УДК 004

Волошко С.В., к.т.н., с.н.с.
Курца Д.О.
Полтавський національний технічний
університет імені Юрія Кондратюка

ІНФОРМАЦІЙНА БЕЗПЕКА В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

У даній роботі здійснено аналіз загроз інформаційним ресурсам, які обробляються в системах з використанням безпроводових сенсорних мереж. Систематизовано можливі типи атак на сенсорні мережі та запропоновані механізми забезпечення безпеки в сенсорних мережах, які дозволяють значно мінімізувати загрози інформаційній безпеці безпроводових сенсорних мереж.

Ключові слова: *безпроводові технології, передача даних, сенсорні мережі, інформаційна безпека*

Вступ

Бурхливий розвиток інформаційних технологій сприяє створенню досконалих засобів зібрання та опрацювання великої кількості різноманітної інформації. Серед таких засобів особливе місце займають безпроводові сенсорні мережі (БСМ). В загальному випадку під безпроводовими сенсорними мережами (Wireless Sensor Network) розуміють мережі, які складаються із множини безпроводових інформаційних вузлів, розміщених у просторі і призначених для моніторингу параметрів навколишнього середовища або об’єктів, які в ньому знаходяться.

Основні цілі забезпечення інформаційної безпеки в БСМ можна умовно розділити на першочергові і другорядні. Першочергові цілі широко відомі і включають в себе забезпечення конфіденційності, цілісності, аутентифікації і

доступності даних. Другорядні цілі забезпечення безпеки включають в себе такі поняття як «свіжість» даних, самоорганізація, часова синхронізація, захищена локалізація.

Атаки на безпроводові сенсорні мережі

Більшість загроз інформаційній безпеці в безпроводових мережах схожі з загрозами і атаками на проводові мережі, за винятком того, що безпроводові мережі важче захистити внаслідок використання відкритого середовища в якості носія даних і широкомовної природи безпроводових з'єднань. Нижче розглянемо основні мережеві атаки в БСМ.

Пасивні атаки. Аналіз трафіку і прослуховування комунікаційного каналу неавторизованими особами класифікується як пасивна атака. Атаки, націлені виключно на отримання даних, що передаються є пасивними по своїй природі. Найбільш частими є наступні види атак, спрямовані на порушення конфіденційності даних:

Моніторинг і прослуховування. Даний вид атаки зустрічається найбільш часто. За допомогою підслуховування зловмисник може з легкістю отримати доступ до даних, що передаються. При передачі контрольної інформації про конфігурацію мережі, дана техніка може становити найбільшу небезпеку для конфіденційності даних.

Аналіз трафіку. Навіть коли інформація передається в зашифрованому вигляді, залишається ймовірність використання зловмисником техніки аналізу комунікаційних патернів. Активність сенсорів потенційно може розкрити досить інформації для нанесення зловмисником шкоди сенсорній мережі.

Активні атаки. Різні модифікації даних під час комунікації, що здійснюються авторизованими особами, класифікуються як активні атаки. Нижче надведено характеристики активних атак.

Атаки маршрутизації. Атаки, які здійснюються на мережевому рівні (network layer) моделі OSI називаються атаками маршрутизації. Наступні атаки

маршрутизації зустрічаються найбільш часто:

– Змінена маршрутна інформація. До впливу даної атаки найбільш схильні децентралізовані мережі, де кожен вузол є маршрутизатором і відповідно може змінювати маршрутну інформацію. Внаслідок даної атаки може відбуватися створення кільцевого маршруту, збільшуватися час доставки пакету даних до точки призначення і т. д.

– Вибіркова розсилка. Скомпрометований вузол сенсорної мережі може вибірково видаляти певні пакети. Особливо ефективною дана атака може бути в комбінації з атаками, які збирають велику кількість трафіку на даному вузлі мережі. В результаті даної атаки серйозно страждає цілісність і доступність даних, що може істотно знизити рівень якості надання сервісу сенсорною мережею.

– Атака Воронки (Sinkhole Attack). Дана атака характерна тим, що скомпрометований вузол мережі починає діяти по типу воронки, збираючи весь трафік сенсорної мережі. Особливо в мережах з протоколом маршрутизації, заснованому на широкомовній розсилці, зловмисник прослуховує запити на маршрутну інформацію і відповідає сенсорним вузлам, що «знає» найкоротший маршрут до базової станції. Як тільки скомпрометованому вузлу вдалося стати між транслюючим сенсорним вузлом і базовою станцією, він може виконувати будь-які дії з пакетам даних, що надходили.

– Атака Sybil attack. Під час даної атаки один скомпрометований вузол може використовувати кілька псевдоідентифікаторів, видаючи себе від-разу за кілька вузлів. Подібні атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі і т.д. По суті будь-яка мережа з рівноправними вузлами (особливо безпроводові і децентралізовані мережі) є схильними до даної атаки.

– Атака Wormhole attack. Дана атака передбачає створення спеціального шляху між двома і більше скомпрометованими вузлами сенсорної мережі для передачі по ним перехоплених пакетів, доступних тільки для атакуючої

системи. Подібні атаки представляють серйозну загрозу безпеці сенсорної мережі тому, що не вимагають компрометації вузла сенсорної мережі. Тоді, коли вузол (базова станція або звичайний вузол) використовує трансляцію розсилки для запиту маршруту, зловмисник отримує даний запит і перенаправляє його до найближчого сусіда. Будь-який вузол, який отримав подібний перенаправлений запит розглядає себе як вузол, що знаходиться в зоні досяжності вузла і запам'ятовує вузол, як свого «батька». Навіть, якщо цей вузол знаходиться на великій відстані від вузла і його відокремлюють від вузла безліч сенсорних вузлів, він буде розглядати вузол як найближчий від себе.

– Флуд атака (HELLO flood attack). Дана атака є широкомовною атакою, яка служить для того, щоб передати в сенсорну мережу масу необов'язкових повідомлень, які повинні позбавити мережу різноманітних ресурсів – канальної ємності, обчислювальної потужності, енергетичних ресурсів і т.д. Під час подібної атаки зловмисник за допомогою високочастотного радіопередавача з достатньою обчислювальною потужністю розсилає Hello пакети безлічі вузлів сенсорної мережі. Вузли, які отримали Hello пакети, розглядають скомпрометований вузол як свого сусіда. Під час наступної передачі даних, вони будуть використовувати отриману адресу з Hello пакетів для відправки. Таким чином, зловмисник отримає доступ до даних.

Фізичні атаки. Вузли сенсорної мережі часто встановлюються в середовищах із зовнішніми впливами. В таких середовищах маленький форм-фактор вузлів сенсорної мережі в поєднанні з відсутністю постійного нагляду за ними робить їх схильними до різних фізичних атак. На відміну від інших видів атак, фізичні атаки руйнують сенсори незворотньо.

Механізми забезпечення безпеки

Механізми забезпечення безпеки використовуються для ідентифікації, запобігання і відновлення після атак. Механізми забезпечення безпеки можна умовно розділити на механізми високого і низького рівня.

Механізми забезпечення безпеки низького рівня

Управління ключами і встановлення довіри. Через лімітовані ресурси, особливо ресурси енергетичної батареї, асиметричне шифрування ключами не повинно використовуватися для сенсорних мереж. Таким чином, необхідно використовувати симетричне шифрування. Техніки встановлення і управління ключами повинні бути придатними для використання в мережах з сотнями і тисячами вузлів.

Секретність і аутентифікація. Сенсорні мережі вимагають захисту від прослуховування, ін'єкцій і модифікації пакетів. Криптографія є стандартним захистом. Складнощі виникають в процесі застосування криптографії для сенсорних мереж.

Стійкість до відмов в обслуговуванні. Причинами відмови в обслуговуванні можуть бути проблеми апаратного забезпечення, помилки в програмному забезпеченні, недостатність ресурсів, несприятливі умови зовнішнього середовища або сукупність впливу вище перерахованих факторів. Технологія розширення спектру використовується для захисту сенсорних мереж від подібних атак. Вона передбачає використання методів навмисного розширення діапазону частот сигналу. Діапазон частот стає більшим, ніж необхідно для передачі повідомлення. Передача такого сигналу схожа на шум, що дозволяє знизити ризики навмисного інтерференційного впливу на інформаційний сигнал з боку зловмисників.

Захищена маршрутизація. Маршрутизація є ключовим процесом, без якого неможливо здійснювати комунікацію між вузлами сенсорної містять безліч вразливостей інформаційної безпеки. Найпростіші атаки можуть мати на меті впровадження скомпрометованої маршрутної інформації в сенсорну мережу, що згодом створює проблеми в передачі даних від відправника в кінцеву точку призначення. Розробка нових схем аутентифікації і захищених протоколів маршрутизації може захистити мережі від подібних атак.

Механізми забезпечення безпеки високого рівня

Захищене управління групою. Кожен вузол безпроводової сенсорної мережі обмежений в обчислювальних ресурсах і комунікаційних можливостях. Однак, такі функції як агрегацію мережевих даних і їх аналіз може здійснювати група вузлів сенсорної мережі. Наприклад, група сенсорів мережі може виконувати спільне стеження за пересуванням певного об'єкта.

Ідентифікація вторгнень. Безпроводові сенсорні мережі схильні до різних вторгнень. Основне завдання механізмів ідентифікації вторгнень полягає в моніторингу сенсорної мережі, ідентифікації можливих спроб проникнення і розсилки відповідних повідомлень користувачам.

Захищена агрегація даних. Дані, які збираються з вузлів сенсорної мережі, потім часто агрегуються на рівні базової станції. Завдяки агрегації даних за допомогою сенсорної мережі можна розрахувати середню температуру в географічному регіоні, комбінувати дані сенсорних вузлів для розрахунку місця розташування і швидкості транспортного засобу і т. д.

Висновок

Для підвищення надійності автоматизованих систем з використанням безпроводових сенсорних мереж необхідна швидка ідентифікація пошкоджених інформаційних вузлів та їх графічне представлення. Існуючі засоби ідентифікації в переважній більшості стосуються пошуку одиничних пошкоджених елементів мережі. Відомі методи не дають можливості забезпечити надійність роботи безпроводових сенсорних мереж при швидкому збільшенні кількості вузлів мережі та при «атаці» на групу сенсорів.

Майбутні дослідження мають на меті виявлення недоліків безпроводових сенсорних мереж з точки зору забезпечення конфіденційності, цілісності та доступності в архітектурі «клієнт-сервер-шлюз-вузол», дослідження протоколів захисту, їх недоліків та можливих шляхів удосконалення.

Посилання

1. Максим Сергиевский. Беспроводные сенсорные сети [Електронний ресурс] – Режим доступу до ресурсу: http://www.compress.ru/Article.aspx?id=17950.

2. H. Karl and A. Willig. Protocols and Architectures for Wireless Sensor Networks. John Wiley & Sons, May 2005.

3. Александр Карабуто. Сенсорные сети [Електронний ресурс] – Режим доступу до ресурсу: http://offline.computerra.ru/2004/553/35459/

Рецензент: Сомов Сергій Вікторович, к.т.н., доцент, ПолтНТУ

Authors: Voloshko S.V., Kurtsa D.O.

INFORMATION SECURITY IN WIRELESS SENSOR NETWORKS

Abstract. In this work, the analysis of threats to the information resources that are processed in systems using wireless sensor networks. Systematized the possible types of attacks on sensor networks and the proposed security mechanisms in sensor networks that can significantly minimize threats to information security of wireless sensor networks.

Keywords: wireless technology, data transmission, sensor networks, information security.

Авторы: Волошко С.В., Курца Д.А.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Аннотация. В данной работе проведен анализ угроз информационным ресурсам, которые обрабатываются в системах с использованием беспроводных сенсорных сетей. Систематизированы возможные типы атак на сенсорные сети и предложены механизмы обеспечения безопасности в сенсорных сетях, которые позволяют значительно минимизировать угрозы информационной безопасности беспроводных сенсорных сетей.

Ключевые слова: беспроводные технологии, передача данных, сенсорные сети, информационная безопасность.