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

Інститут телекомунікаційних систем
(повне найменування інституту, факультету)

Кафедра телекомунікацій
(повна назва кафедри)

До захисту допущено
В.о. завідувача кафедри
_____ Валерій ЯВІСЯ
(підпис) (Ім'я, прізвище)
"___"_____2020_р.

Дипломна робота

на здобуття освітнього ступеня "бакалавр"
(назва ОС)

Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

на тему: Способи забезпечення інформаційної безпеки сенсорних мереж_____
_____
_____

Виконав: студент __4_ курсу, групи _ТЗ-62___
(шифр групи)

Суліковський Олексій Сергійович _____ _____
(прізвище, ім'я, по батькові) (підпис)

Керівник в.о. зав. кафедри телекомунікацій к.т.н. доцент Явіся В.С.___ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

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

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

Студент _____
(підпис)

Київ – 2020_ року

РЕФЕРАТ

Тема роботи: способи забезпечення інформаційної безпеки в сенсорних мережах.

Текстова частина дипломної роботи: 50с, 9 таблиць, 17 рисунків, 13 посилань.

Мета роботи – описати причини необхідності забезпечення інформаційної безпеки у WSN. Визначити основні проблеми забезпечення ІБ у WSN. Детально проаналізувати способи забезпечення ІБ у WSN. Провести аналіз ІБ в відомих технічних реалізаціях бездротових сенсорних мереж. Та комплексне порівняння алгоритмів шифрування для використання в бездротових сенсорних мережах

Результатом даної роботи є обґрунтування актуальності проблем забезпечення інформаційної безпеки у WSN. Описано особливості побудови WSN, наведено кількісні та якісні показники обмежень наявних при побудові WSN. Було проведено комплексний аналіз алгоритмів шифрування, що використовуються у WSN, за яким були надані рекомендації вибору алгоритму при побудові мережі.

Бездротові сенсорні мережі, WSN, інформаційна безпека, алгоритми шифрування, ZigBee, LoRaWan, SNEP, Rijndael.

ABSTRACT

The goal of the work: ways to ensure information security of sensor networks.

The text part: 50p, 9 tables, 17 pictures, 13 references.

The purpose of the work is to describe the reasons for the needs for information security in WSN. Identify the main problems of IS provisioning in WSN. Analyze in detail the ways to provide IS in WSN. To analyze IS in known technical implementations of wireless sensor networks. And a comprehensive comparison of encryption algorithms for use in wireless sensor networks

The result of this work is substantiating of the relevance of information security issues in WSN. The peculiarities of WSN construction are described, quantitative and qualitative indicators of limitations at WSN construction are given. A comprehensive analysis of encryption algorithms used in WSN was conducted, which provides recommendations for the choice of algorithm when building a network

Wireless sensor networks, information security, encryption algorithms, ZigBee, LoRaWan, SNEP, Rijndael

ПЕРЕЛІК СКОРОЧЕНЬ

WSN	wireless sensor network
LPWAN	low-power wide-area Network
IoT	Internet of Things
IIoT	Industrial Internet of Things
SPINS	Security Protocols for Sensor Networks
MAC	Message authentication code
UDP	User datagram protocol
DoS	denial-of-service
ECC	Elliptic Curve Cryptography
ПУК	Протокол управління ключами
KDC	Key Distribution Center KDC
LEAP	Localized encryption and authentication protocol
PIKE	Peer intermediaries for key establishment
BLE	Bluetooth Low Energy
MAC	Medium Access Control
MITM	Men in the middle
APS	Application Support sub-layer
ZDB	ZigBee Device Object
ISM	Частотний діапазон Industrial, Scientific, Medical
RPL	Routing Protocol for Low-Power and Lossy Network
SAP	Service Access Point

ВСТУП

Сьогодні мабуть кожен чув про таке речі, як IoT, IIoT, розумний будинок, розумний офіс чи квартира. Та про те, що зовсім скоро безліч речей починаючи від лампочок в квартирах, до складних пристроїв для моніторингу здоров'я людини, в не залежності від її місця знаходження, таких як глюкометр, будуть підключені до єдиної мережі інтернет. Так багато хто з нас уявляє найближче майбутнє.

Однак для досягнення цього, необхідно вирішити ряд критично важливих завдань. Одним із таких завдань є забезпечення інформаційної безпеки всіх пристроїв в цій мережі майбутнього. Проблема полягає в тому, що пристрої цієї мережі часто неможливо підключити до постійного джерела живлення а передачу даних виконувати через проводові мережі. Лише уявіть скільки додатково ресурсів необхідно для того, щоб створити мережу моніторингу вільних місць для паркування автомобілів в місті, якщо до кожного датчика, що відслідковує є парко місце вільним чи ні необхідно було провести лінію енергопостачання та кабель для підключення його до мережі. І навіть, якщо в містові це можливо зробити пішовши на великі витрати, то для розгортання мереж для сейсмічного моніторингу чи моніторингу станів лісів, води така реалізація неможлива. Виходячи з цього було сформовано визначення нового типу мереж WSN- wireless sensor network.

WSN складається з сотень чи навіть тисяч малих пристроїв, вузлів, кожен з яких має сенсор, процесор та обладнання для комунікації, їх завданням є моніторинг за навколишнім світом. Для прикладу їх можна використовувати для: медичного моніторингу, управління електроенергією, управління логістикою та запасами, моніторингу поля боя під час проведення військових операцій чи контролю за кордоном.

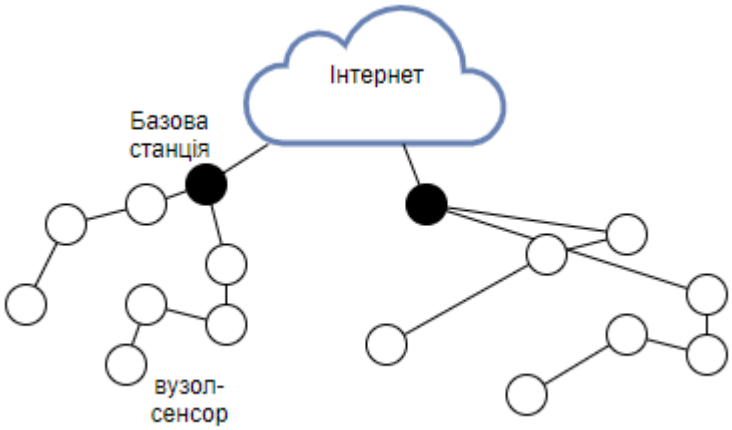

Рисунок 1.1. архітектура типової WSN

Ці мережі встановлюються на великих відкритих територіях куди складно дістатися людині, та де умови роботи часто є екстремальними для пристроїв. На даний час вже існує безліч додатків основаних на WSNs, де мережі розгорнуті як в приміщеннях таких, як офіси, житлові будинки, склади, заводи тощо так і на відкритих територіях, так для прикладу компанія Газпром розгорнула WSN для контролю тиску в підземних сховищах. Як свідчать передові компанії, які працюють в цій сфері к-сть пристроїв, що підключені до таких мереж буде стрімко рости рисунок. 1.2.

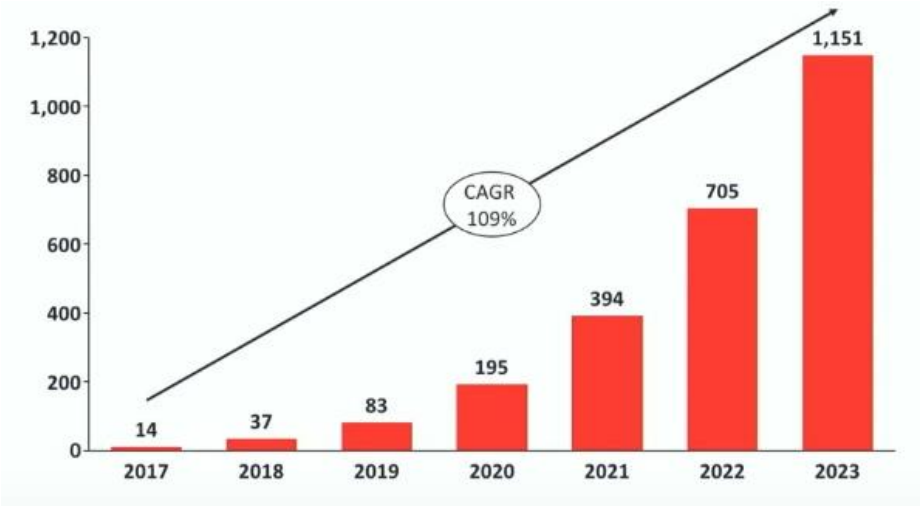

Рисунок 1.2. Розмір ринку LPWAN по к-сті підключених пристроїв (мільйони)

Однак через значні технічні обмеження у вузлах мережі, та їх встановлення у віддалені райони, WSNs являться вразливими до великого

числа загроз інформаційній безпеці таких як блокування доступності інформації чи її спотворення. Проблема може нести серйозну загрозу, коли подібні мережі використовуються в критично важливих сферах, таких як військова чи медична. Де на основі отриманої з них інформації виносяться рішення, що мають вплив на фізичний світ. Іншим прикладом реальної загрози може бути так званий виробничий шпіонаж, коли атака спрямована на сенсорну мережу, що розгорнута на заводі для управління процесом виробництва. Ціллю такої атаки є отримання інформації, що являється комерційною таємницею. Ситуацію ускладнює те, що сенсори які є вузлами мережі мають значні обмеження в їх ресурсах, пам'яті, потужності процесора, та енергозатратах. Ці обмеження продиктовані економічною складовою, адже для розгортання WSN необхідна значна к-сть сенсорів, тому їх ціна повинна буди мінімальною. Оптимальною вважається, що ціна одного вузла мережі повинна складати 1 долар. Наразі жоден виробник не зміг досягнути цієї ціни, так ціна сенсор UC11-T1, що призначений для моніторингу вологості та температури на відкритій території становить 90 доларів США. Як результат вузли таких мереж мають малі обчислювальні ресурси, тому використання традиційних методів забезпечення безпеки з їх великими накладними витратами на комунікацію та обчислення є досить складним у WSNs. Тому перед нами гостро постає питання, розроблення та імплементації способів забезпечення інформаційної безпеки у WSN, що будуть потребувати мінімум додаткових затрат. На даний час існує декілька ефективних протоколів маршрутизації [1-4] та агрегації даних [5-6], що відповідають вимогам WSN.

Додатково до традиційних проблем безпеки, як безпечна маршрутизація та агрегація даних, механізми безпеки розвернуті у WSNs також включають комунікацію між вузлами яка має децентралізований характер. В реальному світі сенсори не можуть бути підключені до мережі, на основі апріорної довіри. Тому дослідники сконцентрувалися на побудові моделі реєстрації сенсорів в мережі для розв'язання проблем які значно виходять за межі традиційних криптографічних механізмів.

1 ОСОБЛИВОСТІ ПОБУДОВИ WSN

Інформаційна безпека- це стан системи обробки і зберігання даних, при якому забезпечується конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів спрямований на забезпечення захищеності інформаційної особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення.

1.1 Вимоги Безпеки у WSN

WSN є особливим типом бездротової мережі, вона розділяє деякі спільні риси з типовою комп'ютерною мережею. Але також має багато унікальних властивостей. Сервіси безпеки у WSN повинні надавати надійний захист інформації. Найбільш важливими вимогами до WSN з інформаційної безпеки є наступні.

Конфіденційність даних: механізм захисту повинен забезпечити відсутність повідомлень у мережі які є доступними будь-кому, окрім призначеного одержувача. У питанні конфіденційності WSN повинні відповідати наступним вимогам [7]:

1) вузол-сенсор не повинен допускати його читання, сусідніми вузлами. За виключенням коли їм надано санкціонований доступ
2) механізм розповсюдження ключів по вузлах мережі повинен бути максимально надійним.
3) публічна інформація, така як ідентифікатори сенсорів та відкриті ключі вузлів також повинні бути зашифровані у певних випадках для захисту проти атак аналізу трафіку.
4) система не повинна мати доступ до інформації користувача. Так інформація зібрана вузлами не повинна бути доступна любим іншим сервісам окрім, самої WSN мережі та додатку зберігання та обробки користувача .

Цілісність даних: механізм повинен гарантувати, що жодне повідомлення не може бути змінено протягом його передачі від відправника до одержувача. Наприклад в SPINS, це досягається через автентифікацію даних.

Актуальність даних: це означає, що дані є актуальними і гарантує, що ніхто не зможе відтворити старі повідомлення. Ця вимога особливо важлива, коли вузли WSN використовують спільні ключі для комунікації, де потенційний зловмисник може запустити атаку повторного використання старого ключа під виглядом нового та розповсюдити його по всій мережі, оскільки новий ключ оновлюється та розповсюджується на всі вузли WSN. Тому такі мережі повинні мати надійний механізм синхронізації.

Самоорганізація: кожен вузол WSN повинен бути самоорганізованим та здатним до самостійного відновлення. Ця особливість WSN також становить великий виклик для безпеки. Через динамічний характер WSN іноді неможливо розгорнути будь-який попередньо встановлений механізм спільного ключа серед вузлів та базової станції [8]. Запропоновано ряд ключових схем попереднього розподілу в контексті симетричного шифрування [8-9]. Однак для застосування криптографічного шифрування методом відкритого ключа, дуже важливим є механізм передачі ключа, бажано щоб вузли самоорганізовувались не лише для передачі інформації але і для управління механізмом управління ключами.

Автентифікація: зловмисник може не лише модифікувати данні в пакеті але і змінити потік пакетів ін’єкцією сфабрикованих пакетів. Тому для приймача важливо мати механізм верифікації, для підтвердження того факту що пакети прийшли дійсно від актуального відправника. У разі комунікації між двома вузлами, автентифікація даних може бути досягнута через message authentication code (MAC), обчислений на основі спільного ключа

Доступність: данні повинні бути доступні користувачеві коли вони є необхідними

Рисунок 1.3. Основні вимоги інформаційної безпеки у WSN

1.2 Обмеження у WSNs

Для глибшого розуміння складності створення надійних методів захисту інформації у WSN необхідно більш детально ознайомитися з технічними обмеженнями висунутими до вузлів. Кожен вузол має обмежену обчислювальну здатність, дуже малий об'єм внутрішньої пам’яті, та обмежену смугу пропускання.

Енергетичні обмеження: Енергія є найбільшим обмеженням для WSNs. Загалом, енергетичні витрати в вузлах-сенсорах можна класифікувати на три категорії: 1) витрати сенсора на отримання інформації, 2) витрати для зв'язку між вузлами, і 3) витрати на мікропроцесорні обчислення. Дослідження [10] виявило, що кожен біт що передається у WSN споживає приблизно стільки ж енергії, скільки ж виконання 800 - 1000 інструкцій. Таким чином, комунікація коштує дорожче, ніж обчислення у WSN. Будь-яке збільшення обсягу повідомлень, пов'язане з забезпечення безпеки призводить до значного підвищення енергетичних витрат на комунікацію. Крім того, вищий рівні безпеки у WSNs зазвичай відповідають більшим споживанням енергії для криптографічних функцій. Таким чином, WSNs можуть бути поділені на різні рівні безпеки залежно від енергетичних витрат.

Обмеження пам’яті: сенсор- це крихітний пристрій, у якого є лише невелика кількість пам'яті. Вона як правило, включає флешпам'ять і оперативну пам'ять. Зазвичай є в них недостатньо місця для запуску складних алгоритмів після завантаження ОС та коду програми. Так в проєкті SmartDust,

TinyOS, що часто використовується в таких вузлах, споживає близько 4 К байт інструкцій, залишаючи лише 4500 байтів для запуску алгоритмів та програм захисту. Звичайний датчик типу TelosB - має 16-бітний 8 МГц RISC процесор із лише 10КБ RAM та 1024КБ флешпам'яті. Через такі значні обмеження в пам'яті поточні алгоритми шифрування є нездійсненими у WSNs

Ненадійний зв'язок: це ще одна серйозна загроза безпеки сенсора. Зазвичай маршрутизація сенсорних мереж здійснюється на основі пакетів з використанням протоколів, що працюють без встановлення попереднього з'єднання, подібних до UDP, як результат успадковує їх вразливість. Пакети можуть бути пошкодженими через помилки в каналі передачі чи бути відкинутими по причині завантаженості одного з вузлів. В певних ситуаціях, навіть якщо канал надійний, зв'язок може бути не надійним через колізії, які можуть виникнути при передачі пакетів, і вимагати повторної передачі пакетів

Більш висока затримка в комунікації: у WSNs, багато вузловій маршрутизації, перевантаженість мережі та обробка в проміжних вузлах може призвести до більш високої затримки передачі пакетів. Це робить досягнення синхронізації дуже складним процесом. Проблеми синхронізації можуть бути дуже критичними для забезпечення безпеки, оскільки часто механізми безпеки покладаються на сповіщення про критичні події та доставлення криптографічних ключів.

Розташування мережі у віддалених регіонах: у більшості випадків вузли WSNs розгорнуті в віддалених регіонах і залишаються без нагляду. Існує висока ймовірність, що сенсор може зазнати фізичної атаки та бути зламаним. Виявити фізичне підроблення вузла практично неможливо. Це робить забезпечення безпеки всієї WSN надзвичайно складним завданням

1.3 Вразливості в бездротових сенсорних мережах.

У цьому розділі ми розглянемо найбільш поширені атаки на WSN, адже краще розуміння можливих атак дасть змогу створити більш надійну систему захисту. WSN вразливі до широкого спектра атак. Ці атаки можуть бути грубо класифіковані наступним чином:

- Атаки на конфіденційність та автентифікацію: це перехват повідомлень, повторна передача пакетів, та модифікація пакетів. Стандартні криптографічні техніки можуть захистити від цього типу атак на комунікаційні канали.
- Атаки на доступність мережі: атаки цього типу часто відносяться до так званих denial-of-service (DoS). DoS атаки можуть бути направлені на будь-який рівень мережі.
- Приховані атаки проти цілісності мережі: при таких атаках метою є заставити мережу приймати неправдиву інформацію. Наприклад, зловмисник, отримавши доступ до одного з вузлів можу здійснювати ін’єкцію неправдивої інформації. Такі атаки можуть бути катастрофічними, у випадках коли на основі даних отриманих з мережі приймаються життєво важливі рішення. Наприклад, в медицині.

Нижче наведений більш детальний огляд цих типів атак.

Атака реплікації вузла: при цій атаці зловмисник, намагається підключитися до WSN за допомогою реплікації/копіювання існуючого вузла мережі. Репліковий та підключений вузол потенційно може створити ряд загроз передачі пакетів, через спотворення та маршрутизацію пакету на невірний вузол мережі. Додатково якщо зловмисник має фізичний доступ до всієї мережі, для нього відкривається можливість скопіювати криптографічні ключі, що використовуються при передачі пакетів. Є очевидним той факт, що у такому випадку зловмисник матиме доступ до даних, що передаються мережею.

Атака на конфіденційність

Оскільки WSN здатні до автоматичного збору даних, ці мережі також вразливі до потенційних атак на отримання зібраних даних. Збереження конфіденційності даних у WSN є особливо важким викликом.

Окрім того, зловмисник може збирати, здавалося б без обідні дані, для отримання конфіденційної інформації якщо він знає, як агрегувати, зібрану інформацію з декількох вузлів.

Нижче наведені загальні атаки на конфіденційність інформації у WSN

- Підслуховування та пасивний моніторинг. Це найбільш часта та досить легка у виконанні атака на конфіденційність. Якщо пакети передаються мережею без шифрування, зловмисник легко може розпізнавати та збирати контент. Також WSN передає пакети зі службовою інформацією, маючи цю інформацію зловмисник може здійснювати інші типи атак, аж до захоплення всієї мережі.
- Аналіз трафіку. Для виконання ефективної атаки на конфіденційність підслуховування може комбінуватися з аналізом трафіку. Який використовується для ідентифікації вузлів, які відіграють специфічну роль у мережі. Так наприклад раптове зростання трафіку, що передається між певними вузлами, може свідчити про особливу роль цих вузлів, таку як пере генерацію криптографічних ключів
- Маскування. Зловмисник може отримати доступ до одного вузлів чи ввести в мережу свій під маскування справжнього вузла мережі, з метою подальшої маніпуляції маршрутизацією пакетів. Таким чином зловмисник може керувати маршрутизацією та перенаправляти пакети на певні вузли де виконувати збирання та аналіз інформації.

Слід зауважити, що WSNs мережі зазвичай після збору інформації передають її на сервери по протоколу TCP/IP, таким чином вони також являються вразливими до відомих атак на TCP/IP рівні.

Атаки відмови сервісу Denial of Service

DoS атака це будь-яка подія спрямована на зменшення здатності мережі виконувати її функції. Прості DoS атаки спрямовані на виснаження ресурсів мережі, через відправлення великої кількості непотрібних пакетів інформації до мережі, наприклад велику к-сть запитів на реєстрацію нового вузла в мережі. Це призводить до низки проблем для мережі. Перш за все якщо в

зловмисника є достатня к-сть ресурсів він може заповнити весь трафік мережі непотрібною інформацією що унеможливить виконання нею функцій збору та передачі інформації. По друге це призводить до додаткових енергетичних витрат, таким чином сенсорні вузли, що працюють на батареях можуть значно скоріше розрядитися. Ще однією проблемою являється можливість зловмисника заблокувати доступ до інформації в режимі реального часу. Таким чином прості в реалізації DoS атаки являються серйозною загрозою інформаційній безпеці та потребують ефективного механізму боротьби з ними.

У WSNs DoS атаки можливі на різних рівнях передачі даних. На фізичному рівні це може бути глушіння радіосигналу (jamming). На канальному рівні це можу бути спроба створення колізій. Тоді як на мережевому рівні це дезорієнтація передачі пакетів, чорні дірки, коли один з вузлів мережі викидає певні пакети. Чорні діри особливо важко виявити коли вузол викидає лише певні пакети по випадковому правилу, такі атаки ще називають сірими дірами. Механізми боротьби з ними включають строгу автентифікацію та ідентифікацію трафіку, також можлива плата за ресурси мережі.

Висновки з розділу 1

Основні вимоги до інформаційної безпеки у WSN є: конфіденційність, автентифікація, актуальність, цілісність, доступність та самоорганізація. Головними проблемами для забезпечення безпеки у WSN є можливість фізичного доступу зловмисників до мережі та значні обмеження в ресурсах вузлів-сенсорів, що продиктовані економічною складовою, такі як: енергетичні, обмеження в пам’яті, та обчислювальної потужності процесорів. В той час, як основні атаки на WSN можуть бути спрямовані на такі механізми мережі, як встановлення та розповсюдження криптографічних ключів мережею, з цілю отримати криптографічні ключі. Також WSN є вразливими до DoS атак, та атак реплікації вузлів-сенсорів.

2 МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У WSN

2.1 Криптографія у WSN

Вибір криптографічного методу шифрування даних являється ключовим завдання для побудови надійної WSN. Слід зауважити що наразі не існує одного рішення яке відповідало б різним типам WSN. Тому при побудові мережі необхідно оцінювати бажані характеристики мережі такі як, очікувана к-сть вузлів та швидкість передачі даних, енергоспоживання, вартість та необхідний рівень безпеки. В даному розділі ми розглянемо основні характеристики різних типів шифрування які можуть бути використані в сенсорних мережах.

2.1.1 Асиметричне шифрування

Більшість дослідників вважають, що через такі параметри як розмір коду, даних, та процесорний час алгоритмів шифрування закритим ключем, робить їх використання неможливим в сенсорних мережах.

Головною проблемою їх використання є великі додаткові обчислювальні витрати. Оскільки вони потребують тисячі чи навіть мільйони операцій множення, було виявлено, що для виконання простої операції множення з 128-бітним результатом мікропроцесор споживає тисячі нано-джоулів. Для порівняння симетричні методи та алгоритми основані на використанні хеш-функцій споживають значно менше ресурсів. Так для шифрування блока інформації розміром 1024-біти алгоритмом RSA на мікропроцесорі MC68328 DragonBall необхідно 42mJ. Тоді, як при використанні AEC витрати значно менші і становлять 0,104mJ.

Однак дослідженні також показали, що використання алгоритмів відкритого ключа є можливим за умови правильного вибору алгоритму та підбору основних параметрів, пов’язаних з оптимізацією для пониження споживання енергії. Так значну увагу привертають ECC (Elliptic Curve Cryptography), оскільки вони надають аналогічну надійність як і RSA при цьому потребують менший розмір ключа, що відповідно скорочує витрати

процесорного часу та витрати пов’язані з комунікацією. Для прикладу ECC з розміром ключа 160 біт відповідає такому ж рівню безпеки як і RSA з розміром ключа 1024 біт. В таблиці 1.1 підведено підсумок необхідного процесорного часу для ECC та RSA на Atmel ATmega128 процесорі.

Таблиця 1.1. Необхідна к-сть процесорного часу для асиметричних алгоритмів шифрування на процесорі Atmel ATmega128.

Algorithm	Operation Time (s)
ECC secp160r1	0.81
ECC secp224r1	2.19
RSA-1024 public key $e = 2^{16} + 1$	0.43
RSA-1024 private key (with Chinese Remainder Theorem)	10.99
RSA-2048 public key $e = 2^{16} + 1$	1.94
RSA-2048 private key (with Chinese Remainder Theorem)	83.26

Отже, використання асиметричних ключів є досить складним у WSN, через великі витрати на обчислення, но є можливим за умови правильної оптимізації.

2.12 Симетричне шифрування

Механізми симетричного шифрування використовують один криптографічний ключ, що відомий обом сторонам. В той час, як енергозатрати при використанні симетричного шифрування є значно меншими, передача ключа між вузлами мережі є серйозним викликом. Оскільки не завжди існує можливість попереднього встановлення ключа в вузли перед розгортанням мережі, тому WSN потребують надійної схеми передачі ключа.

В досліджені [11] було проаналізовано шість симетричних алгоритмів шифрування: RC5, RC6, Rijndael, MISTY1, KASUMI, та Camellia на IAR Systems’ MSP430F149. Критеріями оцінювання були: розмір коду, необхідний розмір пам’яті та к-сть циклів CPU. Результати оцінювання приведені в таблиці 2.1 [12].

Таблиця 2.1. Ефективність алгоритмів симетричного шифрування виконаних на сенсорах WSN.

By Key Steps						
Rank	Size Optimized			Speed Optimized		
	Code Memory	Data Memory	Speed	Code Memory	Data Memory	Speed
1	RC5-32	MISTY1	MISTY1	RC6-32	MISTY1	MISTY1
2	KASUMI	Rijndael	Rijndael	KASUMI	Rijndael	Rijndael
3	RC6-32	KASUMI	KASUMI	RC5-32	KASUMI	KASUMI
4	MISTY1	RC6-32	Camellia	MISTY1	RC6-32	Camellia
5	Rijndael	RC5-32	RC5-32	Rijndael	Camellia	RC5-32
6	Camellia	Camellia	RC6-32	Camellia	RC5-32	RC6-32
By Encryption (CBC/CFB/OFB/CTR)						
Rank	Size Optimized			Speed Optimized		
	Code Memory	Data Memory	Speed	Code Memory	Data Memory	Speed
1	RC5-32	RC5-32	Rijndael	RC6-32	RC5-32	Rijndael
2	RC6-32	MISTY1	MISTY1	RC5-32	MISTY1	Camellia
3	MISTY1	KASUMI	KASUMI	MISTY1	KASUMI	MISTY1
4	KASUMI	RC6-32	Camellia	KASUMI	RC6-32	RC5-32
5	Rijndael	Rijndael	RC6-32	Rijndael	Rijndael	KASUMI
6	Camellia	Camellia	RC5-32	Camellia	Camellia	RC6-32

В якій алгоритми ранжируються по двох ключовим параметрам розмір та швидкість виконання. Результат показує що, Rijndael(також AEC) рекомендований для високої безпеки та енергоефективності, MISTY1 для пристроїв з невеликим розміром пам’яті та оптимальної енергоефективності.

Час виконання алгоритмів симетричного шифрування визначається наступними факторами:

- Розрядність шини даних: багато криптографічних алгоритмів оптимізовані під 32-bit машинне слово, в той час як більшість мікропроцесорів мають 8-bit чи 16-bit розмір машинного слова.
- Архітектура набору команд (ISA): так наприклад багато мікропроцесорів не підтримують ROL (Rotate bit left) інструкцію, яка є необхідною в багатьох симетричних алгоритмах, як ось RC5.

Підсумовуючи аналіз використання криптографічних методів у WSN. Можна сказати, що не дивлячись на те, що вибір криптографічного методу являється фундаментальним для забезпечення безпеки WSN мереж, на разі він залежить від обчислювальної та комунікаційної здатності сенсорів-вузлів.

Перелік відкритих проблем варіюється від вибору криптографічних методів до розробки апаратного забезпечення, також однією з проблем є необхідність розробки надійної схеми передачі та управління ключами.

2.1.3 Протоколи управління ключами

Цілю механізмів управління ключами, являється встановлення криптографічних ключів в вузлах мережі в надійний та безпечний метод. Додатково механізм повинен підтримувати приєднання та від'єднання вузлів. На рисунку нижче наведено класифікацію відомих протоколів управління ключами.

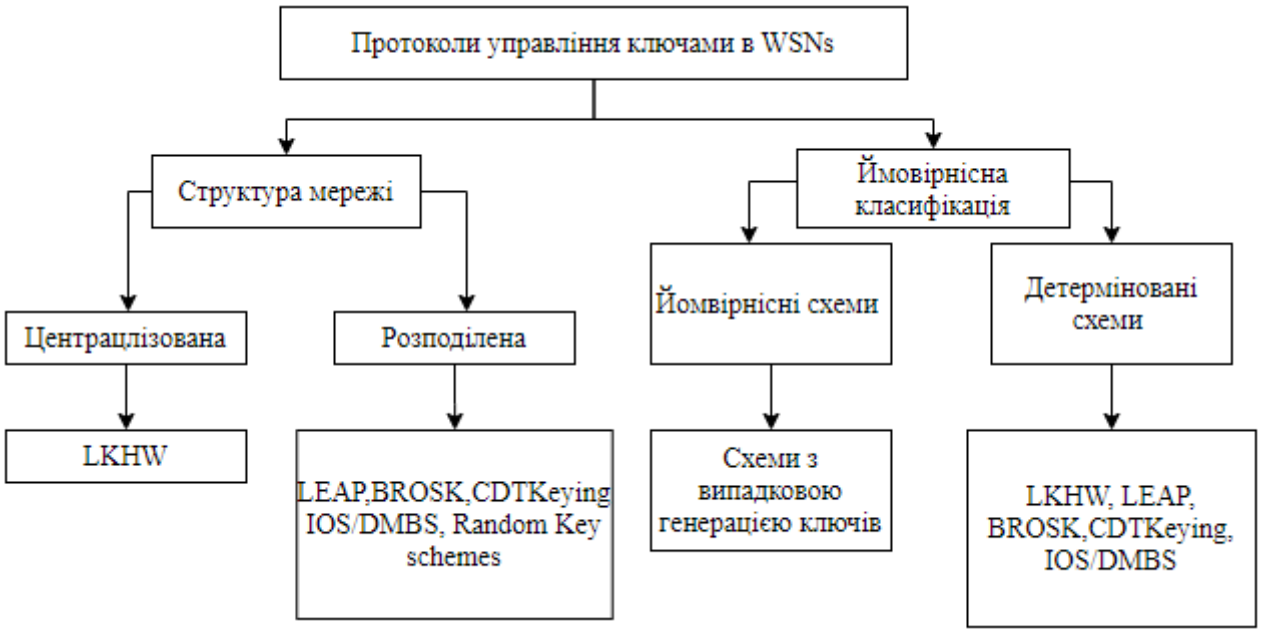

Рисунок 2.1. Класифікація протоколів управління ключами у WSNs

В цьому розділі надано короткий огляд одних з найважливіших протоколів управління ключами.

В залежності від структури мережі ПУК (протокол управління ключами) може бути централізованим чи розподіленим. В централізованій схемі управління лише один об'єкт контролює генерує та розподіляє ключі мережую. Цей об'єкт називається Key Distribution Center (KDC). Відомий

лише один протокол, що базується на централізованій схемі, це LKHW схема. LKHW базується на логічній ієрархії ключів LKH. В цій схемі базова станція являється KDC і всі ключ розподіляється по дереву мережі з KDC. Головним недоліком такої схеми, являється те що лише один об’єкт відповідає за весь механізм. Так якщо KDC вийде зі строю чи зловмисник отримає доступ до нього безпека всієї мережі зазнає краху. Також недоліком є відсутність можливості до масштабування.

В розподіленій схемі різні об’єкти відповідають за управління ключами. Тому протоколи, що базується на цій схемі не мають вразливості в одній точці мережі як при централізованій схемі. Ці протоколи можуть бути віднесені до детермінованих чи ймовірнісних як показано на схемі.

LEAP є протоколом управління ключами WSN, що базується на симетричних алгоритмах шифрування. Він використовує різні механізми управління в залежності від вимог безпеки. Так за ним у вузлах мережі встановлюється чотири типи ключів 1) індивідуальний ключ, що є спільним між вузлом і базовою станцією (попередньо конфігурується). 2) груповий ключ для всіх вузлів мережі, також попередньо конфігурується. 3) парний ключ, що відомий між сусідніми вузлами 4) кластерний ключ, що розділяється між групою вузлів та використовується для локальної комунікації вузлів мережі.

Цей протокол припускає, що час який необхідний для атаки на вузол є більшим ніж час встановлення мережі, протягом якого всі вузли встановлять контакт з сусідніми вузлами мережі. Спільний ключ для ініціалізації мережі встановлюється в вузли перед початком її розгортання. Кожен вузол вираховує головний ключ, який залежить від спільного ключа та унікального ідентифікатора вузла. Далі вузли обмінюються HELLO повідомленням, яке може бути аутентифіковане отримувачем (оскільки спільний ключ та ідентифікатор відомий головний ключ сусіднього вузла може бути вирахуваний). Тоді вузли можуть обрахувати спільний ключ базуючись на їхніх головних ключах. Спільний ключ видаляється на всіх вузлах по

завершені ініціалізації і припускається, що до даного моменту жоден вузол не був скомпрометованим. Оскільки після цього зловмисник не може отримати спільний ключ, то ін’єкція даних ззовні є неможливою. Також жоден вузол не може підробити головний ключ іншого вузла

Була в [13] запропонована схема розповсюдження ключа по WSN з використанням теорії комбінаторного проєктування. За схемою генеруються симетричні ключі з параметрами $n^2 + n + 1, n + 1,1$. Схема підтримує

$n^2 + n + 1$ вузлів та використовує пул ключів розміром $n^2 + n + 1$. Генерується $n^2 + n + 1$ послідовносте ключів з розміром $n + 1$ де кожна пара послідовностей має точно один спільний ключ і кожен ключ появляється рівно в $n + 1$ послідовностях. Так після розгортання мережі кожна пара вузлів має точно один спільний ключ. Недоліком цієї схеми є те, що параметр n повинен бути відомим, тому розмір мережі є фіксованим.

PIKE (peer intermediaries for key establishment). За цією схемою всі вузли мережі організовані в двовимірний простір рисунок 2.2 де координати кожного вузла є (x;y) та x, y ε {0, 1,.. √N – 1}. Кожен вузол має спільний ключ з 2(√N – 1) вузлами, які мають одинакові x чи y координати. Для двох вузлів, що не мають спільних координат використовується маршрутизатор. Однак накладні витрати на комунікацію за цією схемою досить високими, оскільки безпечне з’єднання може бути встановлене лише з 2 / √N вузлами, що означає що кожен вузол повинен встановити ключ майже для кожного з своїх сусідів по всьому шляху передачі.

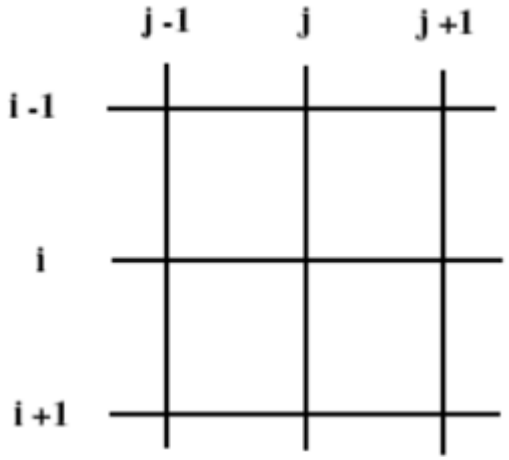

Рисунок 2.2. PIKE схема: вузли-сенсори організовані в двовимірний простір

2.2 Протоколи безпеки у WSN

В даному розділі надано огляд набору протоколів оптимізованих для WSN:SPINS (Security Protocols for sensors networks). SPINS складаються з двох блоків: SNEP та μTESLA. SNEP забезпечує: конфіденційність даних, двосторонню автентифікацію, та актуальність даних. μTESLA надає автентифікацію для широкомовної передачі даних.

Далі будуть використанні наступні позначення для опису протоколів

- A, B відповідають вузлам-сенсорам
- N_A випадкове число бітів згенероване вузлом A
- χ_{AB} спільний головний ключ (master secret key) вузлів A,B. Він не містить жодної інформації про напрямок передачі тому $\chi_{AB} = \chi_{BA}$.
- K_{AB} і K_{BA} позначають спільні криптографічні ключі вузлів A,B.
- K'_{AB} і K'_{BA} секретні криптографічні MAC ключі.
- $MAC(K'_{AB}, M)$ позначає обчислення MAC повідомлення M р MAC ключем K'_{AB}

2.2.1 SNEP

Для виконання вимог безпеки описаних раніше було розроблено два блоки захисту μTESLA і SNEP. Як було вже сказано SNEP забезпечує конфіденційність даних і двосторонню комунікацію вузлів A та B, які мають спільний головний ключ (master secret key) χ_{AB}. Та виводять незалежані ключі використовуючи функцію псевдовипадкових чисел F : ключі шифрування $K_{AB} = F_\chi(1)$ та $K_{BA} = F_\chi(3)$ та MAC ключі $K'_{AB} = F_\chi(2)$ і $K'_{BA} = F_\chi(4)$ для кожного напрямку комунікації. Зашифрована інформація має наступний формат $E = \{D\}_{<K,C>}$, де D це данні, K ключ шифрування та C лічильник. MAC можна виразити наступною формулою $M = MAC(K', C||E)$. Повне повідомлення, що відправляється з вузла A до B можна має наступний вигляд.

$$A \to B: \{D\}_{<K_{AB},C_A>),}\ MAC(K'_{AB}C_A||\{D\}_{<K_{AB},C_A>)}$$

SNEP має наступні переваги

- Семантичну безпеку. Так, як лічильник інкрементується після кожного повідомлення, кожне повідомлення шифрується по різному. Число лічильник є достатньо довге, щоб не повторюватися в рамках життєвого циклу вузла.
- Автентифікація даних. Отримувач може підтвердити, що повідомлення прийшло від оригінального відправника перевіривши MAC.
- Захист від атак повторного відтворення. Наявність лічильника в MAC, що представляє номер поточного повідомлення надає захист від атак повторного відтворення.
- Слабка актуальність повідомлень. Отримувач може перевірити, що повідомлення було отримане після попереднього, що гарантує порядок повідомлень.
- Невеликі додаткові витрати на комунікацію. Стан лічильника зберігається на обох сторонах, тому не повинен передаватися з відправленням кожного повідомленням.

SNEP надає слабку актуальність даних, лише через те що він гарантує порядок повідомлень відправлених з вузла B до вузла A, но не те що повідомлення було відправлене з вузла B у відповідь на запит вузла A.

Вузол A може досягти строгої актуальності даних для відповіді вузла B з використанням N_A. Так вузол A генерує випадкове число N_A та відправляє його з запитом R_A. до вузла B. Далі вузол B відправляє N_A разом з відповіддю R_B.

Однак замість явного повернення N_A, з метою оптимізації вузол B може використовувати N_A при обчислені MAC. Тоді обмін повідомленнями може бути описаний наступними виразами.

$$A \rightarrow B: N_A, R_A$$

$$B \rightarrow A: \{R_B\}_{<K_{BA}, C_B>}\ MAC(K'_{BA}, N_A || C_B || \{R_B\}_{<K_{BA}, C_B>})$$

Після перевірки MAC, вузол A може бути впевненим, що відповідь була згенеровано вузлом B на запит R_A.

Протокол обміну станом лічильника. Для досягнення малих розмірів повідомлень, припускається, що дві сторони A та B знають стан лічильника один одного. Тому C_A та C_B можна не додавати до повідомлень. Однак на практиці, повідомлення можуть бути втрачені під час передачі і C_A та C_B матимуть не цілісний стан і потребується синхронізація їх значень. Для цього використовується наступний протокол обміну значеннями C_A та C_B.

$$A \rightarrow B: C_A$$

$$B \rightarrow A: C_{B,} MAC(K'_{BA} C_A || C_B)$$

$$A \rightarrow B: MAC(K'_{AB} C_A || C_B)$$

Слід зауважити що значення C_A та C_B не потребують шифрування, оскільки не є секретними. Також слід звернути увагу, що MAC не містить імена вузлів A та B, та ключі K'_{BA} та K'_{AB} неявно зв'язують повідомлення до вузлів що забезпечую правильний напрямок передачі повідомлення. Коли вузли A, виявляє що C_B не є в синхронізованому стані, A може зробити запит C_B до B використовуючи N_A, для гарантії актуальності даних.

$$A \rightarrow B: N_A$$

$$B \rightarrow A: C_{B,} MAC(K'_{BA} N_A || C_B)$$

Для запобігання потенційним DoS атаками, коли зловмисник відправляє фіктивні повідомлення з метою виконання синхронізації станів лічильників без необхідності, вузли можуть перемикатися в режим передачі лічильників з кожним зашифрованим повідомленням. Інший полягає в виявлені таких атак, додаючи інший короткий MAC до повідомлень, який не залежить від лічильника.

2.2.2 μTESLA: протокол автентифікації широкомовної передачі.

Протокол μTESLA, це модифікація протоколу TESLA. Він був розроблений оскільки використання TESLA у WSN було неможливе через високі обчислювальні затрати. Окрім відповідно до TESLA, кожен пакет містить орієнтовно додатково 24 байти робочих даних. Так в сенсорних мережах, де вузли відправляють невеликі повідомлення розмірами ~30байт, є

не практичним, оскільки з 64 бітним ключем та MAC частина пакета пов’язана з TESLA буде складати 50%.

Враховуючи описані вище недоліки TESLA, було розроблено μTESLA протокол в якому були вирішені наступні проблеми TESLA:

- TESLA виконує автентифікацію початкового пакета використовуючи цифровий підпис, що потребує занадто великих обчислювальних ресурсів в порівняні з можливостями сенсорів-вузлів.
- TESLA шифрує повідомлення за допомогою асиметричних алгоритмів з відкритим ключем, що також потребує серйозних затрат на обчислення.

Широкомовна передача з базової станції.

μTESLA вимагає строгої синхронізації між базовою станцією та вузлами. Для відправлення пакету, базова станція обчислює MAC з секретним ключем, що є відомим лише базовій станції в даний момент. Коли вузол, отримує пакет він може перевірити, що базова станція ще не розкрила секретний ключ (завдяки строгій синхронізації по часу, та графіку по якому ключ буде розкритий). Так оскільки ключ, ще не розкритий вузол, може бути впевненим що пакет не був пошкодженим чи модифікованим зловмисником під час передачі. Вузол зберігає пакет в буфер. Далі базова станція передає секретний ключ до вузлів, які можуть його перевірити (більш детально буде описано нижче). Якщо ключ пройшов перевірку, вузли можуть використовувати його для автентифікації пакету що зберігався в буфері.

Кожен MAC ключ це ключ з ланцюга ключів згенерований односторонньою функцією *F*. Для генерації ланцюжка односторонніх ключів, відправник випадково вибирає останній K_n з ланцюжка і повторно застосовує функцію F для обчислення $K_i = F(K_{i+1})$. Кожен вузол може легко отримати ключ автентифікації з ланцюжка ключів використовуючи SNEP протокол.

Приклад. На рисунку нижче зображено ланцюжок ключів μTESLA в часових інтервалах, і послідовність пакетів що були відправлені з базової станції. Кожен ключ з ланцюга знаходиться в певному часовому інтервалі і всі

пакети, що були відправлені протягом цього інтервалу зашифровані одним ключем.

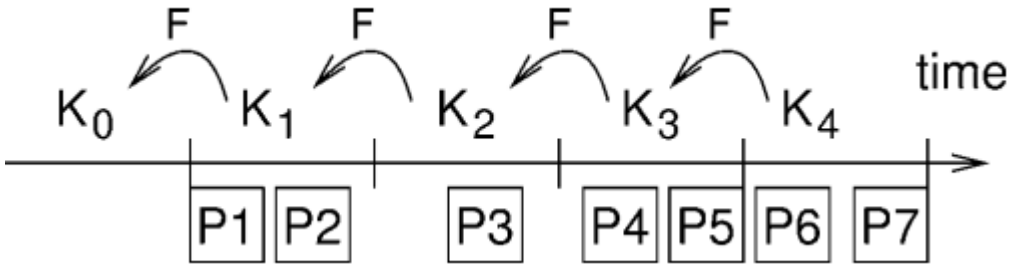

Рисунок 2.3. Ланцюг ключів μTESLA

В даному випадку відправник розкриває секретний ключ, через один часовий інтервал після того як його було використано для обчислення MAC. Припускається, що отримувачі синхронізовані по часі з відправником і знають ключ K_0. Пакети P_1 та P_2 відправлені в перший часовий інтервал і зашифровані ключем K_1. Пакет P_3 має MAC, що був обчислений використовуючи ключ K_2. Припустимо, що пакети P_4, P_5 , P_6 були втрачені під час передачі, оскільки і пакет з ключем K_1, так отримувач не може виконати автентифікацію пакетів P_1, P_2 та P_3. В інтервал 4 базова станціє відправляє ключ K_2, який перевіряють порівнюючи відоме їм значення ключа K_0 та обчисленим значення ключа K_0 двічі застосувавши функцію F

$$K_0 = F(F((K_2))$$

Далі вузли можуть, вивести значення першого ключа $K_1 = F(K_2)$, після чого виконати автентифікацію пакетів P_1, P_2 ключем K_1 та P_3 ключем K_2.

Розкриття ключів, відбувається незалежно від широкомовної передачі пакетів. І прив’язане до часових інтервалів. Також в μTESLA відправник періодично відправляє поточний ключ, в спеціальному пакеті.

μTESLA має декілька фаз: налаштування відправника, відправлення автентифікованих пакетів, налаштування отримувача, автентифікація пакетів.

Налаштування відправника (базової станції). Відправник з початку генерує послідовність секретних ключів. Для цього він за допомогою генератора випадкових чисел, створює останній ключ послідовності K_n, та множино застосовує до нього односторонню функцію F (наприклад MD5),

$K_j = F(K_{j+1})$. Оскільки F є односторонньою функцією, ніхто не може обчислити наступні ключі, наприклад обчислити $K_0 \ldots K_j$ знаючи K_{j+1}. З іншої сторони ніхто також не може знайти K_{j+1} знаючи $K_0 \ldots K_j$. Система одноразових паролів S/Key використовує подібний підхід.

Відправлення автентифікованих пакетів. Час поділений на уніфіковані інтервали і відправник асоціює один ключ одному часовому інтервалу. В часовий інтервал *i* відправник використовує поточний ключ K_i для обчислення MAC. В часовий інтервал (i+ δ), відправник розкриває ключ K_i. Час затримки розкриття ключа, повинен завжди бути більшим ніж час передачі пакета до найвіддаленішого вузла мережі.

Налаштування отримувача. В протоколі μTESLA отримувач може легко і ефективно перевірити підпослідовність ключів ланцюга ключів, маючи один ключ. Так, якщо отримувач має ключ K_i з ланцюжка ключів, він може виконати автентифікацію ключа K_{i+1} застосувавши функцію F $K_{i+1} = F(K_i)$. Для налаштування μTESLA, кожен вузол повинен мати хоча б один ключ з послідовності ключів. Також як говорилося раніше відправник і отримувач повинні бути синхронізовані по часу, отримувач повинен знати графік розкриття ключів. Для цього отримувач відправляє запит з N_R до відправника *S*. Відправник(базова станція) S відповідає повідомленням, що містить поточний час T_s , ключ K_i що був використаний в пройдений часовий інтервал i , час початку інтервалу T_i, тривалість інтервалу T_{int}, та час затримки δ (останні три параметри описують графік розкриття ключів). Цей процес можна описати наступними виразами:

$$M \rightarrow S: N_M$$

$$S \rightarrow M: T_s | K_i | T_i | T_{int} | \delta \ \text{MAC}(K_{MS}, N_M | T_s | K_i | T_i | T_{int} | \delta)$$

MAC використовує спільний ключ, що відомий вузлам і базовій станції, N_M використовується для забезпечення свіжості даних.

Автентифікація широкомовних пакетів. Коли отримувач отримує пакети, він повинен перевірити що вони не були пошкодженими зловмисником під час передачі. Коли зловмисник знає ключ певного часового

інтервалу він може, пошкодити пакети оскільки йому відомий ключ, що був використаний для обчислення MAC. Так отримувач повинен знати що: пакет не пошкоджений і відправник не розкрив ключ, що був використаний в MAC цього пакету. Якщо, пакет не є пошкодженим, отримувач повинен зберегти його в буфері в іншому випадку пакет повинен бути відкинутим.

Як тільки, отримувач отримує ключ, він перевіряє його перевіряючи на рівність з останнім ключем, що він знає. Використовуючи застосування невеликої к-сті разів односторонньої функції

$$F: K_u = F^{i-u}(K_i)$$

Якщо перевірка пройшла успішно виконати автентифікацію усіх пакетів, що були відправлені в часові інтервали з u до i. Отримувач також, заміняє збережений ключ K_i ключем K_u.

Виконання широкомовної передачі з вузла. Оскільки сенсор-вузол є обмежений в пам'яті, він не може зберігати послідовність ключів односторонньої функції. Тим більше обчислення кожного ключа з початкового K_n є дорогим процесом. Також для вузла досить складно мати спільний ключ з кожним отримувачем. Наступним викликом є те, що розкриття ключа також занадто дорогий процес, для вузлів що мають батареї не великої місткості. Було запропоновано наступні рішення цих проблем:

- Виконувати широкомовну передачу з базової станції. Так, вузол передає повідомлення на базову станцію по протоколу SNEP, а вже базова станція виконує широкомовну передачу.
- Вузол виконує широкомовну передачу, однак базова станція використовується для зберігання послідовності ключів, і передає ключі до вузла за необхідністю. Для збереження енергії вузла, виконання розкриття ключів може виконуватися також базовою станцією та налаштування нового отримувача.

Слід зауважити, що перший варіант має переваги, оскільки при здійснені широкомовної передачі з вузла, всі отримувачі повинні бути синхронізовані

додатково, ще і з цим вузлом та знати його графік розкриття ключів. Що обмежує к-сть вузлів, що можуть виконувати широкомовну передачу.

Висновки з розділу 2

Основними механізмами забезпечення інформаційної безпеки WSN є криптографічні методи шифрування даних. Так асиметричне шифрування хоч і може бути використаним, за умови оптимізації енергетичних витрат не є оптимальним для WSN. Тоді як симетричні алгоритми краще підходять для вузлів-сенсорів з їх значними обмеженнями в ресурсах, так Rijndael рекомендований для високої безпеки та енергоефективності, MISTY1 для пристроїв з малим розміром пам’яті. Однак симетричні методи потребують надійні протоколи управління ключами, вибір яких залежить від структури мережі та способом генерації та розповсюдження ключів. Також слід зауважити, що саме протоколи управління ключами часто являються слабким місцем WSN.

Комбінація протоколі SNEP та μTESLA надає високий рівень відповідності WSN мереж вимогам, та можливість виконувати захищене широкомовне мовлення в рамках мережі, що є значною перевагою.

3 АНАЛІЗ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В РЕАЛІЗОВАНИХ ТЕХНОЛОГІЯХ WSN

Даний розділ містить короткий огляд найбільш популярних технології, що вже використовуються при побудові WSN та аналіз загроз безпеці одного з найпопулярніших протоколу WSN ZigBee. В той час, як повний технічний розбір наявних технологій далеко виходить за межі цієї роботи, основну увагу було спрямовано на аналіз механізмів, що забезпечують інформаційну безпеку в цих технологіях.

Спектр задач WSN мереж є дуже широким, з різними вимогами до параметрів мережі. Як результат було створено різні типи комунікаційних технологій, що краще підходили для вирішення поставлених задач. В таблиці 3.1 наведені основні характеристики найбільш відомих технологій комунікацій, що використовуються у WSN

Таблиця 3.1. Технічні характеристики відомих WSN рішень.

	LR-WPAN	LoRaWAN	BLE	RFID
Стандарт	IEEE 802.15.4	LoRAWAN R1.1	IEEE 802.15.1	ISO/IEC 18000
Діапазон частот	868/915/2450 MHz	868/900 MHz	2.402-2.481 GHz	125 або 134 KHZ для низькочастотних RFID; 13.56 MHz для високочастотних RFID систем. 860 ~ 960 MHz для ультра високих
Дальність передачі	10-20 м	Декілька кілометрів (2-5км в міській місцевості та до	10-100 м	До 100м

		15 км на відкритій місцевості		
Швидкість передачі	40-250 Kbps	0.3-50 Kbps	Теоретично до 1Mbps, на практиці від 10-20 Kbps	6.7-848 Kbps
Споживання енергії	Низьке	Дуже низьке	Дуже низьке	Низьке
Вартість	Низька	Висока	Низька	Низька

Як можна побачити з таблиці 3.1, основними характеристиками є дальність передачі, long-range або short-range та low power consumption(низьке споживання енергії).

3.1 Безпека в Short-Range Low Power WSN мереж

3.1.1 6LoWPAN

Низько швидкісні бездротові мережі близької зони дії базуються на стандарті IEEE 802.15.4, стандарт для низько швидкісних без дротових мереж. Цей стандарт імплементований такими технологіями як 6LoWPAN (IETF стандарт), ZigBee, Z-Wave та EnOcean (стандарт для автоматичного управління домами та будівлями), та SNAP (Simple Network Access Protocol). Ідея 6LoWPAN полягає в комбінації IPv6 з IEEE 802.15.4. LoWPAN дозволяє використовувати стандарт IPv6 поверх IEEE 802.15.4 без дротової мережі. Ряд протоколів для пристроїв автоматизації домів працює на основі 6LoWPAN.

6LoWPAN мережа складається з одної чи декількох LoWPAN мереж підключених до інтернету з використанням маршрутизатора, що контролює вхідний та вихідний потік даних. В мережі LoWPAN пристрої не використовують IPv6 адреси чи UDP протокол для передачі, оскільки вся інформація необхідна для виходу в інтернет залишається на розмежувальному маршрутизаторі. В той час, як завдання маршрутизації в LoWPAN вирішується

робочою групою IETF-ROLL, яка розробляє RPL протокол який по факту є протоколом для Low-Power and Lossy Networks.

Безпека в 6LoWPAN повинна обмежити доступ до даних лише авторизованим користувачам, забезпечити цілісність даних та бути здатна виявити вторгнення зловмисника в мережу. Оскільки технологія об’єднує IPv6 та LoWPAN система виявлення вторгнення повинна аналізувати трафік з обох сторін мережі.

Недолік авторизації на рівні LoWPAN та обмеженість в пам’яті пристроїв мережі робить механізм фрагментації пакетів вразливим [14]. Для прикладу зловмисник можу зупинити коректну зборку пакета на цвілевому вузлі. Також зловмисник можу виконати атаку відправивши один protocol-complaint 6LoWPAN фрагмент [14]

3.1.2 RPL

Протокол маршрутизації IPv6 для LLN (RPL) призначений для маршрутизації трафіку IPv6 в мережах малої потужності, реалізованих поверх 6LoWPAN, з великими або непередбачуваними втратами пакетів. Захист RPL використовує поле "Захист" після 4-байтового заголовка повідомлення ICMPv6. Інформація в цьому полі вказує на рівень захисту та алгоритм криптографії, який використовується для шифрування повідомлення. RPL пропонує підтримку автентичності даних, семантичну безпеку, захист від атак повторного відтворення, конфіденційність та керування ключами. Атаки на RPL включають селективну переадресацію, sinkhole, Сибіл, Hello flooding, чорну дірку та відмову в обслуговуванні.

3.2 Безпека в Bluetooth Low Energy

Протокол BLE - це малопотужна версія бездротового зв'язку Bluetooth 2,4 ГГц

протокол . Хоча швидкість передачі даних і радіодіапазон даних BLE нижче, ніж однакові показники в класичному Bluetooth, BLE призначений для

додатків з низькою потужністю, які працюють на акумуляторах з невеликою місткістю (наприклад, популярний CR2032). Мала потужність і тривалий час роботи акумулятора дозволяють BLE сенсорові працювати довгі роки, не потребуючи нового акумулятора. Для підвищення безпеки версія BLE 4.2 представляє нову модель BLE Secure Connections. Давайте коротко

переглянути основні способи вирішення найбільш популярних атак на BLE: пасивне підслуховування та атака «людина в середині» MITM.

Підслуховування. Захист від пасивного підслуховування базується на шифруванні комунікації ключем. У той час як в більш ранніх версія BLE (Bluetooth 4.1 або старіших версій) пристрої використовували легко вгадуванні тимчасові ключі для шифрування, в BLE 4.2 використовується

Federal Information Processing Standard (FIPS), сумісний із стандартом Elliptic Curve Diffie-Hellman (ECDH) для генерації ключів Diffie-Hellman Key – DHKey, що значно ускладнює проведення атаки підслуховування.

Атаки "Людина в середині" (MITM). Захист від атак MITM полягає у забезпеченні того факту, що пристрій починає комунікацію з призначеним пристроєм, а не з тим що є неавторизованим та видає себе за такого. BLE Secure Connections забезпечує захист від MITM використовуючи числовий метод порівняння.

3.3 ZigBee протокол

3.3.1 Короткий Огляд протоколу

The ZigBee Alliance розробив стандарт ZigBee бездротової двосторонньої комунікаційної мережі з низьким енергоспоживанням. Він використовується при розробці систем автоматизації домів та будинків, контролі виробництва, в медичних сенсорних додатках, іграшках. ZigBee оснований на IEEE 802.15.4 стандарті.

Стек архітектури протоколу ZigBee закладається з блоків що називаються рівнями. Кожен рівень визначає ряд сервісів для рівня, що знаходиться вище. Кожна одиниця сервісу відкриває інтерфейс для вищого

рівня через Service Access Point (SAP), та кожен SAP підтримує ряд примітивних функцій для забезпечення бажаного сервісу.

IEEE 802.15.4 визначає два нижні рівні: фізичний та підрівень управління доступом до мережі Medium Access Control (MAC) sub-layer. The Zigbee Alliance базуючись на цих рівнях розробив мережевий рівень NWK та фреймворк для прикладного рівня. Фреймворк прикладного рівня складається з прикладного підтримуючого підрівня Application Support sub-layer(APS) та об’єкта ZigBee пристрою ZigBee Device Object (ZDB). Об’єкт додатку прикладного рівня, який визначається виробником використовує фреймворк прикладного рівня та ділить APS і служби безпеки з ZDO.

Фізичний рівень працює на двох окремих частотних діапазонах 2.4GHz та 868/915 MHz. Нижній діапазон фізичного рівня покриває обидва ISM діапазони Європейський та 868 MHz та 915 MHz діапазон, який використовується в таких країнах, як Америка та Австралія. Тоді як вищий діапазон в 2.4GHz використовується практично у всьому світі. В таблиці 3.2 наведені основі технічні характеристики ZigBee

Таблиця 3.2. Технічні характеристики протоколу ZigBee.

Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH
Network Device Types	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Network Size (theoretical # of nodes)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band / Channels	2.4 GHz (ISM band) 16-channels (2 MHz wide)
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer AES-128 available at Application Layer
Communication Range (Average)	Up to 300+ meters (line of sight) Up to 75-100 meter indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)
Legacy Profile Support	Zigbee 3 devices can join legacy Zigbee profile networks. Legacy devices may join Zigbee 3 networks (based on network's security policy)
Logical device support	Each physical device may support up to 240 end-points (logical devices)

MAC- рівень контролює доступ до радіоканалів використовуючи CSMA-CA механізм. Його відповідальність також включає передачі сигнальних кадрів, синхронізацію, забезпеченні надійного механізму передачі. На рисунку 3.1 показана схема архітектури ZigBee

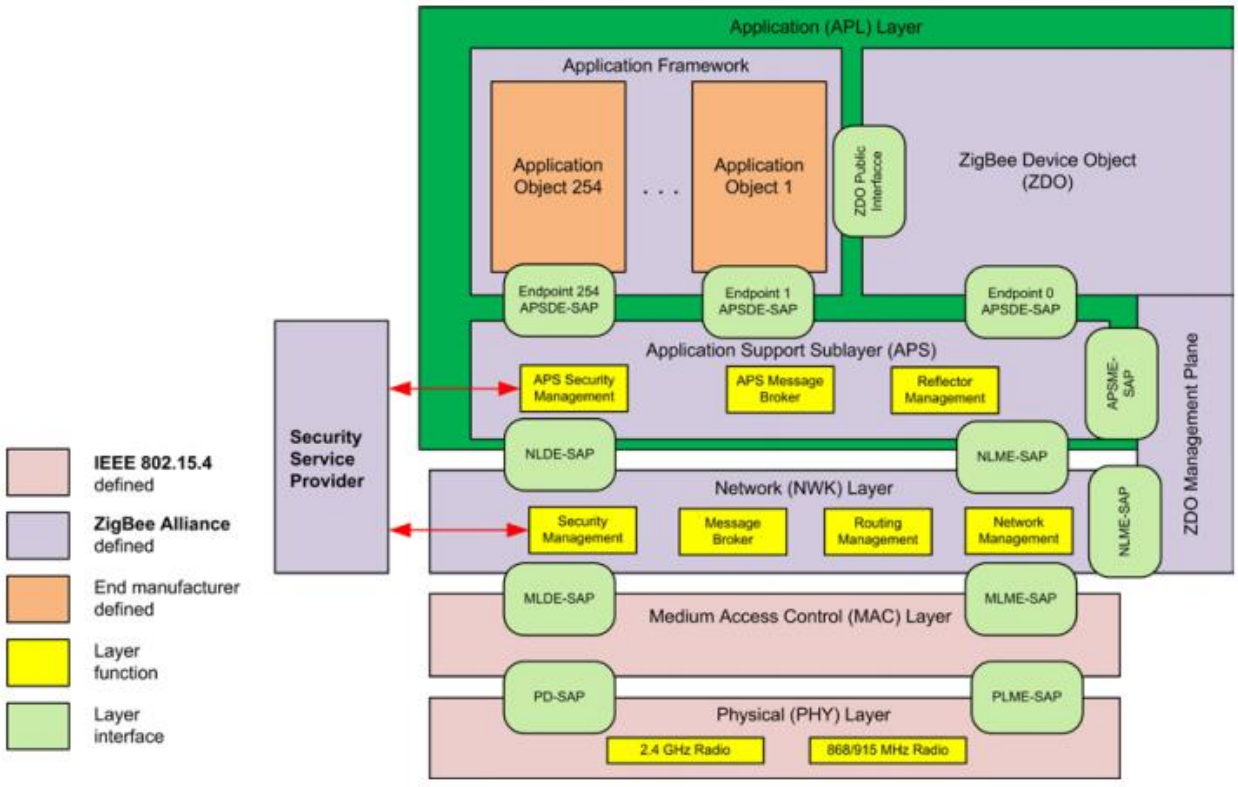

Рисунок 3.1. Архітектура протоколу ZigBee

3.3.2 Топологія мережі

Мережевий рівень ZigBee підтримує три типи топології мереж: зірка(star), дерево (tree), сітка (mesh) див. рисунок 3.2. При топології зірка мережа контролюється одним єдиним пристроєм, що називається ZigBee координатор. ZigBee координатор відповідає за ініціалізацію мережі та підтримку пристроїв. Всі інші прилади є кінцевими і не знають про існування один одного, вони спілкуються напряму з координатором. В mesh та tree топології ZigBee координатор відповідає за ініціалізацію мережі та встановлення ключових параметрів мережі, також мережа може бути розширена з використанням ZigBee маршрутизатора. При деревоподібний топології маршрутизатори передають дані що керують повідомлення через мережу використовуючи ієрархічну стратегію маршрутизації.

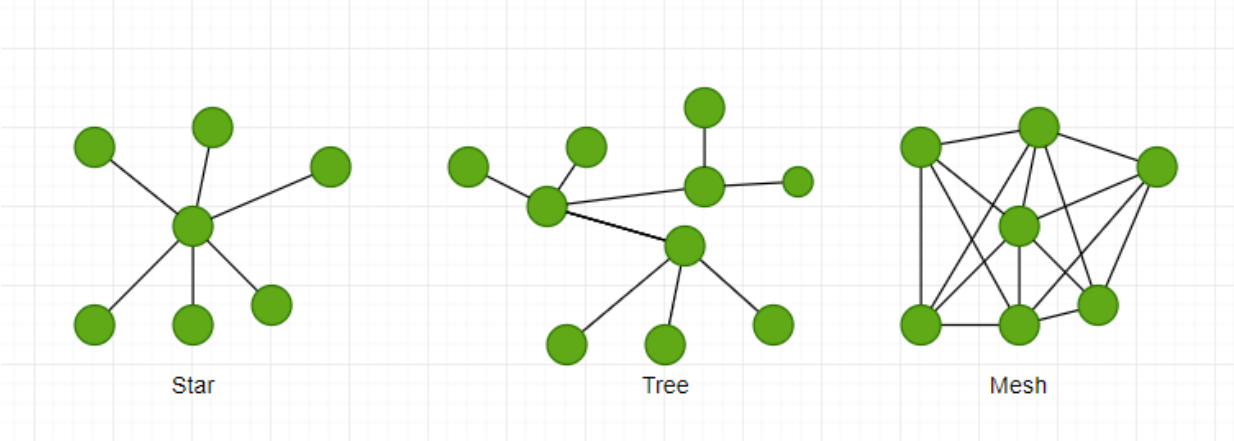

Рисунок 3.2. Топології Star, Tree, Mesh

3.3.3 Система безпеки в ZigBee

ZigBee стверджує, що надає повний функціонал сучасних інструментів забезпечення безпеки та відповідає всім вимогам мереж такого типу. Захист мережі базується на симетричній криптографії, при якій дві сторони повинні ділити один спільний ключ. ZigBee використовує AEC алгоритм для шифрування. При цьому захист мережі побудований на основі відкритої моделі «довіри», при якій стек рівнів протоколу довіряють один одному, та використовують один спільний ключ, що зберігається на пристрої для

шифрування даних різних рівнів. Тому можливе забезпечення захисту даних лише при передачі між кінцевими пристроями, но не між рівнями. Також для спрощення забезпечення сумісності кінцевих пристроїв мережі, ZigBee використовує один рівень безпеки для всіх пристроїв мережі та всіх рівнів пристрою.

Додатково ZigBee команди включають лічильник кадрів, для забезпечення захисту від атак повторного відтворення. Пристрій, що отримує кінцеве повідомлення завжди перевіряє лічильник кадрів та відкидає повторні повідомлення.

ZigBee також забезпечує гнучку зміну частоти для захисту від глушіння сигналу.

3.3.3.1 Схеми захисту

Для забезпечення вимог широкого спектра кінцевих пристроїв та підтримки їх дешевої ціни та малого споживання енергії. ZigBee надає дві архітектурні моделі захисту, централізовану та розподілену. Різниця між ними полягає в тому, як вони приймають нові пристрої в мережу та захищають повідомлення.

Розподілена схема надає менший захист та є більш проста. При її побудові використовується маршрутизатор. Так маршрутизатор забезпечує захист та передачу ключів. Коли новий маршрутизатор з кінцевими пристроями приєднуються до мережі, попередній маршрутизатор в мережі надає їм мережевий ключ, що шифрується ключем приєднання (link-key). При цьому всі пристрої повинні мати link-key, тобто бути попередньо сконфігурованими.

Централізована схема, є більш надійною, вона включає центр «довіри» (Trust Center), який зазвичай знаходиться в координаторі. Trust Center, далі TC, конфігурує мережу та відповідає за автентифікацію маршрутизаторів та приєднання нових пристроїв. TC встановлює link-key для кожного пристрою при його приєднанні та link-key для пари пристроїв по запиту. Також TC генерує і передає мережевий ключ (network-key). Як і в розподіленій моделі

всі пристрої повні бути попередньо сконфігурованими з link-key, який використовується для шифрування передачі мережевого ключа для пристроїв, що приєднуються до мережі. Обидві схеми проілюстровані на наступному рис.

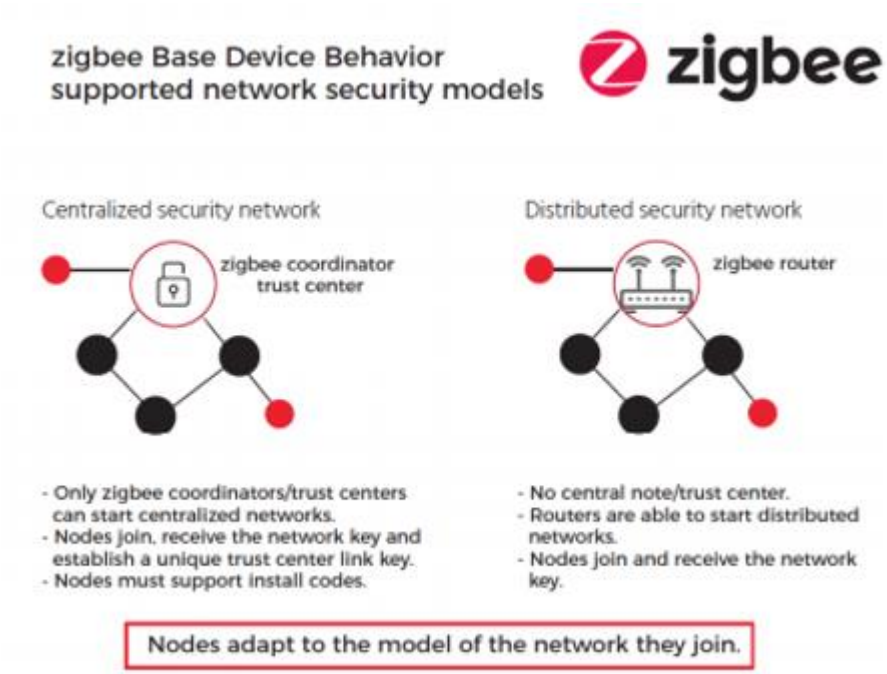

Рисунок 3.3. Централізована та розподілена схема захисту

3.3.3.2 Припущення щодо системи безпеки

Як наслідок відкритої моделі «довіри», на якій побудована система захисту ZigBee. Безпека такої мережі залежить від наступних припущень.

- Безпечне зберігання симетричних ключів. ZigBee стандарт припускає, що симетричні ключі що використовуються при шифруванні повідомлень не доступні ззовні, та всі передачі ключів є зашифрованими. Виключенням може бути лише короткий момент часу(на практиці до 8мс), під час ініціалізації мережі, протягом якого один ключ, що передається може бути не зашифрованим. Це створює короткий момент вразливості.
- Всі схеми безпеки реалізовані. Тобто централізована та розподілена схема захисту імплементовані в кінцевому пристрої та відповідно використовується в залежності від схеми, що використовується всією мережею
- Відповідні криптографічні механізми коректно імплементовані та пристрій дотримується всіх правил безпеки. Розробники ZigBee

протоколу, тут припускають, що протокол реалізований повністю на кінцевих пристроях. ZigBee також припускає, що використовується надійний генератор випадкових чисел.

3.3.3.3 Ключі безпеки

ZigBee пристрої використовують network key та link key для комунікації. Так сторона, що отримує повідомлення знає який ключ необхідно використовувати для розшифровування повідомлення.

Network-key- спільний 128-бітний ключ, що використовується для широкомовного мовлення. Існує два типи network-key- стандартний та підвищеної безпеки. Цей ключ потребує шифрування в той час коли він передається мережею при ініціалізації мережі чи приєднанні нових пристроїв. Для цього використовується link-key, який є відомий всім пристроям в розподіленій схемі та між Trust Center і одним вузлом при централізованій схемі.

Link-key- також є 128-бітним ключем. В розподіленій схемі є два типи link-key глобальний та унікальний. В той час, як при централізованій схемі є три типи link-key: 1) глобальний, використовується TC та всіма вузлами мережі. 2) унікальний, відомий лише TC та одному з вузлів. 3) link-key прикладного рівня, використовується між парою вузлів. Так зазвичай link-keys, пов’язані з TC центром зазвичай є попередньо сконфігурованими за межами ZigBee. Як приклад це може бути QR код на упаковці пристрою, в той час як link-keys між вузлами мережі генеруються TC та шифруються мережевим ключем.

3.3.3.4 Модифікація ключів безпеки

В централізованій схемі TC, періодично генерує, розповсюджує та переключає network-keys для мінімізації часу протягом якого зловмисник може заволодіти мережевим ключем. Новий мережевий ключ шифрується з генерованим TC TCLK(Trust Center Link Key), та передається до вузлів мережі. Коли вузол отримує новий мережевий ключ він не замінює автоматично старий на новий, а зберігає його. Так вузол може зберігати більше ніж один

мережевий ключ, в той час як TC ідентифікує поточний мережевий ключ за допомогою унікальної послідовності чисел. Аналогічно TC може замінити application link ключ.

Також ZigBee надає можливість оновлення через повітря OTA(over-the-air updates), що дозволяє виробникам оновлювати пристрої та застосовувати нові методи безпеки після виявлення нових загроз. ZigBee забезпечує багаторівневий захист OTA, так пакет оновлення шифрується унікальним ключем далі підписується іншим унікальним ключем, та шифрується протягом виготовлення. Що дозволяє лише кінцевому пристрою розшифрувати пакет оновлення. Коли пристрій отримує новий пакет оновлення, завантажувач ОС розшифровує та валідує підписи пакету оновлення і лише тоді запускає процес оновлення.

3.3.3.4 Архітектура системи захисту

Як було сказано раніше, ZigBee побудований на стандарті IEEE 802.15.4 який визначає фізичний та MAC рівень. APL рівень включає APS підрівень, ZDO та власне додатки. ZDO відповідає за управління політикою безпеки та конфігурацією пристрою. APS надає необхідні служби для ZDO та додатків. Нижче коротка діаграма. стеку архітектури ZigBee.

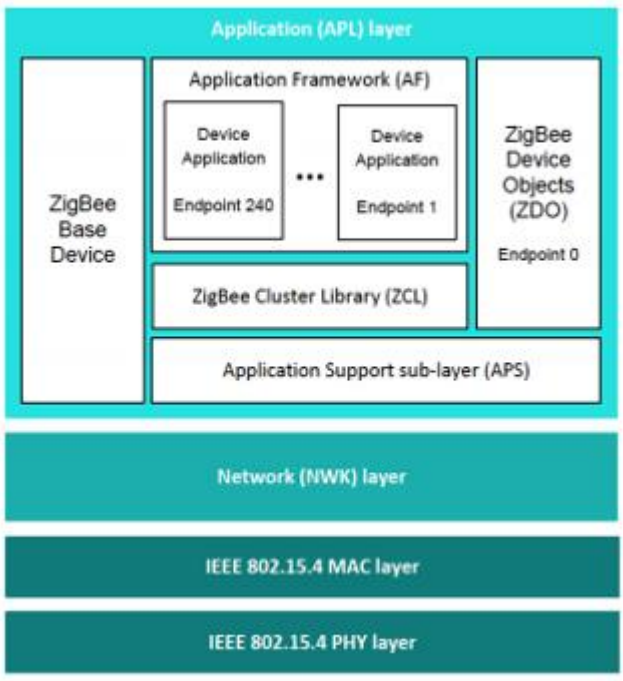

Рисунок 3.4. Діаграма стеку архітектури ZigBee

Так дана архітектура ZigBee включає механізми захисту на трьох рівнях: MAC, NWK, APL.

Механізм захисту на MAC рівні базується на основі IEEE 802.15.4 та підсилена CCM*. Базуючись на відкритій моделі «довіри» ключ, яким шифруються данні на MAC рівні встановлюється рівнем вище і відповідає активному ключі мережі. На рис. нижче зображено вихідний MAC frame після застосування шифрування.

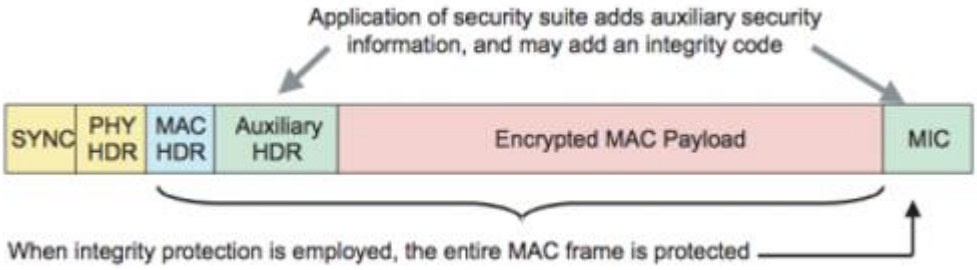

Рисунок 3.5. ZigBee пакет з захистом на MAC рівні.

По аналогії з MAC рівнем працює NWK рівень, що відповідає за безпечну передачу пакетів та маршрутизацію. На рис. нижче зображено вихідний frame NWK рівня

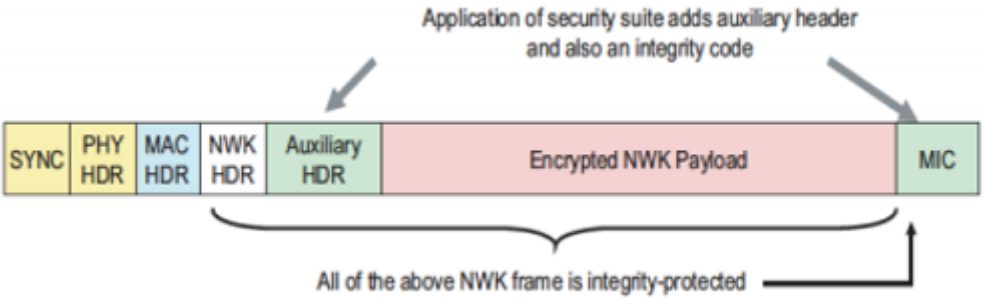

Рисунок 3.6. ZigBee пакет з захистом на NWK рівні.

Механізми безпеки прикладного рівня (APL) виконуються в APS підрівні. Додатково виконання відповідних інструкцій по забезпеченню безпечної передачі пакетів APS відповідає за встановлення та управління ключами. На рис. нижче показаний вихідний frame APL рівня.

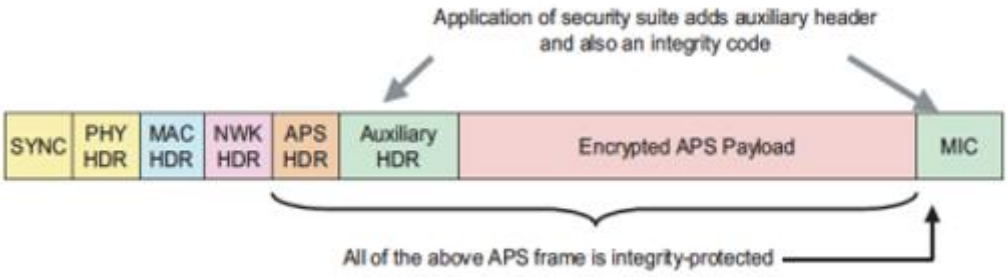

Рисунок 3.7. ZigBee пакет з захистом на APL рівні.

В версії ZigBee 3.0 був доданий application-level secure link між парою вузлів мережі, з використанням набору AEC-ключів, для забезпечення підвищеного рівня безпеки певних вузлів мережі. Прикладом його використання може бути домашня сенсорна мережа, де замок від вхідних дверей та гаражу є вузлами такої мережі. Так між цими замками-вузлами може бути встановлений додатковий рівень захисту з використанням application-level secure link key для запобігання можливості відкрити замки зловмиснику після захоплення ключа мережі.

3.3.3.5 Аналіз системи захисту ZigBee

Відповідно до тестування [13]. Найбільш очевидною загрозою безпеки мережі основаній на протоколі ZigBee, являється процес передачі мережевого ключа під час ініціалізації. Так була протестована мережа, що складалась з трьох пристроїв: Samsung SmartThings Hub v2, Centralite Smart Outlet як ZigBee маршрутизатор, Iris Contact Sensor- магнітний сенсор, що відправляє повідомлення при відкритті/закритті дверей чи вікон. Для тестування використовувався Atmel Raven RZUSB модуль для перехвату та ін’єкції даних в мережі 802.15.4, та спеціальне ПО: zbdump для конвертації перехоплених пакетів у файли libpcap чи Daintree SNA; zbstumbler для знаходження ZigBee та IEEE 802.15.4 мереж; Wireshark для аналізу перехоплених пакетів.

Так під час тестування вдалося перехопити мережевий ключ, що фактично дає повний контроль над мережею зловмиснику.

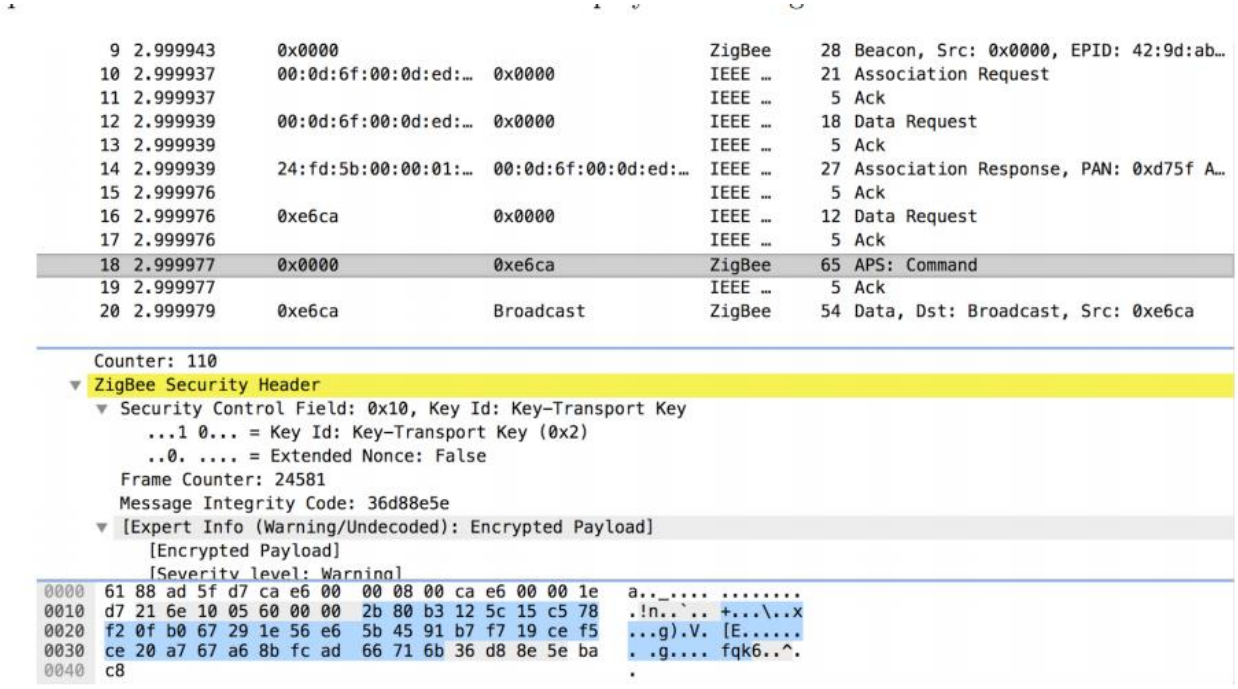

Рисунок 3.8. Перехоплений пакет APS команди. ПО Wireshark

На рис. вище зображений перехоплений пакет APS команди в програмі Wireshark, в якому передається зашифрований мережевий ключ. Відповідно до специфікації протоколу він був зашифрований з використанням Trust Center Default Link Key, який є публічно відомий [17]. Тому його вдалося розшифрувати з використанням AEC де шифрувальником. Результат нижче

```
ef bf bd ef bf bd ef bf bd 7d 11 29 23 ef bf bd 3b 44 ef bf bd 0c ef bf bd 45 ef bf
bd 79 ef bf bd 70 30 ef bf bd 1b ef bf bd 3f 44 ef bf bd ef bf bd 5e 49 ef bf bd ef
bf bd ef bf bd e5 bc a3 ef bf bd 1c ef bf bd ef bf bd ef bf bd ef bf bd ef bf bd 75
                                5f 65 0a
```

Рисунок 3.9. Розшифрований Default Link Key

Атаку відтворення не вдалося реалізувати, так з використанням лічильника повідомлень, кінцевий пристрій відкидав навмисне надіслані повідомлення з Atmel Raven RZUSB. Однак теоретично, можливо прослідкувати номер останнього повідомлення, та підкоригувавши відповідно пакет відтворити цей тип атаки.

Атака на підміну пристрою. Ціллю атаки було підкоригувавши Association Request замінивши в ньому MAC адрес на зовнішній пристрою, підключити свій кінцевий пристрій до мережі. Однак через технічні обмеження, відповідь на Association Request та передача мережевого ключа з Hub’a відбувалася менше ніж за 0.00004 секунд, за такий короткий час не

вдавалось переключити Atmel Raven RZUSB з режиму прослуховування в режим передачі для відправлення пакету на підтвердження приєднання. Однак ця атака може бути легко реалізована за наявністю двох пристроїв Atmel Raven RZUSB один для прослуховування інший для передачі.

Висновки: ZigBee надає досить строгий режим безпеки, з використанням AES алгоритмів для шифрування. Однак передача мережевого ключа при ініціалізації мережі та приєднанні нового пристрою залишається серйозною проблемою. Також слід зауважити, що не дивлячись на те, що специфікація протоколу є досить надійною, часто через короткі терміни реалізації та ринкову складову індустрії, імплементація протоколу є досить ненадійною.

Висновки з розділу 3

В залежності від кінцевих потреб, було розроблено WSN технології, що можна поділити на два типи long-range and low power або short-range and low power.

В даному розділі було проведено детальний аналіз протоколу ZigBee який базується на стандарті IEEE 802.15.4. Так він надає досить надійні та гнучкі механізми безпеки. Було проаналізовано ряд спроб проведення атак на мережу, що працює за цим протоколом. Так, через завідому слабке місце в протоколі, це момент ініціалізації мережі, протягом якого розповсюджується спільний ключ, зловмисники можуть провести атаки прослуховування та підміни вузла. Не дивлячись на те, що час протягом якого ZigBee є досить коротким, зловмисник може повторно ініціювати повторну ініціалізацію мережі, що наддасть йому можливість провести атаку.

4 ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ ДЛЯ WSN

4.1 Опис аналізу

Даний розділ представляє порівняння алгоритмів шифрування, що можуть бути використані у WSN. Метою цього розділу є наглядно показати різницю між вибраними алгоритмами, для полегшення вибору між ними при побудові WSN.

Основуючись на дослідженні [11] були вибрано наступні алгоритми для порівняння їх характеристик при використанні у WSN: RC5, RC6, Rijndael, MISTY1, KASUMI, Camellia. Всі обрані алгоритми є симетричними, оскільки так як було сказано в розділі 2, симетричні алгоритми потребують значно менше витрат на обчислення.

При порівнянні були використані наступні показники:

- Розмір коду
- Розмір оперативної пам’яті, що використовується при виконані
- Надійність
- Розмір ключа
- Швидкодія

4.1.1 Аргументація вибору даних алгоритмів

RC5 був обраний так, як є загальновідомим алгоритмом з 1995 року, не має відомих вразливостей. Не дивлячись на той факт, що був зламаний 64bit RC5 в RSA Laboratories Secret-Key Challenge після 1757 днів обчислень, стандарт має 128 бітний розмір ключа і пройшов не одну криптографічну перевірку протягом років. Рівень захисту: високий.

RC6 є спадкоємцем RC5 та має його переваги, такі як малий розмір коду та велику гнучкість при використанні. Рівень захисту: високий

Rijndael був обраний для порівняння оскільки наразі являється стандартом Advanced Encryption Standard. Рівень захисту: дуже високий.

MISTY1 був обраним оскільки є рекомендованим CRYPTREC стандартом шифрування. Базуючись на останніх дослідженнях, має менший

рівень захисту в порівняні з Rijndael, однак з виконанням повної к-сті раундів надає значний рівень безпеки.

KASUMI є спадкоємцем алгоритму MISTY1, однак в ньому були найдені вразливості, тому він не набув широкої популярності. Не дивлячись на це надає середній рівень безпеки і може бути використаний у WSN, що не потребують високого рівня безпеки.

Camellia був обраним оскільки є одним з рекомендованих алгоритмів NESSIE і CRYPTREC. Рівень безпеки: високий

В таблиці 3.3 наведено підсумок основних параметрів обраних алгоритмів.

Таблиця 3.3. Характеристика обраних алгоритмів.

	Розмір ключа (біти)	К-сть раундів	Розмір блоку	Надійність
RC5	128	18	64	Висока
RC6	128	20	128	Висока
Rijndael	128	10	128	Дуже висока
MISTY1	128	8	64	Середня
KASUMI	128	8	64	Середня
Camellia	128	18	128	Висока

4.2 Порівняння характеристик

Ефективність алгоритму оцінюється по двом ключовим параметрам це необхідний розмір пам’яті та енергоефективність. Тому було проведено порівняння на основі цих параметрів результати якого наведені в таблицях 6 та 8. Які надають можливість наочно побачити різницю в даних алгоритмах за цими ключовими параметрами. При цьому, були найдені та використані дві реалізації кожного з алгоритмів, в одній вони оптимізовані за споживанням пам’яті в той час як в другій за швидкодією.

Таблиця 4.1. Порівняння за необхідним розміром пам’яті.

	Вимоги до пам’яті в байтах			
	Оптимізовані за споживанням пам’яті		Оптимізовані на швидкодію	
	Flash	RAM	Flash	RAM
RC5	1079	54,6	4439	96,2
RC6	1635	69	1735	69
Rijndael	10683	64,6	11080	64,6
MISTY1	5337	43,4	6055	43,4
KASUMI	7475	57,4	8116	54,2
Camellia	13333	113,8	20128	113,8

Як видно з таблиці 4.1, Camellia потребує найбільше як оперативної так і довготривалої пам’яті. А RC5 RC6 мають приблизно однакові показники з невеликою перевагою в сторону RC6.

Для кращої візуалізації, було побудовано графік (див. рисунок 4.1), в якому показано який % пам’яті споживатиме обраний алгоритм при використані реалізації оптимізованої за споживанням пам’яті, на одних з найбільш популярних процесорах що використовуються у WSN (Smart Dust, EYES node, Intel mote, ATmega328P). Їхні характеристики наведені в таблиці нижче.

Таблиця 4.2. Параметри процесорів, використаних в відомих WSN.

	Smart Dust	EYES node	Intel mote	ATmega328P
CPU	8-bit, 4 MHz	16-bit, 8 MHz	16-bit, 12 MHz	8-bit, 16MHz
Flash memory	8 KB	60 KB	512 KB	32 KB
RAM	512 B	2 KB	64 KB	2 KB

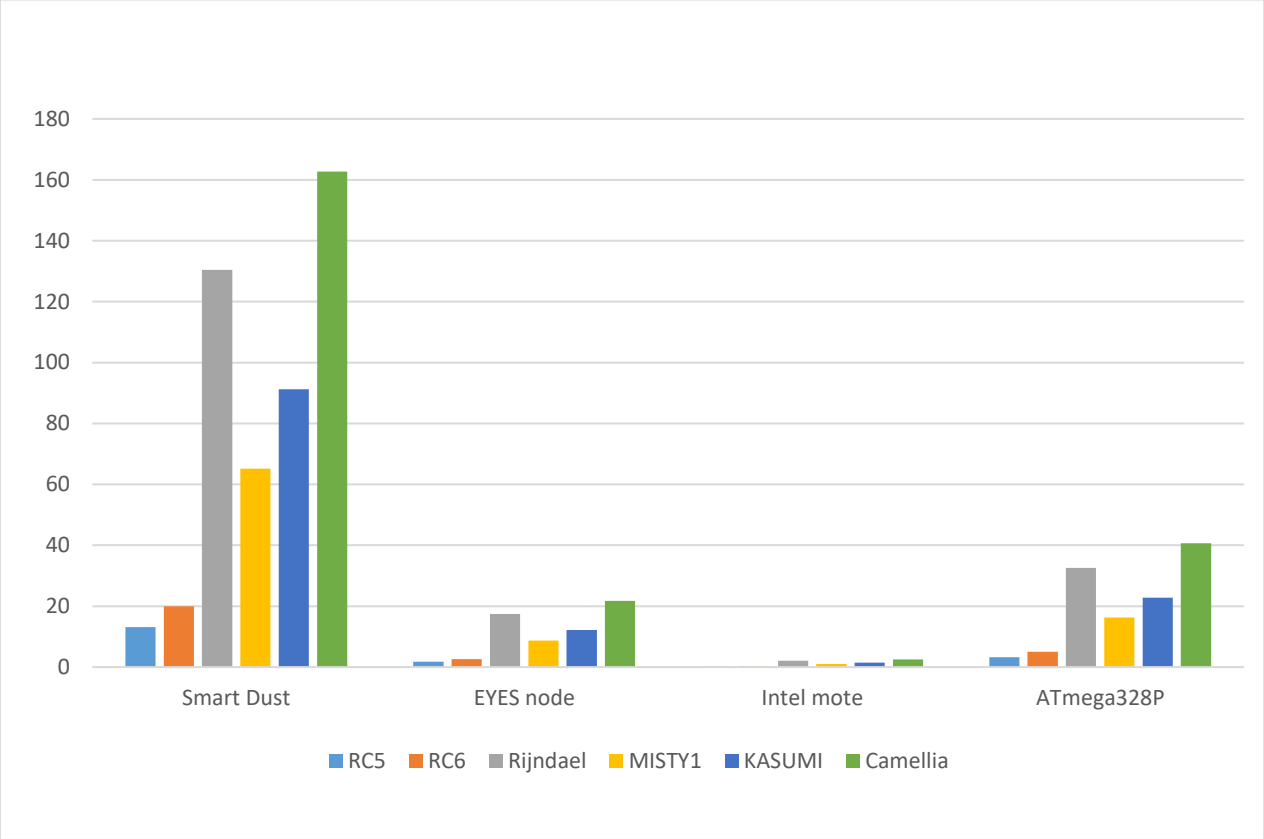

Рисунок 4.1. Порівняння алгоритмів за % споживання Flash пам’яті на різних процесорах.

Як видно з рисунка 4.1, не дивлячись на високу надійність алгоритмів Rijndael та Camellia їх використання може бути неможливим через малий розмір пам’яті вузлів мережі. Також слід звернути увагу, що на трьох процесорах алгоритми Rijndael , Camellia, Kasumi споживають понад 15%, залишаючи не так багато вільного місця для завантаження ОС та ПО необхідного для роботи WSN мережі.

Порівняння за енергоефективністю. К-сть спожитої енергії обраховується за формулою $E = P * t = U * I * t$. Враховуючи, що батарея подає на вузол однакову напругу і припускаючи, що кожна інструкція процесора потребує однакової сили струму (в [11] було показано, що відхилення є незначним до 0,05% на 16-bit RISC MSP430F149, тому для спрощення ми знехтуємо цим відхиленням.) Енергоефективність залежить від необхідного часу виконання, тобто ми можемо її оцінювати в к-сті циклів CPU необхідних для виконання операції.

Таблиця 4.3. Порівняння алгоритмів за енергоефективністю.

	Продуктивність Необхідна кількість циклів CPU для операції на 1 байт			
	Оптимізовані за споживанням пам'яті		Оптимізовані на швидкодію	
	Шифрування	Дешифрування	Шифрування	Дешифрування
RC5	17332,4	17337	8663	8660
RC6	19996	20001,2	19436	19662
Rijndael	599,6	1606,04	432	1177
MISTY1	552,2	552,2	531	532,2
KASUMI	1982	962,2	833,8	835,2
Camellia	5429	5435	3408	3408,8

Як видно з таблиці 4.3, за енергоефективністю обрані алгоритми можна представити в наступному порядку.

1. MISTY1
2. Rijndael = 1,51*MISTY1
3. KASUMI = 1,56 * MISTY1
4. Camellia = 6,41*MISTY1
5. RC5 = 16,29* MISTY1
6. RC6 = 36,77* MISTY1

Так MISTY1 є найбільш енергоефективним і його енергоефективність для побудови списку вище було прийнято за 1. Тоді як наступні відсортовані за спаданням їх енергоефективності та також їх енергоефективність представлена у відносній величині до енергоефективності MISTY1.

Висновки з розділу 4

Опираючись на аналіз, вище не можна однозначно сказати який з алгоритмів є найкращим. Оскільки наприклад Rijndael, що є стандартом AEC і надає найвищий рівень безпеки фактично неможливо використати на вузлі SmartDust через необхідний розмір Flash пам’яті та він же потребує понад 20% Flash пам’яті на EYES node. При цьому він є другим по енергоефективності.

Так вибір залежить від вихідних параметрів мережі, таких як місткість батареї вузлів, характеристики процесора: пам'ять, частота, розмір машинного слова. Однак підсумовуючи можна сформулювати загальні рекомендації:

1) Rijndael є оптимальним вибором для забезпечення високого рівня безпеки та енергоефективності.
2) MISTY1 надає середній рівень безпеки та необхідний розмір пам’яті при цьому має високу енергоефективність.
3) RC6 маючи найгірші показники енергоефективності можна використовувати в мережах де сенсори мають значний запас батареї чи є підключичними до постійного джерела живлення, однак мають малий розмір пам’яті та потребують високий рівень безпеки.

ВИСНОВКИ

Мережі WSN все більше почали набувати популярності не лише в з наукової точки зору, а і з практичної. На ринку вже існує ряд технологій що реалізують без дротові сенсорні мережі. Не дивлячись на те, що існує ряд відкритих питань забезпечення інформаційної безпеки таких мереж. Наявні рішення мають ряд слабких місць це: протокол управління ключами, механізми ініціалізації та розподілу спільних ключів, захист від глушіння сигналів, та захист кінцевих вузлів від фізичного доступу до секретних ключів. Так, основним методом забезпечення інформаційної безпеки являється криптографічне шифрування.

В даній роботі було описано основні вимоги до інформаційної безпеки в сенсорних мережах: автентифікація, актуальність, цілісність, доступність та конфіденційність даних, та самоорганізація вузлів мережі. Було описано обмеження з якими зустрічаються розробники WSN мереж при реалізації безпеки.

Також було проведено аналіз використання різних типів криптографічних методів шифрування в сенсорних мережах з урахуванням їх обмежень, так оптимальним є використання алгоритму Rijndael. Хоча кінцевий вибір може бути пов'язаний з бажаним рівнем безпеки та параметрами мережі. Протоколи SNEP та μTESLA є базою для подальшої оптимізації, використання WSN.

ПОСИЛАННЯ

1. Papadimitratos, P. “Secure Routing for Mobile Ad hoc Networks.” / Z.J. Haas. //Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2002) -January 2002. -P27-31, San Antonio, TX, USA.

2. Tanachaiwiwat “Routing on Trust and Isolating Compromised Sensors in Location-Aware Sensor Networks.” /S., P. Dave /R. Bhindwale/ A. Helmy. November 2003. In Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (ACM SenSys’03), 324-325, Los Angeles, USA

3. Estrin, D., R. Govindan, J. S. Heidemann, and S. Kumar. 1999. “Next Century Challenges: Scalable Coordination in Sensor Networks.” In Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom’99), 263-270, Seattle, Washington, USA, August 1999.

4. Hu, L., and D. Evans. 2003. “Secure Aggregation for Wireless Networks.” In Proceedings of theInternational Symposium on Applications and the Internet (SAINT’03) Workshops, 384, Orlando, Florida, USA, January 2003, IEEE Computer Society

5. Carman, D. W., P. S. Krus, and B. J. Matt. 2000. “Constraints and Approaches for Distributed Sensor Network Security.” Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA.

6. Eschenauer L., and V. D. Gligor. November 2002. “A Key-Management Scheme for Distributed Sensor Networks.” In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS’02), 41-47, Washington DC, USA.

7. Chan, H., A. Perrig, and D. Song. May 2003. Random Key Pre-Distribution Schemes for Sensor Networks.” In Proceedings of the IEEE Symposium on Security and Privacy (S&P’03), 197, Berkeley, California, USA.

8. Hill, J., R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. 2000. “System Architecture Directions for Networked Sensors.” In Proceedings of the 9th International Conference on Architectural

9. Law, Y. W., J. M. Doumen, and P. H. Hartel. October 2004. “Benchmarking Block Ciphers for Wireless Sensor Networks (Extended Abstract).” In Proceedings of the 1st IEEE International Conference of Mobile Ad-hoc and Sensor Systems, 447- 456,IEEE Computer Society Press

10. Ganesan, P., R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu. 2003. “Analyzing and Modeling Encryption Overhead for Sensor Network Nodes.” In Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, 151-159, New York: ACM Press.

11. Lai, B., S. Kim, and I. Verbauwhede. 2002. “Scalable Session Key Construction Protocols for Wireless Sensor Networks.” In Proceedings of the IEEE Workshop on Large Scale Real Time and Embedded Systems (LATES’02), 1-6, Austin, Texas, USA.

12. Komerling O., and M. G. Kuhn. 1999. “Design Principles for Tamper-Resistant Smart Card Processors.” In Proceedings of USENIX Workshop on Smartcard Technology, 9-20, Chicago, Illinois, USA

13. https://courses.csail.mit.edu/6.857/2017/project/17.pdf