УДК 004.056

АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОТОКОЛУ ZIGBEE ДЛЯ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Фукс М.А.
Науковий керівник – к.т.н, доцент Куля Ю.Е.
Харківський національний університет радіоелектроніки
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
e-mail: maksymillian.fuks@nure.ua

The Internet of Things (IoT) is becoming extremely popular not only among big companies or businesses but also among people in their homes since more and more devices are designed to collect, process, and exchange vital data via the network. A wireless technology “Zigbee” was supposed to provide a low-power and cost-effective wireless IoT network. In terms of security, the technology also gives opportunities to create a highly secure network, yet it is optional since it depends on a manufacturer, which is responsible for finding a balance between security and the price of a system.

Zigbee Alliance – некомерційна організація, що займається стандартами IoT, у 2003 році створює новітню технологію на основі радіо стандарту IEEE 802.15.4 – ZigBee. Відкритий стандарт безпроводової мережі ZigBee концентрується на впроваджені сумісності Machine-to-Machine (M2M) продуктів різноманітних виробників. Більш того, впровадження зазначеного стандарту значно підвищує відмовостійкість системи, збільшує строк життя кінцевих пристроїв від однієї батареї, передбачає велику кількість підключень, а також низьку вартість. До типової структури ZigBee мережі можна віднести наступні компоненти [1]:

- координатор – грає роль центра довіри для контролю безпеки;
- роутер – відповідає за зв’язування координатора з кінцевими пристроями (забезпечення маршрутизації мережевого трафіку);
- кінцевий пристрій – звичайні пристрої, які можуть спілкуватися лише через батьківські вузли.

Довірчі відносини складають основу безпеки розглянутої мережі. Відповідно до специфікації, технологія ZigBee заснована на 128-бітному симетричному алгоритмі блочного шифрування AES, а тому обидві сторони мають знати загальний ключ для комунікації [2]. Необхідно розуміти, що стандарт IEEE 802.15.4 визначає перші два рівня – Physical Layer та Medium Access Control Layer, а ZigBee вже надбудовує додаткові рівні: Network та Application Layers. На останніх трьох рівнях забезпечується безпека передачі фреймів. Моделі безпеки, що відрізняються можливостями прийняття нового пристрою до мережі та методами захисту даних, доволі сильно впливають на роботу усієї мережі, наприклад, розподілена модель містить лише роутери та кінцеві пристрої, тому й вважається простішою, але й менш захищеною.

Кожен з роутерів може генерувати network keys, а для підключення до такої мережі кінцеві пристрої мають містити правильний pre-configured global link key, за допомогою якого, останні розшифровують повідомлення з network key від батьківських роутерів. Network key необхідний кожному з пристроїв для підтримання комунікації у мережі. Централізована система, у свою чергу, набагато безпечніша, але й складніша. Вона передбачає застосування ZigBee Trust Center (TC), що й грає роль координатора мережі. Він встановлює унікальний Global link key для використання ним та кожним з вузлів, Unique link key для кожного зі з'єднань TC-вузол, що згодом змінюється на згенерований TC link key, а також Application link key для комунікації між парою пристроїв. Насправді, ключі, які пов'язані з TC є сконфігуруваними завчасно, наприклад, у вигляді QR коду, а link keys між пристроями генеруються та шифруються з network key для передачі від TC. Він також визначає network key. Новий пристрій повинен мати pre-configured global link key для приєднання. Такий ключ може бути визначений через стандарт, як «ZigBeeAlliance09», для можливості приєднання сторонніх пристроїв, або створений виробником для обмеження такої можливості. При відсутності такого ключа координатор має можливість відправити network key у відкритому вигляді, що, звичайно, відкриє дірку у безпеці. Такий варіант поширення network key є стандартним, що є недопустимим до використання. З іншого боку, навіть знаючи link key, зловмисник може злегкістю отримати network key через захват пакетів у мережі за допомогою спеціального сніферу. Саме тому вибір та впровадження pre-configured global link key має колосальне значення, що не регулюється специфікацією ZigBee та повністю покладається на уважність виробника. Безперечно, задання власного pre-configured global link key значно підвищить безпеку усієї мережі, але така дія ускладнить впровадження нового пристрою до мережі для звичайного користувача. Отож, у залежності від цілей виробника, він може гнучко налаштовувати рівень безпеки розгортаємої мережі ZigBee. На жаль, більшість з них вкрай недооцінюють важливість запровадження достатніх рівнів безпеки, побоюючись значний ріст ціни на продукцію. Згідно зі звітом компанії Cisco вже у 2023 році кількість M2M з'єднань досягне 14.7 мільярдів, що на 15% більше у порівнянні з 2018 роком [3]. Саме тому з ростом популярності IoT пристроїв питання безпеки конфіденційної інформації повинне розглядатися більш гостро.

Список використаної літератури:

1. Security Analysis of Zigbee / Xueqi Fan., 2017. – 18 с. ZigBee Specification, 2004. – (ZigBee Alliance). Cisco Annual Internet Report (2018–2023). // White paper Cisco public. – 2020. – С. 35.