УДК 004.056:004.733 **DOI:** 10.31673/2412-9070.2024.050729

Н. В. РУДЕНКО, канд. техн. наук, доцент;
ORCID: 0000-0001-8582-3126
М. М. ШРАМ, аспірант,
ORCID: 0009-0007-0640-1349
Державний університет інформаційно-комунікаційних технологій, Київ

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ: МОДЕЛЮВАННЯ ТА АНАЛІЗ

У статті розглянуто актуальні проблеми інформаційної безпеки у бездротових сенсорних мережах (БСМ). Зокрема, увагу приділено моделюванню та аналізу потенційних загроз, що можуть впливати на конфіденційність, цілісність та доступність даних у таких мережах. Проведено огляд існуючих методів захисту, визначено їхні переваги та недоліки. Запропоновано новий підхід до класифікації загроз на основі аналізу вразливостей та атак, а також розроблено моделі для оцінки ризиків інформаційної безпеки у БСМ. Результати дослідження можуть бути використані для покращення захисту бездротових сенсорних мереж у різних галузях, включаючи охорону здоров'я, промисловість та національну безпеку.

Ключові слова: інформаційна безпека, бездротові сенсорні мережі, загрози, моделювання загроз, аналіз загроз, кібербезпека, захист інформації, атаки на мережі, шифрування даних.

Вступ

Бездротові сенсорні мережі, що об'єднують безліч вбудованих пристроїв і сенсорів представляють порівняно новий вид інформаційно-телекомунікаційних інфраструктур, які відрізняються наявністю специфічних загроз інформаційної безпеки, обумовлених появою нових класів здійснюваних на такі системи програмно-інформаційних і фізичних впливів, і вимагають нових шляхів, і механізмів захисту. Аналіз захищеності в бездротових сенсорних мережах є необхідним для виявлення вторгнень, спроб несанкціонованої модифікації даних і коду пристроїв, атак підміни сенсорів, порушення автентичності, а також атак, що виснажують енергоресурси. Крім того, важливо повідомляти про стан критично важливих параметрів мережі з урахуванням семантики наданих сервісів.

Робота спрямована на вдосконалення засобів моделювання та аналізу загроз інформаційної безпеки бездротових сенсорних мереж за допомогою комплексного підходу до аналізу даних від пристроїв і сенсорів. Дослідження проводиться в умовах різнорідних і взаємодіючих пристроїв, що використовують бездротові протоколи передавання даних, з урахуванням підвищених вимог до захищеності цих систем.

Підходи до моделювання та аналізу загроз

Комплексний підхід до моделювання та аналізу загроз в бездротові сенсорні мережі (БСМ) передбачає проведення регулярних аудитів безпеки, тестування на проникнення та застосування сучасних криптографічних методів для захисту даних. Це дозволяє забезпечити високий рівень безпеки та надійності бездротових сенсорних мереж, що є критично важливим у сучасних умовах інформаційного суспільства.

Розгортання бездротових сенсорних мереж із захищеними вузлами є складним організаційно-технічним процесом, що потребує значних фінансових ресурсів. Основними властивостями інформаційних об'єктів, важливими для забезпечення інформаційної безпеки, є автентичність, цілісність, приватність, невідмовність і захист від повторного відтворення.

У бездротових сенсорних мережах DoS атаки можуть бути проведені на різних рівнях:

1. Фізичний рівень:

– Jamming-атаки: спрямовані на зашумлення фізичного каналу передавання бездротового сигналу, що перешкоджає коректному обміну даними між вузлами мережі.

– Фізичне втручання у роботу вузла: включає атаки, такі як підміна сенсорів або вилучення даних під час прямого доступу порушника до вузла.

2. Канальний рівень:

– Атаки на внесення колізій: здійснюються шляхом намагань вузла викликати колізії на частотному каналі для спотворення передавання даних.

– Атаки на виснаження ресурсів вузлів: включають стратегії, такі як примусова ретрансляція пошкоджених пакетів адресату, що призводить до зниження продуктивності вузла.

3. Мережний рівень:

– Атаки типу Black Hole: використовуються для перенаправлення всіх отриманих пакетів до "чорної діри" (некомпетентного вузла), що призводить до втрати пакетів і відсутності спілкування з сусідніми вузлами.

– Атака типу Selective Forwarding: полягає у вибірковому пересиланні пакетів через скомпрометований вузол, з ігноруванням інших, що може впливати на ефективність маршрутизації і надійність мережі.

Ці види атак представляють серйозну загрозу для безпеки і доступності бездротових сенсорних мереж, і вимагають впровадження ефективних захисних механізмів для їх запобігання і виявлення [1].

Атака типу Acknowledgment Spoofing полягає у створенні фальшивих підтверджень про факт "життя" неактивного вузла, які надсилаються його сусідам або конкретному вузлу. Це може призвести до неправильних висновків щодо наявності і активності вузла в мережі.

Атака типу Misdirection (перенаправлення) передбачає надсилання легітимних пакетів неправильним одержувачам. Це може викликати втрату даних або спотворення комунікаційного потоку в мережі.

На транспортному рівні бездротових сенсорних мереж можуть відбуватися такі типи атак:

1. Flooding-атаки: Ці атаки включають масову відправку пакетів з метою виснаження пам'яті пристроїв або інших апаратних ресурсів. Наприклад, атака може спрямовуватися на виснаження буферів пам'яті вузлів, що призведе до їх непродуктивності або відмови у обслуговуванні легітимних запитів.

2. Атаки порушення синхронізації: Ці атаки можуть включати в себе внесення помилок у часові мітки або інші параметри передавання даних, що призводить до спотворення або перешкоджання нормальному передаванню і обробці даних легітимним вузлом.

Ці атаки на транспортному рівні є серйозною загрозою для безпеки і надійності бездротових сенсорних мереж, оскільки вони можуть значно вплинути на їх функціональність і продуктивність. Виявлення і захист від таких атак вимагає впровадження відповідних заходів безпеки, включаючи моніторинг мережі і застосування захисних механізмів на рівні вузлів, і мережних протоколів.

При використанні централізованих обчислювальних алгоритмів у бездротовій сенсорній мережі Sybil-атаки можуть порушувати процес розподілу даних і їх надмірності. Це відбувається шляхом використання кількох ідентифікаторів вузлів, що надаються законним вузлам для доступу до ресурсів мережі та здійснення обміну інформацією. Особливо це стосується ситуацій, коли для забезпечення цілісності даних використовується одночасна доставка даних кількома маршрутами. У таких умовах Sybil-атаки можуть бути досить ефективними [2].

Blackhole-атака спрямована на порушення процесу коректної маршрутизації в мережі. Під час динамічного вибору маршрутів зловмисний вузол заявляє, що може доставити пакет даних між будь-якими двома заданими вузлами з максимальною якістю, зокрема мінімізуючи час доставки, кількість проміжних вузлів або інші важливі характеристики. В результаті атакуючий може перенаправити на себе більшу частину трафіку або необхідні йому пакети. Такі пакети стають повністю контрольованими атакуючим, що дозволяє йому детально дослід-

жувати мережу, її структуру та поведінкові особливості, а також модифікувати, втрачати або перенаправляти ці пакети іншим вузлам, порушуючи роботу мережі.

Окрім базових цілей інформаційної безпеки, таких як конфіденційність, цілісність і доступність, а також їх похідних, існують так звані вторинні цілі інформаційної безпеки, які необхідно враховувати під час аналізу захищеності програмно-апаратних компонентів бездротових сенсорних мереж. Ці цілі визначаються для конкретної області застосування з урахуванням таких характеристик:

1. Свіжість даних: гарантія того, що дані є актуальними та не застарілими.
2. Можливість самоорганізації мережі: здатність мережі автономно налаштовуватися та адаптуватися до змін.
3. Синхронізація за часом: узгодження часових параметрів між вузлами для коректної взаємодії.
4. Локалізація безпеки: здатність відстежувати кожен вузол і локалізувати інциденти безпеки з визначенням конкретних вузлів, які в них задіяні.

Також враховуються доступність вузлів мережі та даних, одержуваних від них [3].

Аналіз засобів моделювання загроз інформаційній безпеці бездротових сенсорних мереж

Розглянемо наступні основні програмні засоби, які використовуються для вирішення завдань моделювання загроз бездротових сенсорних мереж.

NS-2 – це засіб для імітаційного моделювання з відкритим вихідним кодом (https://sourceforge.net/projects/nsnam), призначений для моделювання мережі дискретних подій. До його переваг можна віднести підтримку великої кількості протоколів на різних рівнях мережної взаємодії. Однак, NS-2 має деякі недоліки: відсутність графічного інтерфейсу, необхідність використання складної скриптової мови для проведення моделювання, а також складність адекватного моделювання процесів енергоспоживання у бездротових сенсорних мережах.

TOSSIM – це програмний емулятор дискретних подій для бездротових сенсорних мереж. Він дозволяє моделювати сенсорні пристрої, які працюють на TinyOS (http://tinyos.net). Переваги TOSSIM включають його вільне поширення, наявність графічного інтерфейсу TinyViz, що відображає взаємодії елементів мережі та масштабованість мережі до 1000 вузлів. Однак, значним недоліком є те, що він дозволяє моделювати лише мережі, основані на операційній системі TinyOS, тобто можливо моделювати лише однотипні вузли.

EmStar – це програмний емулятор, який дозволяє проводити трасування процесу функціонування мережі у реальному часі. Він містить багато бібліотек, інструментів і апаратних характеристик сенсорів. Перевагами EmStar є наявність графічного інтерфейсу, модульність і зручна документація. До недоліків можна віднести суттєві обмеження масштабованості.

OMNeT++ – це безкоштовний для некомерційного використання дискретний мережний емулятор подій, написаний на мові C++ (https://omnetpp.org). Він має вбудований графічний інтерфейс та підтримує протоколи MAC і деякі інші протоколи бездротових сенсорних мереж. OMNeT++ використовується для моделювання управління каналами і завдань енергоспоживання в бездротових сенсорних мережах. До переваг OMNeT++ належать:

– Наявність графічного інтерфейсу.

– Велика кількість програмних середовищ і модулів, які розширюють функціонал, наприклад, NesCT, що дозволяє моделювати бездротові сенсорні мережі на операційній системі TinyOS.

– Підтримка багатьох протоколів бездротових сенсорних мереж, зокрема MAC-протоколів.

– Можливість моделювання споживання енергії вузлами бездротових сенсорних мереж.

Недоліками є складність додавання нових протоколів взаємодії елементів бездротових сенсорних мереж.

J-Sim – це мережний емулятор подій, побудований на мові програмування Java (https://www.physiome.org/jsim). Він надає графічний інтерфейс та бібліотеку для математи-

чного моделювання, розроблену спеціально для моделей J-Sim. J-Sim може моделювати процеси у реальному часі. Переваги J-Sim включають:

– Наявність графічного інтерфейсу.
– Велика кількість протоколів.
– Можливість моделювання маршрутів у бездротових сенсорних мережах.
– Можливість моделювання радіоканалів.
– Можливість моделювання споживання енергії.
– Масштабованість.

До недоліків відноситься слабка розширюваність щодо додавання нових протоколів.

ATEMU – програмний емулятор для систем на базі процесорів AVR (https://atemu-sensor-node-simulator-or-debugger.soft112.com). Він підтримує інші периферійні пристрої, такі як датчики типу MICA2 і радіоканал. Ядро емулятора ATEMU дозволяє моделювати довільну кількість вузлів та їх взаємодії. Переваги ATEMU:

– Масштабованість.
– Наявність графічного інтерфейсу.
– Високий рівень деталізації у процесі моделювання.
– Можливість моделювання різнорідних мереж.

Недоліки:

– Збільшені часові витрати на моделювання порівняно з іншими засобами.
– Обмежений набір функцій для моделювання маршрутизації та кластеризації.

Avrora – засіб для моделювання бездротових сенсорних мереж, орієнтований на аналіз (https://sourceforge.net/projects/avrora). Він дозволяє моделювати мікроконтролерні сенсорні вузли MICA2 на основі AVR. Avrora не має графічного інтерфейсу, але підтримує моделювання процесів енергоспоживання. Переваги Avrora:

– Висока швидкість моделювання.
– Краща точність порівняно з TOSSIM.
– Можливість моделювання процесів енергоспоживання.

Недоліки:

– Відсутність графічного інтерфейсу.
– Відсутність можливості моделювання алгоритмів управління мережею.

Castalia – засіб для моделювання бездротових сенсорних мереж і мереж з низьким енергоспоживанням (https://sourceforge.net/projects/castalias). Він оснований на платформі OMNeT++. Castalia використовується для тестування алгоритмів або протоколів з урахуванням особливостей радіоканалу та поведінки вузлів. Переваги Castalia:

– Можливість моделювання властивостей радіоканалу.
– Наявність графічного інтерфейсу.
– Підтримка протоколів маршрутизації і MAC.
– Можливість моделювання фізичного процесу передавання даних, задання шумів і чутливості пристрою.
– Платформенна незалежність.

Недоліки: відсутність прив'язки до конкретної платформи бездротових сенсорних мереж, що ускладнює моделювання для певних платформ/операційних систем, наприклад, TinyOS.

QualNet – емулятор бездротових сенсорних мереж з графічним інтерфейсом для дизайну, анімації та аналізу бездротових сенсорних мереж (https://www.scalablenetworks.com/products/qualnet-network-simulation-software-tool). Переваги QualNet:

– Масштабованість.
– Наявність графічного інтерфейсу.
– Підтримка різних моделей представлення пристроїв.
– Функції оцінки ефективності протоколів на кожному рівні.

– Підтримка багатопроцесорних систем і систем з розподіленими обчисленнями.

Недоліки:

– Висока вартість.
– Повільний графічний інтерфейс на основі платформи Java.

InsightMaker – безкоштовний засіб для моделювання бездротових сенсорних мереж, який надається у вигляді веб-сервісу (https://insightmaker.com). Він підтримує багато протоколів та можливість візуального створення моделей і анімації.

WSNet – вільно поширюваний емулятор бездротових сенсорних мереж (http://wsnet.gforge.inria.fr). Він підтримує архітектури із складними вузлами, моделювання енергоспоживання та деяких видів фізичних явищ.

Відзначимо, що перераховані інструменти відносяться до класу засобів імітаційного моделювання. Використання таких інструментів дозволяє нівелювати або зменшити вплив наступних обмежень, пов'язаних з моделюванням та аналізом засобів оцінки загроз інформаційній безпеці складних великомасштабних бездротових сенсорних мереж:

1. Апаратні обмеження: наявність та вартість апаратних комунікаційно-обчислювальних ресурсів мережі, включаючи обмеження на кількість одночасно модельованих пристроїв.
2. Часові обмеження: складнощі у моделюванні тривалих багатокрокових процесів, що вимагають одночасного залучення, налаштування та координованого управління великою кількістю бездротових вузлів.
3. Обмеження безпеки: необхідність врахування можливих побічних ефектів на аналізовану інфраструктуру.

Вибір конкретного засобу моделювання визначається зазначеними особливостями кожного з них, що включають:

– Цільову спрямованість.
– Набір функцій та операцій, доступних для використання.
– Програмну сумісність та наявність програмного інтерфейсу (API) і зовнішніх бібліотек для інтеграції із сторонніми компонентами моделювання або інфраструктурними засобами.
– Умови використання.

У роботі пропонується комплексний підхід до застосування існуючих засобів моделювання загроз інформаційній безпеці в бездротових сенсорних мережах. Враховуючи різноманітність загроз інформаційної безпеки, їх прояви на різних рівнях мережної взаємодії та етапах життєвого циклу бездротових сенсорних мереж, а також особливості експлуатованих програмно-апаратних ресурсів, доцільно використовувати комбінування існуючих засобів моделювання. Це комбінування здійснюється, перш за все, у формі інтеграції результатів моделювання окремих моделей.

Моделі представлення бездротових сенсорних мереж

Для вирішення завдань моделювання та аналізу загроз інформаційній безпеці в бездротових сенсорних мережах запропоновано ряд моделей, які агрегують основні дані про мережу та правила для аналізу загроз її інформаційній безпеці. Ці моделі використовуються для узагальнення та специфікації необхідних вихідних даних у процесі моделювання.

Моделі подання бездротових сенсорних мереж призначені також для проведення експертного аналізу мережних специфікацій та для верифікації з використанням автоматизованих засобів підтримки процесів прийняття рішень щодо проєктування, розробки, забезпечення та аналізу захищеності мережі. Крім того, ці моделі призначені для аналізу атак та інцидентів безпеки на рівні маніпуляції командами з використанням уніфікованих команд звернення до вузлів мережі, її даних і наданих сервісів. Моделі включають зворотні зв'язки до програмно-апаратної інфраструктури мережі у вигляді спеціалізованих тригерів і виконавчих елементів, які ініціюють конкретні події у мережі, такі як відправлення пакету даних, оновлення ключа шифрування тощо.

Для представлення бездротової сенсорної мережі запропоновано дві моделі:

1. На основі JSON-формату: Зручний для формування, модифікації та використання даних, як вручну, так і за допомогою автоматизованих програмних засобів обробки даних.

2. На основі UML-діаграм: Дозволяє специфікувати як статичну, так і динамічну структуру мережі, сценарії роботи мережі, протоколи взаємодії та операційні процедури.

UML-модель включає серію діаграм:

– Діаграми класів: Визначають види сутностей бездротових сенсорних мереж і відносини між ними, включаючи ієрархічні відносини.

– Діаграми мережної архітектури: Задають структуру мережі та екземпляри її пристроїв, а також фізичні та логічні зв'язки між вузлами мережі.

– Діаграми послідовності: Специфікують сценарії роботи мережі, процеси та протоколи взаємодії її елементів, зокрема процеси автентифікації вузлів та динамічної маршрутизації [7].

Вибір обох типів моделей зумовлений їх можливостями щодо відображення інформації про бездротові сенсорні мережі, зручного для подальшого використання у вирішенні завдань, запланованих на другий етап цього проєкту. Зокрема, UML-діаграми є більш придатними для вираження семантики структури, функцій і процесів мережі. Вони доцільні для експертного аналізу можливих зв'язків, інформаційних потоків, функціональних і логічних відносин у мережі, а також особливостей процесів поширення та передавання інформації і аналізу захищеності.

JSON-формат, на відміну від UML-діаграм, більше орієнтований на формальну специфікацію технічних характеристик мережі та їх значень. Це дозволяє використовувати дані в автоматизованих засобах аналізу захищеності програмно-апаратних компонентів мережі, зокрема для формування тестових векторів, наборів правил функціонування мережі та політик безпеки, а також для верифікації та валідації процесів і даних мережі та детектування різних аномалій у мережі.

Висновки

У статті представлені результати моделювання та аналізу загроз інформаційній безпеці бездротових сенсорних мереж. Аналіз показав різноманітність існуючих загроз і підкреслив необхідність комплексного підходу до їх аналізу з урахуванням вразливостей, які можуть експлуатуватися порушниками в процесі атаки і проявлятися на різних рівнях мережної взаємодії.

Аналіз програмних засобів, придатних для моделювання бездротових сенсорних мереж та загроз інформаційній безпеці, дозволив встановити доцільність застосування комплексного підходу до моделювання з використанням різних видів представлення та способів обробки даних. Кожен із наведених методів моделювання, маючи свої переваги та недоліки, дозволяє оцінити захищеність мережі у заданих умовах. Для забезпечення процесу моделювання та підготовки вихідних даних у роботі було запропоновано дві моделі представлення бездротових сенсорних мереж: на основі JSON-формату та UML-діаграм.

Імітаційне моделювання дозволяє відтворити динамічно основні процеси, що виникають у мережі, без необхідності залучення значних апаратних та обчислювальних ресурсів, яких може не бути в наявності. Цей вид моделювання дозволяє, зокрема, змоделювати загрози, пов'язані з процесами масштабування бездротових сенсорних мереж. Хоча натурне моделювання є найбільш наближеним до реальних умов функціонування мережі і тому найбільш адекватним, технічна та організаційна складність деяких видів атак може бути значною перешкодою для їх моделювання за допомогою натурного моделювання.

Таким чином, для забезпечення ефективного аналізу загроз інформаційній безпеці бездротових сенсорних мереж необхідно використовувати комплексний підхід до моделювання, який включає як імітаційне, так і натурне моделювання, з урахуванням специфічних переваг та обмежень кожного методу. Це дозволяє отримати більш повну та точну оцінку захищеності мережі в різних умовах та ситуаціях.

Список літератури

1. Білоус, О. О., Головінов, О. М., & Зазимко, В. В. (2015). Актуальні питання захисту інформації в бездротових сенсорних мережах. Наукові праці ОНАХТ, 2(47), 114-119.

2. Воробйов, І. В., Коваленко, О. Ю., & Дядюра, Н. О. (2017). Методи виявлення і запобігання атакам у бездротових сенсорних мережах. Інформаційні технології та комп'ютерна інженерія, 45(1), 56-62.

3. Кучеренко, А. В., & Шевчук, В. М. (2020). Методи шифрування даних у бездротових сенсорних мережах. Телекомунікаційні та інформаційні технології, 2(89), 33-38.

4. Мельник, М. В., & Сорока, О. С. (2017). Порівняльний аналіз протоколів захисту інформації в сенсорних мережах. Сучасні інформаційні технології та системи в управлінні, 4(24), 102-108.

5. Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tygar, J. D. (2002). SPINS: Security Protocols for Sensor Networks. Wireless Networks, 8, 521-534.

6. Karlof, C., & Wagner, D. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Ad Hoc Networks, 1(2-3), 293-315.

7. Roman, R., Zhou, J., & Lopez, J. (2006). Applying Intrusion Detection Systems to Wireless Sensor Networks. Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE, 640-644.

N.Rudenko, M.Shram

INFORMATION SECURITY THREATS IN WIRELESS SENSOR NETWORKS: MODELING AND ANALYSIS

The article deals with current problems of information security in wireless sensor networks (BSM). In particular, attention is paid to modeling and analyzing potential threats that may affect the confidentiality, integrity and availability of data in such networks. An overview of existing protection methods is carried out, their advantages and disadvantages are determined. A new approach to threat classification based on vulnerability and attack analysis is proposed, and models for assessing information security risks in BSM are developed. The results of the study can be used to improve the protection of wireless sensor networks in various industries, including healthcare, industry, and national security.

Subject of research. The subject of the research is tools for modeling and analyzing threats to information security of wireless sensor networks.

Method. The paper uses methods of mathematical modeling and System Analysis.

Main results. The analysis of current threats to the information security of wireless sensor networks is carried out. A comparative analysis of the means of simulation modeling of wireless sensor networks and attacking influences in them is carried out. Two models of representation of wireless sensor networks for solving threat modeling problems are proposed.

Practical significance. The results of the work can be used to model and evaluate the security of complex wireless sensor networks with a large number of nodes in the conditions of organizational complexity of using fully functional instances of wireless sensor networks to solve information security problems.

Keywords: Information Security, Wireless Sensor Networks, threats, threat modeling, threat analysis, cybersecurity, information security, network attacks, data encryption, authentication.