АНАЛІЗ БЕЗПЕКИ ЕЛЕМЕНТІВ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Комарець К.А.
Науковий керівник – доцент каф. БІТ Ляшенко О.С.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. Безпеки інформаційних технологій, тел. (057) 702-14-25)
e-mail: kateryna.komarets@nure.ua

Security and privacy are important issues in all types of networks. These problems are of particular importance in wireless sensor networks, because the unique characteristics of these networks and the purpose of the programs they serve, make them attractive targets for intrusions and other attacks. To solve the problem of security and protection of information in wireless sensor networks, but now technologies are developing very fast and newer methods of attacks are appearing, so this process is relevant at the moment and requires constant research and updating of methods of combating attacks.

Комп'ютерна і мережева безпека – це сукупність всіх стратегій, механізмів і служб, які надають комп'ютерній системі або мережі необхідний захист від несанкціонованого доступу та непередбачуваного використання. Більшість механізмів безпеки створено для трьох основних моделей безпеки: приватна власність, цілісність і доступність. При застосуванні бездротових сенсорних мереж виникає безліч унікальних проблем, які потрібно розглянути, звертаючись до проблем безпеки, які можуть виникнути в додатках сенсорної мережі:

1. Обмеження ресурсу.
2. Відсутність центрального управління.
3. Віддалене розташування.
4. Зв'язок, схильний до втрат.

Ідея бездротової безпеки полягає в тому, щоб використовувати бездротові властивості, запропоновані самим способом для розробки легких механізмів безпеки. Можливі наступні показники, щоб оцінити, чи схема безпеки відповідає вимогам безпроводових сенсорних мереж:

- безпека;
- відмова;
- енергоефективність;
- гнучкість;
- масштабованість;
- відмовостійкість;
- самовідновлення.

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

Атаки на безпроводові сенсорні мережі здійснюються на всіх рівнях. Починаючи від фізичного втручання, коли вплив відбувається на сам сенсор і закінчуючи втручанням в роботу програм керування мережею. Особливості експлуатації значно ускладнюють процес забезпечують процес захисту безпеки. На фізичному рівні атаки характеризуються фізичним втручанням в структуру мережі, а також діями. що спричиняють виснаження ресурсів самого датчика.

Атаки на канальному рівні викликають затримки в передачі даних, а, відповідно, інформація, що передається, втрачає свою актуальність, або викликають повторну передачу пакетів даних.

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

В наш час існує багато методів для забезпечення захисту інформації в мережах, але враховуючи особливості роботи БСМ не всі вони можуть застосовуватися в безпроводових сенсорних мережах.

Список використаної літератури:

1. Половко А.М., Гуров С. В. Основы теории надежности. – СПб.: БХВ Петербург 2006. – 560 с.

2. Острейковский В.А. Теория надежности. – М.: Высшая школа, 2000. –464 с. Шахнович И.А.

3. Современные технологии беспроводной связи. – М.: Техносфера, 2006. – 288 с