УДК 004.056
DOI: 10.31673/2412-9070.2021.043740

Б. І. СВЕРДЛЮК, магістр;
Ю. К. КАГРАМАНОВА, магістр;
В. О. ХОМЕНЧУК, аспірант;
К. П. СТОРЧАК, доктор техн. наук, професор;
В. Р. МИКОЛАЙЧУК, ст. викладач,
Державний університет телекомунікацій, Київ

БЕЗПЕКА В МЕРЕЖАХ ZigBee

З кожним роком цікавість до IoT дедалі зростає, адже на ринку з'являються різноманітні вирішення, що різняться ціною, екосистемою та протоколами, що використовуються.

Одним із найпопулярніших протоколів Розумного будинку сьогодні є ZigBee. Незважаючи на те, що ZigBee розроблено з урахуванням безпеки, було досягнуто компромісів щодо забезпечення низької вартості, низької енергоємності і високої сумісності пристроїв. До прикладу, використання однакових ключів шифрування на різних рівнях OSI одного пристрою. Подібні компроміси неминуче призводять до ризиків безпеки. Метою статті є дослідження основних моделей безпеки ZigBee та недоліків безпеки мережі.

Ключові слова: безпека ZigBee; недоліки безпеки мережі; висока сумісність пристроїв; IoT; моделі безпеки ZigBee.

ВСТУП

ZigBee — це безпроводова технологія **PAN (***Personal Area Network***)**, розроблена для підтримання автоматизації, M2M зв'язку, віддаленого керування та моніторингу пристроїв IoT. Переваги ZigBee перед іншими стандартами полягають у низькому енергоспоживанні/тривалому терміну служби батареї, підтриманні значної кількості вузлів в одній мережі (до 65 000), спрощеному розгортанні, низьких витратах та використанні в усьому світі.

Мета дослідження — проаналізувати можливі теоретичні атаки на мережу та визначити й описати ризики безпеки ZigBee мереж.

ОСНОВНА ЧАСТИНА

ZigBee — технологія, яку засновано на радіо-стандарті IEEE 802.15.4 і призначено для стандартизації малопотужних пристроїв M2M різних виробників. З особливостей мережі можна виокремити високу стійкість до відмов, тривалий термін служби кінцевих пристроїв від однієї батареї, підтримання великої кількості підімкнень і спільну роботу пристроїв різних виробників. ZigBee передбачає передавання інформації в радіусі від 5 до 75 (на відкритій місцевості до 200) метрів із максимальною швидкістю 250 кбіт/с. Стандарт ZigBee працює поверх специфікації фізичного радіо IEEE 802.15.4. Повний стек протоколів ZigBee зображено на рис. 1.

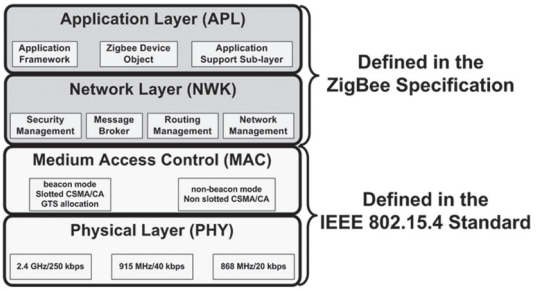

Рис. 1

Існують два типи моделей безпеки в мережах ZigBee. Вони відрізняються реалізацією механізмів, приєднанням до мережі та захистом повідомлень — централізована мережа безпеки та розподілена мережа безпеки.

Централізована модель безпеки є складною, але більш безпечною і має у своєму складі Центр довіри (координатор мережі). Тільки координатори ZigBee із Центром довіри можуть створювати централізовані мережі. Вузли приєднуються до мережі, отримують ключ мережі та встановлюють унікальний ключ зв'язку з Центром довіри.

Центр довіри відповідає за такі функції (рис. 2):

- налаштування та автентифікацію маршрутизаторів і кінцевих пристроїв, які приєднуються до мережі;
- створення мережного ключа, який буде використовуватися для зашифрованого зв'язку в мережі;
- періодичне або за потреби перемикання на новий мережний ключ як спосіб захисту;
- у разі отримання зловмисником мережного ключа, останній матиме обмежений термін служби;
- установлення унікального ключа посилання для кожного пристрою під час приєднання їх до мережі;
- підтримання загальної безпеки мережі.

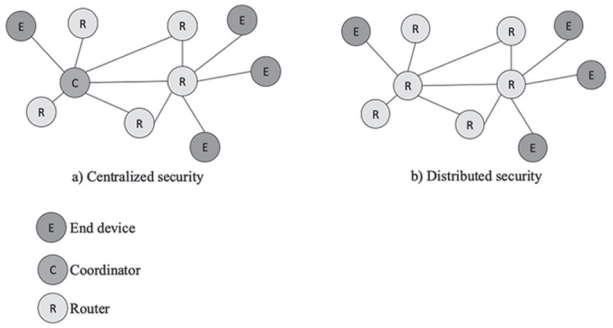

Рис. 2

Розподілена модель безпеки проста, але менш безпечна. Ця модель підтримує тільки маршрутизатори та кінцеві пристрої. Маршрутизатори знаходять свою роль у форматуванні розподіленої мережі і відповідають за реєстрацію інших маршрутизаторів та кінцевих пристроїв. Маршрутизатори публікують мережні ключі (які застосовуються для шифрування повідомлень) на щойно приєднаних маршрутизаторах і кінцевих пристроях. Усі вузли мережі використовують один і той самий мережний ключ для шифрування повідомлень. Окрім того, перш ніж увійти в мережу, всі вузли попередньо налаштовано за допомогою ключа посилання (використовується для шифрування мережного ключа), оскільки немає координатора та Центру довіри.

Ключі безпеки Zigbee

Існує три типи 128-бітових симетричних ключів, визначених стандартом Zigbee: мережний, ключ зв'язку і розподілений ключ.

Мережний ключ використовується в широкомовному зв'язку. Кожному вузлу потрібен мережний ключ для безпечного зв'язку з іншими пристроями в мережі. Центр довіри генерує мережний ключ і поширює його на всі пристрої в мережі.

Пристрій у мережі отримує мережний ключ за допомогою транспортування ключа (використовується для захисту транспортованих мережних ключів) або попереднім встановленням.

Є два різних типи мережних ключів: *стандартні* (надсилаються без шифрування) і *високобезпечні* (зашифрований мережний ключ).

Ключ зв'язку використовується в одноадресному зв'язку та застосовується APS стека ZigBee. Пристрій отримує ключі зв'язку або за допомогою транспортного ключа (ключ завантаження ключа використовується для захисту транспортованих ключів зв'язку), або попереднім установленням (наприклад, під час заводського монтажу). Установлення ключа — це конкретна процедура, яка ініціюється на основі профілю безпеки пристрою.

Ключ зв'язку забезпечує рівень безпеки на рівні APL на додаток до безпеки на рівні NWK, що задовольняється мережним ключем. Повідомлення між вузлами шифруються як мережним ключем, так і посиланням.

ZigBee визначає два типи ключів посилань — *глобальні* та *унікальні*. Ключі глобального зв'язку встановлюються між Центром довіри та пристроєм. Зазвичай ключі посилань, пов'язані з Центром довіри, попередньо налаштовані за допомогою позасмугового методу, наприклад QR-код на упаковці.

Унікальні ключі або ключі посилання на програму встановлюються між двома пристроями в мережі без Центру довіри. Обидва типи ключів можна використовувати в мережі, але пристрій має застосовувати лише один тип. Тип ключа посилання визначає, як пристрій обробляє різні повідомлення Центру довіри (команди APS), включно із шифруванням APS.

Крім того, кожен вузол також може мати такі попередньо налаштовані ключі посилання, які будуть використовуватися для отримання ключа посилання Центру довіри.

Ключ посилання глобального Центру довіри за замовчуванням, визначений Connectivity Standard Alliance, має значення за замовчуванням. Він використовується або підтримується пристроєм, якщо під час приєднання програмою не вказано інший ключ посилання.

Розподілений ключ глобальної безпеки зв'язку — це спеціальний ключ виробника, який використовується для взаємодії між пристроями одного виробника.

Усі пристрої ZigBee можуть містити унікальний код установлення (попередньо налаштований ключ посилання), випадкове 128-бітове число, захищене 16-бітовою перевіркою циклічної надмірності (CRC).

Центр довіри може вимагати, щоб кожен новий пристрій використовував унікальний код установлення для приєднання до централізованої мережі безпеки, а код установлення має відповідати коду, введеному раніше в Центрі довіри.

Після перевірки коду інсталяції пристрій, що під'єднується, і Центр довіри отримують унікальний 128-бітовий ключ посилання на Центр довіри з коду встановлення за допомогою хеш-функції Matyas-Meyer-Oseas (MMO).

Попередньо налаштований ключ підімкнення Touchlink використовується для пристроїв, які під'єднуються до мережі за допомогою процедури введення в експлуатацію Touchlink.

Головний ключ є основою для довгострокової безпеки між двома пристроями. Його функція полягає в тому, щоб зберегти конфіденційність обміну ключами посилання між двома вузлами в протоколі SKKE. Пристрій отримує головний ключ за допомогою транспортування ключа, попереднього встановлення або даних, уведених користувачем, таких як PIN-код або пароль.

Керування ключами

ZigBee підтримує різні механізми керування ключами. Розглянемо деякі з них.

Попереднє встановлення — виробник установлює ключ у пристрій. Якщо в пристрої попередньо встановлено кілька ключів, клієнт може вибрати один із установлених ключів за допомогою ряду перемичок у пристрої.

Метод установлення ключа для генерації ключів посилання на ***основі головного ключа***. Різні служби безпеки мережі ZigBee використовують

ключ, отриманий з односторонньої функції (з ключем посилання як вхід), щоб уникнути витоку безпеки через небажану взаємодію між службами. Це встановлення ключа базується на протоколі SKKE.

Пристрої, які беруть участь у зв'язку, повинні мати головний ключ, який може бути отриманий попереднім установленням, транспортуванням ключа або введенням користувачем.

Транспортування ключа. Мережний пристрій робить запит до Центру довіри щодо ключа. Цей метод дійсний для запиту будь-якого з трьох типів ключа в комерційному режимі, тоді як у житловому режимі Центр довіри містить лише мережний ключ. Ключ завантаження ключа використовується Центром довіри для захисту транспортування головного ключа.

Крім того, в централізованій моделі ключі можна поширювати за допомогою протоколу встановлення ключа на основі сертифіката (CBKE). CBKE надає механізм узгодження симетричних ключів із Центром довіри на основі сертифіката, що зберігається в пристроях під час виготовлення, підписаного центром сертифікації (CA).

Проблеми безпеки ZigBee мереж

ZigBee має деякі вразливості безпеки, що робить його схожим на інші безпроводові технології. Реалізація мереж ZigBee має виконуватися з урахуванням можливих загроз безпеці. Атаки безпеки та несанкціоноване використання цілком можливі, оскільки технологія ZigBee застосовна для дистанційного керування та моніторингу чутливих ресурсів, інфраструктури чи безпеки будинку.

Безпека мереж ZigBee залежить від надійності зберігання ключів, а також наявності в пристроях попередньо встановлених симетричних ключів. Попереднє встановлення потрібне для того, щоб не було змоги передати ключ у незашифрованому вигляді.

Проте навіть і в цьому разі є слабка сторона. Коли новий і не налаштований попередньо пристрій входить у мережу, він надсилає один незахищений ключ для забезпечення зашифрованого зв'язку.

Отже, розкриття ключів шифрування ставить під загрозу безпеку всієї мережі. Незважаючи на це, терміни для такого компромісу безпеки, здавалося б, вузькі: хакер може застосовувати різні методи, щоб скористатися цією вразливістю.

Іншим способом проникнення в мережі ZigBee є фізичний доступ до деяких типів пристроїв Розумного дому, зокрема давачів температури та вимикачів світла. Через їхню низьку вартість та обмежені можливості передбачається, що їх апаратне забезпечення не є захищеним від несанкціонованого доступу, чого, у свою чергу, може бути достатньо, щоб зловмисник отримав конфеденційну інформацію мережі.

Типи теоретичних атак проти ZigBee

ZigBee і протокол 802.15.4 було розроблено з урахуванням безпеки, але час від часу розробники не забезпечують безпеку. Можливі атаки загалом можна поділити на три категорії: фізичні, ключові та повторне відтворення/ін'єкція.

Фізичні атаки. Пряма фізична взаємодія може виявитися шкідливою для цілісності цільової мережі ZigBee. Насправді, багато радіоприймачів, що перебувають у мережі, використовують жорстко закодований ключ шифрування, який завантажується в оперативну пам'ять після підімкнення пристрою. Будучи поширеним через завантажувач на всіх пристроях у мережі ZigBee, імовірність зміни ключів дуже низька.

Озброївшись цими знаннями, хакери можуть вдатися до налаштування послідовних інтерфейсів на пристрої ZigBee, щоб перехопити ключі шифрування, переміщені з флеш-пам'яті в оперативну пам'ять під час увімкнення живлення. Цей експлойт можна виконати за допомогою різноманітних недорогих інструментів із відкритим кодом, наприклад GoodFet і Bus Pirate

Після фізичного підімкнення до пристрою ZigBee через послідовний інтерфейс, такий як Bus Pirate, зловмисник може розкрити безпеку всієї мережі ZigBee та потенційно перехопити та змінити дані.

Атаки на ключ. Віддалені атаки, спрямовані на вилучення ключів шифрування, можливі завдяки методології, відомій як доставляння ключів повітрям (OTA) і загальний ключ, іманентний ZigBee. OTA зазвичай застосовується до більш складних мереж ZigBee для забезпечення кращої безпеки та оновлення.

Його захист безпеки можна обійти за допомогою пристрою, який імітує вузол ZigBee і вибирає передачі, якими обмінюються внутрішні пристрої; ці пакети можна проаналізувати або розшифрувати пізніше. Такий напад буде майже неможливо виявити.

KillerBee — це набір інструментів, що поєднує апаратне та програмне забезпечення, яке ефективно перехоплює та аналізує пакети 802.15.4. Віддалені атаки також відрізняються високою прихованістю. Зловмисник може навіть розширити діапазон покриття, створюючи потужні передавачі або спеціальні антени Yagi.

Повторні та ін'єкційні атаки. Це атака на основі ключа в поєднанні з відтворенням пакетів і/або ін'єкцією, метою якої є змусити пристрої ZigBee виконувати несанкціоновані дії.

Блоки ZigBee особливо вразливі до цих атак, оскільки їх оснащено полегшеною конструкцією протоколу зі слабким захистом від повтору. Отже, захоплені пакети з вузлів ZigBee надсилаються назад у такий спосіб, щоб це мало вигляд, ніби вони надходять від вихідного вузла. Мінімальної пере-

вірки сеансу одиницями ZigBee буде недостатньо, аби розкрити обман, і мережа буде розглядати трафік так, начебто він надходить від дійсного вузла.

ВИСНОВКИ

Передбачається, що до 2023 року на один будинок статистично налічуватиметься понад 500 розумних пристроїв. Існують серйозні проблеми з конфіденційністю, що виникають із домашньої автоматизації, оскільки вона генерує величезні обсяги даних, які можна пов'язати з людиною. Виробникам потрібно якомога швидше вирішити питання безпеки та конфіденційності, щоб пом'якшити загрози.

ZigBee є надійним стандартом, якщо його правильно застосовувати. Однак ця стаття показала, що з тих чи інших причин реальність часом інша. З цього приводу Тобіас Зіллнер з Cognosec доходить висновку:

«Недоліки та обмеження [...], виявлені в ZigBee, створені виробниками. Компанії хочуть створювати новітні продукти, а це сьогодні означає, що вони, імовірно, підімкнені до Інтернету. Прості пристрої, зокрема вимикачі світла, мають бути сумісними з цілою низкою інших пристроїв, і, як не дивно, вимогам безпеки приділяється мало уваги — швидше за все, для зниження витрат. На жаль, ризик безпеки в ZigBee можна вважати дуже високим».

Список використаної літератури

1. ***Бауерс Б.*** *Wireless Security ZigBee: інструментарій для тестувальника проникнення нового віку. 2012. [Електронний ресурс]. URL:*

http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4

2. ***Кондліфф Дж.*** *Лампочки Philips Hue легко зламати. 2013. [Електронний ресурс]. URL:*

http://gizmodo.com/how-philips-hue-light-bulbs-are-highly-hackable-1133092324

3. ***Дханджані Н.*** *Злом лампочок. 2013. [Електронний ресурс]. URL:*

http://www.dhanjani.com/blog/2013/08/hacking-lightbulbs.html

4. ***Хейс Дж.*** *Вади бездротової безпеки Zigbee загрожують пристроям IoT. 2015. [Електронний ресурс]. URL:*

http://eandt.theiet.org/news/2015/aug/zigbee-cognosec.cfm

5. ***Кумар М.*** *Як дрони можуть знаходити та зламати пристрої Інтернету речей з неба. 2015. [Електронний ресурс]. URL:*

http://thehackernews.com/2015/08/hacking-internet-of-things-drone.html

6. ***Лейден Дж.*** *У центрах Internet of Stuff виявлено загрозу кіберполтергейсту. 2015. [Електрон-ний ресурс]. URL:*

http://www.theregister.co.uk/2015/07/23/home_hub_insecurity_iot_stalking?page=2

7. ***The image*** *models of combined correlation-extreme navigation system of flying robots / A. Tantsiura, A. Bondarchuk, O. Ilin [et al.] // International Journal of Advanced Trends in Computer Science and Engineering, 2019. № 8(4). P. 1012–1019.*

Б. И. Свердлюк, Ю. К. Каграманова, В. О. Хоменчук, К. П. Сторчак, В. Р. Миколайчук

БЕЗОПАСНОСТЬ В СЕТЯХ ZIGBEE

С каждым годом интерес к IoT все более возрастает, ведь на рынке появляются различные решения, отличающиеся ценой, экосистемой и используемыми протоколами.

Одним из самых популярных протоколов Умного дома в настоящее время является ZigBee. Несмотря на то, что ZigBee разработан с учетом безопасности, были приняты компромиссы для обеспечения низкой стоимости, низкой энергоемкости и высокой совместимости устройств. К примеру, использование одинаковых ключей шифрования на разных уровнях OSI одного устройства. Подобные компромиссы неизбежно приводят к риску безопасности. Целью статьи является исследование основных моделей ZigBee безопасности и недостатков безопасности сети.

Ключевые слова: безопасность ZigBee; недостатки сети безопасности; высокая совместимость устройств; IoT; модели безопасности ZigBee.

B. I. Sverdlyuk, Y. K. Kagramanova, V. O. Khomenchuk, K. P. Storchak, V. R. Mykolaychuk

SECURITY IN ZIGBEE NETWORKS

When people start using home automation, they always feel the control of the home first: they believe that the future is now, and their application will be their console for life and do not pay attention to what they are losing. And suddenly the switch no longer works? After coming home at night, you have to pull out the phone, open the application, allow it to connect, and finally turn on the light. You can solve this problem with a presence sensor. Luminaires must work both with a switch (or button) at the entrance to the room and through a presence detector.

Home automation should be compatible with the current workflow, not replace it. The only interface that can be more convenient and accessible to visitors of all ages is the voice interface. Take, for example, Apple: the only way to manage your HomeKit devices is Siri. Amazon has taken another step forward with Amazon Echo by providing a connected speaker/microphone that always listens.

Voice interfaces are also not perfect. Command processing speed is low because you have to wait for an answer. There are also issues with command visibility, accent recognition, and cloud dependency for processing your voice.

Good home automation is never annoying, it works unnoticed. Every year the interest in IoT grows, as various solutions appear on the market, differing in price, ecosystem and protocols used.

One of the most popular smart home protocols today is ZigBee. Although ZigBee has been designed with security in mind, trade-offs have been made to ensure low cost, low power consumption and high device compatibility. For example, using the same encryption keys at different OSI levels of the same device. Such compromises inevitably lead to security risks. The aim of the article is to study the main security models of ZigBee and the shortcomings of network security.

Keywords: ZigBee security; network security flaws; high device compatibility; IoT; ZigBee security models.