УДК 621.396

ЗАХИСТ ІНФОРМАЦІЇ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Туранська О. С., Лисенко О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: turanska.o.s@gmail.com

Information Security in Wireless Sensor Networks

The question of information security is very popular nowadays for all types of networks, wireless sensor networks are no exception. Wireless sensor networks are often used in battle, monitoring infrastructureor in disaster area, that's why is very important that the information is coming from the sensor was authentic and in time.

Питання безпеки інформації є дуже популярним в наш час для всіх типів мереж і безпроводові сенсорні мережі не є виключенням. Безпроводові сенсорні мережі часто використовуються в полі бою, для моніторингу звичайної інфраструктури чи в зоні стихійних лих і тому дуже важливо щоб інформація, яка поступає від сенсорів була достовірною і вчасною. В таких зонах сенсори часто залишаються без нагляду і тому стають мішенями для фізичних атак та несанкціонованого доступу до інформації.

В усіх типах побудови мережі є фундаментальні механізми для забезпечення основних служб безпеки. Таких як: конфіденційність, цілісність та доступність. Ці механізми повинні гарантувати те, що тільки ймовірний отримувач зможе правильно інтерпретувати повідомлення, що повідомлення не може бути змінено в процесі передачі та гарантувати здатність системи чи мережі виконувати задачі в будь-який час без перебоїв. Це першочергові цілі забезпечення безпеки мережі. Другорядними ж є актуальність даних, самоорганізація, часова синхронізація. Актуальність даних дозволяє перевірити, що повідомлення було відправлено вперше, а не є копією вже застарілого, самоорганізація дозволяє забезпечити досить незалежну і гнучку роботу сенсорів для можливості самовідновлення в топології в критичних ситуаціях, на часовій синхронізації базується успішна робота різних механізмів і протоколів в БСМ, вона використовується для визначення загальної часової шкали для всіх вузлів мережі.

Більшість атак на БСМ схожі на загрози, які можуть виникати при атаках в проводових мережах, але безпроводові мережі більш уразливі за рахунок своєї широкомовної природи і відкритих каналів передачі даних.

Атаки можуть бути активними і пасивними. Пасивні атаки – це атаки, ціллю яких є виключно отримання інформації, яка передається. Частіш за все це моніторинг та прослуховування. Дана техніка являє собою найбільшу загрозу для конфіденційності даних.

Активні атаки – це атаки при яких відбуваються зміна даних, що передаються, неавторизованими особами. Найпоширеніші активні атаки:

- Атака маршрутизації. Атаки відбувають на мережевому рівні моделі OSI. Найчастіше зустрічаються: змінна маршрутна інформація (можуть виникати закільцювання маршрутів та збільшення часу передачі пакетів); вибіркове розсилання (вузли, на які здійснюється вплив, можуть вибірково видаляти повідомлення призначені для передачі в мережі); атака «бездонна воронка»(вузол, на який здійснюється вплив, перенаправляє весь трафік в мережі через себе); атака «переповнення» (широкомовна атака, яка використовується для перенаправлення в сенсорну мережу необов'язкових повідомлень, для знищення таких ресурсів як канальна ємність, обчислювальної потужність та ін.)
- Захват вузла. Призводить до отримання важливої інформації, наприклад криптографічних ключів.
- Спотворення повідомлень. Будь-яке спотворення повідомлення злочинцями несе в собі загрозу цілісності інформації.
- Фізичні атаки. Часто БСМ розміщують в місцях, де сенсори знаходяться без нагляду, тому вони є схильними до фізичного пошкодження, що пошкоджує сенсори без можливості відновлення.

Стандартним захистом від прослуховування та модифікації пакетів є криптографія. У мережах з рівноправними вузлами, криптографія з міжкінцевим шифруванням дозволяє досягти високого рівня безпеки, однак вимагає встановлення ключів між усіма вузлами мережі і є несумісною з широкомовною розсилкою і пасивною участю (технологія, завдяки якій вузол, що прослуховує сусідній до нього вузол мережі, може вирішити не передавати дані, в разі якщо точно такі дані передаються сусіднім вузлом). Криптографія на канальному рівні спрощує установку ключів і підтримує пасивну участь і трансляцію розсилку, проте дозволяє проміжним вузлів перехоплювати і змінювати повідомлення.

Досить розповсюдженими в сенсорних мережах є атаки відмови в обслуговуванні (DoS). Вони вимагають ефективних заходів, для їх уникнення та перешкоджання їх поширенню по всій мережі. Наприклад, коли виявляється або підозрюється атака перешкод, сенсорна мережа може спробувати ізолювати порушену область, направивши трафік навколо відключених частин мережі.

На канальному рівні атаки зіткнень і вичерпання можуть втілюватись шляхом використання кодів корекції помилок (які додають витрати обробки і комунікації) і схем, що обмежують розмір, що дозволяють пристрою ігнорувати запити, які можуть привести до передчасного енергетичного виснаження. Перетворення може бути адресовано на мережевому рівні за допомогою коду аутентифікації повідомлень, яка може бути розглянута як криптографічно безпечна контрольна сума повідомлення. Ці контрольні суми дозволяють одержувачу перевірити, імітувалося або змінювалося чи повідомлення.

Популярний протокол, який використовують для роботи БСМ – це стандарт IEEE 802.15.4 і специфікація ZigBee. Цей стандарт забезпечує чотири основних моделі безпеки: управління доступом, цілісність повідомлень, конфіденційність повідомлень і захист відтворення.

Стандарт розрізняє вісім наборів безпеки, кожен з різними рівнями захисту для переданих даних. Перший набір не передбачає захист, другий набір передбачає тільки шифрування (AES - CTR), супроводжуваний групою наборів тільки з аутентифікацією (AES - CBC - MAC), і групою наборів і з аутентифікацією і з шифруванням (AES - CCM). Набори, які пропонують аутентифікацію, відрізняються за розмірами MAC, які варіюються від 32 до 128 бітів. Для кожного набору, який пропонує шифрування, IEEE 802.15.4 також пропонує додатковий захист відтворення, що складається з монотонно збільшених порядкових чисел для повідомлень, щоб дозволити одержувачу виявляти атаки відтворення.

На додаток до засобів захисту IEEE 802.15.4 специфікація ZigBee також представляє поняття центру довіри, відповідальність зазвичай прийнята на координатора ZigBee. Центр довіри відповідальний за аутентифікацію пристроїв, що бажають приєднатися до мережі (адміністратор довіри), підтримка і розподіл ключів (адміністратор мережі) і включення наскрізний безпеки між пристроями (менеджер конфігурації).

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

Подібно специфікаціям в стандарті IEEE 802.15.4, у ZigBee є кілька рівнів безпеки, включаючи нульова безпеку, тільки шифрування, тільки аутентифікація, і обидва і шифрування і аутентифікація.

Безпроводові сенсорні мережі використовуються в багатьох сферах нашого життя. Оскільки, як і будь-які комп’ютерні мережі, безпроводові теж піддаються загрозам та атакам, тому необхідно використовувати спеціальні протоколи та методи для захисну інформації, для зменшення ризиків потрапляння інформації, що передається в мережі, в чужі руки. У зв’язку із тенденцією до спрощення структури БСМ, необхідно вдосконалювати існуючі методи і розвивати нові.

Література

1. Kui Ren, Wenjing Lou “Communication Security in Wireless Sensor Networks”, year 2007
2. Murat Dener, “Security Analysis in Wireless Sensor Networks”, year 2014
3. Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM, Page 53—57, year 2004.