УДК 007.51

Ковальова Ю.В., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ МОНІТОРИНГУ

Сучасні тенденції, спрямовані на розвиток розподілених систем управління, вказують, що незважаючи на значні успіхи в області безпеки АСКОЕ, недостатня увага приділяється питанням захисту та безпеки бездротових сенсорних мереж [1]. У зв'язку з цим набуває значення ступінь уразливості мереж енергозабезпечення, порушення цілісності яких несе за собою колосальний економічний і соціальний збиток на державу в цілому.

Для бездротових мереж моніторингу основною метою безпеки є збереження конфіденційності, гарантія недоторканності і забезпечення доступності інформації. Для того щоб вжити заходів для захисту розгорнутої мережі необхідно провести оцінку основних видів загроз безпеки. Загрози конфіденційності на рівні передачі комерційної та технологічної інформації можуть принести серйозної шкоди. За ступенем важливості виділяються атаки за допомогою яких визначається несуча частота, розмір повідомлення, рівень сигналу і відомості про маршрутизації інформації.

Ці дані виходять за допомогою мережевого сніфферу, який здійснює прослуховування інформації про маршрутизації даних. Зловмисники можуть встановити голкові контакти з кожного боку чіпа інтелектуального лічильника, щоб перехоплювати і аналізувати електричні сигнали для розуміння програмної начинки пристрою. Аналогічним чином можуть бути перехоплені і радіосигнали.

Дослідниками [2] було встановлено, що в поширених інтелектуальних лічильниках можливо провести реверс-інжиніринг комунікаційних протоколів, а також атаки типу «маскарад» (spoofing). Це дозволяє втручатися в роботу лічильника, спотворювати показання і керувати ним. Атаки типу «маскарад» призводять до втрати цілісності даних і їх спотворення. В системах інтелектуального обліку не передбачена аутентифікація. Крім того, перевірка на вході також відсутня. При отриманні кількох пакетів з однаковим ID і різними показниками лічильника, зчитувач приймає пакет з найсильнішим сигналом. При використанні більш сучасної моделі зчитувача, який виробляє таку перевірку, існує можливість простого блокування пакетів з легітимного лічильника і перенаправлення зчитувача на прийом пакетів з підставного пристрою.

Одним з можливих рішень захисту інтелектуальних лічильників є Smartsynch Universal Communications Model – модель інтелектуального лічильника в збірці, що дозволяє замінювати застарілі контролери на нові, що підтримують аутентифікацію і шифрування, без необхідності видалення з мережі лічильника.

При вивченні схеми проходження трафіку сенсорної мережі можна простежити розташування базової станції або іншого стратегічно розташованого вузла. Більш того, протоколи маршрутизації многоскачкового зв'язку надають можливість зловмиснику простежити весь потік повідомлень і визначити джерело інформації. Будь-який аналіз мережевого трафіку або декодування пакетів може бути здійснений в реальному часі, або в режимі офлайн (при відсутності підключення) за допомогою наявної бази даних описів пакетів. Більшість бездротових атак підпадають під одну з наступних категорій [3]:

- Атаки на конфіденційність: дані атаки намагаються перехопити секретну інформацію, що надсилається засобами бездротової передачі.
- Атаки на недоторканність: дані атаки посилають фрейми (структурні одиниці інформації) помилкового контролю, управління або містять дані для виникнення збою на одержувача, або використовуються для полегшення проведення іншого типу атак.
- Атаки на доступність: ці атаки перешкоджають доставці бездротових повідомлень для легалізації користувачів за допомогою виводу з ладу мережевих ресурсів.

Формування неправдивих команд локальної автоматики, в загальному випадку, може привести до аварійної ситуації, так як віддалене управління в більшості випадків зводиться тільки до зміни налаштувань, що призводить до неоптимального режиму роботи обладнання.

Найбільш вірогідним є загрози трафіку, які полягають у введенні шкідливої зайвої інформації в мережу, поява «лавини» повідомлень. Даний вид погроз може привести до збільшення затримок при передачі даних або до втрат пакетів, що призведе до недостовірної оцінки стану об'єкта і, відповідно, призведе до можливості прийняття катастрофічних рішень.

Для випадку системи моніторингу та управління об'єктом, втрата якості управління E оцінюються формулою:

$$E = (1 - B) * N_A * z_e$$
$$B = N_S / N_A \quad (1.1)$$

де *ze* – середнє значення збитку при втраті одного абонента;

NS – кількість обслужених абонентів за час експлуатації;

NA – загальна кількість даних абонентів в системі за час експлуатації.

Система повинна забезпечити виконання умови:

$$B \geq B_{tr} \quad (1.2)$$

де *B, Btr* – відповідно поточний і необхідний баланс споживання в системі.

Втрата пакетів від кінцевих вузлів *D* досягається зловмисником двома основними способами:

- введення сенсора SD рівня кінцевих вузлів, який проводить DDOS-атаку;
- введення сенсора SM рівня маршрутизаторів, який порушує роботу механізму маршрутизації.

Введення в систему зловмисником вузла SD призводить до збільшення навантаження на маршрутизатор і не здатності виконувати задані функції. Поява вузла *SM* призводить до втрати даних кінцевих сенсорів, підключених до даного маршрутизатора. Одним з ефективних способів боротьби з даними видами атак є використання шифрування даних на різних рівнях і механізмів аутентифікації. При цьому необхідно враховувати обмеження, пов'язані з невеликими обчислювальними ресурсами вузлів і невеликим об'ємом пам'яті. Це не дозволяє використовувати асиметричні алгоритми шифрування. Симетричні алгоритми шифрування володіють

такими перевагами, як низькі вимоги до продуктивності вузлів і енергоспоживанню, мають низьку захищеність, пов’язану з тим, що, дізнавшись ключ, зловмисник може отримати доступ до всіх вузлів мережі.

Для боротьби зі складними і швидко зростаючими загрозами питання безпеки повинні бути ретельно розглянуті на кожному етапі розробки продукту - від проектування і тестування до установки і обслуговування. Для захисту важливих секторів інфраструктури необхідно забезпечити сучасні вимоги з безпеки для інсталяції захищених пристроїв і систем, готових протистояти найскладнішим атакам. Захист польових пристроїв «Інтернету речей» має пріоритетний характер, так як уразливі саме вони, а не встановлені на них додатки. Цим покладено новий етап в індустрії захисту інформації - захист мереж збору даних інтелектуальних датчиків і пристроїв обліку енергоресурсів, що володіють обмеженими обчислювальними ресурсами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Почта Ю.В. Управление энергоресурсами на базе беспроводных технологий передачи данных.- Materialy VIII mezinarodni vedecko-prakticka koference.-Dil 27 Technicke vedy, 20.01.2012-05.02.2012, Praha, s.78-81

2. 34 Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu, Rob Miller: Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems.- Proceeding CCS ‘12 Proceedings of the 2012 ACM conference on Computer and communications security. Pages 462-473 . ACM New York, NY, USA ©2012

35 Joe Biron and Jonathan Follett. - Foundational Elements of an IoT Solution.- Published by O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA95472. Copyright ˝ 2016 O’Reilly Media, Inc.