УДК 621.396

ШИФРУВАННЯ ДАНИХ В СЕНСОРНІЙ МЕРЕЖІ, НА ПРИКЛАДІ ZIGBEE

Зубик С.О., Лисенко О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail zubyk.sergey@gmail.com

Data encryption in the sensor ZigBee-network

The use of wireless data networks in applications such as data collection from energy meters, safety and industrial telemetry require the protection of transmitted information and prevent unauthorized connection of undesirable devices. The article deals with practical issues of data encryption in ZigBee-networks using the example of popular XBee radio modules.

У мережах ZigBee передбачено кілька механізмів криптографічного захисту даних (Security), всі або деякі з яких можуть бути задіяні розробником:

- шифрування AES 128-біт;
- 2 типу ключів шифрування;
- підтримка центру довіри (Trust Center);
- механізми перевірки цілісності повідомлення (Integrity) і перевірки його справжності (Authentication).

Специфікація ZigBee включає три режими безпеки (Security modes) - локальний (residential), стандартний і підвищений. Локальна безпека була вперше введена в стандарті ZigBee 2006. Вона вимагає, щоб ключ шифрування був встановлений на всіх пристроях, що підключаються до мережі. Стандартний режим безпеки додає деякі опціональні можливості, а також вводить шифрування на рівні додатку (APS layer link key). Підвищена безпека передбачає перевірку справжності і деякі інші удосконалення, які в даний час не підтримуються виробниками ZigBee-стеків в достатній мірі.

Модулі XBee ZB, в основному, підтримують стандартний режим безпеки. У той же час, кінцеві пристрої, що підтримують локальний режим безпеки, можуть підключатися і взаємодіяти з вузлами мережі, що працюють зі стандартним режимом безпеки. Далі розглядаються різні аспекти шифрування даних саме для режиму стандартної безпеки.

Безпека в ZigBee використовується як на мережевому рівні, так і на рівні додатку. Передана по ефіру інформація шифрується за допомогою алгоритму AES з довжиною ключа 128 біт. Як ключів шифрування застосовується мережевий ключ (Network Key) і опціональний зв'язковий ключ (Link Key). Ключі шифрування є деякою 128-бітною послідовністю (16 байт), яка вручну завантажується в модуль або формується самостійно. Витягти ключ з модуля неможливо. Тільки ті два ZigBee-вузла, які містять однакові ключі шифрування, можуть взаємодіяти між собою. Роутери та кінцеві пристрої, які працюють в мережі з включеною безпекою, повинні отримати правильні ключі шифрування.

Центр довіри в мережі ZigBee з безпекою авторизує підключаються до мережі вузли і виконує розсилку ключів шифрування. Зазвичай в якості центру довіри

виступає координатор.

Ключ мережі застосовується для шифрування даних користувача (Application Data) і додаткової інформації верхнього рівня (APS Layer). APS Layer - це надбудова над корисними даними, пов'язана з поняттям «профілів» в ZigBee (включає інформацію про профілі, кластери і кінцеві точки). Крім захисту власне корисного навантаження (Payload), безпеку на мережевому рівні забезпечується шифруванням даних, пов'язаних зі службовими мережевим операціями, такими як прокладка маршрутів і команди рівнів APS і ZDO. Мережева безпека не поширюється на MAC-рівень. Якщо в ZigBee-мережі включений режим безпеки, то всі пакети з даними передаються тільки в зашифрованому вигляді за допомогою 128-біт алгоритму AES (див. Рис. 1).

Рис. 1. Шифрування на мережевому рівні

Мережевий заголовок зашифрованого пакета включає 32-біт лічильник фреймів. Кожен вузол в мережі підтримує власний 32-біт лічильник фреймів, який збільшується на 1 при відправці будь-якого пакета. Додатково, кожен вузол відстежує лічильники фреймів всіх сусідніх вузлів. Якщо отримується пакет від сусіднього вузла має номер фрейма менший, ніж був до цього, такий пакет відкидається. Лічильники фреймів використовуються для протистояння та злому захисту шляхом заміщення оригіналу (Replay attacks).

В безпечної ZigBee-мережі пакет дешифрується і шифрується за будь-якої ретрансляції на всьому маршруті проходження. Проміжний вузол дешифрує пакет і перевіряє його цілісність. Якщо пакет призначений не цьому вузлу, то дані знову зашифровуються і аутентифіковані на основі лічильника фреймів і мережевої адреси (входять в мережевий заголовок) проміжного вузла. Додаткові операції в мережі з безпекою збільшують затримки при доставці повідомлень. Крім того, максимальний обсяг корисних даних в пакеті зменшується на 18 байт за рахунок додавання лічильника фреймів, адреси джерела, MIC-коду і деяких інших службових байтів.

Безпека на рівні додатку (APS layer security) дозволяє зашифрувати корисні дані за допомогою ключа шифрування, відомому тільки відправнику і одержувачу пакета. У той час як мережеве шифрування на базі мережевого ключа застосовується до всіх повідомлень всередині мережі, шифрування на рівні додатку є необов'язковим і може використовуватися тільки при надсиланні конкретного пакета. Шифрування на рівні програми не може застосовуватися до широкомовних розсилок. Шифрування корисних даних і формування коду цілісності повідомлення виробляється на основі 128-біт

алгоритму AES (див. Рис. 2).

Рис. 2. Шифрування на рівні додатку

Код цілісності повідомлення (APS Message Integrity Code, aMIC-код) в даному випадку відрізняється від nMIC-коду, одержуваного при шифруванні на рівні мережі (Network Message Integrity Code). Одержувач повідомлення не буде використовувати прийнятий пакет, якщо обчислюється їм хеш-функція над корисними даними дасть результат, відмінний від aMIC-коду в самому пакеті. При шифруванні на рівні програми використовуються два типи ключів - зв'язковий ключ для обміну даними з центром довіри і ключ шифрування даних програми. Проміжні вузли мережі не можуть отримати доступ до цих даних, тому що ключ шифрування даних додатка відомий тільки відправнику і одержувачу. Використання безпеки на рівні додатку зменшує максимальну величину корисних даних на 9 байт. На малюнку 3 наведена діаграма пакета для випадку одночасного використання безпеки на рівні мережі і на рівні додатку.

Рис. 3 . Шифрування на рівні мережі та додатку

Література

1. M. Di Francesco, G. Anastasi, M. Conti, S.K. Das, and V. Neri. “Reliability and Energy-Efficiency in IEEE 802.15.4/ZigBee Sensor Networks: An Adaptive and Cross-Layer Approach,” IEEE Journal on Selected Areas in Communications, 29(8), pp. 1508-24, Sept. 2011.
2. Mao G. Wireless sensor network localization techniques / G. Mao, B. Fidan, B. Anderson // Computer Networks, 51(10), pp. 2529 – 2553, 2007.
3. Chaczko Z. Methods of sensors localization in wireless sensor networks / Z. Chaczko, R. Klempous, J. Nikodem, M. Nikodem // In Engineering of Computer-Based Systems, 2007. ECBS’07. 14th Annual IEEE International Conference and Workshops, pp. 145–152. IEEE, 2007.