АНАЛІЗ МЕХАНІЗМІВ БЕЗПЕКИ ZIGBEE В СИСТЕМАХ РОЗУМНОГО БУДИНКУ

Касьяненко С.Ф., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Система «розумного будинку» базується на мережі взаємопов'язаних пристроїв, які обмінюються даними для забезпечення автоматизованого та безперебійного керування. У даних IoT системах широко застосовується протокол ZigBee - бездротовий протокол зв'язку, розроблений для мереж з низьким енергоспоживанням і невеликою швидкістю передачі даних.

Попри наявність механізмів захисту, ZigBee має низку слабких місць:

- перехоплення ключа мережі (особливо під час приєднання пристрою);
- Replay-атаки при неправильній реалізації лічильників;
- атаки типу "Man-in-the-Middle";
- використання стандартних (default) ключів;
- фізичний доступ до пристроїв (витяг ключів із пам'яті).

Однією з ключових загроз у таких системах є атака типу «людина посередині» (Man-in-the-Middle), під час якої зловмисник може перехоплювати передані дані, отримувати несанкціонований доступ до пристроїв або навіть встановлювати контроль над центральним вузлом керування. Для ефективного захисту від подібних атак необхідно впроваджувати комплексні заходи безпеки, що включають надійний контроль доступу, використання криптографічного шифрування даних та механізми перевірки їх цілісності. Такі підходи дозволяють мінімізувати ризики несанкціонованого втручання та забезпечити безпечне функціонування системи [1].

Метою доповіді є аналіз механізмів захисту від MitM-атак у системах «розумного будинку» на прикладі технології ZigBee.

Технологія ZigBee забезпечує надійну передачу даних у мережі завдяки механізмам маршрутизації. Якщо пряме з'єднання з пристроєм відсутнє, дані передаються альтернативними шляхами через інші вузли мережі, доки не досягнуть кінцевого отримувача. Це підвищує стійкість системи до збоїв і забезпечує безперервність обміну інформацією. Архітектура ZigBee має багаторівневу будову і включає чотири основні рівні прикладний, мережевий, рівень керування доступом до середовища MAC та фізичний рівень. Кожен із цих рівнів виконує окремі функції, що забезпечують організацію передавання даних, керування мережею та фізичну взаємодію пристроїв. Такий підхід дозволяє досягти ефективної роботи мережі, її гнучкості та надійності [2].

Основними рівнями, на яких реалізуються механізми безпеки в ZigBee, є рівень керування доступом до середовища (MAC) та мережевий рівень. У межах цієї технології передбачено три базові механізми захисту контроль доступу, який здійснюється через авторизацію пристроїв, шифрування даних, що забезпечує їх доступність лише для уповноважених користувачів, а також

контроль цілісності, який реалізується за допомогою використання мережевого ключа.

Водночас технологія має певні обмеження [4]. Зокрема, призначений мережевий ключ не підлягає зміні, що може створювати потенційні ризики для безпеки системи. ZigBee є вразливим до MitM-атак через: бездротову природу передачі даних; обмежені ресурси пристроїв (спрощені механізми безпеки); складність централізованого управління в mesh-мережах.

Механізми захисту ZigBee забезпечують базовий рівень протидії Man-in-the-Middle attack, однак їх ефективність значною мірою залежить від правильної реалізації та конфігурації засобів захисту. Найбільш критичним аспектом є безпечне управління ключами та процес приєднання пристроїв до мережі.

У зв'язку з цим використання ZigBee у системах «розумного будинку» потребує додаткового посилення захисту. Доцільним є впровадження механізмів регулярної ротації ключів, використання багатофакторної автентифікації та застосування захищених протоколів передавання даних, що дозволяє підвищити загальний рівень безпеки мережі.

Отже, системи «розумного будинку» є вразливими до атак типу «людина посередині», що може призвести до перехоплення даних і несанкціонованого контролю над пристроями.

Використання технології ZigBee забезпечує надійну передачу інформації та базові механізми захисту, зокрема контроль доступу, шифрування та перевірку цілісності даних [5].

Водночас наявні обмеження, такі як неможливість зміни мережевого ключа, знижують загальний рівень безпеки. Тому для ефективного захисту системи необхідне впровадження додаткових заходів, зокрема ротації ключів, багатофакторної автентифікації та використання захищених протоколів обміну даними. Це дозволяє підвищити стійкість мережі до атак і забезпечити її надійне та безпечне функціонування.

Список літератури

1. Бабич, М.Г., Городецький, С.Л. (2025). Архітектура системи розумного будинку для людей з інвалідністю // Збірник наукових праць за матеріалами XI Всеукраїнської наук.-практ. конф. «Електронні та мехатронні системи: теорія, інновації, практика», 18 грудня, 2025 р. / Національний університет «Полтавська політехніка імені Юрія Кондратюка». – Полтава, 10.

2. Zillner, T., & Strobl, S. (2015). ZigBee exploited: The good, the bad and the ugly. Black Hat–2015. Available online: https://www. blackhat. com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly. pdf (accessed on 21 March 2018).

3. Д'якова, Н.Є., Сєвєрінов, О.В. (2021). Аналіз загроз безпеки у системах розумного будинку (ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ).

4. Zohourian, A., Dadkhah, S., Neto, E. C. P., Mahdikhani, H., Danso, P. K., Molyneaux, H., & Ghorbani, A. A. (2023). IoT Zigbee device security: A comprehensive review. Internet of Things, 22, 100791.