**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**
Інститут телекомунікаційних систем
(повна назва інституту/факультету)

Кафедра телекомунікацій
(повна назва кафедри)

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ В.С. Явіся
(підпис) (ініціали, прізвище)
“___”_____2018 р.

# Магістерська дисертація

**на здобуття ступеня магістра**

зі спеціальності 172 Телекомунікації та радіотехніка _____
(код і назва)

на тему: Розвиток методів захисту інформації в безпроводових сенсорних мережах

Виконала: студентка VI курсу, групи ТЗ-61м
_____Туранська Олена Сергіївна_____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник_____д.т.н., професор Лисенко О.І. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

**Національний технічний університет України**
**«Київський політехнічний інститут імені Ігоря Сікорського»**

Інститут (факультет) Інститут телекомунікаційних систем _____
(повна назва)

Кафедра Телекомунікаційних систем _____
(повна назва)

Рівень вищої освіти – другий (магістерський)

Спеціальність 172 Телекомунікації та радіотехніка_____
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.С. Явіся
(підпис) (ініціали, прізвище)

“___”_____2018 р.

**ЗАВДАННЯ**
**на магістерську дисертацію студенту**
Туранській Олені Сергіївні
(прізвище, ім’я, по батькові)

1. Тема дисертації: Розвиток методів захисту інформації в безпроводових сенсорних мережах
науковий керівник дисертації Лисенко Олександр Іванович, д.т.н., професор
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «___»_____ 20__ р. №_____
2. Термін подання студентом дисертації «___»_____ 20__ р.
3. Об’єкт дослідження безпроводові сенсорні мережі
4. Предмет дослідження атаки на мережу та методи захисту інформації
5. Перелік питань, які потрібно розробити
   - дослідження особливостей експлуатації БСМ;
   - дослідження показників надійності системи безпеки в БСМ;
   - визначення найрозповсюдженіших атак на мережі такого типу;
   - дослідження існуючих методів захисту інформації в БСМ;
   - розробка математичної моделі запропонованого методу покращення захисту інформації в БСМ.

6. Перелік ілюстративного матеріалу

Плакат №1 «Тема, мета та завдання магістерської дисертації»

Плакат №2 «Публікації за результатами магістерської дисертації»

Плакат №3 «Характеристики та вимоги до БСМ»

Плакат №4 «Аналіз атак на безпроводові сенсорні мережі»

Плакат №5. «Аналіз запропонованої структури протоколу маршрутизації»

Плакат №6. «Висновки»

7. Перелік публікацій

1. Туранська О.С., Лисенко О.І. Захист інформації у безпроводових сенсорних мережах // Туранська О.С., Лисенко О.І. - «Проблеми телекомунікації»: одинадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-17) 18-21 квітня 2017 р., К.: с. 420…422;
2. Туранська О.С., Петрова В.М. Керівні принципи та підходи до захисту інформації у безпроводових сенсорних мережах // Туранська О.С., Петрова В.М. - «Проблеми телекомунікації»: дванадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-18) 16-20 квітня 2018 р., К.: с. 383…385.

8. Дата видачі завдання _____

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів виконання магістерської дисертації | Термін виконання етапів магістерської дисертації | Примітка |
|---|---|---|---|
| 1 | Розробка, оформлення узгодження та затверджень технічного завдання на роботу. | 30.09.16 | Робочі матеріали |
| 2 | Вибір напрямку досліджень. Аналітичний огляд інформаційних матеріалів. | 25.10.16 | Робочі матеріали |
| 3 | Опрацювання першого розділу. Дослідження основних параметрів БСМ та основних проблем, які виникаю при втіленні методів захисту інформації | 28.12.16 | Робочі матеріали |
| 4 | Підготовка тез та доповіді на конференцію ПТ-17 | 28.02.17 | Тези |
| 5 | Опрацювання другого розділу. Вивчення атак, які відбуваються на мережу БСМ. Ознайомлення з їх особливостями та принципах впливу | 20.04.17 | Робочі матеріали |
| 6 | Опрацювання другого розділу. Ознайомлення з існуючими методами захисту інформації в безпроводових сенсорних мережах. | 29.05.17 | Робочі матеріали |
| 7 | Опрацювання третього розділу. Розробка структури та математичної моделі для протоколу маршрутизації в БСМ | 01.11.17 | Робочі матеріали |
| 8 | Підготовка тез та доповіді на конференцію ПТ-18 | 22.02.18 | Тези |
| 9 | Оформлення дипломної роботи згідно діючих правил | 15.04.18 | Рукопис |

Студент _____ /О.С. Туранська/
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ /О.І. Лисенко/
(підпис) (ініціали, прізвище)

# РЕФЕРАТ

Робота містить 67 сторінку, 4 ілюстрацій, 1 таблиць. Було використано 23 джерела інформації.

**Актуальність.** В наш час проблема захисту інформації є дуже важливою і для її вирішення витрачається дуже багато ресурсів. Оскільки, безпроводові сенсорні мережі в наш час стають все популярнішими і знаходять своє застосування в багатьох галузях нашого життя, збільшуються і вимоги до такого типу мереж. Безпроводовий зв'язок і особливості експлуатації таких мереж вимагають особливого підходу до питання захисту безпеки в БСМ. Тому дана тема є актуальною.

**Метою** даної роботи є дослідити особливості експлуатації безпроводових сенсорних мереж, атаки на мережу та існуючі методи захисту інформації. А також запропонувати новий метод захисту інформації в БСМ.

Для досягнення поставленої мети в роботі вирішуються наступні задачі:

- дослідження особливостей експлуатації БСМ;
- дослідження показників надійності системи безпеки в БСМ;
- визначення найрозповсюдженіших атак на мережі такого типу;
- дослідження існуючих методів захисту інформації в БСМ;
- розробка математичної моделі запропонованого методу покращення захисту інформації в БСМ.

**Об’єкт дослідження** – безпроводові сенсорні мережі.

**Предмет дослідження** – атаки на мережу та методи захисту інформації.

**Наукова новизна** роботи полягає у створенні покращеного методі захисту інформації в безпроводових сенсорних мережах.

**Апробація.** Результати, що включені у дану роботу, були оприлюднені на двох міжнародних наукових конференціях:

1. XI Міжнародна Науково-технічна Конференція "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ 2017" 18.04-21.04.2017р. на базі Інституту телекомунікаційних систем та НДІ телекомунікацій НТУУ "КПІ";

2. XII Міжнародна Науково-технічна Конференція "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ 2018" 16.04-20.04.2018р. на базі Інституту телекомунікаційних систем та НДІ телекомунікацій КПІ ім. Ігоря Сікорського.

**Публікації:**

3. Туранська О.С., Лисенко О.І. Захист інформації у безпроводових сенсорних мережах // Туранська О.С., Лисенко О.І. - «Проблеми телекомунікації»: одинадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-17) 18-21 квітня 2017 р., К.: с. 420…422;
4. Туранська О.С., Петрова В.М. Керівні принципи та підходи до захисту інформації у безпроводових сенсорних мережах // Туранська О.С., Петрова В.М. - «Проблеми телекомунікації»: дванадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-18) 16-20 квітня 2018 р., К.: с. 383…385.

**Ключові слова:** безпроводова сенсорна мережа, сенсорний вузол, захист інформації, атака на мережу, математична модель.

## ABSTRACT

The work contains 67 pages, 4 illustrations, 1 tables, 23 sources of information were used.

**Topicality.** Nowadays the problem of information security is very important and a lot of resources are spent to solve it. Because wireless sensory networks are becoming more popular in our day and are used in many areas of our lives, requirements for such networks also increase. Wireless communication and the features of the operation of such networks require a special approach to security issues in the WSN.

**The aim** of this work is to explore the features of the operation of wireless sensor networks, attacks on the network and existing methods of information protection. And also to propose a new method of information security in WSN.

To achieve this goal, the following tasks were set:

- study of the features of the operation of the WSN;
- study of reliability indicators of the security system in the WSN;
- determining the most common attacks on the network of this type;
- research of existing methods of information security in WSN;
- development of a mathematical model of the proposed method for improving the protection of information in WSN.

**The object** of research - wireless sensor networks.

**The subject** of research - attacks on the network and methods of information protection.

**Scientific novelty** of work is to create an improved method for protecting information in wireless sensory networks.

**Approbation.** The results included in this work were presented at two international conferences:

1. XI International Scientific Conference "Problems TELECOMMUNICATIONS 2017" 18.04-21.04.2017r. at the Institute

of Telecommunication Systems and Telecommunications Research Institute KPI them. Igor Sikorsky.

2. XII International Scientific Conference "Problems TELECOMMUNICATIONS 2018" 16.04-20.04.2018r. at the Institute of Telecommunication Systems and Telecommunications Research Institute "KPI";

Publications:

1. Turanska OS, Lysenko OI Information Security in Wireless Sensor Networks // Turanska OS, Lysenko OI - "Problems of Telecommunications" eleventh international scientific conference dedicated to the Day of Science and World Day of Telecommunications (PT-17) 18-21 April 2017, K .: with. 420…422;
2. Turanska OS, Petrova VM Guiding principles and approaches to information security in Wireless Sensor Networks// Turanska OS, Petrova VM - "Problems of Telecommunications", the twelfth international scientific conference dedicated to the Day of Science and World Day of Telecommunications (PT-18), 16-20 April 2017, K .: p. 383…385;

**Key words:** wireless sensor networks, sensory node, security of information, attack on the network, mathematical model

**ЗМІСТ**

## ПЕРЕЛІК СКОРОЧЕНЬ

| | | |
|---|---|---|
| **AES** | Advanced Encryption Standard | Симетричний алгоритм блочного шифрування |
| **AODV** | Ad hoc On-Demand Distance Vector | Протокол динамічної маршрутизації для мобільних ad-hoc мереж |
| **DES** | Data Encryption Standard | Симетричний стандарт шифрування даних |
| **DoS** | Denial of Service | Відмова в обслуговуванні |
| **DSR** | Dynamic Source Routing | Динамічна маршрутизація від джерела |
| **IDEA** | International Data Encryption Algorithm | Міжнародний алгоритм шифрування даних |
| **IEEE** | Institute of Electrical and Electronics Engineers | Інститут інженерів з електротехніки та електроніки |
| **FHSS** | Frequency Hopping Spectrum Spreading | Псевдовипадкове перестроювання робочої частоти |
| **MAC** | Media Access Control | Управління доступом до носія |
| **OSI** | Open Systems Interconnection Basic Reference Model | Базова еталонна модель взаємодії відкритих систем |
| **RTS** | Request To Send | Запит на відправку |
| **CTS** | Clear To Send | Дозвіл на відправку |
| **SPINS** | Security Protocols for Sensor Networks | Протокол захисту для сенсорних мереж |
| **TCP** | Transmission Control Protocol | протокол керування передачею |
| **UDP** | User Datagram Protocol | Протокол датаграм користувача |
| **БС** | | базова станція |
| **ОВ** | | основний вузол |
| **ПВ** | | підпорядкований вузол |

# ВСТУП

Безпека і конфіденційність – є важливими проблемами у всіх типах мереж. Ці проблеми мають особливе значення в безпроводових сенсорних мережах, оскільки унікальні характеристики цих мереж і цілі програми, яким вони служать, роблять їх привабливими мішенями для проникнень і інших атак.

У таких додатках як спостереження і оцінка поля бою, відстеження цілей, моніторинг цивільної інфраструктури, таких як мости і тунелі, і оцінка зон лиха, щоб ввести дії екстреного реагування, будь-яке порушення безпеки, дискредитація інформації або порушення коректної поведінки додатки можуть мати дуже серйозні наслідки. Сенсорні мережі часто використовуються у віддалених областях, залишені працювати без нагляду, і тим самим стають легкою мішенню для фізичних атак, несанкціонованого доступу і пошкоджень. Сенсорні вузли зазвичай дуже обмежені ресурсами і працюють в жорстких умовах, що в подальшому полегшує дискредитацію і ускладнює знаходження відмінностей порушень безпеки від збоїв вузлів, змінюючи якість каналу і інші знайдені проблеми в сенсорних мережах. У висновку, ці обмеження ресурсів потребують механізми безпеки, які розраховані на додатки БСМ, так щоб ефективно використовувати обмежені ресурси.

Для вирішення проблеми безпеки та захисту інформації в безпроводових сенсорних мережах в наш час проводиться багато досліджень, але в наш час технології розвиваються дуже швидко і з’являються все новіші методи атак, тому такий процес є актуальним на даний момент і потребує постійних досліджень та оновлень методів боротьби з атаками

У першому розділі розглянуто основні принципи мережевої безпеки, проблеми та труднощі, які виникають при втіленні існуючих моделей та принципів в безпроводових сенсорних мережах. Розглянуто особливості

БСМ, які потрібно враховувати при створенні методів захисту інформації, а також розглянули основні показники для оцінки надійності мережі.

У другому розділі розглянуто та проаналізовано найпоширеніші варіанти атак на безпроводові сенсорні мережі. Розглянуто їх особливості, характер впливу та можливі наслідки. Оскільки безпроводові сенсорні мережі розгортають на віддалених територіях і без нагляду, захиститись від атак ще складніше. В наш час вони можуть здійснюватися на всіх рівнях моделі OSI, тому вирішення цієї проблеми є дуже важливим.

У третьому розділі описується запропонована структура протоколу маршрутизації для безпроводових сенсорних мереж, яка дозволяє забезпечити надійну аутентифікацію вузлів в мережі і економити ресурси вузла.

# РОЗДІЛ 1. ОСНОВНІ ПРИНЦИПИ МЕРЕЖЕВОЇ БЕЗПЕКИ

Комп'ютерна і мережева безпека - це сукупність всіх стратегій, механізмів і служб, які надають комп'ютерній системі або мережі необхідний захист від несанкціонованого доступу та її непередбаченому використанню. Більшість механізмів безпеки створено для трьох основних моделей безпеки: приватна власність, цілісність і доступність. Нижче ці моделі описано більш детально:

Конфіденційність: Механізми безпеки повинні гарантувати, що тільки передбачуваний одержувач може правильно інтерпретувати повідомлення, і що несанкціонований доступ і використання унеможливлені. Наприклад, конфіденційність гарантує, що секретна інформація, така як номер соціального страхування людини або інформація про кредитну картку не може бути отримана неуповноваженою особою.

Цілісність: Механізми безпеки повинні гарантувати, що повідомлення не може бути змінено, оскільки воно передається від відправника до одержувача, тобто неавторизовані користувачі не повинні мати змогу знищити або змінити зміст секретної інформації.

Доступність: Механізми безпеки повинні гарантувати, що система або мережа і її додатки можуть виконати завдання в будь-який час без переривання. Доступність часто вимірюється в процентному співвідношенні в робочому стані і в стані простою.

Рис1.1 ілюструє приклади атак на передачу між відправником і вказаним одержувачем. Підслуховування, відноситься до прийому повідомлення неавторизованою особою. Цього можна запобігти, використовуючи заходи щодо забезпечення конфіденційності. Атака "людина посередині" відноситься до ситуації, де неавторизована особа або самі системні позиції між відправником і отримувачем, впливають на повідомлення відправника і в результаті до одержувача ретранслюються перервані та змінені повідомлення (в такій ситуації

одержувач вважає, що отримане повідомлення прибуло безпосередньо від початкового відправника). Це ілюструє потребу в механізмах забезпечення цілісності. Нарешті, атака "відмова в обслуговуванні" відноситься до спроби противника зірвати передачу або роботу послуги, надану відправником. Наприклад, противник може так завантажити відправника запитами і завданнями, що відправник не в змозі буде своєчасно передати своє повідомлення одержувачу. Цей тип атаки вимагає механізмів безпеки, які гарантують доступність.

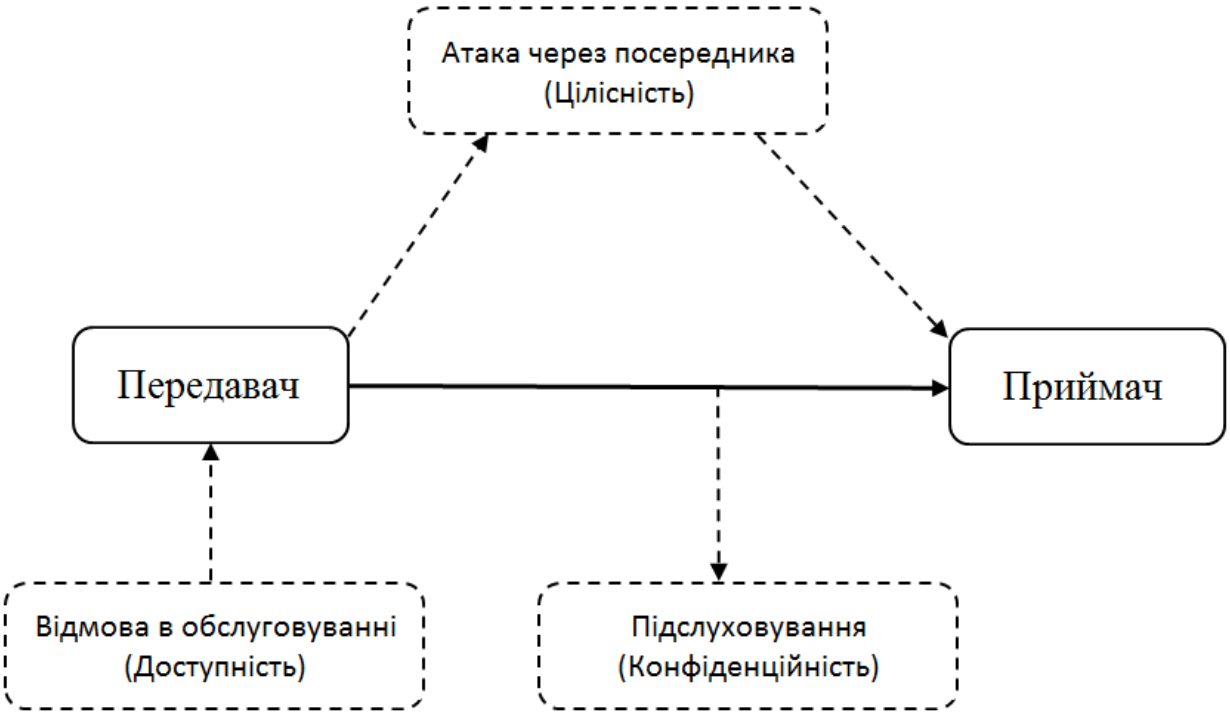


Рисунок 1.1 Приклади атак на БСМ.

Як механізм безпеки також використовується аутентифікація. Вона відноситься до процесу встановлення або підтвердження ідентифікації користувача або пристрою, гарантуючи, що повідомлення прибуло від того, хто стверджує, що його послав. Так цифрові підписи часто використовуються, щоб підтвердити і аутентифікацію і непідробленість, але також використовуються для того, щоб впевнитись в тому, що повідомлення не було змінено (тобто, цілісність збережено).

У всіх типах зв'язку мереж є кілька фундаментальних механізмів безпеки, які можуть бути використані, щоб забезпечити конфіденційність, цілісність і доступність. Криптографія - процес приховування і захисту інформації, що використовує механізми кодування та декодування. У криптографії з використанням симетричного ключа, між двома сторонами, які встановлюють зв'язок, використовується єдиний ключ для шифрування і дешифрування повідомлень.

Головна проблема у використанні симетричного ключа у криптографії - це безпечний розподіл ключів, які використовуються в даному підході, між відправником та приймачем. Популярними прикладами механізмів шифрування з використанням симетричного криптографічного ключа включає DES, AES і IDEA.

На відміну від цього підходу, шифрування з відкритим ключем, добре відомий алгоритм RSA або протокол узгодження ключів Diffie-Hellman, покладається на пару ключів. Вузол генерує і закритий і відкритий ключі, де закритий ключ ніколи не буде передаватися іншому вузлу в мережі. З іншого боку, відкритий ключ, може вільно використовуватись для передачі будь-кому в мережі. Будь-яке повідомлення, зашифроване закритим ключем, може бути дешифровано тільки відповідним відкритим ключем (наприклад, він може використовуватися, щоб аутентифікувати дані відправника). Будь-яке повідомлення, зашифроване відкритим ключем, може бути дешифровано тільки відповідним закритим ключем (наприклад, він може бути використаний для забезпечення конфіденційності).

## 1.1 Особливості використання безпроводових сенсорних мережах

Безпека залишалась проблемою для обчислювальних системах і мережах протягом декількох десятиліть, під час яких типи атак, заходи безпеки і механізми, що протистоять їм, удосконалилися і значно розвинулися, особливо із-за широкого застосування глобальної мережі

Інтернет. У порівнянні з традиційними атаками і механізмами безпеки, розробленими для мережі Інтернет, при застосуванні безпроводових сенсорних мереж виникає безліч унікальних проблем, які потрібно розглянути, звертаючись до проблем безпеки, які можуть виникнути в додатках сенсорної мережі:

1. Обмеження ресурсу: Традиційні механізми безпеки, які мають високі витрати, не придатні для БСМ з обмеженими ресурсами. Багато механізмів безпеки в обчислювальному відношенні дорогі або вимагають зв'язку з іншими вузлами чи "віддаленими" пристроями (наприклад, з метою авторизації), що призводить до енергетичних витрат. Маленькі сенсорні пристрої також обмежені в своїй доступній пам'яті і ємностях пристрою, що запам'ятовує. У загальних сенсорних пристроїв є дуже обмежені обсяги пам'яті, наприклад, у пристроїв TelosB тільки 10-кБайт RAM і 48-кБайт доступної флеш-пам'яті. Традиційні алгоритми безпеки, що вимагають істотної кількості пам'яті, неможливі для таких сенсорів.
2. Відсутність центрального управління: Часто неможливо мати центральну точку управління в сенсорних мережах, наприклад, із-за їх великого масштабу, обмежень ресурсу і мережевої динаміки (топологічних змін, поділу мережі). Тому, рішення щодо забезпечення безпеки повинні бути децентралізовані, і вузли повинні співпрацювати, для досягнення безпеки.
3. Віддалене розташування: Перша лінія захисту проти атак безпеки - це забезпечення тільки контрольованого фізичного доступу до сенсорного вузла. Багато БСМ залишають без обслуговування, тому що вони управляються в віддалених і важкодоступних місцях, розгорнутих в середовищах, відкритих для публічного доступу, або настільки великих, що буде неможливо постійно контролювати і захистити сенсорні вузли від атак. Ці проблеми заважають запобігати несанкціонованому доступу і виявляти підробку в багатьох сенсорних пристроях, особливо, тому що

низька вартість багатьох сенсорних вузлів може завадити вдосконаленню заходів безпеки.

4. Зв'язок, схильний до втрат: Пакети в БСМ можуть бути втрачені або пошкоджені через низку причин, включаючи помилки каналу, провали в маршрутизації і колізії. Це може перешкоджати деяким механізмам безпеки або їх можливості отримувати критичні звіти події.

З іншого боку, певні характеристики сенсорних мереж спрощують умови безпеки. Наприклад, самоврядування і самовідновлення природи безпроводових сенсорних мереж можуть дозволити їм продовжувати працювати, навіть якщо сенсор або усі регіони сенсорної мережі були поставлені під загрозу. Надмірність в сенсорних мережах дозволяє збирати інформацію про події в середовищі, навіть коли деякі сенсори недоступні через атаки. Крім того, ця надмірність може використовуватися, щоб виявити, ізолювати, і замаскувати потенційно скомпрометовані вузли.

Дані, зібрані сенсорами, можуть містити конфіденційну інформацію і не повинні бути пропущені до несанкціонованих пристроїв. Далі, ключі шифрування і інформація про самі сенсори (наприклад, ідентифікаційні дані, місце розташування, і т.д.), повинні бути захищені, щоб запобігти підслуховуванню і атаки, засновані на аналізі потоків інформації. Ці проблеми вимагають заходів, які забезпечують конфіденційність даних для сенсорних мереж. Цілісність потрібно, щоб перешкоджати тому, щоб противники змінили дані сенсора, наприклад, з метою введення помилкових даних і отже впливу відповіді на сенсорні дані. Аутентифікація необхідна, щоб гарантувати, що будь-які дані, поширювані в сенсорної мережі, походять з коректного джерела, особливо коли єдиний вузол керує всією мережею (наприклад, базова станція, що встановлює маршрути або розподіляє широкомовно інформацію про дерево). Далі, у багатьох атак безпеки в сенсорних мережах є мета - зруйнувати коректне функціонування мережі в цілому, вимагаючи заходів, які гарантують мережеву доступність. Додаткова вимога в сенсорних мережах - потреба в актуальності даних, яка гарантує, що

дані сенсора недавні, і ніякі старі записи таких даних не відтворюються. Це особливо важливо для ключових схем розподілу, наприклад, атакуючий, міг записати спільно використані ключі, якими обмінюються в мережі і відтворити ці ключові повідомлення розподілу через деякий час. Нарешті, багато обов'язків з управління вузлом і мережею, притаманні безпроводовим сенсорним мережам, надають противникам можливості для атак. Наприклад, локалізація сенсорного вузла важлива для того, щоб правильно інтерпретувати дані сенсора для географічних протоколів маршрутизації, і для усунення надмірності. Однак багато методів локалізації вимагають обміну інформацією серед сенсорів (наприклад, маяки, які переносять позиції, мітки часу і інформацію про ідентифікаційних даних) і в таких випадках виникає потреб в шифруванні. Так само синхронізація часу в сенсорних мережах заснована на обміні повідомленнями серед сенсорних вузлів, де противник міг ввести неправдиві мітки часу, щоб збільшити помилки синхронізації серед сенсорів.

## 1.2 Проблеми, що виникають при забезпеченні захисту інформації в безпроводових сенсорних мережах

Безпроводові сенсорні мережі мають велику кількість програм у військовій, внутрішній безпеці та інших областях. Тому багато сенсорних мереж мають критично важливі завдання. Безпека має вирішальне значення для тих мереж, що використовуються в ворожих середовищах, а проблеми безпеки залишаються серйозною перешкодою для широкого застосування такого виду мереж. Питання безпеки в БСМ є більш складними, ніж у традиційних дротових комп'ютерних мережах та в Інтернеті. Більшість сенсорних мереж активно контролюють їх оточення, і часто легко виводять іншу інформацію, крім даних, що підлягають моніторингу. Такий небажаний витік інформації часто призводить до порушень конфіденційності та потрапляння інформації в навколишнє середовище. Крім того, безпровідний

зв'язок, що використовується мережами датчиків, полегшує супротив та введення шкідливих даних супротивником. Комбінація цих факторів вимагає забезпечення безпеки сенсорних мереж ще на стадії проектування, щоб забезпечити безпеку роботи, секретність та конфіденційних даних. Для вирішення проблеми затрачено значні зусилля і проведені дослідження з метою підвищення рівня безпеки безпровідних мереж. В даний час існує три рівні безпеки в бездротових мережевих середовищах [25].

Безпека в мережах датчиків ускладнюється обмеженими можливостями обладнання сенсорних вузлів та властивостями розгортання.

- Загальна вартість БСМ повинна бути настільки низькою, наскільки це можливо.
- Датчики чутливі до фізичного захоплення, але, через цільову низьку вартість, не вдасться створити пристрої, захищені від несанкціонованого доступу. Датчики використовують безпровідний зв'язок, який особливо легко прослухувати.
- Аналогічним чином, зловмисник може легко ввести шкідливі повідомлення в безпровідні мережі.
- Сучасні технології боротьби з перешкодами, такі як обмеження розповсюдження частотного сплеску та фізичний захист вузлів від вторгнення, загалом неможливі в сенсорній мережі за рахунок вимог більшої конструктивної складності та більшого енергоспоживання.
- Використання радіопередачі разом із забезпеченням малих розмірів, низької вартості та обмеженою енергією робить БСМ більш чутливими до атак на відмову в обслуговуванні.
- Спеціальна мережева топологія БСМ полегшує зловмисників для різних типів лінійних нападів, починаючи від пасивного підслуховування до активного втручання. Нападки на БСМ можуть надходити з усіх напрямків і цілей на будь-якому вузлі, що веде до витоку секретної інформації, перешкоджаючи повідомленню, висміюючи вузли тощо.

- Безпека також потребує масштабування для широкомасштабного розгортання. Найбільш сучасні стандартні протоколи безпеки були розроблені для двопартійних налаштувань і не масштабуються для великої кількості учасників.
- Існує суперечливий інтерес між мінімізацією споживання ресурсів та максимізацією рівня безпеки. Найкраще рішення насправді дає гарний компроміс між цими двома.
- Оскільки сенсорні вузли, як правило, суворо обмежені, асиметрична криптографія часто є надто дорогою для багатьох застосувань. Таким чином, перспективним підходом є використання більш ефективних симетричних криптографічних альтернатив.
- Замість цього більшість схем захисту використовують симетричну криптографію ключових слів. В обох випадках потрібно використовувати ключі для безпечного спілкування. Керування розподілом ключів не є унікальним для WSN, але знову ж таки обмеження, такі як мала місткість пам'яті, дозволяють зробити централізовані методи маніпулювання неможливими.

Метою безпеки є надання засобів безпеки для захисту від усіх видів загрози, описаних у цій главі. У роботі наведено аналіз вимог безпеки та живучості, що стосуються конструктивних цілей масштабованості, ефективності, ключових з'єднань, стійкості та надійності. Служби безпеки включають наступне: [11], [47]

Аутентифікація гарантує, що інший кінець з'єднання або ініціатор пакета - це вузол, на який вказано отримувачем. Контроль доступу запобігає несанкціонованому доступу до ресурсу. Конфіденційність захищає загальний вміст або поле в повідомленні. Також може знадобитися конфіденційність для запобігання аналізу трафіку противником. Конфіденційність не дозволяє противникам отримувати інформацію, яка може мати приватний зміст. Приватна інформація може бути отримана шляхом аналізу траєкторій, тобто частоти, джерела вузла, маршрутів тощо. Авторизація: авторизує

інший вузол для оновлення інформації (авторизація імпорту) або отримання інформації (авторизація експорту). Анонімність приховує джерело пакета або кадру. Це служба, яка може допомогти в конфіденційності вузлів та в конфіденційності даних. Підтвердження підтверджує джерело пакета. При аутентифікації джерело підтверджує свою ідентичність. Невідхилення забороняє джерелу відмовляти в тому, щоб він відправив пакет. Актуальність гарантує, що шкідливий вузол не перезавантажувати раніше захоплені пакети. Наявність переважно орієнтована на атаки DoS і є здатністю підтримувати функціональні можливості мережі без будь-яких переривань у зв'язку із загрозами безпеки. Стійкість до атак, необхідних для підтримання функціональності мережі, коли частина вузлів скомпрометована або знищена. У секретній системі датчик не повинен мати змогу читати будь-які повідомлення після його виходу з мережі. У секретній частині зворотного зв'язку приєднувальний датчик не повинен мати змогу читати будь-яке повідомлення, яке передавалось раніше. Виживання - це здатність забезпечувати мінімальний рівень обслуговування при наявності втрат потужності, збоїв або атак. Можливість змінити рівень безпеки як зміни ресурсу ресурсів - деградація служб безпеки.

Як початковий внесок у розробку парадигми захисту мереж датчиків на основі цілісного підходу до забезпечення декількох шарів у стек протоколу, Ванг [24] запропонував набір принципів для вирішення проблеми безпеки в безпроводових сенсорних мереж. Рішення в контексті цих принципів підтримує диференціальну службу безпеки, яку можна динамічно налаштовувати, щоб впоратись із зміною стану мережі.

- Безпека мережі визначається безпекою всіх шарів.
- У масово розподіленій мережі, заходи безпеки повинні бути піддані динамічній реконфігурації та децентралізованому управлінню.

- У певній мережі в будь-який час витрати, понесені внаслідок заходів безпеки, не повинні перевищувати витрат, нарахованих через ризики безпеки на той час.
- Якщо фізична безпека вузлів у мережі не гарантується, заходи безпеки повинні бути стійкими до фізичного втручання в області експлуатації.

Цілісний підхід має на меті покращити ефективність безпроводових сенсорних мереж щодо безпеки, витривалість та з'єднання при зміні екологічних умов. Цілісний підхід до проблем безпеки полягає у залученні всіх шарів для забезпечення загальної безпеки в мережі. Для такої мережі єдине рішення безпеки для одного шару може бути не ефективним рішенням, а безпека повинна бути забезпечена для всіх шарів стек протоколу, який використовує цілісний підхід, може бути кращим варіантом.

Оскільки сенсорні мережі створюють унікальні проблеми, традиційні методи захисту, що використовуються в традиційних мережах, не можуть бути застосовані безпосередньо. Через різноманітних обмежень у БСМ при розробці схеми безпеки слід уважно розглянути наступні аспекти: енергоефективність, щільність вузла та надійність, адаптивна безпека, самостійна конфігурація, простота та локальний ідентифікатор. Для ефективного вирішення вищезазначених проблем може виявитися вигідним порушити правила звичайного накладання на мережеве програмне забезпечення.

Складні схеми безпеки виявилися неадекватними та/або неефективними внаслідок таких обмежень:

1. Резервне забезпечення безпеки: без систематичного перегляду окремі протоколи безпеки, розроблені для різних індивідуальних протокольних шарів, можуть надавати резервні служби безпеки і, відповідно, споживають більше ресурсів БСМ, ніж це необхідно.

2. Неадаптовані служби безпеки. Оскільки атаки на БСМ відбуваються з будь-яких шарів будь-яких протоколів, схема контратаки на деякому рівні протоколу навряд чи гарантує безпеку постійно.
3. Неефективність енергії. При розробці сенсорної мережі дуже важливою проблемою, яку ми повинні враховувати, є енергоефективність. Дизайн енергоефективності не можна повністю вирішувати на будь-якому окремому шарі в мережі.

Завдяки своїй крайній вразливості, задовільне забезпечення безпеки в БСМ має вирішальне значення. Однак, безпека на основі розшарованого дизайну часто є недостатньою. Більш того, високо захищений механізм неминуче часто споживає досить велику кількість системних ресурсів, що, у свою чергу, може ненавмисно викликати атаку служби безпеки і призвести до відмови в обслуговуванні. Як наслідок, дизайн поперечних шарів забезпечує кращу безпеку.

Кожен криптографічний дизайн базується на принципах плутанини та розповсюдження, як це видно в оригінальному документі Шеннона "Теорія систем комунікації таємності" [21]. Плутанина відноситься до секретних ключів і текстів шифру. Дифузія спрямована на зменшення будь-якого статистичного зв'язку між текстовим повідомленнями та текстом шифру, наскільки це можливо.

Цікаво, що таке дифузне співвідношення між входом і виходом також може бути знайдено у безпроводовому зв'язку. Добре досліджено, що навіть невелика зміна фізичного положення, антенної орієнтації або тонких змін фізичного середовища сильно впливають на сигнал, виміряний на приймачі, особливо в передавальних системах, що не мають прямої видимості. Замість використання заміщення та транспозиції, щоб викликати хаотичні властивості, фізичні явища поширення хвилі, такі як відбиття, дифракція, розсіювання та затухання, мають властивості, подібні до плутанини та дифузії. У контексті безпеки це означає, що визначення точної фізичної конфігурації, яка створює певний набір властивостей сигналу у приймачі,

може дорівнювати вичерпній атаці грубої сили на пошуковий простір, визначений наявними фізичними положеннями, частотами, рівнями потужності передачі тощо. Ідея бездротової безпеки полягає в тому, щоб використовувати бездротові властивості, запропоновані самим способом для розробки легких механізмів безпеки.

Можливі наступні показники, щоб оцінити, чи схема безпеки відповідає вимогам безпроводових сенсорних мереж.

- Безпека: схема безпеки повинна відповідати вимогам, які обумовлені умовами використання БСМ.
- Відмова: якщо кілька вузлів скомпрометовані, схема захисту повинна все ще захищатись від нападів.
- Енергоефективність: схема захисту повинна бути енергоефективною, щоб максимально збільшити тривалість роботи вузла та мережі.
- Гнучкість: управління ключами повинно бути гнучким, щоб передбачати різні способи розгортання мережі, такі як випадкове розсіяння вузлів та попередньо визначений розмір вузла.
- Масштабованість: схема захисту повинна мати змогу масштабувати, не порушуючи вимог безпеки.
- Відмовостійкість: схема безпеки повинна продовжувати надавати послуги безпеки за наявності таких несправностей, як помилки вузлів.
- Самовідновлення: датчики можуть не працювати або вичерпатися енергії. Решта датчиків, можливо, доведеться реорганізувати, щоб підтримувати певний рівень безпеки.
    - Інформативність: забезпечення - це можливість поширювати різноманітну інформацію на різних рівнях для кінцевих користувачів. Схема безпеки повинна запропонувати вибір щодо бажаної надійності, затримки тощо.

**Висновки до розділу 1:**

В даному розділі розглянуто основні принципи сучасних систем безпеки в мережевих технологіях. Розглянуто особливості та проблеми, які виникають при експлуатації безпроводових сенсорних мереж та при застосуванні засобів для захисту інформації БСМ. До них можна віднести обмежений ресурс, вартість, віддалене розташування від центру керування і відсутність можливості оперативно реагувати на атаки фізичного характеру. Все це випливає в певні вимоги та характеристики, які потрібно враховувати при розробці та налагоджування таких мереж.

В розділі також наведено основні показники для оцінки системи безпеки основним вимогам, такі як: безпека, відмова, енергоефективність, гнучкість, масштабованість, відмовостійкість, самовідновлення та інформативність. Всі ці показники відіграють важливу роль, оскільки висвітлюють всі особливості роботи таких мереж.

# РОЗДІЛ 2. АТАКИ НА БЕЗПРОВОДОВІ СЕНСОРНІ МЕРЕЖІ ТА ПРИНЦИПИ ЗАХИСТУ

Сенсорні мережі уразливі для безлічі атак, які намагаються поставити під загрозу роботу мережі і дані, що генерують сенсорні вузли. Зокрема, коли сенсорні мережі служать цілям програм, таких як оцінки поля битви і контроль цивільної інфраструктури, вони вимагають захисту від несанкціонованого доступу і втручання.

## 2.1 Відмова в обслуговуванні

Атака Denial-of-Service (Відмова в обслуговуванні) (DoS) може характеризуватися як спроба противника зупинити функціонування мереж або зруйнувати служби забезпечення мережі. У бездротових сенсорних мережах атаки DoS можуть відбуватися на різних рівнях стека протоколу, деякі можуть впливати на декілька рівнів одночасно або спробувати використовувати взаємодію між ними.

### 2.1.1 Фізичний рівень DoS

Бездротовий носій, який використовується в БСМ, спрощує безліч атак. Атака постановки перешкод відбувається, коли противник втручається в радіочастоти БСМ. При хорошому розташуванні, кілька вузлів атаки можуть відключити всю мережу, навіть якщо число атакуючих вузлів набагато менше, ніж число вузлів в мережі. Навіть один атакуючий вузол може відключити всю мережу, якщо він близько розташований до «критичного» вузла (наприклад, шлюз, який запобігає будь-яким спробам виходу сенсорних даних з сенсорної мережі), або потужність передачі настільки велика що всі вузли в мережі можуть бути зблоковані для коректного отримання будь-яких важливих даних. Загальний метод проти перешкод

використовується в широкосмугового зв'язку в добре відомих стандартах, таких як IEEE 802.11 і Bluetooth. Наприклад, в стрибкоподібної перебудови частоти з розширеним спектром (FHSS), пристрої зв'язку часто скачуть між частотами відповідно до визначеної послідовності стрибкоподібного руху. Передавач перешкод або повинен знати, що ця послідовність в змозі створити перешкоди коректної частоти для безперервного руйнування, або повинен створити перешкоди більшої смуги частот. Крім того, сенсорні мережі повинні вміти виявити і відповісти на атаки перешкод в мережі, Вузли, також, можуть попередити шлюзову станцію або базову станцію, про атаку на мережі. Наприклад, вузли, які виявляють атаку перешкод, можуть випустити короткі попереджувальні повідомлення своїм сусідам, і якщо, принаймні, один з цих сусідів знаходиться поза зоною атаки (тобто, в змозі отримати аварійне повідомлення без інтерференції), повідомлення може бути поширене до інших вузлів, включаючи базову станцію.

Атака втручання в сенсорної мережі відбувається, коли противник отримує фізичний доступ до сенсорного вузла, дозволяючи атакуючому знищити або змінити пристрій, отримує доступ до конфіденційної інформації (наприклад, криптографічні ключі), або використовує пристрій як точку входу для подальших атак в мережі. Можливі різні стратегії, які дозволяють захищати пристрій від втручання і наслідків, наприклад, використання матеріалів для корпусу, які будуть стійкими до зовнішніх впливі чи видалення інформації з пристрою або його виключення, коли виявлена атака. Наприклад, метод, часто використовуваний в системах, що обробляє конфіденційну інформацію, повинен стерти їх дані кожного разу, коли активується світлочутливий сенсор (наприклад, якщо відкривається корпусу терміналу).

### 2.1.2 Канальний рівень DoS

Атака зіткнень на канальному рівні впливає на передачу пакетів, викликаючи, таким чином, процедури експоненційної затримки і повторні передачі в деяких протоколах MAC. В цей самий час використовуються коди з корекцією помилок, щоб відновитися від пошкоджених бітів в пакеті, вони можуть бути не в змозі відновитися від всіх типів втручань (наприклад, якщо було пошкоджено занадто багато бітів), і піддаються додатковому ресурсу і енергетичним витратам. Атакуючий міг також спробувати викликати зіткнення близько кінця фрейму, змусивши вузол неодноразово ретранслювати весь пакет. Мета атакуючого могла полягати в тому, щоб викликати передчасне виснаження енергетичних ресурсів вузла (атака вичерпання). За таким же принципом шкідливий вузол міг використовувати певні методи квитирування, які часто знаходяться в протоколах MAC. Наприклад, атакуючий міг постійно випускати повідомлення RTS (протокол IEEE 802.11), щоб запросити відповідь CTS від іншого вузла, в кінцевому рахунку, вичерпавши енергетичні ресурси обох вузлів.

## 2.2 Атаки на маршрутизацію

Один із прикладів атаки на протоколи маршрутизації сенсорних мереж - Атака Чорної діра. З цим типом атаки противник намагається бути засобом передачі даних для одного або більше маршрутів по мережі. В такому випадку, шкідливий вузол може просто відкинути весь трафік, який повинен пройти через цей вузол, тому такий трафік ніколи не досягає місця призначення. Подібна атака називається селективною експедиторською атакою, де відкинуті тільки пакети, які відповідають певним критеріям, замість того, щоб відкинути всі пакети без розбору. Селективні експедиторські атаки набагато складніше виявити і впливати на них, ніж на

атаки чорної діри, оскільки їх набагато складніше відрізнити від пакетних втрат через помилки каналу або мобільності.

Атака Стрімкий натиск в сенсорної мережі використовує природу процедури відкриття маршруту на вимогу протоколів маршрутизації, наприклад, в таких протоколах, як AODV і DSR. У цьому типі атаки, шкідливий вузол відразу передає вхідні повідомлення запиту маршруту своїм сусідам, тому "мчать" ці повідомлення без дотримання будь-яких правил протоколу (наприклад, встановлює певний час очікування або організовує чергу, перш ніж передати). Як наслідок, у вузла зростає ймовірність бути частиною обраного маршруту між джерелом і пунктом призначення.

Атака Воронки - другий варіант атаки чорної діри. Однак, щоб залучити якомога більше трафіку, шкідливий вузол намагається розташуватися на шляху якомога більшої кількості потоків мережі. Тому трафік відтягнуть до цього водостічного колодязя, надавши атакуючому можливість зруйнувати або втрутитися в якомога більшу кількість трафіку.

Атака Сібіл відбувається, коли атакуючий стверджує, що має кілька ідентифікаційних даних в мережі. За таким же принципом в протоколах маршрутизації заснованих на місці розташування, атакуючий стверджує, що знаходиться в декількох місцях одночасно. Якщо багато вузлів вважають, що цей шкідливий вузол їх сусід - є хороший шанс, що вони виберуть цей вузол в якості вузла передачі їх мережевого трафіку.

Інша атака на процедуру маршрутизації сенсорної мережі - Атака червоточини. Це атака виконується вузлами, які мають більше ресурсів в наявності, ніж типові сенсорні вузли в мережі. Наприклад, двоє атакуючих. що співпрацюють між собою, можуть спробувати обдурити іншу частину мережі, володіючи позасмуговим каналом зв'язку між собою. Для іншої частини мережі це є швидким, високим каналом пропускної здатності, який бажаний для багатьох методів маршрутизації.

### 2.3 Атаки на транспортному рівні

Транспортний рівень стека мережевого протоколу відповідальний за управління з'єднаннями від початку до кінця, наприклад, два відомих протоколу транспортного рівня - Протокол Управління Передачею (TCP) - для надійної комунікації на основі потоків, і Протокол Користувальницької Дейтаграми (UDP) - для ненадійною комунікації на основі пакета . Атака лавинної розсилки використовує факт, що багато транспортних протоколів (таких як TCP) підтримують конфіденційну інформацію і тому уразливі до виснаження пам'яті. Наприклад, атакуючий може неодноразово робити нові запити на встановлення з'єднання, кожного разу додаючи більше конфіденційної інформації в несправному вузлі, потенційно призводить до відмови вузла від подальших з'єднань через вичерпання ресурсу. Це, в свою чергу, не дає можливості успішно підключитися законним вузлам.

В атаці десинхронізації противник намагається зруйнувати зв'язок між двома робочими вузлами в мережі, неодноразово підробляючи повідомлення до цих вузлів. Наприклад, надійні протоколи транспортного рівня можуть використовувати порядкові номери, щоб відстежувати успішно отримані пакети, ідентифікувати пакетну втрату і виявити копії. Підроблені пакети, випущені противником, можуть використовувати ці порядкові номери, щоб змусити вузол вважати, що пакети не досягли місця призначення, таким чином, виявивши дорогі ресурсом повторні передачі.

### 2.4 Атаки на агрегацію даних

Агрегація даних і злиття даних часто використовуються, щоб об'єднати багаторазові сенсорні дані і усунути надлишкову інформацію. Агрегація може часто мати сприятливі ефекти на вимоги ресурсів сенсорних потоків, наприклад, зменшуючи частоту передач або розмірів пакета. Навіть прості функції агрегації можуть легко опинитися під таким впливом атакуючого, що

поведінка мережі може бути змінено. Наприклад, середня функція $f(x_1 \ldots x_n)= (x_1 + \cdots + x_n)/n$ небезпечна навіть в присутності одного шкідливого вузла. Шляхом заміни одного реального розміру $x_1$ на фальшиві дані $x^*_1$, середнє число зміниться від $y = f(x_1, \ldots, x_n)$ до $y^* = f(x^*_1, x_2, \ldots, x_n) = y + (x^*_1 x_1)/n$. Атакуючий може вільно вибрати значення $x^*_1$ і, отже, може управляти результатом агрегації.

Так само не є безпечними функції суми, мінімуму і максимуму. Сума $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n$ за бажанням може бути замінена реальних даних $x_1$ на фальшиві дані $x^*_1$. Мінімальна функція $f(x_1, \ldots, x_n) = \min(x_1, \ldots, x_n)$ також небезпечна, навіть при тому, що заміна реальних даних на підроблені значення не завжди впливає на результат функції. Тобто заміна $x_1$ на $x^*_1$ тільки підвищує мінімум, якщо $x_1$ - унікальна найменша сенсорна дана, читаюча серед всіх $x_i$. Однак атакуючий може змінити обчислений мінімум, вибравши $x^*_1$ дуже маленьким в порівнянні з усіма коректними даними. В силу симетрії, максимальна функція також небезпечна, оскільки зловмисник може підняти максимальне значення шляхом захоплення одного свідчення сенсора. На відміну від цього, ефект захоплення єдиного свідчення сенсора може бути відносно невеликий для операції зчитування, якщо кількість правильних даних досить велике. Функція лічильника аналогічна функції суми, за винятком того, що кожен показання сенсора вкладає тільки 0 або 1 в результат операції. Тобто атакуючий з керуванням компромісних вузлів k може змінити результат функції більшості k, який може бути незначним, якщо k маленький в порівнянні із загальною кількістю вводів сенсора.

### 2.5 Атаки на конфіденційність

Загрози безпеці, описані раніше спрямовані на руйнування роботи мережі від коректної роботи, велика кількість інформації зібране в самій безпроводовій сенсорній мережі, також знаходяться в небезпеці через потенційного зловживання. Тобто противник може спробувати отримати

секретну інформацію, отримавши доступ до інформації, що зберігалася на сенсорному вузлі або підслухавши мережу. Широкомовна природа безпроводових мереж спрощує контроль і отримання передачі між вузлами, особливо коли ніякі криптографічні механізми не використовуються для захисту сенсорних даних. Підслуховування може також бути об'єднано з аналізом трафіка, який може використовуватися супротивником, щоб ідентифікувати сенсорні вузли інтересу в мережі. Наприклад, збільшення зв'язків між певними вузлами може вказати на високий рівень активності (і отже на наявність даних, які можуть опинитися під загрозою) в тій частині мережі. За таким же принципом аналіз трафіку може використовуватися, для ідентифікації вузлів, які можуть бути набагато важливіше для операцій мережі, ніж інші, такі як базові станції та шлюзи.

### 2.6 Протоколи і механізми безпеки

Щоб захиститися від багатьох можливих атак в безпроводових сенсорних мережах, можна використовувати безліч протоколів захисту та інші захисні механізми. Далі описано різноманітність цих протоколів і механізмів їх застосування в БСМ.

#### 2.6.1 Симетричні і відкриті криптографічні ключі

У той час як шифрування з відкритим ключем може використовуватися, для забезпечення конфіденційності, цілісності і аутентифікації, алгоритми з відкритим ключем в обчислювальному відношенні дуже дорогі, що унеможливлює їх використання в сенсорних мережах з обмеженим бюджетом. Підходи криптографії симетричного ключа можуть бути значно ефективнішими з точки зору ресурсів, що робить їх кращим вибором в БСМ, навіть при тому, що існують реалізації RSA і ECC (криптографія еліптичних кривих) для сенсорів з обмеженим ресурсом. Головний недолік підходів

симетричного ключа - проблема розподілу ключів, тобто спільно використовуваний симетричний ключ повинен спочатку бути відомий обом зв'язується вузлів, перш ніж вони зможуть надійно обмінюватися даними.

Симетричні криптографічні схеми - кращий вибір для сенсорних мереж, коли обмеження ресурсу забороняють використання більш складних схем з відкритим ключем. Однак головний недолік симетричної криптографії - потреба в управлінні ключами, тобто надійне і безпечне встановлення спільно використовуваних криптографічних ключів серед сусідніх вузлів в БСМ. Наприклад, підхід Рівноправні Посередники для Створення Ключа (PIKE) - метод, який використовує сенсорні вузли в якості довірених посередників для розподілу ключів. У цьому підході, кожен сенсор спільно використовує різні парні ключі з кожним O($\sqrt{n}$) інших вузлів, де n- число вузлів в мережі. Крім того, ключі розгорнуті таким чином, що для будь-якої пари вузлів A і B, існує, принаймні, один вузол C, який спільно використовує парний ключ і з A і з B. Кожен сенсор в PIKE має ID форми (x,y), де x, y ∈ {0,1,2, ..., $\sqrt{n}$-1}. Тобто сенсорна мережа представлена як матриця з рядками і стовпцями $\sqrt{n}$, де позиція вузла в матриці і є ID вузла. Потім кожен вузол (x,y) спільно використовує попарний ключ з кожним вузлом в наступних двох наборах:

$$(i,y)\ \forall i \in \{0,1,2, ..., \sqrt{n}\text{-}1\} \quad (2.1)$$

$$(x,j)\ \forall j \in \{0,1,2, ..., \sqrt{n}\text{-}1\} \quad (2.2)$$

Наприклад, вузол (x,y) спільно використовує ключ K (x,y), (1,y) з вузлом (1,y), а інший ключ K (x,y), (2,y) з вузлом (2,y). В цілому вузол підтримає 2($\sqrt{n}$-1) ключа. На рис2.1 показано віртуальний простір ID для 100 вузлів, де кожне число являє ID вузла. Темні тіньові поля ідентифікують всі вузли, які спільно використовують ключ з вузлом 91, в той час як світлі заштриховані поля, вказують на всі вузли, які спільно використовують ключ з вузлом 14.

Завдяки цьому підходу, будь-які два вузла в мережі зможуть знайти два ID вузла , які спільно використовують попарні ключі з ними обома. Зокрема, якщо у вузла A є ID (xA, yA), а у вузла B є ID (xB, yB), то вузли з ID (xA, yB) і (xB, yA) будуть спільно використовувати попарні ключі і з A і з B. Якщо вузол (наприклад, вузол 14 на рис. 2.1) хоче виконати ключове встановлення з іншим вузлом (наприклад, вузол 91), A може ідентифікувати потенційних посередників, шляхом пошуку перехресних тіньових полів. Наприклад, вузол 94 знаходиться в тому ж рядку що 91, і в тому ж стовпці що 14, отже, спільно використовує ключі з ними обома і може служити посередником. Тоді вузол 14 шифрує новий ключ, який спільно використовується з вузлом 91, використовуючи існуючий ключ попарно використовуваний з вузлом 94, а потім відправляє зашифрований ключ до вузла 94. Вузол 94 дешифрує повідомлення, шифрує його знову ключем, спільно використовуваних з вузлом 91, і відправляє нове повідомлення до вузла 91. Вузол 91 дешифрує повідомлення, отримує новий ключ, і підтверджує отримання нового ключа, відповідаючи на вузол 14.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | ... | 09 |
| 10 | 11 | 12 | 13 | 14 | 15 | ... | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | ... | 29 |
| 30 | 31 | 31 | 33 | 34 | 35 | ... | 39 |
| . . | . | . | . | . | . | | |
| . . | . | . | . | . | . | | |
| . . | . | . | . | . | . | | |
| 90 | 91 | 92 | 93 | 94 | 95 | ... | 99 |

Рисунок 2.1 Простір віртуальних ідентифікаторів в PIKE

### 2.6.2 Захист проти DoS атак

Атаки відмови в обслуговуванні (DoS) в сенсорних мережах поширені і вимагають ефективних заходів, щоб уникнути їх або перешкодити їх поширенню по всій мережі. Наприклад, коли виявляється або підозрюється атака перешкод, сенсорна мережа може спробувати ізолювати порушену область, направивши трафік навколо відключених частин мережі. На канальному рівні атаки зіткнень і вичерпання ресурсів можуть бути адресовані шляхом використання кодів корекції помилок (які додають витрати на обробку і комунікації) і схем, які обмежують розмір, що дозволяють пристрою ігнорувати запити, які можуть привести до передчасного енергетичного виснаження. Спуфінг і перетворення може бути адресовано на мережевому рівні за допомогою коду аутентифікації повідомлень або MAC (щоб не бути переплутаним з керуванням доступу до середовища передачі) яка може бути розглянута як криптографично безпечна контрольна сума повідомлення. Ці контрольні суми дозволяють одержувачу перевірити, чи імітувалося або змінювалося повідомлення.

Атака відмову в обслуговуванні на основі шляху - це атака, в якій атакуючий крушить вузли в віддаленій сенсорної мережі, лавинно розсилаючи мультитранзитну ділянку наскрізного каналу зв'язку або з відтвореними пакетами, або з пакетами, введеними в довільному порядку. Ланцюжки одностороннього хешу - послідовність чисел, де тривіально, обчислити y=F(x), але в обчислювальному відношенні нездійсненно обчислити x=F-1(y). Кожен вузол в мережі використовує ланцюжок хешування, щоб перевірити отриманий пакет, тобто вузол систематично циркулює через ланцюжок, щоб визначити, чи є пакет з довіреного джерела. Якщо пакет не може бути перевірений, він відкидається.

### 2.6.3 Захист проти атак агрегації

Як обговорювалося раніше багато простих функцій агрегації таких як сума, мінімум і максимум по суті небезпечні. Однак може використовуватися кілька методів для поліпшення стійкості функцій агрегації, наприклад, два таких методу - затримка агрегації і затримка аутентифікації.

У цих методах передбачається, що базова станція генерує односторонній ланцюжок для ключів використання загальнодоступної односторонньої функції F, де $K_i = F(K_i + 1)$. Кожен пристрій зберігає ключ $K_0$ перед розподілом, де $K_0=F_n(K)$ (тобто F застосовується до секретного ключа $K_n$ раз). Далі передачі станцій першої стадії будуть зашифровані, використовуючи ключ $K_1 = F_n\text{-}1(K)$. Після того, як всі повідомлення, що передаються з використанням $K_1$ були отримані, базова станція виявляє $K_1$. Як наслідок всі вузли можуть обчислити $F(K_1) = F(F_n\text{-}1(K))$ і перевірити, що він відповідає $K_0=F_n(K)$. Далі, сенсорні вузли можуть дешифрувати повідомлення, які раніше були передані зашифрованими $K_0$. Аналогічним чином, послідовні ключі можуть бути виявлені до тих пір, поки не буде досягнута $K_n=K$ (якщо необхідно більше ключів, тоді базова станція може запустити нову послідовність). Припустімо, що чотири сенсорних вузла A-D відправляють повідомлення на базову станцію в мережу, структуровану як дерево, як показано на рис.2.2. Кожне повідомлення вузла містить ID відправника, сенсорні дані і MAC обчислені на основі даних, використовуючи тимчасовий ключ. Батьківський вузол сенсорного вузла ще не в змозі перевірити MAC до тих пір, поки ключ з дочірнього елемента не буде переданий до батьківського вузла. Батьківський вузол (тобто вузол E на рис 2.2) зберігає це повідомлення і ретранслює його до свого власного батька після певного часу очікування. Повідомлення E до свого батька G містить повідомлення, отримані від його дочірніх елементів (наприклад, вузлів A і B) і MAC, розрахованих за сукупністю даних A і B, використовуючи ключ E. Цей процес продовжеється, тобто, кожен проміжний вузол комбінує дані, що

надходять з дочірніх елементів, і додає свій власний MAC за сукупністю всіх даних, використовуючи свій власний ключ. Незабаром базова станція отримує повідомлення від своїх дочірніх елементів і може обчислити заключне підсумкове значення.

У базовій станції є спільний тимчасовий ключ з кожним сенсорним вузлом, тому він може перевірити, чи було отримане повідомлення надіслане від H, обчисливши MAC агрегації використовуючи $K_{Hi}$ і порівняти його з MAC в повідомленні. У той час як він перевіряє, що H відправив заключне повідомлення, він не перевіряє, чи правильно повідомлення відображає показання з інших вузлів. Щоб перевірити дані, базова станція показує тимчасові ключі вузла мережі, відправляючи кожен ключ (разом з MAC) до всіх сенсорним вузлів, використовуючи свій власний поточний ключ $K_i$. Після відправлення всіх ключів вузла базова станція відправляє свій поточний ключ $K_i$, таким чином, щоб вузли змогли перевірити передані значення MAC і вдосконалюватися до наступного ключа в ланцюжку для майбутніх повідомлень.

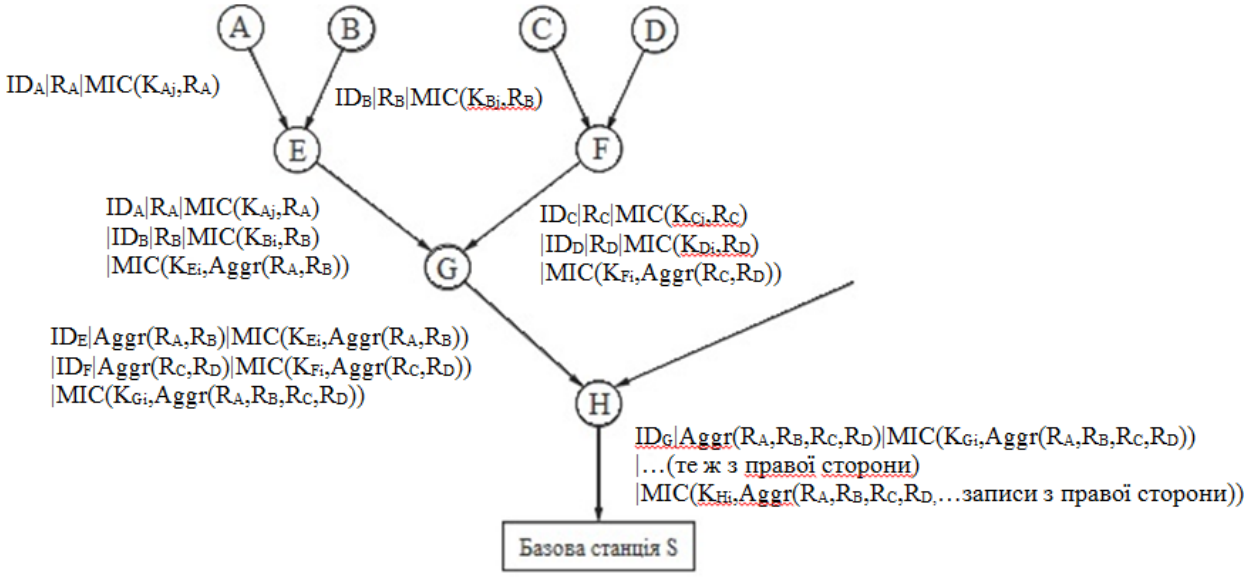


Рисунок 2.2 Приклад безпечної агрегації.

Таким чином, описаний процес затримує і агрегацію, і аутентифікацію, наприклад, агрегація не відбувається на першому хопі, що можливо було б зробити, але відбувається на другому хопі. Хоча це може збільшити витрати ресурсів, він також може дозволити гарантії цілісності, де послідовні вузли не будуть під загрозою.

### 2.6.4 Захист проти атак маршрутизації

Більшості атак «із зовні» мережі можна запобігти, використовуючи шифрування на канальному рівні і аутентифікацію з використанням глобального загального ключа. Оскільки противнику перешкоджають приєднатися до мережі, такі атаки як вибіркова передача або водостічні колодязі неможливі. Однак коли мережі піддаються нападу «зсередини», використовуючи компрометуючий вузол, цей підхід неефективний, і необхідні більш складні рішення.

Атаки Сібіл можна запобігти шляхом перевірки ідентичності сенсорних вузлів. Наприклад, кожен сенсорний вузол може спільно використовувати унікальний симетричний ключ з довіреної базовою станцією, яка може бути використана для перевірки ідентифікаційних даних один одного. Базова станція може також обмежити число сусідів, яких дозволено мати вузлу, тобто навіть коли вузол скомпрометований, він може зв'язатися тільки з перевіреними сусідами.

Проти атаки Воронка важко захиститися в протоколах, де маршрути встановлені на основі інформації, яку важко перевірити, наприклад надійність або енергетичні показники. Маршрути, засновані на мінімальній кількості хопів легше перевірити, але кількість хопів може бути спотворено через червоточину. Категорія протоколів, стійка до цих атак називається географічна маршрутизація, тому що мережі, використовуючи засновані на місцезнаходженні методи маршрутизації, встановлюють топологію на вимогу на основі локалізованих взаємодій та інформації без ініціювання з базової

станції. Так як трафік "природно" спрямований до фізичного розташування базової станції, важко перенаправити трафік в інше місце, щоб створити воронку. В атаці стрімкого натиску мета вузла полягає в тому, щоб використовувати процес відкриття маршруту в протоколах маршрутизації на вимогу, щоб привернути до себе якомога більше маршрутів. Однак, щоб запобігти таким атаки, може використовуватися комбінація декількох заходів захисту. Наприклад, деякі зловмисники можуть передати запити маршруту за рамки нормального діапазону радіопередач (наприклад, використовуючи високу потужність передачі) тим самим пригнічуючи наступні повідомлення запиту від цього виявлення маршруту. Підхід виявлення безпечного сусіда може використовуватися, щоб дозволити і для відправника і для одержувача запити на перевірку маршруту, підтвердження, що інша сторона фактично на нормальному діапазоні передачі. Наприклад, протокол взаємної аутентифікації з трьома циклами з жорстким часом затримки може бути розгорнутий. У першому циклі вузол передає пакет сусіднього клопотання (або через широкомовну передачу або через одноадресну передачу до певного вузла). У другому циклі вузол, який отримує пакет клопотання, відповідає сусіднім відповідним повідомленням, а в третьому циклі, ініціатор цієї комунікації квитирування відправляє сусіднє повідомлення перевірки, яке включає трансляцію аутентифікацію мітки часу і посилання від джерела до місця призначення.

### 2.6.5 Протоколи безпеки для Сенсорних мереж

Проект Протоколи захисту для сенсорних мереж (SPINS) робить два основних вклади в захист від атак: Протокол шифрування безпеки мережі (SNEP) і "мікро" версія Протокол синхронізованої, ефективної, з можливістю передавання потоків, стійкою до втрати аутентифікації (μTESLA). Основна мета протоколу SNEP полягає в тому, щоб забезпечити конфіденційність, двопартійну аутентифікацію даних і актуальність даних, в той час як μTESLA

забезпечує аутентифікацію для широкомовної передачі даних. Кожен вузол, як передбачається, спільно використовує закритий ключ з базовою станцією.

SNEP бере до розгляду обмеження ресурсу типових сенсорних вузлів, покладаючись на прості алгоритми для шифрування, аутентифікації і генерації випадкових чисел. Ключові властивості SNEP - її симетрична безпеку, відтворення захисту і низькі накладні витрати зв'язку. Симетрична безпека стосується до того факту, що одне й те саме повідомлення кожного разу шифрується по-іншому. Щоб досягти двопартійної аутентифікації і цілісності, SNEP використовує MAC, де більше MAC більш складне для противника, щоб вгадати відповідний код для повідомлення. З іншого боку великі коди означають великі розміри пакетів.

Два суміжних вузла A і B спільно використовують головний секретний ключ, який використовується, щоб вилучити чотири незалежних ключа, використовуючи псевдовипадкову функцію. Двоє з цих ключів використовуються для шифрування повідомлень в кожному напрямку (KAB і KBA), і два ключа використовуються в якості кодів цілісності повідомлення, знову один для кожного напряму ($K'_{AB}$ і $K'_{BA}$). У повного зашифрованого повідомлення такий вигляд:

$$A \rightarrow B: \{D\}_{<KAB, CA>}, MAC(K'_{AB}C_A||\{D\}_{<KAB, CA>}) \qquad (2.3)$$

де D - дані, зашифровані ключем шифрування K, а лічильник - C.

MAC обчислюється в формі M=MAC(K', C||E). SNEP забезпечує аутентифікацію даних (використовуючи MAC), захист відтворення (використовуючи значення лічильника MAC), актуальність (значення лічильника здійснюють упорядкування повідомлень), семантичну безпеку (тому що, лічильник зашифрований кожним повідомленням, і кожне повідомлення буде зашифровано кожен раз по-різному) і низькі накладні витрати зв'язку (що передбачає, що стан лічильника збережено в кожній кінцевій точці і не відправлено в повідомленні). Актуальність даних в рамках

SNEP вважається слабкою тільки через те, що SNEP здійснює порядок передачі в вузол B, але не дає ніякої гарантії вузлу A, що повідомлення було створено вузлом B, у відповідь на подію в вузлі A. Щоб досягти актуальності, випадок (тобто, випадкове число таке довге, що вичерпний пошук всіх можливих випадків неможливий) може бути включений в протокол. Вузол в довільному порядку генерує випадок $N_A$ і відправляє його разом з повідомленням запиту до вузла B. Потім вузол B повертає випадок з відповідним повідомленням у аутентифікованому протоколі, який працює в такий спосіб:

$$A \rightarrow B: N_A, R_A \tag{2.4}$$

$$B \rightarrow A: \{R_B\}_{<KBA, CB>}, MAC\ (K'_{BA}, N_A||CB||\{R_B\}_{<KBA, CB>}) \tag{2.5}$$

Якщо MAC перевіряє правильно, вузол A знає, що вузол B генерував свою відповідь після запиту A.

Протокол μTESLA фокусується на потребі в аутентифікованій широкомовної передачі в бездротових сенсорних мережах. Він покладається на симетричні механізми, забезпечені SNEP, для аутентифікації першого пакету в широкомовному повідомленні. Це розширення TESLA, не було розроблено для використання в середовищах з обмеженими обчислювальними ресурсами. TESLA використовує цифрові підписи, щоб аутентифікувати початковий пакет і має витрати 24 байта за пакет, які можуть бути значними для сенсорних мереж, де повідомлення зазвичай дуже маленькі. Аутентифікована широкомовна передача вимагає асиметричного механізму (інакше, будь-який компрометуючий одержувач зможе підробити повідомлення від відправника), але асиметричні криптографічні механізми часто з високими вимогами до ресурсів. Замість цього μTESLA емулює асиметрію за допомогою затримання розкриття симетричних ключів. μTESLA передбачає, що базова станція і сенсорні вузли вільно синхронізовані за часом і кожен вузол знає верхню межу максимальної помилки синхронізації. Коли базова станція відправляє повідомлення, вона

аутентифікує його, обчислюючи MAC на пакеті з ключем, який є закритим в цій точці. Коли вузол отримує пакет, і ключ невідомий, вузол знає, що ключ MAC відомий тільки базової станції. Вузол зберігає пакет до базової станції, під час ключового розкриття, широкомовно передає ключ перевірки всім одержувачам. Тепер вузол може використовувати ключ, щоб аутентифікувати збережений пакет.

### 2.6.6 TinySec

Структура TinySec - легкий і універсальний пакет захисту на канальному рівні, які розробники можуть легко інтегрувати в додатках сенсорної мережі. Він підтримує два різних параметра безпеки: аутентифіковане шифрування (TinySec-AE), де корисне навантаження даних зашифрована і MAC використовується, щоб аутентифікувати пакет, і тільки аутентифікація (TinySec- Auth), де весь пакет аутентифікується з MAC ( але корисне навантаження залишається незашифрованим). TinySec покладається на ланцюжок цифрових блоків і спеціально відформатований 8-байтовий вектор ініціалізації для шифрування. Для аутентифікації TinySec покладається на ефективну і швидку конструкцію ланцюжка цифрових блоків (CBC MAC) для обчислень і перевірки MAC. Перевага CBC MAC полягає в тому, що, він покладається на цифровий блок, він мінімізує число криптографічних примітивів, які повинні бути реалізовані, що вигідно для сенсорних вузлів з обмеженими ємностями зберігання. Довжина MAC обрана бути тільки 4 байта, тобто противник може неодноразово робити спроби сліпих підробок, які привели б до успіху найбільше після $2^{32}$ спроби. Хоча це число здається маленьким, потрібно відзначити, що противник має оцінити достовірність коду, відправивши його авторизованому одержувачу. Що в подальшому означає, що до $2^{32}$ повідомлень повинні бути передані, що забезпечує достатній рівень безпеки для сенсорних мереж.

### 2.6.7 Локалізоване шифрування і протокол аутентифікації

Локалізоване шифрування і протокол аутентифікації (LEAP) - протокол управління ключами для сенсорних мереж, розроблених, щоб підтримувати мережеву обробку. Ключова мотивація цього протоколу - спостереження за тим, щоб різні типи повідомлень (наприклад, контрольні пакети в порівнянні з пакетами даних) в сенсорної мережі мали різні вимоги до захисту. Єдиний механізм маніпулювання не може підходити для зустрічі цих різних вимог, наприклад, в той час як аутентифікація може бути необхідна для всіх типів пакетів, конфіденційність, може бути необхідна тільки для певних типів повідомлень (наприклад, агрегованих сенсорних даних).

LEAP забезпечує чотири механізми маніпулювання: окремі ключі, ключі групи, кластерні ключі, і попарно спільно використовувані ключі. В індивідуальному ключовому механізмі у кожного вузла є свій власний унікальний ключ спільно використовуваний з базовою станцією. Цей ключ використовується для конфіденційного зв'язку або для обчислень кодів аутентифікації повідомлень, якщо вузол хоче, щоб базова станція перевірила свої виявлені дані. Груповий ключ - ключ, який використовується глобально і спільно. Він використовується базовою станцією для передачі зашифрованих повідомлень до всієї сенсорної мережі. Кластерний ключ - ключ, яким користуються одночасно сенсорним вузлом і його сусіди, і використовується для забезпечення локальних широкомовних повідомлень (наприклад, повідомлення про маршрут). І нарешті, попарно - спільно використовуваний ключ - ключ, яким користуються сенсорним вузлом і одним з його безпосередніх сусідів. LEAP використовує ці ключі для безпечних комунікацій серед пар вузлів, наприклад, дозволяючи вузлу надійно розподілити кластерний ключ своїм сусідам або надійно передати свої сенсорні дані до вузла агрегації. LEAP також забезпечує метод для локальної широкомовної аутентифікації.

Кожен вузол генерує однобічний ланцюжок для ключів певної довжини і передає перший ключ в ланцюжок кожному сусідові, зашифрований попарно спільно використовуваних ключем. Кожен раз, коли вузол відправляє повідомлення, він бере наступний ключ з ланцюжка (кожен ключ називають ключем AUTH), і приєднує його до повідомлення. Ці ключі розкриті в зворотному порядку їх генерації, і одержувач може перевірити повідомлення на основі першого отриманого ключа або недавно відкритого ключа AUTH.

### 2.6.8 IEEE 802.15.4 і Захист ZigBee

Стандарт IEEE 802.15.4 і специфікація ZigBee - популярний вибір протоколу для безпроводових сенсорних мереж.

Даний стандарт широко використовується при побудові безпроводових сенсорних мереж і працює на фізичному та канальному (підрівень MAC) рівнях моделі OSI.

Стандарт IEEE 802.15.4 забезпечує чотири основні моделі безпеки: управління доступом, цілісність повідомлення, конфіденційність повідомлення і захист відтворення. Безпека в IEEE 802.15.4 оброблена рівнем MAC, і додаток може вибрати певні вимоги до захисту, встановивши належні параметри в радіо-стеку (за замовчуванням, безпека не включена). Стандарт розрізняє вісім наборів безпеки (Таблиця 1.1), кожен з різними рівнями захисту для переданих даних. Перший набір не пропонує захист, другий набір пропонує тільки шифрування (AES - CTR), супроводжуваний групою наборів тільки з аутентифікацією (AES - CBC - MAC), і групою наборів і з аутентифікацією і з шифруванням (AES - CCM). Набори, які пропонують аутентифікацію, відрізняються за розмірами MAC, які варіюються від 32 до 128 бітів. Для кожного набору, який пропонує шифрування, IEEE 802.15.4 також пропонує додатковий захист відтворення, що складається з монотонно

збільшених порядкових чисел для повідомлень, щоб дозволити одержувачу виявляти атаки відтворення.

**Таблиця 2.1** Наборы безопасности поддерживаемые в IEEE 802.15.4

| **Name** | **Description** |
|---|---|
| Null | No security |
| AES – CTR | Encryption only, CTR mode |
| AES – CBC – MAC – 128 | 128-bit MAC |
| AES – CBC – MAC – 64 | 64-bit MAC |
| AES – CBC – MAC – 32 | 32-bit MAC |
| AES – CCM – 128 | Encryption and 128-bit MAC |
| AES – CCM – 64 | Encryption and 64-bit MAC |
| AES – CCM – 32 | Encryption and 32-bit MAC |

Перший набір Null не забезпечує захист. Всі інші набори безпеки використовують цифровий блок Вдосконаленого стандарту шифрування (AES), який також відомий як Rijndael. Національний інститут стандартів і технологій визначає п'ять режимів роботи, включаючи лічильник (CTR) і режим ланцюжка цифрових блоків (CBC). Коли необхідна аутентифікація, може використовуватися один з трьох AES - CBC - MAC варіантів, які обчислюють код цілісності повідомлення, використовуючи цифровий блок в режимі CBC. Три набору AES - CCM комбінують шифрування і аутентифікацію за допомогою режиму Лічильника і режиму CBC (CCM закоротка для Лічильника CBC - MAC).

На додаток до засобів захисту IEEE 802.15.4 специфікація ZigBee також представляє поняття центру довіри, відповідальність зазвичай прийнята на координатора ZigBee. Центр довіри відповідальний за

аутентифікацію пристроїв, що бажають приєднатися до мережі (адміністратор довіри), підтримку і розподіл ключів (адміністратор мережі) і включення наскрізний безпеки між пристроями (менеджер конфігурації).

ZigBee також диференціюється між житловим і комерційним режимом. У житловому режимі центр довіри дозволяє вузлам приєднуватися до мережі, але не встановлює ключі з мережевими пристроями. У комерційному режимі він генерує і підтримує ключі, і свіжість лічильників з кожним пристроєм в мережі. Недолік комерційного режиму - вартість пам'яті, яка росте з розміром мережі.

Специфікація ZigBee використовує режим CCM* для своїх служб безпеки, яка також є комбінацією режимів CTR і CBC - MAC. У порівнянні з режимом CCM, CCM * пропонує можливості тільки для шифрування і тільки для цілісності. Подібно специфікаціям в стандарті IEEE 802.15.4, у ZigBee є кілька рівнів безпеки, включаючи нульова безпеку, тільки шифрування, тільки аутентифікація, і обидва і шифрування і аутентифікація. Рівні, які забезпечують аутентифікацію, використовують MAC, який може змінюватися від 4 до 16 байтів.

**Висновки до розділу 2:**

Атаки на безпроводові сенсорні мережі здійснюються на всіх рівнях. Починаючи від фізичного втручання, коли вплив відбувається на сам сенсор і закінчуючи втручанням в роботу програм керування мережею.

Особливості експлуатації значно ускладнюють процес забезпечують процес захисту безпеки.

В даному розділі розглянуто приклади найбільш поширених атак на безпроводові сенсорні мережі на всіх рівнях. Вказано можливі варіанти вирішення даних проблем.

На фізичному рівні атаки характеризуються фізичним втручанням в структуру мережі, а також діями. що спричиняють виснаження ресурсів

самого датчика. Атаки на канальному рівні викликають затримки в передачі даних, а, відповідно, інформація, що пережається, втрачає свою актуальність, або викликають повторну передачу пакетів даних. Атаки на мережевому рівні втручаються в процес передачі даних. В таких випадках шкідливий вузол стає основним вузлом в мережі і весь трафік буде передаватися через нього і виходити з мережі. Зазвичай, вузли уразливі до виснаження пам'яті і тому після таких атак можуть відмовляти у встановленні зв’язку з іншими вузлами. Наслідки атаки на конфіденційність небезпечні тим, що шкідливий вузол може отримати секретну інформацію, отримавши доступ до інформації, що зберігалася на сенсорному вузлі або підслухавши мережу.

В наш час існує багато методів для забезпечення захисту інформації в мережах, але враховуючи особливості роботи БСМ не всі вони можуть застосовуватися в безпроводових сенсорних мережах. В даному розділі також наведено методи захисту інформації в БСМ, які існують в наш час та особливості їх застосування.

# РОЗДІЛ 3. МАТЕМАТИЧН МОДЕЛЬ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ ДЛЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

В більшості випадків застосувань бездротових сенсорних мереж потрібні мобільні сенсорні вузли. Проте їх мобільність збільшує проблеми безпеки в безпроводових сенсорних мережах і, відповідно, вони стають більш уразливими до різних видів атак. Динамічна БСМ має дві найпоширеніші проблеми, пов'язані з автентифікацією рухомих сенсорних вузлів та безпекою в області зв'язку та розподілу ключів. Після можливого переміщення датчика вузол вимагає перевірки автентичності знову і знову від базової станції або деяких інших надійних вузлів. Аналогічним чином, конфіденційність у комунікації та розподілі ключів є важливим фактором проти нападу на мережу. Раніше більшість досліджень безпеки БСМ зосереджувалися на статичному середовищі. Хоча в таких випадках схеми є безпечними та ефективними, але недостатніми для забезпечення мобільного середовища безпроводових сенсорних мереж. У цій роботі описано нову структуру протоколу та відповідну математичну модель для зв'язку з безпечним каналом маршрутизації та розподілу ключів у мобільних БСМ. Після цього ми застосовуємо цю модель для оцінки продуктивності на основі статичного та динамічного сценаріїв для різної кількості вузлів, що показує, що наша система задовільно підходить для динамічних додатків БСМ.

## 3.1 Особливості роботи безпроводових сенсорних мереж з мобільними вузлами

Безпроводові сенсорні мережі здобувають все більшу популярність у галузі досліджень. Причиною такої популярності є не тільки програми для їх застосування, але і головні переваги таких мереж. Такі як безпека,

автентифікація, керування ключами, маршрутизація, агрегація даних, і поширення тощо.

В основному БСМ складаються з малих пристроїв неоднорідного типу, що являють собою сенсорні вузли, що мають такі властивості як малий розмір, малу пам'ять та обмежену ємність батареї, а також можливості зондування. Вузли датчиків можуть збирати інформацію з навколишнього середовища, яка пов’язана з подіями, що відбуваються в його діапазоні. Дані, на основі деякого набору правил, вони поширюють цю інформацію до базової станції через безпроводове середовище.

Більшість досліджень безпроводових сенсорних мереж зосереджує увагу на статичних датчиках, які потребують одноразової автентифікації в мережі. Проте робота сервера із мобільними вузлами може спричинити різні типи викликів та проблеми, пов'язані з безпекою. Наприклад, мобільний вузол підвищує швидкість відмови в передачі даних через постійну зміну маршруту в мережі, чи збільшується затримка при доставці пакетів, що призводить до поганого впливу в реальному часі. Проблеми, які пов’язані з безпекою, наприклад, мобільні вузли, потребують автентифікації та повторної автентифікації через зміни в регіоні, а також дуже схильні до різних типів активних та пасивних атак зловмисниками або вторгнень.

Кожного разу, коли мобільний вузол підключається до БСМ, основний вузол повинен аутентифікувати цей підпорядкований вузол. У випадку, якщо мобільний вузол переходить до діапазону іншого основного вузла, основний вузол повинен ще раз перевірити цей підпорядкований вузол. Отже, в умовах високої мобільності основні вузли повинні постійно, раз за разом перевіряти підлеглий вузол, навіть якщо він раніше підтверджувався будь-якими іншими основними вузлами тієї ж мережі. Подібним чином, для вузла в мережі конфіденційність зв'язку відіграє важливу роль, оскільки під час атаки

на мережу може здійснюватися втручання в зв'язок між комунікаціями і завдати шкоди шляхом зміни інформації. Розповсюдження аутентифікованого ключа в безпроводових сенсорних мережах є однією з основних проблем безпеки. Оскільки, сенсорні вузли, які використовуються в БСМ є легкими пристроями, які вони мають обмежену пам'ять та обмежену обчислювальну потужність, використання протоколів захисту інших комп'ютерних мереж у БСМ недостатньо. У результаті основними проблемами в дослідженнях безпеки в безпроводових сенсорних мереж є розробка ресурсооборотного протоколу безпеки. Для ефективного аутентифікованого розподілу ключів було запроваджено низку підходів, таких як попередній розподіл та ієрархічні схеми управління ключем, паралельні та групові ключові угоди. Отже, наші головні цілі - знизити навантаження під час процесу автентифікації, підвищити конфіденційність та забезпечити довготривалість роботи датчика.

### 3.2 Опис структури запропонованого протоколу

У цьому розділі ми описали нашу запропоновану схему протоколів для безпечного зв'язку маршрутизації та розподілу ключів в динамічних БСМ. На рис.3.1 показана блок-схема нашого запропонованого протоколу, що складається з базової станції (БС), двох основних вузлів (S1, S2) та підпорядкованого вузла (N). Ця структура ділиться на п'ять етапів тобто:

a) Етап 0: Визначення основних вузлів
b) Етап 1: Налагодження зв'язку між основними вузлами
c) Етап 2: Розподіл ключів автентифікації основними вузлами
d) Етап 3: Первинна автентифікація підпорядкованих вузлів
e) Етап 4: Вторинна аутентифікація підпорядкованих вузлів

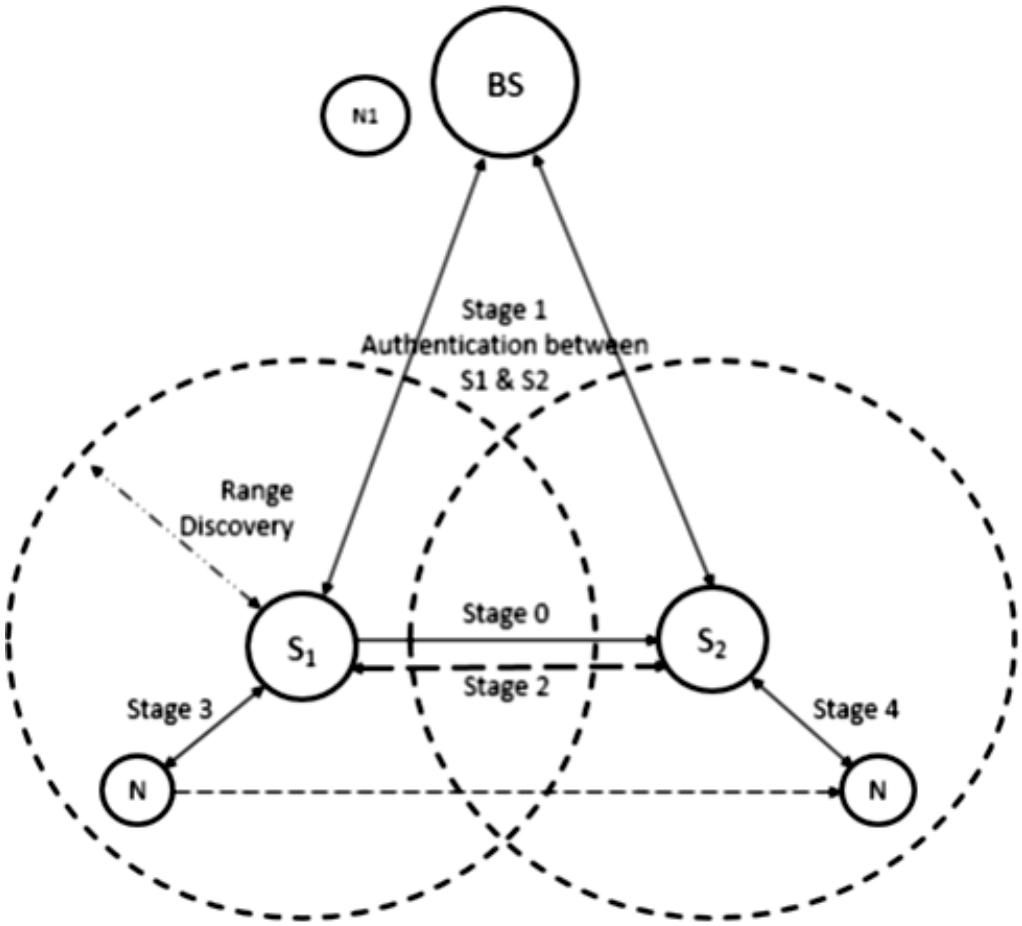


Рисунок 3.1Структурна схема запропонованої мережі

**Етап 0: Визначення основних вузлів**

На першому етапі, де основні вузли починають спілкуватися зі своїми 1-хоп сусідніми основними вузлами, вони транслюють пакет автентифікації в безпроводову сенсорну мережу. Цей пакет аутентифікації, як правило, містить привітне повідомлення, випадкове число R і поточний часовий покажчик, поряд з цими речами пакет також містить хеш-код аутентифікації повідомлень (MAC-хеш-код), щоб перевірити його конфіденційність на стороні приймача. Хеш-код визначає, чи надійний надісланий пакет, чи, можливо, в цій частині мережі спостерігається атака на мережу. Головний вузол S1 генерує пакет аутентифікації, який складається з R та його поточної мітки T, що транслюється в БСМ.

**Етап 1: Налагодження зв'язку між основними вузлами**

Кожного разу, коли основний вузол отримує пакет аутентифікації, який транслюється сусідніми основними вузлами, він ініціює процес налаштування зв'язку. Основний вузла генерує новий P. Поряд з новоутвореним R, основний вузол передає базовій станції отриманий пакет автентифікації та хеш-код для перевірки. З іншого боку, базова станція перевіряє пакети автентифікації та генерує два різних пакети відповідей, обмінюючись випадковими числами, отриманими обома пакетами автентифікації, через які обидва головні вузли створюють ключ цілісності за допомогою функції виведення ключів одним шляхом та отриманих випадкових чисел.

У етапі 0 та етапі 1 основний вузол S2 генерує пакет аутентифікації, який містить новий R з попереднім пакетом автентифікації основного вузла S1 і відправляє його на базову станцію BS. Базова станція, після отримання пакета автентифікації з основного вузла S2, генерує два пакети відповідей RP для S1 і S2, обмінюючи їх випадковими числами для розробки цілісності, використовуючи функцію виведення ключів одним шляхом і отриманих випадкових чисел S1 та S2.

**Етап 2: Розподіл ключів автентифікації основними вузлами**

Це етап, коли основні вузли повинні розділити ключі автентифікації до сусідніх основних вузлів, щоб він генерував два різних значення та відправляв його відповідним сусіднім основним вузлам. Основні вузли, які отримали ці значення, наступним кроком генерують ключі автентифікації, які необхідні для процесу вторинної аутентифікації. Головний вузол S1 та S2 ділиться своїми значеннями, щоб генерувати різні ключі автентифікації для кожного.

### Етап 3: Первинна автентифікація підпорядкованих вузлів

Це незалежний етап для первинної аутентифікації підпорядкованих вузлів. Якщо підпорядкований вузол взагалі не аутентифікується з будь-яким основним вузлом в БСМ, то потрібно спочатку перевірити чи підпорядкований вузол до цього основного вузла і перевірити діапазон підпорядкованих вузлів. Кожного разу, коли підпорядкований вузол отримав широкомовний пакет аутентифікації основного вузла з етапу 0, він генерує вузол R. Підпорядкований вузол надсилає пакет відповіді RP до основного вузла, який містить новостворюваний пакет R, пакета автентифікації основного вузла та хеш-код для цілей верифікації. Після отримання пакета відповідей від підпорядкованого вузла хеш-код створюється основним вузлом для прийнятого пакета і відправляє його на базову станцію з пакетом відповідей. Тут базова станція перевіряє хеш-коди основного та підпорядкованого вузлів і генерує два пакети відповідей, обмінюючи їх випадковими числами, через які основний вузол і підпорядкований вузол генерують бібліотеки автентифікації та відповідний хеш-код.

### Етап 4: Вторинна аутентифікація підпорядкованих вузлів

Коли підпорядкований вузол безперервно рухається в безпроводовій сенсорній мережі і намагається аутентифікувати з іншими основними вузлами, тоді процес описаний в Етапі 3 необхідно, тільки якщо це новий основний вузол, або він не сусід попереднього аутентифікованого основного вузла. Крім цього потрібно перевірити лише чи підпорядкований вузол від основного вузла сусіда. Кожного разу, коли підпорядкований вузол N отримав пакет автентифікації нового основного вузла, він генерує та відправляє пакет до нового основного вузла, який містить його квиток

аутентифікації попереднього основного вузла та хеш-код його квитка аутентифікації. Після цього основний вузол забезпечує новий квиток аутентифікації на підпорядкований вузол для успішної перевірки, і таким чином підпорядкований вузол повторно перевіряється новим основним вузлом.

### 3.3 Запропонована математична модель для безпечного шару маршрутизації протокол

Протокол безпечного маршрутизатора – це наша пропонована схема протоколу для безпечного зв'язку маршрутизації шару та розподілу ключів між основними та підлеглими вузлами. Розглянемо середовище БСМ з 40 вузлів, розміщених у мережі випадковим чином, з яких ми вибрали один вузол як базову станцію, декілька основних вузлів, а інші - підпорядковані вузли.

Тут P - сукупність фаз P = {P1, P2, P3, P4, P5}

**Етап 0**: $P_1=\{AP_I, E_I, M_I\}$

де I={1,2,3…10}

$P_1$ – виявлення і визначення основних вузлів

$AP_I$ – пакет автентифікації основних вузлів I

$E_I$ – зашифрований пакет основного вузла I

$M_I$ – MAC для основного вузла I

$AP_I=S_I+$”HELLO”$+E_I+M_I$

$S_I$ – визначення I-го основного вузла

$E_I=R_I \oplus T_I$

$h: (h(E_I) \oplus h(S_I)) \rightarrow M_I$

$E_I=E_K(E_I \oplus S_I)$

тут, $E_K$ – функція шифрування

$R_I$ – випадкова кількість I-го головного вузла

$T_I$ – поточна позначка часу

h – постійна хеш-функція

$S_I$: $AP_I \rightarrow$Network.

**Етап-1**: $P_2=\{P_{2(a)}, P_{2(b)}, P_{2(c)}, P_{2(d)}\}$

де, $P_2$ – налагодження зв'язку основних вузлів

a. $P_{2(a)}=\{AP_J, E_J, M_I, M_J\}$

де, J={1,2,3…10}

$AP_J$ – пакет аутентифікації основних вузлів J

$E_J$ – зашифрований пакет основного вузла J.

$M_J$ – MAC для головного вузла J.

$AP_J=S_J+B_{ID}+S_I+M_I+E_J+M_J$

$S_J$ –визначення J-го основного вузла

$B_{ID}$ – ідентифікація базової станції

$E_J=R_J \oplus E_I$

h: $(h(E_J)\oplus h(S_J)\oplus h(B_{ID})\oplus h(S_I)\oplus h(M_I)) \rightarrow M_J$

$E_J=E_K(E_J \oplus S_J)$

тут, $D_K$ – функція дешифрування

$R_J$ – випадковий номер J-го основного вузла

$S_J$:$AP_J \rightarrow B_{ID}$

b. $P_{2(b)}=\{RP_B, E_{BI}, E_{BJ}, M_{BI}, M_{BJ}\}$

$RP_B$ – пакет відповіді БС для встановлення зв'язку

$E_{BI}$ – зашифрований пакет від БС для I-го основного вузла.

$E_{BJ}$ – зашифрований пакет від БС для J-го основного вузла

$M_{BI}$ – MAC базової станції для I-го головного вузла

$M_{BJ}$ – MAC базової станції для J-го головного вузла

$RP_B=B_{ID}+S_J+S_I+E_{BJ}+M_{BI}+M_{BJ}$

$D_K(E_J \oplus S_J) \rightarrow E_J$

*Якщо* $M_J=h(h(S_J \oplus B_{ID} \oplus S_I \oplus E_J \oplus M_I))$

$E_I \oplus E_J \rightarrow R_J$

*Якщо* $M_I=h(h(E_I \oplus S_I))$

$E_I \oplus T_I \rightarrow R_I$

$E_{BI}=R_J \oplus T_I$

h: $(h(B_{ID}) \oplus h(S_J) \oplus h(E_{BI})) \rightarrow M_{BI}$

$E_{BJ}=R_I \oplus EBI$

h: $(h(B_{ID}) \oplus h(S_J) \oplus h(R_J) \oplus h(E_{BJ}) \oplus h(M_{BI})) \rightarrow M_{BJ}$

$E_{BI}=E_K(E_{BI} \oplus B_{ID})$

$E_{BJ}=E_K(E_{BJ} \oplus B_{ID})$

$B_{ID}$: $RP_B \rightarrow S_J$

c. $P_{2(c)}=\{RP_{JI}, K_{IJ}, IK_{IJ}, M_{JI}\}$

$RP_{JI}$ – пакет відповіді J-го основного вузла

$K_{IJ}$ – спільний ключ шифрування I-го та J-го основного вузла.

$IK_{IJ}$ – ключ цілісності I-го та J-го основного вузла.

$M_{JI}$ – MAC J-го основного вузла для I-го основного вузла.

$RP_{JI}=S_J+S_I+E_{BI}+M_{BI}+M_{JI}$

*Якщо* $M_{BJ}=h(h(B_{ID}) \oplus h(S_J) \oplus h(E_{BJ}) \oplus h(M_{BI}) \oplus h(R_J))$

$D_K(E_{BJ} \oplus B_{ID}) \rightarrow EBJ$

$K_{IJ}=K_F(0 \oplus R_I \oplus R_J)$

$IK_{IJ}=K_F(1 \oplus R_I \oplus R_J)$

h: $(h(S_J) \oplus h(S_I) \oplus h(R_I) \oplus h(R_J)) \rightarrow M_{JI}$

$S_J$: $RP_{JI} \rightarrow S_I$

d. $P_{2(d)}=\{ACK_C, K_{IJ}, IK_{IJ}, M_{IJ}\}$

$ACK_C$ – пакет підтвердження для налаштування зв'язку

$M_{IJ}$ – MAC I-го основного вузла для J-го основного вузла

$ACK_C=S_I+S_J+$”ACK”$+M_{IJ}$

*Якщо* $M_{JI}=h(h(S_J) \oplus h(S_I) \oplus h(R_I) \oplus h(R_J))$

$D_K(E_{BI} \oplus B_{ID}) \rightarrow E_{BI}$

$K_{IJ}=K_F(0 \oplus R_I \oplus R_J)$

$IK_{IJ}=K_F(1 \oplus R_I \oplus R_J)$

h: $(h(S_I)\oplus h(S_J)\oplus h(R_I)\oplus h(R_J))\rightarrow M_{IJ}$

$S_I$: $ACK_C\rightarrow S_J$

**Етап-2**: $P_3=\{P_{3(a)}, P_{3(b)}\}$

де $P_3$ – розподіл ключа автентифікації основного вузла

a) $P_{3(a)}=\{AKP_I, E_{AI}, M_{AI}\}$

$AKP_I$ – пакет ключової аутентифікації основного I-го вузла

$E_{AI}$ – зашифрований пакет ключів автентифікації I-го ОВ

$M_{AI}$ – MAC для пакету ключів аутентифікації I-го ОВ

$AKP_I=S_I+S_J+E_{AI}+M_{AI}$

$E_{AI}=R_{ASEED}\oplus R_{AI}$

h: $(h(S_I)\oplus h(S_J)\oplus h(E_{AI}))\rightarrow M_{AI}$

$E_{AI}=E_K(S_JE_{AI})$

тут, $R_{ASEED}$ – випадкове значення центрального I-го ОВ

$R_{AI}$ – випадковий номер I-го ОВ

$S_I$: $AKP_I\rightarrow S_J$

b) $P_{3(b)}=\{RKP_J, AK_I, AIK_I\ M_{AJ}\}$

$RKP_J$ – пакет ключів відповідей J-го ОВ

$AK_I$ – ключ автентифікації I-го ОВ

$AIK_I$ – ключ аутентифікації цілісності I-го ОВ

$M_{AJ}$ – MAC пакету відповідей J-го ОВ

$RKP_J=S_J+S_I+$”ACK”$+M_{AJ}$

If $M_{AI}=h(h(S_I)\oplus h(S_J)\oplus h(E_{AI}))$

$D_K(E_{AI}\oplus S_I)\rightarrow E_{AI}$

$R_{ASEED}=E_{AI}\oplus R_{AI}$

$AK_I=K_F(0\oplus R_{ASEED})$

$AIK_I=K_F(1\oplus RASEED)$

h: $(h(S_I)\oplus h(S_J)\oplus h(AIK_I))\rightarrow M_{AJ}$

**Етап 3**: $P_4=\{P_{4(a)}, P_{4(b)}, P_{4(c)}, P_{4(d)}, P_{4(e)}\}$

де $P_4$ – первинна автентифікація підпорядкованого вузла

a) $P_{4(a)}=\{AP_N, E_N, M_N\}$

$N=\{11,12…39\}$

$AP_N$ – пакет перевірки автентифікації N-го ПВ

$E_N$ – зашифрований пакет N-го ПВ

$M_N$ – MAC N-го ПВ

$AP_N=S_N+S_I+E_N+M_N$

$S_N$ – визначення N-го ПВ

$E_N=R_N \oplus E_I \oplus M_I$

$h: (h(S_N)\oplus h(S_I)\oplus h(E_N))\rightarrow M_N$

$S_N: AP_N \rightarrow S_I$

b) $P_{4(b)}=\{AP_{NI}, M_{NI}\}$

$AP_{NI}$ – первинний пакет аутентифікації I-го ОВ для N-го ПВ

$M_{NI}$ – MAC I-го ОВ для N-го ПВ

$AP_{NI}=S_I+B_{ID}+S_N+E_N+M_N+M_{NI}$

$h: (h(S_I)h(B_{ID})h(S_N)h(E_N)h(M_N))\rightarrow M_{NI}$

$E_I=E_K(E_I \oplus S_I)$

$S_I: AP_{NI} \rightarrow B_{ID}$

c) $P_{4(c)}=\{RP_{NB}, E_{BN}, M_{BN}, E_{BI}, M_{BI}\}$

$RP_{NB}$ – пакет відповіді аутентифікації базової станції

$E_{BN}$ – зашифрований пакет БС для N-го ПВ

$M_{BN}$ – MAC базової станції для N-го ПВ

$E_{BI}$ – зашифрований пакет БС для I-го ОВ та N-го ПВ

$M_{BI}$ – MAC БС для I-го ОВ та N-го ПВ

$RP_{NB}=B_{ID}+S_I+E_{BI}+M_{BI}$

*Якщо* $M_{NI}=h(h(S_I)\oplus h(B_{ID})\oplus h(S_N)\oplus h(E_N)\oplus h(M_N))$

$D_K(E_I \oplus S_I)\rightarrow E_I$

$R_N=E_N \oplus E_I \oplus M_I$

$E_{BN}=R_N$

$h: (h(B_{ID})\oplus h(S_N)\oplus h(S_I)\oplus h(E_{BN}))\rightarrow M_{BN}$

$E_{BI}=S_N \oplus E_{BN} \oplus M_{BN}$

h: $(h(S_I) \oplus h(B_{ID}) \oplus h(S_N) \oplus h(R_N) \oplus h(E_{BN})) \rightarrow M_{BI}$

$E_{BI}=E_K(E_{BI} \oplus B_{ID})$

$B_{ID}$: $RP_{NB} \rightarrow SI$

d) $P_{4(d)}=\{RP_{IN}, K_N, AT_{NI}\ M_{ANI}, E_{IN}, M_{IN}\}$

$RP_{IN}$ – пакет відповіді I-го ОВ для N-го ПВ

$K_{NI}$ – ключ шифрування для N-го ПВ з I-го ОВ

$AT_{NI}$ – аутентифікаційний квиток N-го ПВ з I-го ОВ

$M_{ANI}$ – MAC для квитка аутентифікації N-го ПВ від I-го ОВ

$E_{IN}$ – зашифрований пакет I-го ОВ для N-го ПВ

$M_{IN}$ – MAC I-го ОВ для N-го ПВ

$RP_{IN}=S_I+S_N+E_{BN}+M_{BN}+E_{IN}+M_{IN}$

*Якщо* $M_{BN}=h(h(S_I) \oplus h(B_{ID}) \oplus h(S_N) \oplus h(R_N) \oplus h(E_{BN}))$

$D_K(E_{BI} \oplus B_{ID}) \rightarrow E_{BI}$

$E_{BN}=E_{BI} \oplus S_N$

$K_{NI}=K_F(R_J \oplus R_N)$

$AT_{NI}=T_I \oplus R_N \oplus K_{NI}$

h: $(h(S_N) \oplus h(AT_{NI})) \rightarrow M_{ANI}$

$E_{IN}=AT_{NI} \oplus M_{ANI} \oplus T_I$

h: $(h(S_I) \oplus h(S_N) \oplus h(R_I) \oplus h(E_{IN})) \rightarrow M_{IN}$

$E_{BN}=E_K(E_{BN} \oplus S_I)$

тут, $K_F$ – функція одностороннього виведення ключів

$S_I$: $RP_{IN} \rightarrow S_N$

e) $P_{4(e)}=\{ACK_{NI}, M_{AI}\}$

$ACK_{NI}$ – підтвердження пакета N-го ПВ для квитка аутентифікації.

$M_{AI}$ – MAC N-го ПВ для I-го ПВ

$ACK_{NI}=S_N+S_I+M_{AI}$

*Якщо* $M_{IN}=h(h(S_I) \oplus h(S_N) \oplus h(R_I) \oplus h(E_{IN}))$

$D_K(E_{BN} \oplus S_I) \rightarrow E_{BN}$

h: $(h(S_N)\oplus h(S_I)\oplus h(R_N)\oplus h(R_I))\rightarrow M_{AI}$

$S_N$:$ACK_{NI}\rightarrow S_I$

**Етап 4: P5={$P_{5(a)}$, $P_{5(b)}$, $P_{5(c)}$}**

де, $P_5$ – вторинна аутентифікація підпорядкованих вузлів

a) $P_{5(a)}=\{AP_{NJ}, M_{NJ}\}$

$AP_{NJ}$ – пакет аутентифікації N-го ПВ для повторної автентифікації

$M_{NJ}$ – MAC N-го ПВ для повторної автентифікації

$AP_{NJ}=S_N+S_J+AT_{NI}+M_{ANI}+M_{NJ}$

$D_K(E_J\oplus S_J)\rightarrow E_J$

h: $(h(S_N)\oplus h(S_J)\oplus h(AT_{NI})\oplus h(M_{ANI})\oplus h(E_J))M_{NJ}$

$S_N$: $AP_{NJ}\rightarrow S_J$

b) $P5(b)=\{RP_{JN}, K_{NJ}, AT_{NJ}, M_{ANJ}, E_{JN}, M_{JN}, M_{RJ}\}$

$RP_{JN}$ – пакет відповіді J-го ПВ для повторної автентифікації

$K_{NJ}$ – ключ шифрування для N-го ПВ від J-го ОВ

$AT_{NJ}$ – аутентифікаційний квиток N-го ПВ з J-го ОВ

$M_{ANJ}$ – MAC для квитка аутентифікації N-го ПВ з J-го ОВ

$E_{JN}$ – зашифрований пакет J-го ОВ для N-го ПВ

$M_{RJ}$ – MAC J-го ОВ для ключа шифрування

$M_{JN}$ – MAC J-го ОВ для N-го ПВ

$RP_{JN}=S_J+S_N+E_{JN}+M_{JN}$

$K_{NJ}=K_F(R_J\oplus R_N)$

$AT_{NJ}=R_N\oplus K_{NJ}$

h: $(h(S_N)\oplus h(AT_{NJ}))\rightarrow M_{ANJ}$

h: $(h(K_{NJ})\oplus h(R_J))\rightarrow M_{RJ}$

$E_{JN}=R_J\oplus M_{RJ}\oplus AT_{NJ}\oplus M_{ANJ}$

h: $(h(S_N)\oplus h(S_J)\oplus h(M_{ANJ}))\rightarrow M_{JN}$

$S_{ID2}$: $R_{RT}\rightarrow N_{ID1}$

c) $P_{5(c)}=\{ACK_{NJ}, M_{AJ}\}$

$ACK_{NI}$ – підтвердження пакета N-го ПВ для повторного аутентифікації квитка.

$M_{AI}$ – MAC N-го ПВ для J-го ПВ

$ACK_{NJ}=S_N+S_J+M_{AJ}$

*Якщо* $AT_{NJ}=R_N \oplus K_{NJ}$

h: $(h(S_N)\oplus h(S_J)\oplus h(R_N)\oplus h(R_J))\rightarrow M_{AJ}$

$S_N$: $ACK_{NJ}\rightarrow S_J$

### 3.4 Оцінка продуктивності та результат аналіз

Підтримка оновлення ключів є найважливішою необхідністю безпеки та запобігання різним типам атак. В рамках пропонованого протоколу ми використали методику генерації випадкових генераторів для збереження оновлення ключів в мережі безпроводових датчиків. У нашій схемі на кожному етапі ми створили випадкові числа. У стадії 0 основні вузли транслюють пакет, який містить випадкове число, яке зберігає унікальність переданого пакету. У першому етапі основний вузол генерує пакет для цілей верифікації, а пізніше створює ключі цілісності, що містить випадкові числа. На етапі 2, коли основні вузли хочуть обмінюватися ключами автентифікації з його сусідні майстерні вузли містять значення насіння нічого, крім випадкового числа. Аналогічним чином ми використали випадкові числа для первинної та вторинної аутентифікації підлеглих вузлів, як описано в стадіях 3 і 4 нашого пропонованого протоколу.

Конфіденційність агрегації та поширення даних є ще одним важливим питанням в мережах бездротових датчиків. Ми використовували хеш-код (MAC) на кожному етапі нашого пропонованого протоколу, щоб перевірити конфіденційність переданих пакетів у мережі бездротових датчиків. Якщо зловмисник пакує пакет між

повідомленнями вузлів, хеш-код MAC змінює його значення, а на стороні приймача він не перевірятиметься на все.

У рамках запропонованого нами протоколу, коли підпорядкований вузол аутентифікується основним вузлом, підпорядкований вузол отримує квиток аутентифікації. У міру того, як підпорядкований вузол переміщається та запитує повторну автентифікацію до сусіднього основного вузла, новий основний вузол перевіряє квиток аутентифікації підпорядкованого вузла. Після успішного підтвердження основний вузол забезпечує новий квиток аутентифікації для підпорядкованого вузла. Наша методика зменшує робоче навантаження базової станції та відповідну кількість пакунків керування маршрутизацією.

**Висновок до розділу 3:**

У даному розділі розглянуто особливості використанні безпроводових сенсорних мереж з мобільними вузлами.

Також в даному розділі запропоновано структуру протоколу для обміну інформацією по безпечним каналом маршрутизації та розподілу ключів у мобільному БСМ, а також відповідну математичну модель. В основному математична модель дає нам правильний потік системи. Запропонована схема зосереджена на маршрутизації накладних витрат у порівнянні з протоколом DSR, який забезпечує загальну гнучкість результат.

# ВИСНОВОК

В результаті даної магістерської роботи було запропонована нова методика для роботи протоколу маршрутизації в безпроводових сенсорних мережах. Для розробки цієї методики у роботі було проведено аналіз особливостей експлуатації та вимог до характеристик безпроводових сенсорних мереж. Було наведено теоретичне обґрунтування необхідності розвитку систем безпеки для БСМ.

В ході даної роботи було проаналізовано основні принципи та вимоги до використанні безпроводових сенсорних мереж. Розглянуто основні проблеми, які виникають при використанні існуючих методів захисту інформації, а також особливості БСМ, які потрібно враховувати при розробці методів спеціально для таких мереж. Також розглянуті показники надійності для безпроводових сенсорних мереж, які дозволяють оцінити безпечність мережі в цілому при її роботі.

Також в ході даної роботи було розглянуто можливі атаки на мережу. Спосіб їх втілення, прояви та можливі наслідки. Наведено приклади таких атак. Оскільки безпроводові сенсорні мережі розгортаються на віддаленій території і без нагляду, вони є дуже вразливими. Тому такі атаки здійснюються на всіх рівнях моделі OSI. Починаючи фізичним впливом, коли виходить з ладу сам вузом і закінчуючи впливом на додатки, які використовуються для роботи мережі. Таким чином дане питання є важливим і потребує вирішення на всіх рівнях.

В ході роботи було запропоновано структуру протоколу, який дозволяє проводити обмін та розподіл ключів в безпроводових сенсорних мережах з мобільними вузлами. Даний метод дозволяє заощадити ресурси самого вузла та забезпечити надійність аутентифікації та розподілу ключів між основними вузлами та при призначенні цих ключів для підпорядкованих вузлів. А також забезпечує надійну перевірку аутентифікованого вузла при його переміщенні і переході з зони впливу одного основного вузла до іншого.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. C.Siva Ram Murthy, B.S.Manoj ―Ad Hoc Wireless Networks: Architectures and Protocols‖, Prentice Hall, 2004, 880p.
2. Акимов Е.В., Кузнецов М.Н. Вероятностные математические модели для оценки надежности беспроводных сенсорных сетей // Электронный журнал «Труды МАИ». Выпуск № 40// URL: http://www.mai.ru/science/trudy/
3. Половко А.М., Гуров С. В. Основы теории надежности. – СПб.: БХВ-Петербург 2006. – 560 с.
4. Острейковский В.А. Теория надежности. – М.: Высшая школа, 2000. – 464 с.
5. Шахнович И.А. Современные технологии беспроводной связи. – М.: Техносфера, 2006. – 288 с.
6. Смелянский Р. Л. Компьютерные сети. В 2 томах. Том 1. Системы передачи данных. – М.: Академия, 2011. – 304 с.
7. Нечаев Д.Ю., Чекмарев Ю.В. Надежность информационных систем. – М.: ДМК Пресс, 2012. – 64 с.
8. Luis Javier García Villalba , Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera, Cláudia Jacy Barenco Abbas. Routing Protocols in Wireless Sensor Networks // Sensors // – 2009 – 9 – P. 399 – 421.
9. Venkatesan, L.; Shanmugavel, S.; Subramaniam, C. A survey on modeling and enhancing reliability of wireless sensor network. Wirel. Sens. Netw. 2013, 41-51.
10. Senouci, M.R.; Melouk, A.; Senouci, H.; Aissani, A. Performance evaluation of network lifetime spatial-temporal distribution for WSN routing protocols. J. Netw. Comput. Appl. Elsevier 2012, 35, 1317–1328.
11. Zonouz, A.E.; Xing, L.; Vokkarane, V.M.; Sun, Y. Application communication reliability of wireless sensor networks supporting K-coverage. In Proceedings of the 2013 IEEE International Conference on

Distributed Computing in Sensor Systems, Cambridge, MA, USA, 20–23 May 2013; pp. 430–435.

12. Antônio Dâmaso, Nelson Rosa, Paulo Maciel. Reliability of Wireless Sensor Networks, 25 August 2014
13. Ефремов В. В., Маркман Г. З. «Энергосбережение» и «энергоэффективность»: уточнение понятий, система сбалансированных показателей энергоэффективности // Известия Томского политехнического университета. 2007. Т. 311, № 4. С. 146–148.
14. Vullers R., van Schaijk R., Doms I. et al. Micropower energy harvesting //Solid-State Electronics. 2009. Vol. 53, no. 7. P. 684 – 693.
15. Zhang H., Shen H. Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks // IEEE Trans. Parallel Distrib. Syst. 2009. Vol. 20, no. 10. P. 1526–1539.
16. Gun M., Kosar R., Ersoy C. Lifetime optimization using variable battery capacities and nonuniform density deployment in wireless sensor networks // Computer and information sciences, 2007. iscis 2007. 22nd international symposium on. 2007. P. 1–6.
17. Halder S., Ghosal A., Chaudhuri A., DasBit S. A probability density function for energy-balanced lifetime-enhancing node deployment in WSN // Proceedings of the 2011 international conference on Computational science and its applications - Volume Part IV. ICCSA'11. Berlin, Heidelberg: Springer-Verlag, 2011. P. 472–487.
18. Chen Y., Nasser N. Energy-balancing multipath routing protocol for wireless sensor networks // Proceedings of the 3rd international conference on Quality of service in heterogeneous wired/wireless networks. QShine '06. New York, NY, USA: ACM, 2006.
19. Баскаков С. С. Исследование способов повышения эффективности маршрутизации по виртуальным координатам в беспроводных

сенсорных сетях // Вестник МГТУ им. Н. Э. Баумана. Сер. Приборостроение. 2009. № 2. С. 112–124.

20. Комаров М. М., Восков Л. С. Позиционирование датчиков беспроводной сети как способ энергосбережения // Датчики и системы. 2012. Т.1. С. 34–38.
21. Castalia official site URL: http://castalia.research.nicta.com.au/
22. Туранська О.С., Лисенко О.І. Захист інформації у безпроводових сенсорних мережах // Туранська О.С., Лисенко О.І. - «Проблеми телекомунікації»: одинадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-17) 18-21 квітня 2017 р., К.: с. 420…422;
23. Туранська О.С., Петрова В.М. Керівні принципи та підходи до захисту інформації у безпроводових сенсорних мережах // Туранська О.С., Петрова В.М. - «Проблеми телекомунікації»: дванадцята міжнародна науково-технічна конференція, присвячена Дню науки та Всесвітньому Дню телекомунікацій (ПТ-18) 16-20 квітня 2018 р., К.: с. 383…385.