМИ АНАЛІЗУ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Кожен вузол у тестовій мережі є комбінацією апаратного та програмного вузла, що використовує операційну систему Contiki та чіп CC2530 компанії, а код алгоритму вбудовано в тестовий вузол. Кожен вузол з'єднаний з комп'ютером за допомогою послідовного порту для відображення даних зв'язку між вузлами.

Після того, як кластер буде повністю побудований, вузол може бути запущений для надсилання топології мережі на шлюз, який відображатиме топологію кожного кластера через програмне забезпечення відображення топології на стороні комп'ютера. Програмне забезпечення відображає топологію та передачу даних усього мережевого протоколу для перевірки протоколів маршрутизації.

3.1 Перевірка багатошляхової маршрутизації

Вся мережа складається з вузла шлюзу, головного вузла кластера та загального вузла. Вузол шлюзу, який може збирати всю інформацію про топологію мережі, показує топологію мережі, у той же час він може служити як гетерогенний маршрутизатор для реалізації перехресних кластерів зв'язку.

3.1.1 Процедура тестування

1) мережа відображається шлюзом після сповіщення про топологію. Повна топологія мережі показана на рисунку 3.1. Після IPv6 адреси кожного вузла, показується температура та вологість в топології для імітації даних, зібраних датчиками. 16-бітне повідомлення IPv6 використовується для ідентифікації відповідного вузла. Вузол b6fc представляє вузол шлюзу, вузол b5b4 і вузол a1b7 представляють головний вузол кластера, а інші вузли представляють загальний вузол.

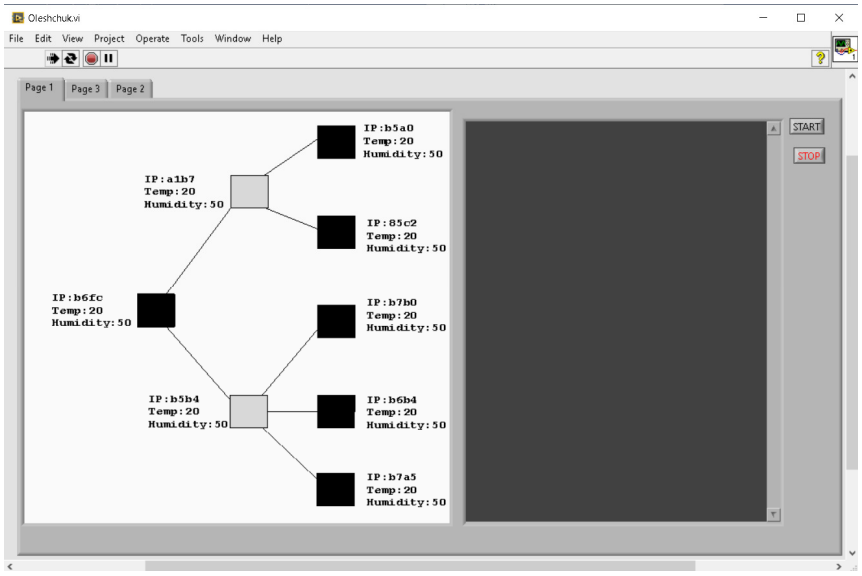


Рисунок 3.1 - Топологія мережі до ввімкнення багатошляхової маршрутизації

2) Вузол 85c2 вибирається як вузол джерела передачі даних, вузол b7b0 вибирається як вузол призначення для прийому даних, де вузол призначення та вузол джерела знаходяться в різних кластерах. Вихідний вузол і адресат підключаються до дисплея, щоб показати надсилання та отримання. Багатошляховість демонструється на вихідному вузлі. Якщо багатошляховий шлях не ввімкнено, програмне забезпечення для відображення не відображає резервний шлях для з'єднання в топології. У цей момент вихідний вузол надсилає дані, а кінцевий вузол може отримати один пакет даних (рисунок 3.2).

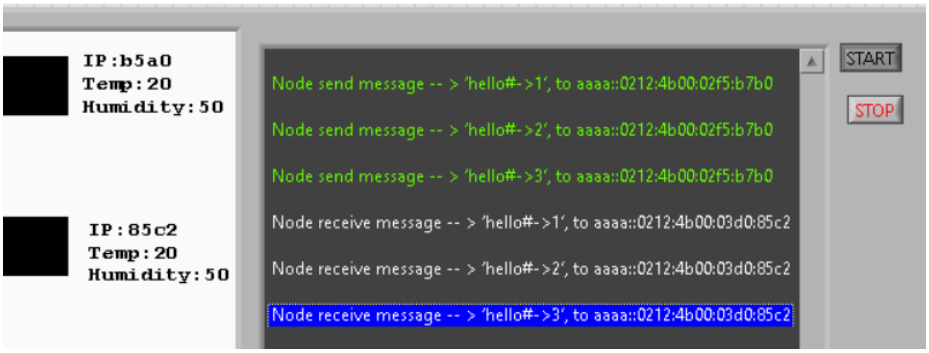


Рисунок 3.2 - Резервний шлях не ввімкнено

3) Коли багатошляховість увімкнено, інформація про відкриття багатошляховості завантажується вихідним вузлом у програмне забезпечення для відображення топології шлюзу. Вихідний вузол відображає підключення до резервного шляху. На рисунку 3.3 пунктирна лінія позначає шлях резервного копіювання.

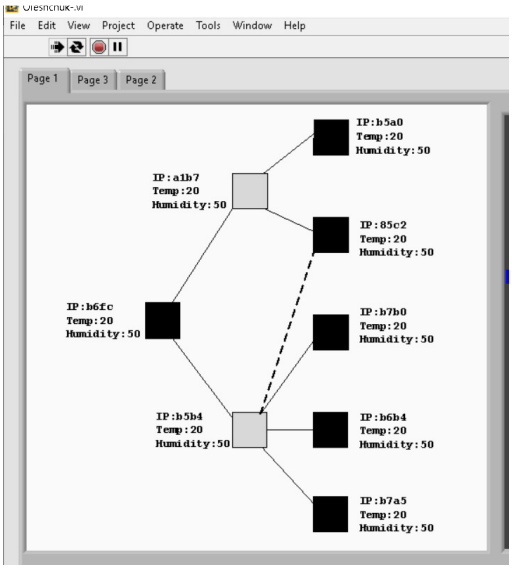


Рисунок 3.3 - Топологія мережі після ввімкнення багатошляхової маршрутизації

4) Після того, як шлях резервного копіювання ввімкнено, вузол-джерело надсилає дані на вузол призначення, у вікні послідовного відображення показується, що вузол призначення отримав два пакети даних. Конкретний процес показаний на рисунку 3.4.

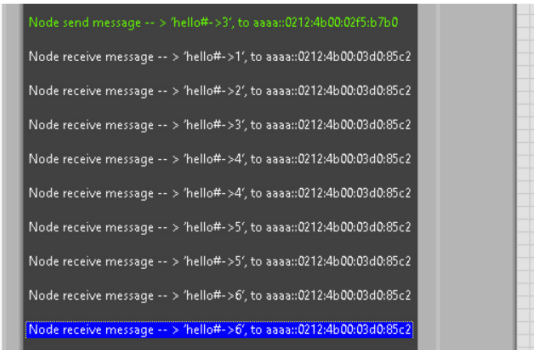


Рисунок 3.4 - Резервний шлях увімкнено

3.2 Тест атаки чорної діри

Було вибрано один вузол в тому ж кластері вузла джерела даних, що й вузол чорної діри. Атака чорної діри ініціюється на вибраному вузлі за допомогою натискання кнопки, і процес атаки чорної діри відображається на підключеному моніторі. Вузол чорної діри візьме інші вузли в кластері як свої дочірні вузли. Інформація про ідентифікацію вузла чорної діри та топології поточного етапу кластерної мережі буде передана шлюзу та відображена в програмному забезпеченні відображення топології шлюзу. На рисунку 3.5 показано топологію в нормальному стані мережі до атаки чорної діри.

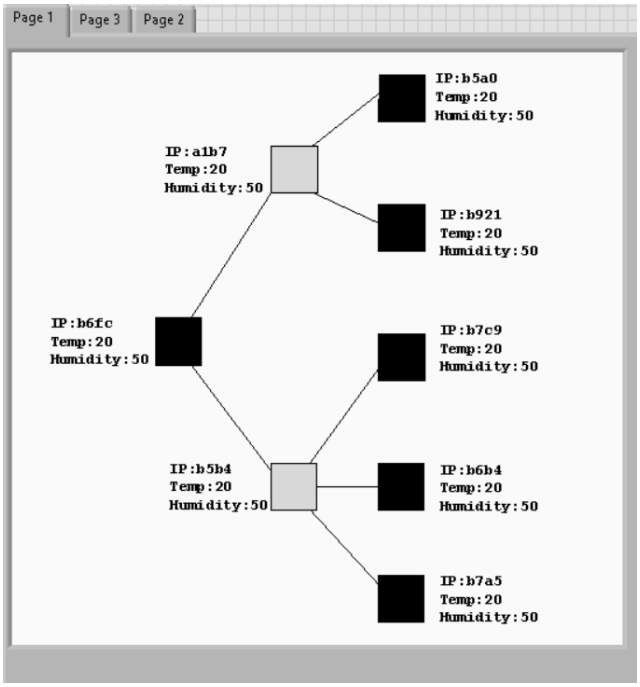


Рисунок 3.5 - Топологія мережі до атаки чорної діри

Загальні вузли можуть отримувати пакети даних перед атакою, вузол-джерело періодично надсилає інформацію про температуру вузлу призначення. Пакет показує адресу IPv6 вихідного вузла, конкретний прийом даних, як показано на рисунку 3.6.

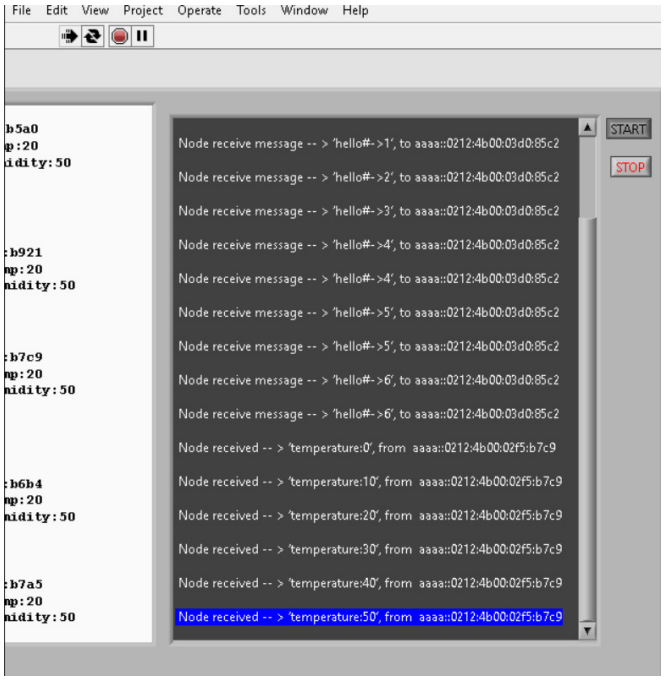


Рисунок 3.6 - Загальні вузли отримують звичайні пакети

На рисунку 3.7 IPv6-адреса вузла атаки – b6b4. Інформація про топологію повідомляється шлюзу після початку атаки.

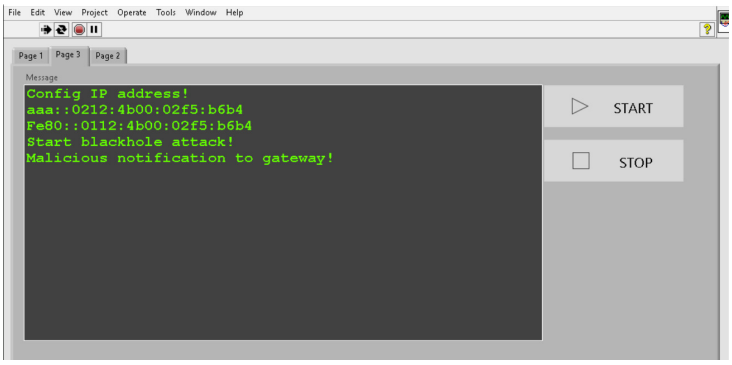


Рисунок 3.7 - Атака шкідливого вузла

Після залучення нова топологія показує, що вузол b6b4 залучає трафік сусідніх вузлів. Його статус еквівалентний головному вузлу кластера, як показано на рисунку 3.8.

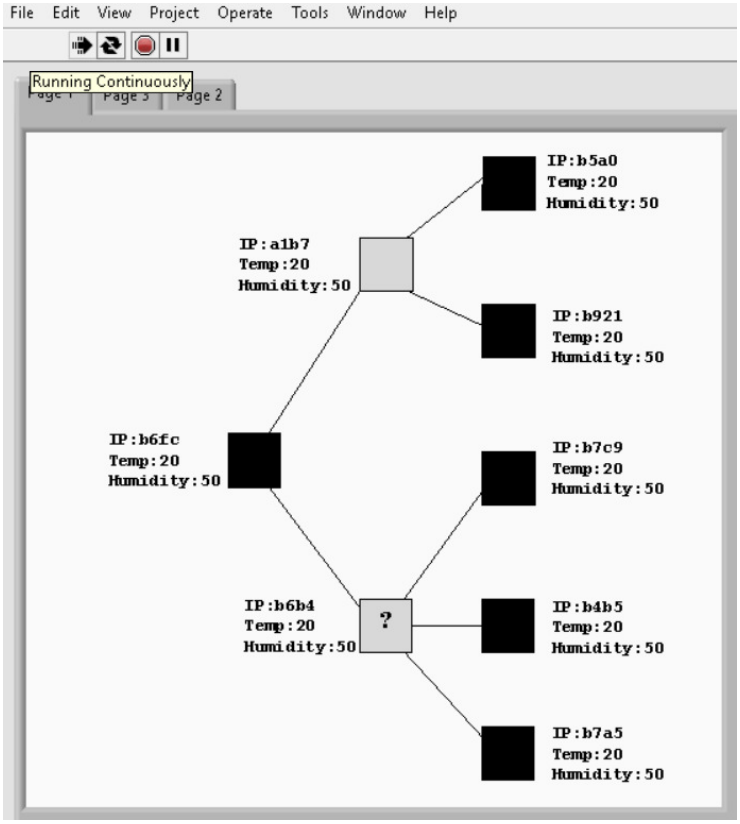


Рисунок 3.8 - Топологія шлюзу після атаки

Загальний вузол отримує помилкову керуючу інформацію від атакуючого вузла, як показано на рисунку 3.9.

Рисунок 3.9 - Загальний вузол отримує неправильну інформацію

У цьому випадку, використовуючи протокол маршрутизації RPL, загальний вузол не може отримати жодних пакетів, оскільки шкідливі вузли перехоплюють усі пакети, як показано на рисунку 3.10.

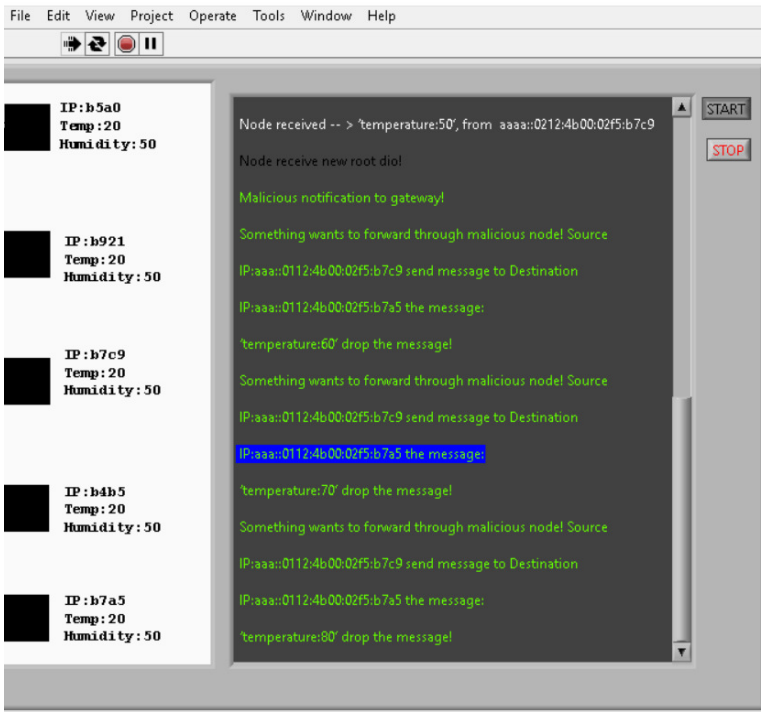


Рисунок 3.10 - шкідливі вузли отримують інформацію

Але в цьому випадку, використовуючи модифікований протокол який представлений у розділі 2.2, загальний вузол може отримувати всі пакети через багатошляховий зв’язок, як показано на рисунку 3.11.

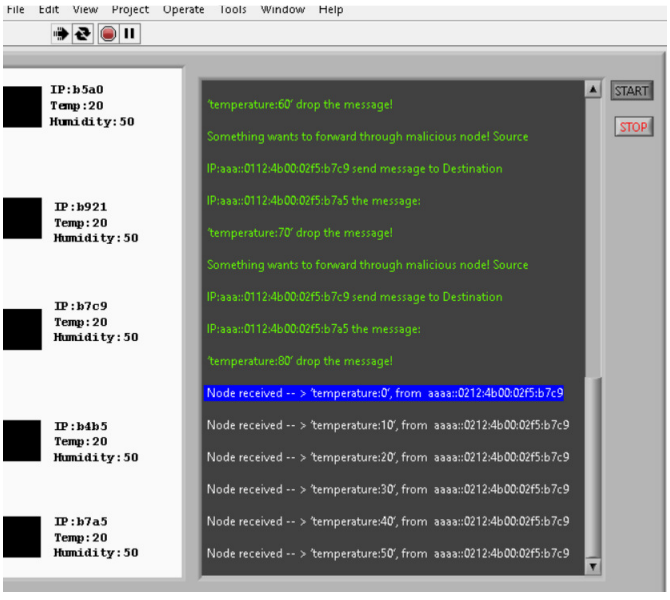


Рисунок 3.11 - Загальні вузли отримують пакети після атаки

3.3 Тестування пропускної здатності та енергоспоживання

3.3.1 Пропускна здатність

Пропускна здатність MRHOF різко знижується під час атак для, як показано на рисунку 3.12. Це пояснюється тим, що вузли вибирають шкідливі вузли як батьківські, а уражені нормальні вузли мають пропускну здатність 0 Кбіт/с, оскільки їхні пакети не досягають вузла-приймача.

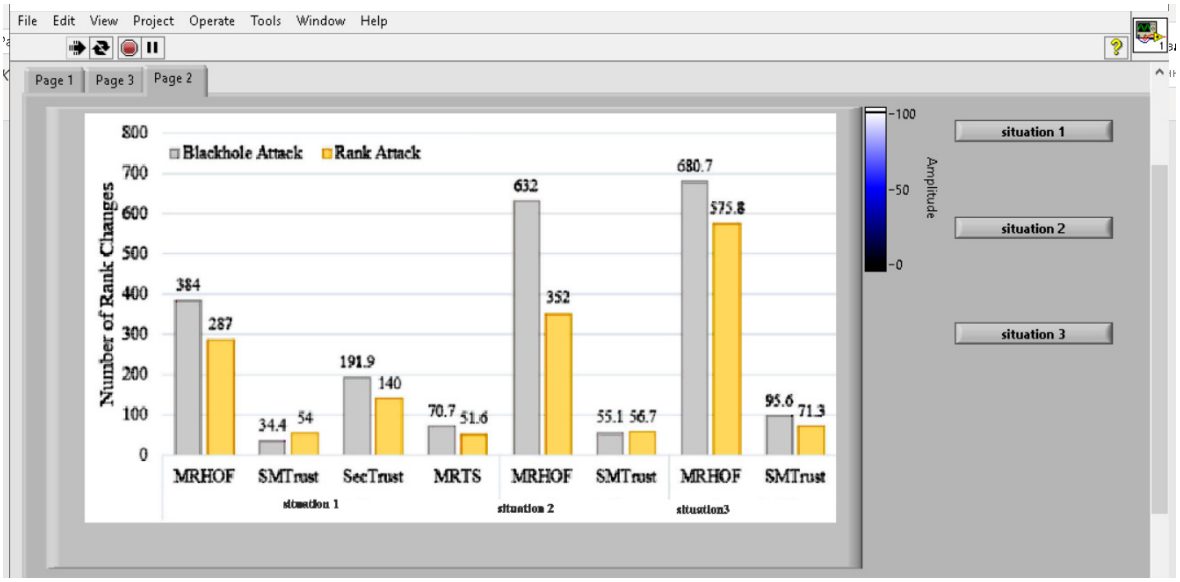


Рисунок 3.12 - Порівняння пропускної здатності (кбіт/с).

Це свідчить про те, що частина мережі паралізована для надсилання пакетів. Більше того, у MRHOF немає механізму захисту від атак, і маршрут встановлюється без урахування жодної метрики довіри на відміну від встановлення надійного маршруту в пропонованій моделі, таким чином підвищуючи пропускну здатність у протоколі RPL на основі SMTrust. SMTrust, SecTrust і MRTS пропонують вищу пропускну здатність завдяки вбудованим механізмам виявлення атак.

Крім того, пропускна здатність вузлів залишається більшою за нуль, що збільшує загальну пропускну здатність. Середнє значення пропускної здатності на 32% і 80,6% під час атак Blackhole і Rank відповідно. Покращення

результатів полягає в тому, що використовується шість різних показників довіри, наприклад, рівень успіху, рекомендовану довіру, історичні спостереження, рівень енергії, а також місце розташування та стабільність зв'язку.

Крім того, різниця в кількісному визначенні та зваженому обчисленні загального індексу довіри, як пояснюється в Розділі 3, логічно виправдовує його кращу продуктивність

У порівнянні з іншими методами, метод який реалізований в моделі показує незначно меншу пропускну здатність, різницю в 0,16 Кбіт/с, під час атаки Blackhole і вищу швидкість втрати пакетів, різницю в 4,3%, під час атаки Rank.

Це означає, що для вбудовування моделі у систему IoT не потрібно апаратне забезпечення. Також такий підхід значно перевершує MRHOF під час атак, як показано на рисунку 3.12. Таким чином, це вказує на важливість моделі довіри та вирішальний вибір показників довіри для створення надійної топології та захисту від атак маршрутизації.

3.3.2 Енергоспоживання

Середнє енергоспоживання показує невелику різницю, оскільки вузли в виконують довірчі обчислення. Хоча SMTrustOF показує менше енергоспоживання для всіх сценаріїв у «Blackhole attack», а також у сценаріях рангової атаки. Енергоспоживання SMTrust дещо вище порівняно з MRHOF (під час атаки за рангом), як показано на рисунку 3.13. Однак різниця є мала - до 0,22 мВт. Це пов'язано з різницею в обчисленнях для індексу довіри, виявлення ttack і вибору довіреного батьківського вузла.

Енергоспоживання в SMTrust більше через обчислення показників довіри та передачі DIO разом із механізмом виявлення атак. Після виявлення та ізоляції атакуючих вузлів загальне енергоспоживання мережі стає стабільним. Даний підхід демонструє порівняно прийнятне збільшення енергоспоживання.

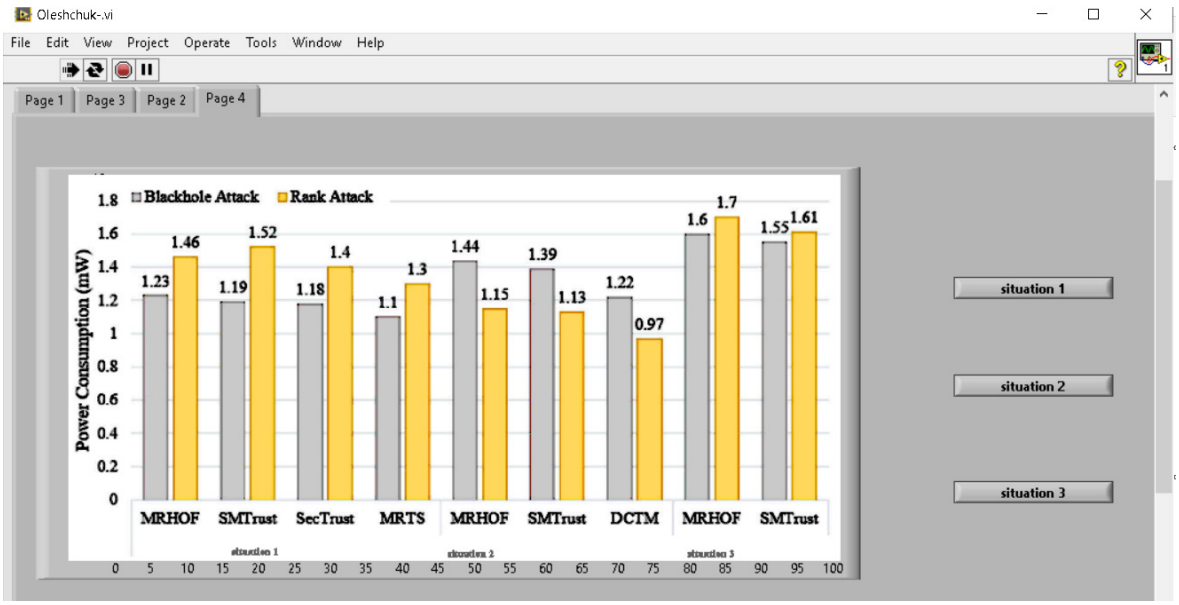


Рисунок 3.13 - Порівняння споживаної потужності (мВт).

Загалом система демонструє кращу продуктивність, як для Rank, так і для Blackhole атак. Крім того, вплив мобільності приймача погіршує продуктивність мережі під час атак Rank і Blackhole Однак SMTrust все ще перевершує загальні параметри продуктивності мережі, включаючи стабільність топології, вимірювання пропускної здатності вузлів, що свідчить про значне покращення порівняно з існуючими системами.

Висновки до розділу 3

1. Використання багатошляхової маршрутизації дозволяє покращити стабільність мережі IoT та забезпечити резервні шляхи для передачі даних. Увімкнення резервного маршруту дозволяє уникати втрати даних у разі пошкодження основного шляху, підвищуючи загальну надійність мережі.

2. Було проведено тестування на вразливість мережі до атак Blackhole та Rank. Зловмисні вузли успішно залучали трафік, блокуючи передачу даних уразливими вузлами. Використання запропонованого протоколу маршрутизації, заснованого на довірі, дозволило забезпечити передачу пакетів

навіть за умов атак, що підтверджує ефективність метрик довіри та багатошляхового зв’язку.

3. Під час атак спостерігалося різке зниження пропускної здатності для стандартного протоколу MRHOF, у той час, як запропонований підхід демонстрував вищу стабільність передачі даних.

4. Запропонований метод забезпечив середнє зростання пропускної здатності на 32% для атак Blackhole та на 80,6% для атак Rank завдяки використанню шести метрик довіри.

5. Незважаючи на додаткові обчислення для індексу довіри та виявлення атак, проявляється незначне зростання енергоспоживання, що залишається прийнятним. Різниця у споживанні не перевищує 0,22 мВт. Після виявлення та ізоляції зловмисних вузлів енергоспоживання мережі стабілізується, демонструючи ефективність управління ресурсами.

6. Під час атак мобільність вузлів може погіршувати продуктивність мережі, однак запропонований метод забезпечує покращення параметрів стабільності топології та пропускної здатності порівняно зі стандартними методами.

Запропонований метод і модель маршрутизації, яка заснована на довірі та багатошляховості, демонструє значні переваги у стабільності, пропускній здатності та захисті мережі від атак. Незначне зростання енергоспоживання є виправданою ціною підвищення безпеки та ефективності мережі IoT.

ВИСНОВКИ

Протокол RPL є ефективним рішенням для забезпечення маршрутизації в мережах IoT, проте залишається вразливим до атак, таких як рангова атака, чорна діра та інші. Виявлення цих загроз підкреслює необхідність вдосконалення безпеки маршрутизації для підвищення стабільності та продуктивності мереж.

1. Запропоновано модель, яка базується на довірі та враховує історичні дані, поточні метрики та поведінку вузлів. Використання метрик довіри дозволяє визначати надійні вузли для маршрутизації, мінімізуючи ризики, пов’язані з атаками. Введення порогових значень рангу обмежує незаконну зміну параметрів вузлів і забезпечує стабільність мережі. Використання автентифікації на основі хеш-ланцюгів сприяє запобіганню внутрішнім атакам, зокрема маніпуляціям з топологією DODAG.

2. Проведено тестування багатошляхової маршрутизації, що продемонструвало ефективність резервного копіювання маршрутів для забезпечення стабільної передачі даних.

3. Запропонований метод успішно протидіє атакам типу Blackhole і Rank, мінімізуючи втрати пакетів і підвищуючи загальну пропускну здатність мережі.

4. Незначне зростання енергоспоживання в межах прийнятного рівня підтверджує, що впровадження додаткових механізмів безпеки не погіршує ефективність роботи мережі. Енергетичні витрати залишаються стабільними після ізоляції шкідливих вузлів.

5. Запропонований метод безпечної маршрутизації підвищує надійність і безпеку мереж IoT, забезпечуючи їхню стабільну роботу навіть в умовах активних загроз.

Розроблений метод безпечної маршрутизації даних для IoT, що базується на довірі та механізмах автентифікації, забезпечує високий рівень захисту від атак і підтримує стабільність мережі. Це створює основу для

подальшого вдосконалення протоколів маршрутизації, орієнтованих на безпеку, ефективність і довговічність мереж IoT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. H.-S. Kim, J. Ko, D.E. Culler, J. Paek, Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): a survey, IEEE Commun. Surv. Tutor. 19 (4) (2017) 2502–2525.

2. Lamaazi, Hanane, and Nabil Benamar. "A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function." Ad Hoc Networks 96 (2020): 102001.

3. J.V.V. Sobral, J. Rodrigues, R.A.L. Rabelo, J. Al-Muhtadi, V. Korotaev, Routing protocols for low power and lossy networks in internet of things applications, Sensors (Basel) 19 (9) (2019) 2144 May 9,.

4. H. Kharrufa, H.A.A. Al-Kashoash, A.H. Kemp, RPL-Based routing protocols in iot applications: a review, IEEE Sens. J. 19 (15) (2019) 5952–5967 Aug 1.

5. IEEE Standard for Low-Rate Wireless Networks, 2016.

6. Taterh, Swapnesh, Yogesh Meena, and Girish Paliwal. "Performance analysis of ad hoc on-demand distance vector routing protocol for mobile ad hoc networks." Computational Network Application Tools for Performance Management (2020): 235-245.

7. Muzammal, Syeda Mariam, et al. "A trust-based model for secure routing against RPL attacks in internet of things." Sensors 22.18 (2022): 7052.

8. Sobral, José VV, et al. "Routing protocols for low power and lossy networks in internet of things applications." Sensors 19.9 (2019): 2144.

9. Manvi, Subodh, K. R. Shobha, and Soumya Vastrad. "Performance analysis of routing protocol for low power and lossy networks (RPL) for IoT environment." International Conference on Distributed Computing and Intelligent Technology. Cham: Springer Nature Switzerland, 2023.

10. Raoof, Ahmed Mohammed. Secure Routing and Forwarding in RPL-based Internet of Things: challenges and solutions. Diss. Carleton University, 2021.

11. Kharrufa, Harith, Hayder AA Al-Kashoash, and Andrew H. Kemp. "RPL-based routing protocols in IoT applications: A review." IEEE Sensors Journal 19.15 (2019): 5952-5967.

12. Ambarkar, Smita Sanjay, and Narendra Shekokar. "An efficient authentication technique to protect iot networks from impact of rpl attacks." Int. J. Eng. Trends Technol 69 (2021): 137-145.

13. ul Hassan, Temur, et al. "CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications." Transactions on Emerging Telecommunications Technologies 32.3 (2021): e4224.

14. Zaatouri, Ibtissem, et al. "Design and performance analysis of objective functions for RPL routing protocol." Wireless Personal Communications 124.3 (2022): 2677-2697.

15. Z.A. Almusaylim, A. Alhumam and N.Z. Jhanjhi / Ad Hoc Networks 101 (2020) 102096

16. D. Sharma, I. Mishra, S. Jain, A detailed classification of routing attacks against RPL in internet of things, Int. J. Adv. Res. Ideas Innov. Technol. 3 (1) (2017) 692–703.

17. Azzedin, Farag, and Hussah Albinali. "Security in internet of things: Rpl attacks taxonomy." Proceedings of the 5th International Conference on Future Networks and Distributed Systems. 2021.

18. Karmakar, Somnath, Jayasree Sengupta, and Sipra Das Bit. "LEADER: low overhead rank attack detection for securing RPL based IoT." 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, 2021.

19. Bang, Ankur, and Udai Pratap Rao. "Impact analysis of rank attack on RPL-based 6LoWPAN networks in Internet of Things and aftermaths." Arabian Journal for Science and Engineering 48.2 (2023): 2489-2505.

20. Shah, Zawar, et al. "Routing protocols for mobile Internet of things (IoT): A survey on challenges and solutions." Electronics 10.19 (2021): 2320.

21. Verma, Abhishek, and Virender Ranga. "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review." IEEE Sensors Journal 20.11 (2020): 5666-5690.

22. Muzammal, Syeda Mariam, et al. "A trust-based model for secure routing against RPL attacks in internet of things." Sensors 22.18 (2022): 7052.

23. Hussain, Muhammad Zunnurain, and Zurina Mohd Hanapi. "Efficient secure routing mechanisms for the low-powered IoT network: A literature review." Electronics 12.3 (2023): 482.

24. Muzammal, S.M.; Murugesan, R.K.; Jhanjhi, N.Z. A comprehensive review on secure routing in Internet of Things: Mitigation methods and trust-based approaches. IEEE Internet Things J. 2020, 8, 4186–4210.

25. Dai, C.; Gong, W. Model of services trust threshold assess based on fuzzy theory. In Proceedings of the 2010 2nd International Conference on E-Business and Information System Security, EBISS 2010, Wuhan, China, 22–23 May 2010; pp. 85–88.

26. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. RFC 6550-RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks; Internet Engineering Task Force: Fremont, CA, USA, 2012.

27. Sabbah, A.I.; El-Mougy, A.; Ibnkahla, M. A survey of networking challenges and routing protocols in smart grids. IEEE Trans. Ind. Informatics 2014, 10, 210–221.

28. Le, A.; Loo, J.; Chai, K.; Aiash, M. A specification-based IDS for detecting attacks on RPL-based network topology. Information 2016, 7, 25.

29. Airehrour, D.; Gutierrez, J.; Ray, S.K. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Gener. Comput. Syst. 2019, 93, 860–876.

30. Персіков, М. А., and В. О. Лемешко. "Безпечна маршрутизація, орієнтована на підвищення продуктивності в критичних інфраструктурах на основі IIoT." (2022).

31. Персіков, М. А., and В. О. Лемешко. "Безпечна маршрутизація для забезпечення кіберстійкості у площині даних програмно-конфігурованих мереж." (2021).

32. Кулаков, Ю., В. Лукашенко, and А. Левчук. "Спосіб організації багатошляхової безпечної маршрутизації в безпроводовій мережі MPLS." Proceedings of National Aviation University 50.1 (2012): 101-105.

33. Лемешко, О. В., О. С. Єременко, and О. С. Невзорова. "Моделі та методи безпечної маршрутизації в інфокомунікаційних мережах." (2020).

34. Yeremenko, Oleksandra. "Огляд теоретичних рішень щодо безпечної маршрутизації в інфокомунікаційних мережах." Проблеми телекомунікацій 1 (24) (2019): 3-23.

35. Гула, Ж. В., and Д. С. Тимофєєв. "Дослідження актуальних векторів атак у інтернеті речей та основних механізмів захисту." (2020).

36. Плєхова, Г. А., et al. "Удосконалення моделі безпечної маршрутизації в програмно-конфігурованих мережах." Біоніка інтелекту 1.100 (2024): 50-57.

37. Лемешко, В. О. Особливості реалізації безпечної маршрутизації в інформаційно-комунікаційних системах. Diss. ХНУРЕ, 2024.

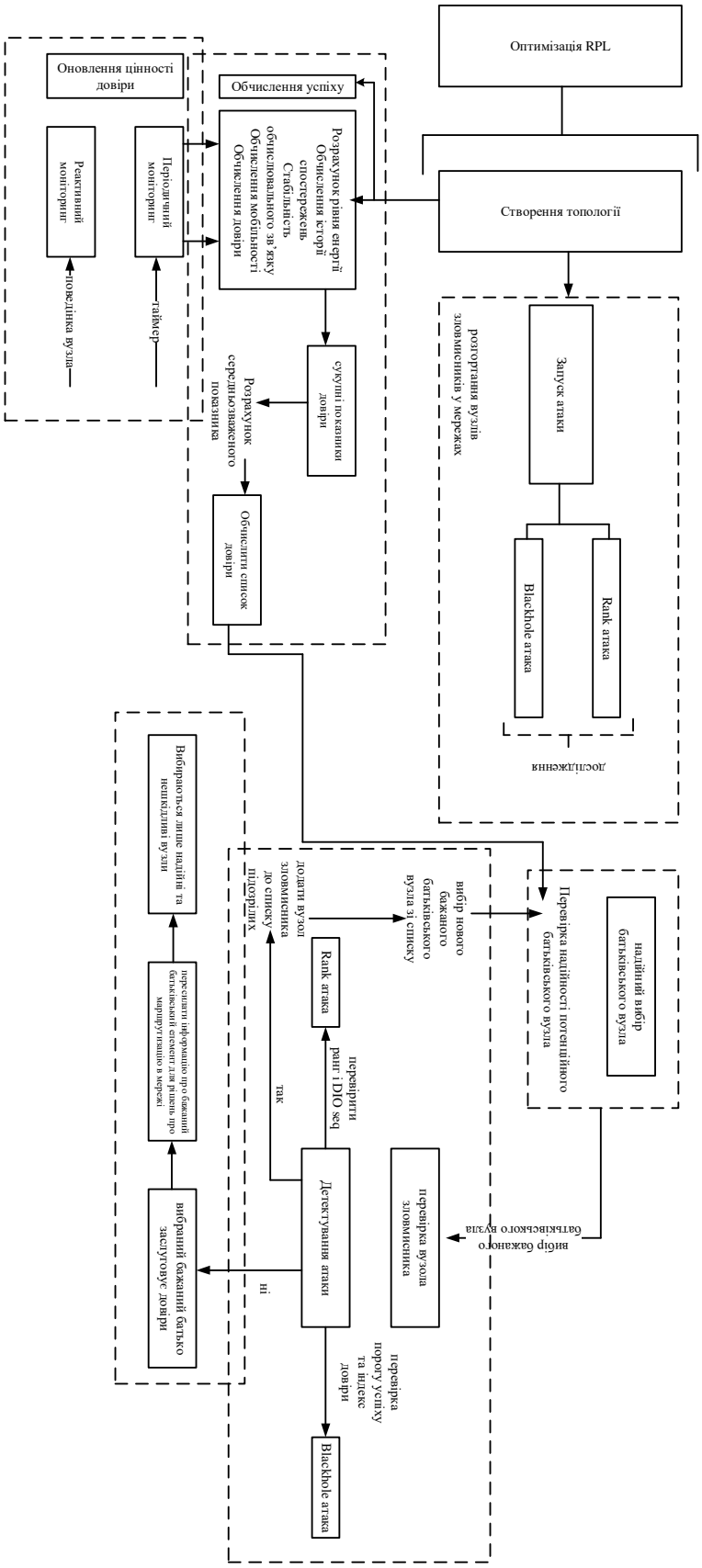
38. Олещук Володимир Андрійович, «Система аналізу безпечної маршрутизації даних для Інтернету речей» матеріали VIII Міжнародної студентської наукової конференції «Актуальні питання та перспективи проведення наукових досліджень» (м. Дніпро, Україна).

39. Олещук Володимир Андрійович, «Модель безпечної маршрутизації в умовах обмежених ресурсів» матеріали IV Міжнародної наукової конференції «Період трансформаційних процесів в світовій науці: задачі та виклики» (м. Рівне, Україна).

40. Комар М.П., Саченко А.О., Васильків Н.М., Загородня Д.І. Методичні рекомендації до виконання кваліфікаційної роботи з освітньо-професійної програми «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» за другим (магістерським) рівнем вищої освіти. – Тернопіль: ЗУНУ, 2024. – 32 с.

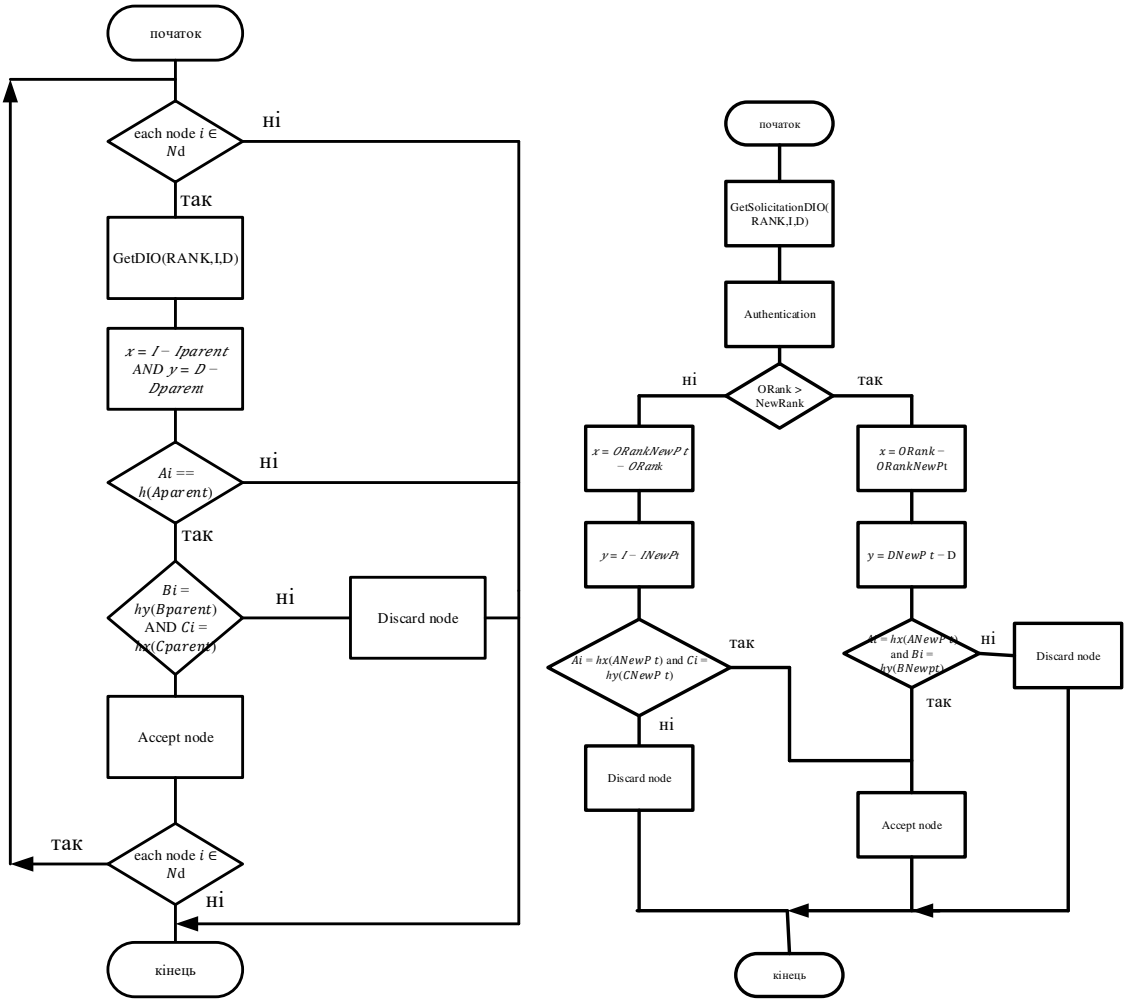
Додаток А

Загальна архітектура моделі



Додаток Б

Блок-схеми алгоритмів фази верифікації та фази оновлення рангу



Додаток В

Код програми визначення фази оновлення рангу

```c
#include <stdio.h>
#include <math.h>
#include <stdbool.h>

// Функція для обчислення хешу (приклад, просто повертаємо значення для спрощення)
int hash(int value) {
    return value * value; // Приклад: хеш - це квадрат значення
}
// Функція для перевірки вузла
bool CheckNode(int ORank, int NewRank, int D, int DNewPt, int INewPt, int Ai, int ANewPt, int Bi, int BNewPt, int Ci, int CNewPt) {
    int x, y;
    if (ORank > NewRank) {
        // Розрахунок x і y
        x = ORank - ORank * NewRank;
        y = DNewPt - D;
        // Перевірка хешів
        if (Ai == hash(ANewPt) && Bi == hash(BNewPt)) {
            return true; // Вузол приймається
        } else {
            return false; // Вузол відхиляється
        }
    } else {
        // Розрахунок x і y
        x = NewRank * ORank - ORank;
        y = INewPt - NewRank;

        // Перевірка хешів
        if (Ai == hash(ANewPt) && Ci == hash(CNewPt)) {
            return true; // Вузол приймається
        } else {
            return false; // Вузол відхиляється
        }
    }
}
int main() {
    // Вхідні дані
    int ORank = 10;
    int NewRank = 5;
    int D = 3;
    int DNewPt = 7;
    int INewPt = 9;
    int Ai = 25;
    int ANewPt = 5;
    int Bi = 49;
    int BNewPt = 7;
    int Ci = 81;
    int CNewPt = 9;

    // Перевірка вузла
    if (CheckNode(ORank, NewRank, D, DNewPt, INewPt, Ai, ANewPt, Bi, BNewPt, Ci, CNewPt)) {
        printf("Node accepted.\n");
    } else {
        printf("Node discarded.\n");
    }
    return 0;
}
```

Додаток Г

Апробація отриманих результатів

МОДЕЛЬ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

Олещук Володимир Андрійович
Магістр спеціальності 122 «Комп'ютерні науки»
Західноукраїнський національний університет, Україна

Науковий керівник: Загородня Діана Іванівна
ORCID ID: 0000-0002-9764-3672
канд. техн. наук, доцент кафедри інформаційно-обчислювальних систем і управління
Західноукраїнський національний університет, Україна

Вступ

В IoT мережах дуже часто використовують протокол маршрутизації з низьким енергоспоживанням і втратами (RPL), який є вразливий до різноманітних атак. Атаки маршрутизації в IoT на основі RPL стають критичними зі збільшенням кількості додатків і пристроїв IoT у всьому світі. Для боротьби з атаками маршрутизації в Інтернеті речей на основі RPL було запропоновано кілька рішень безпеки, таких як методи машинного навчання, системи виявлення вторгнень і підходи на основі довіри. Дослідження показують, що безпека на основі довіри для Інтернету речей можлива завдяки простому інтегруванню та обмеженню ресурсів розумних пристроїв.

Було запропоновано модель на основі безпеки, мобільності та довіри, яка спирається на ретельно підібрані фактори та показники довіри, включаючи показники на основі мобільності.

Модель безпечної маршрутизації

Запропонований дизайн моделі для безпеки протоколу маршрутизації з низьким енергоспоживанням в основному складається з двох етапів: формування довіри та виявлення атак. Формування довіри включає ідентифікацію показників довіри, обчислення показників довіри, розрахунок індексу довіри, рейтинг довіри та моніторинг довіри. Другий етап включає виявлення атак та ізоляцію шкідливих вузлів.

На рисунку 1 зображено системну модель, включаючи різні фази та потоки того, як довіра поширюється протягом операції. Фаза формування довіри та фаза виявлення атак були додатково розділені на підетапи.

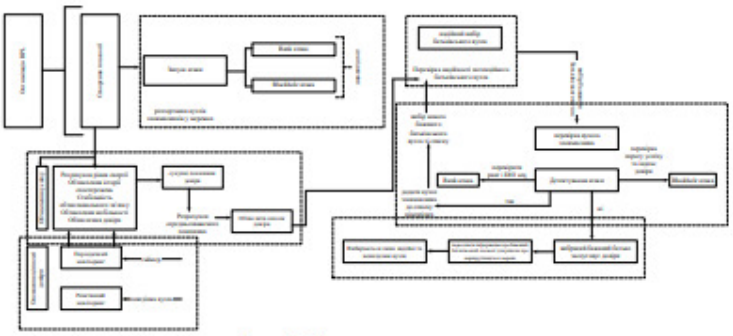


Рис. 1. **Системна модель**

Модель дотримується специфікації RPL RFC 6550 [1] для ініціалізації нормальної схеми маршрутизації. Подібним чином, топологія створюється відповідно до функціонування та функцій протоколу за замовчуванням, що в запропонованій моделі називається створенням топології. Вузли зловмисників розгортаються в мережі для прикладів атак Rank і Blackhole.

Метрики довіри, що використовуються для забезпечення безпеки мереж IoT і маршрутизації, детально досліджувались в роботі [2]. Для моделі розглядаються найбільш відповідні показники довіри, включаючи історичні спостереження, рівень енергії, пряму довіру та рекомендовану довіру. Модель включає мобільність вузлів, враховуючи метрики на основі мобільності в обчисленні довіри. Використовуючи розрахунки метрик довіри, розраховується індекс довіри. Обчислене значення довіри підтримується динамічним шляхом призначення відповідних ваг (w) для розрахунку кожного показника довіри.

Концепція нечіткого порогового механізму використовується в моделі для оцінки рейтингу довіри [3]. Остаточне значення індексу довіри розраховується за допомогою рівняння (1).

$$TrustIndex = \omega_1(TM_{SR}) + \omega_2(TM(H_0)) + \omega_3(TM_{EL}) + \omega_4(TM_{LLS}) + \omega_5(TM_{Mobility}) + \omega_6(TM_{RT}) \quad (1)$$

де $(w_1 + w_2 + w_3 + w_4 + w_5 + w_6) = 1$.

Поточним або прямим значенням довіри надається більша вага, ніж історичні спостереження. Індекс ступеня довіри, оцінюється за

допомогою нечіткого судження і складається з п'яти кортежів, визначених як $T = [t_1, t_2, t_3, t_4, t_5]$, з такими рівнями довіри, відповідно, [«Не довіряю», «Погано довіряю» , «Чесна довіра», «Добра довіра», «Повна довіра». Визначені рівні довіри відповідають заданим діапазонам значень довіри, як [0,0–0,20, 0,21–0,45, 0,46–0,70, 0,71–0,90, 0,91–1,00].

Висновки. У роботі було запропоновано модель безпечної маршрутизації для мереж Інтернету речей (IoT), яка враховує обмеження ресурсів пристроїв, вразливості протоколу RPL та сучасні завдання безпеки. Зокрема, досліджено й інтегровано механізми формування довіри, виявлення атак та ізоляції шкідливих вузлів.

Запропонована модель дає можливість підвищити надійність IoT-мереж та створює перспективи для подальшого вдосконалення протоколів маршрутизації в умовах обмежених ресурсів і зростаючих кіберзагроз.

Список використаних джерел:

1. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, [Electronic resource], Mode of access: https://datatracker.ietf.org/doc/html/rfc6550
2. Muzammal, S.M.; Murugesan, R.K.; Jhanjhi, N.Z. A comprehensive review on secure routing in Internet of Things: Mitigation methods and trust-based approaches. IEEE Internet Things J. 2020, 8, 4186–4210.
3. Dai, C.; Gong, W. Model of services trust threshold assess based on fuzzy theory. In Proceedings of the 2010 2nd International Conference on E-Business and Information System Security, EBISS 2010, Wuhan, China, 22–23 May 2010; pp. 85–88.


МАТЕРІАЛИ VIII МІЖНАРОДНОЇ
СТУДЕНТСЬКОЇ НАУКОВОЇ
КОНФЕРЕНЦІЇ
АКТУАЛЬНІ ПИТАННЯ ТА
ПЕРСПЕКТИВИ ПРОВЕДЕННЯ
НАУКОВИХ ДОСЛІДЖЕНЬ
ISO
М. ДНІПРО, УКРАЇНА
13 ГРУДНЯ
2024 РІК

СЕКЦІЯ 18.
ФІЗИКО-МАТЕМАТИЧНІ НАУКИ

СЕКЦІЯ 19.
СОЦІОЛОГІЯ ТА СТАТИСТИКА

СЕКЦІЯ 20.
ФІЛОЛОГІЯ ТА ЖУРНАЛІСТИКА

Олещук Володимир Андрійович, магістр спеціальності 122 "Комп'ютерні науки"
Західноукраїнський національний університет, Україна

Науковий керівник: Загородня Діана Іванівна, канд.техн.наук, доцент кафедри інформаційно-обчислювальних систем і управління
Західноукраїнський національний університет, Україна

СИСТЕМА АНАЛІЗУ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Вступ

В Інтернеті речей все, що нас оточує, можна додати до комунікаційної мережі та підключити до традиційного Інтернету, такі пристрої можуть вільно спілкуватися, обмінюватися інформацією. «Речі» IoT відносяться до інтелектуальних пристроїв, які мають зв'язок і доступ до Інтернету. Спеціальний протокол маршрутизації [1] потрібен для керування та організації цих інтелектуальних пристроїв для ефективних і безпечних мереж, а також для їх інтеграції з традиційним Інтернетом. Він дозволяє ефективно використовувати енергію розумних пристроїв, обчислювальні ресурси, створювати гнучку топологію та маршрутизацію даних. Проте такий протокол маршрутизації не враховує безпеку мережі на стадії розгортання мережі та не забезпечує безпеку мережі за допомогою механізмів відновлення маршрутизації, коли мережа побудована, і тому вона не зможе своєчасно відновитись після атаки.

Тому потрібно мати надійний механізм/систему для аналізу безпечної маршрутизації.

Тестування системи

Кожен вузол у тестовій мережі є комбінацією апаратного та програмного вузла, а код алгоритму вбудовано в тестовий вузол. Кожен вузол з'єднаний з комп'ютером за допомогою послідовного порту для відображення даних зв'язку між вузлами.

Програмне забезпечення відображає топологію та передачу даних усього мережевого протоколу для перевірки маршрутизації. Мережа відображається шлюзом після сповіщення про топологію. Повна топологія мережі показана на рисунку 1. Після IPv6 адреси кожного вузла, показується температура та вологість в топології для імітації даних, зібраних датчиками. Вузол b6fc представляє вузол шлюзу, вузол b5b4 і вузол a1b7 представляють головний вузол кластера, а інші вузли представляють загальний вузол.

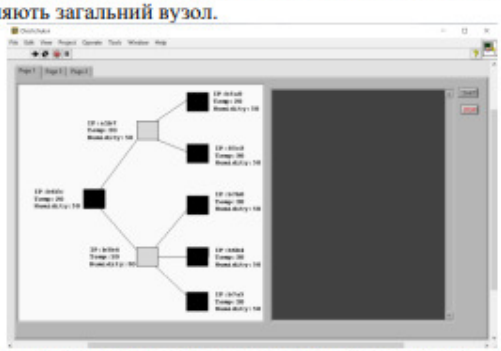


Рис. 1. **Топологія мережі до ввімкнення багатошляхової маршрутизації**

Вузол 85c2 вибирається, як вузол джерела передачі даних, вузол b7b0 вибирається, як вузол призначення для прийому даних, де вузол призначення та вузол джерела знаходяться в різних кластерах. Вихідний вузол і адресат підключаються до дисплея, щоб показати надсилання та отримання.

Багатошляховість демонструється на вихідному вузлі. Якщо багатошляховий маршрут не ввімкнено, програмне забезпечення для відображення не буде показувати резервний шлях для з'єднання в топології. У цей момент вихідний вузол надсилає дані, а кінцевий вузол може отримати один пакет даних.

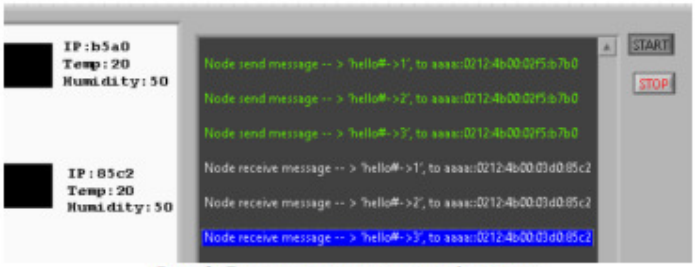


Рис. 2. **Резервний шлях не ввімкнено**

Коли багатошляховість увімкнено, інформація про відкриття багатошляховості завантажується вихідним вузлом у програмне забезпечення для відображення топології шлюзу. Вихідний вузол відображає підключення до резервного шляху. На рисунку 3 пунктирна лінія позначає шлях резервного копіювання.

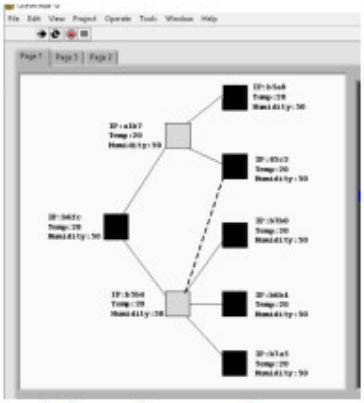


Рис. 3. **Топологія мережі після ввімкнення багатошляхової маршрутизації**

Після того, як шлях резервного копіювання ввімкнено, вузол-джерело надсилає дані на вузол призначення, у вікні послідовного відображення показується, що вузол призначення отримав два пакети даних. Конкретний процес показаний на рисунку 4.

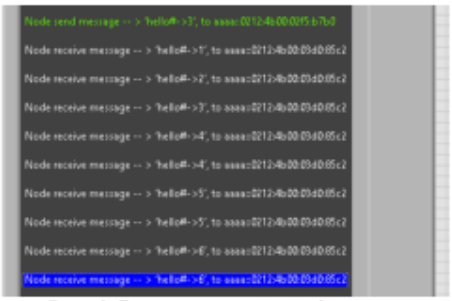


Рис. 4. **Резервний шлях увімкнено**

Висновки. Було реалізовано тестову мережу, яка побудована для перевірки продуктивності протоколу маршрутизації, за допомогою якого можна моделювати атаки типу Blackhole [2] та Rank [3]. Результати показують, що протокол може ефективно протистояти таким типам атак і забезпечувати надійну маршрутизацію даних. Незначне зростання енергоспоживання є виправданою ціною підвищення безпеки та ефективності мережі IoT.

Список використаних джерел:

1. T. Winter, P. Thubert, A. Brandt, et al. RPL: IPv6 routing protocol for low-power and lossy networks,RFC6550, s.l.: IETF Mar. 2012. [Online]. Available: http://tools.ietf.org/html/rfc6
2. Boudouaia, Mohammed Amine, et al. "Security against rank attack in RPL protocol." IEEE Network 34.4 (2020): 133-139.
3. HaddadPajouh, Hamed, et al. "A survey on internet of things security: Requirements, challenges, and solutions." Internet of Things 14 (2021): 100129.