УДК 004.4

ПІДВИЩЕННЯ БЕЗПЕКИ СПОЛУЧЕННЯ IOT ПРИСТРОЇВ ШЛЯХОМ АНАЛІЗУ БЕЗПРОВІДНИХ СИГНАЛІВ

Педан С.І., Мельник М.В., Алєксєєв М.О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: stas.pedan@gmail.com, 8102002melpnik2@gmail.com, alexeyev@its.kpi.ua

IMPROVING SECURITY OF IOT DEVICES PAIRING BY WIRELESS SIGNALS ANALYSIS

The work is devoted to the topical issue of increasing the security of connecting simple IoT devices and protecting this process from man-in-the-middle attacks. Simple devices are the basis of the rapid development of the IoT sphere. A rapid increase in the number of simple devices is accompanied by an increase in the number of attacks in the field of security of their connection and communication. Simple devices do not have the technical resources to implement complex cryptographic protocols, which reduces their level of security, for example, the inability to protect against man-in-the-middle attacks. The paper proposes a method of increasing the security of connection of IoT devices by determining the proximity of their location based on the results of the analysis of the characteristics of the wireless signal. Calculations are presented that prove that the proposed method ensures the security of connecting IoT devices at a close distance and protection against man-in-the-middle attacks.

Інтернет речей (Internet of Things, IoT) – це нова парадигма, в якій велика кількість пристроїв та датчиків співпрацює шляхом комунікації через Інтернет, надаючи інноваційні сервіси для різних викликів і проблем сучасного життя [1]. Застосування технологій IoT забезпечує соціальний, технологічний та фінансовий розвиток суспільства, забезпечуючи розумне управління рухом транспортних засобів, безпекою і спостереженням, автоматизацією сільського господарства, охороною здоров’я та медициною, розумними містами та будинками, енергоспоживанням [2].

Останній звіт «Стан IoT – Весна 2023» від IoT Analytics [3] показує, що кількість глобальних підключень IoT зросла на 18% у 2022 році до 14,3 мільярдів активних пристроїв IoT. Хоча прогнозувалося, що зростання у 2023 році буде дещо нижчим (на 16% або до 16 мільярдів активних пристроїв), ніж у 2022 році, очікується, що кількість підключень пристроїв IoT продовжуватиме зростати протягом багатьох наступних років. Серед технологій комунікації IoT пристроїв домінують Wi-Fi, Bluetooth та стільниковий зв'язок. Bluetooth підключення займають 27% від загальної кількості. Bluetooth Low Energy (BLE) забезпечує надійне підключення при обмеженому споживанні енергії, що є кращим варіантом IoT пристроїв з живленням від батареї. Прикладами таких пристроїв можуть бути датчики розумного дому або трекери персональних речей.

Хоча складні системи відіграють важливу роль в IoT, саме розробка, інтеграція та використання простих пристроїв насправді сприяє широкому впровадженню та впливу цієї технології [4]. Прості пристрої, такі як датчики і приводи, є основою Інтернету речей. Вони забезпечують безперебійне з’єднання та зв’язок між різними об’єктами в повсякденному житті: розумні системи безпеки

будинку використовують прості пристрої, такі як датчики руху та датчики дверей, щоб виявляти будь-яку надзвичайну активність та надсилати сповіщення власникам будинку. В основі пристроїв IoT, включаючи перелічені прості пристрої, лежить їх здатність спілкуватися та ділитися даними.

В той же час, прості пристрої IoT ставлять перед розробниками серйозні задачі по забезпеченню їх безпеки. Більшість простих пристроїв IoT за своєю суттю незахищені через їхні малі або обмежені розміри, які здатні вмістити лише малопотужні вбудовані мікроконтролери, прості датчики, виконавчі механізми, блоки живлення та інші крихітні електронні компоненти. Це обмеження розміру в поєднанні з вимогами до низького енергоспоживання, простими або базовими операційними системами та обмеженою обчислювальною потужністю часто перешкоджає застосуванню передових або навіть сучасних криптографічних методів, не кажучи вже про цілі рішення безпеки [5]. Активне розповсюдження простих IoT пристроїв у повсякденному житті у поєднанні з низькою захищеністю робить їх прибутковою мішенню для кіберзлочинців.

Для сполучення з простими IoT пристроями, які не мають інтерфейсу користувача (дисплею, мікрофону, динаміку, засобів введення інформації, таких як клавіатура) і, як наслідок, можливості ввести або підтвердити ключ доступу, використовують метод JustWorks[6]. Для BLE пристроїв він забезпечує найбільш прийнятий режим сполучення, оскільки майже всі BLE IoT пристрої не мають жодних можливостей введення та виведення інформації, наприклад лампочки, розумні замки, холодильники, брелоки, монітори серцевого ритму. Основною особливістю цього режиму сполучення є те, що для завершення процедури з'єднання не потрібна автентифікація[7]. Будь-хто може підключитися до будь-якого пристрою BLE, який використовує Just Works. В результаті, створене з'єднання захищене від пасивного прослуховування завдяки шифруванню, але безсиле перед атакою посередника (Man in the middle, MITM). Сценарій заволодіння IoT пристроєм зловмисником в результаті атаки посередника представлений на рис. 1.

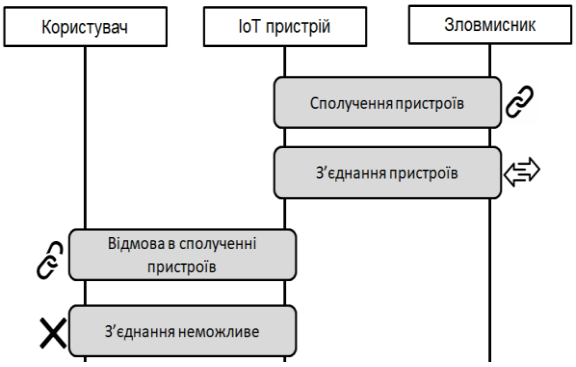

Рис. 1. Актуальний сценарій заволодіння IoT пристроєм зловмисником в результаті атаки посередника

Задачею роботи є підвищення безпеки методу сполучення простих BLE IoT пристроїв для захисту від атак посередника. Дослідники з Microsoft Research запропонували метод Move2Auth[8], що забезпечує автентифікацію простих IoT пристроїв на основі визначення їх близькості. Метод вимагає від користувача тримати смартфон і виконувати один із двох жестів рукою (випадково вибраних смартфоном) перед пристроєм IoT, у той час як пристрій IoT продовжує надсилати пакети. Два жести, тобто переміщення смартфона до пристрою IoT і від нього, а також обертання смартфона, призводять до значної (близько 15 дБ) зміни потужності отриманого сигналу (RSS) через швидку зміну затухання та поляризації антени відповідно. По рівню кореляції RSS-варіацій з показами датчиків руху смартфона (акселерометер та

гіроскоп) можливо виконати надійне виявлення близькості пристроїв. Це дозволяє ефективно розрізняти близькі та далекі пристрої і таким чином захистити процедуру сполучення двох близьких пристроїв від далеко розташованого зловмисника, який може довільно підсилити потужність передачі свого сигналу.

В даній роботі пропонується замість використання специфічних рухів смартфоном піднести його на максимально близьку відстань до IoT пристрою і провести взаємну автентифікацію по потужності безпровідного сигналу.

Потужність сигналу, яку вимірює перший пристрій, зменшується зі збільшенням відстані до другого пристрою. Таку залежність можна описати наступною формулою:

$$\mathrm{RSSI_{d1}} = \mathrm{RSSI_{d0}} - 20\log(\frac{\mathrm{d1}}{\mathrm{d0}}) \quad (1)$$

де d0 – початкова відстань між пристроями, d1 – кінцева (збільшена) відстань між пристроями, $\mathrm{RSSI_{d0}}$ – потужність сигналу на відстані d0, $\mathrm{RSSI_{d1}}$ – потужність сигналу на відстані d1.

Відповідно до отриманих експериментальних даних, RSSI для відстані до 10 сантиметрів має середнє значення -10dBm. Для того, щоб перевести dBm у вати, будемо використовувати наступну формулу:

$$\mathrm{P(W)} = \frac{10^{\frac{\mathrm{P(dBm)}}{10}}}{1000}, \quad (2)$$

де P(W) – потужність сигналу у ватах, P(dBm) – потужність сигналу у dBm. Таким чином, відповідно до формули [1], якщо зловмисник знаходиться на відстані 10 метрів від IoT пристроя, рівень його сигналу буде на $20\log\left(\frac{\mathrm{d1}}{\mathrm{d0}}\right) = 20\log\left(\frac{10}{0.1}\right) = 20 \cdot 2 = 40\mathrm{dBm}$ меньше, ніж аутентичного пристрою на відстані 10 сантиметрів при однаковій вихідній потужності антени BLE. Для того, щоб створити на IoT пристрої ілюзію знаходження пристрою на близькій відстані, зломиснику необхідно збільшити потужність сигналу на 40 dBm, або 10 Ват за формулою [2]. Враховуючи правила FCC та ETSI, максимальна вихідна потужність антени, яка дозволена протоколом BLE, становить 20 dBm.

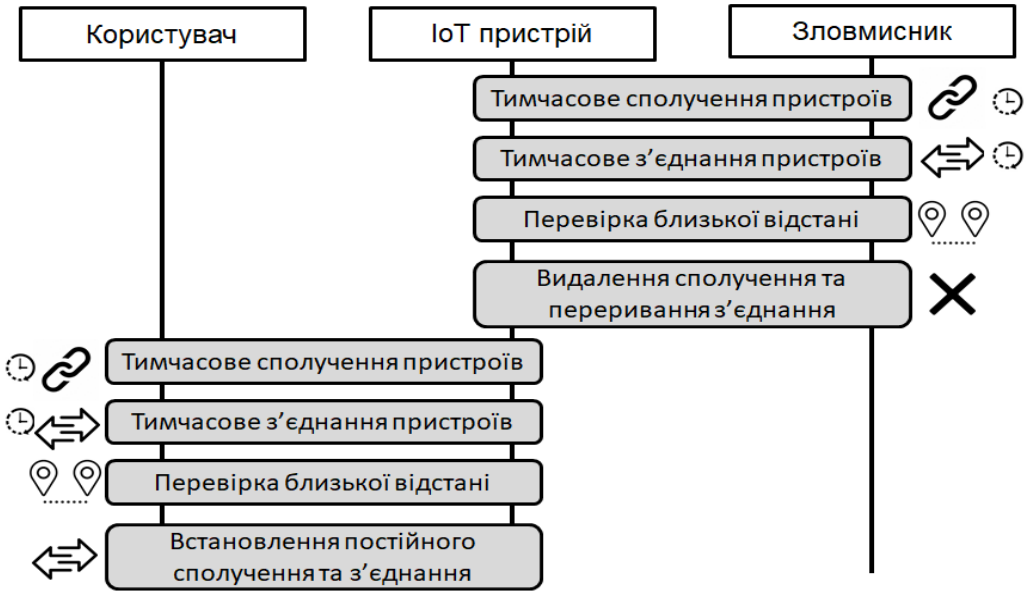

Рис. 2. Сценарій захисту від заволодіння IoT пристроєм зловмисником з використанням запропонованого методу.

Таким чином, запропонований метод забезпечує захист процесу сполучення з IoT пристроєм на близькій відстані.

Висновки.

1. Активний розвиток технологій IoT та збільшення кількості пристроїв підвищує вимоги до безпеки сполучення та комунікації таких пристроїв.

2. Прості пристрої, що є основою індустрії IoT, не мають технічних ресурсів для реалізації складних криптографічних протоколів, що знижує рівень їх безпеки, наприклад, неспроможність захиститися від атак посередника.

3. Безпека сполучення простих IoT пристроїв може бути підвищена за рахунок їх автентифікації по близькості розташування шляхом аналізу потужності безпровідного сигналу (такого, як BLE).

4. Приведені розрахунки, які доказують, що запропонований метод забезпечує безпеку сполучення IoT пристроїв на близькій відстані та захист від атак посередника.

Література

1. Sachin Kumar, Prayag Tiwari and Mikhail Zymbler, Internet of Things is a revolutionary approach for future technology enhancement: a review, Journal of Big Data, 6, Article number: 111 (2019): Онлайн: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2
2. S Choudhary, G Meena, Internet of Things: Protocols, Applications and Security Issues, Procedia Computer Science, Volume 215, 2022, Pages 274-288: Онлайн: https://www.sciencedirect.com/science/article/pii/S1877050922021019
3. IoT Analytics, State of IoT 2023: Онлайн: https://iot-analytics.com/wp/wp-content/uploads/2023/05/Insights-Release-State-of-IoT-2023-Number-of-connected-IoT-devices-growing-16-to-16.0-billion-globally.pdf.
4. Tomorrow Bio, Understanding IoT: How Simple Devices Can Drive Big Changes, 2023: Онлайн: https://www.tomorrow.bio/post/understanding-iot-how-simple-devices-can-drive-big-changes-2023-06-4732281520-iot
5. Mohammed Aziz Al Kabir, Wael Elmedany & Mhd Saeed Sharif (2023) Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques, Journal of Cyber Security Technology, 7:4, 199-223: Онлайн: https://doi.org/10.1080/23742917.2023.2228053.
6. AN1302: Bluetooth Low Energy Application Security Design Considerations in SDK v3.x and Higher, Silicon Laboratories: Онлайн: https://www.silabs.com/documents/public/application-notes/an1302-bluetooth-application-security-design-considerations.pdf.
7. Karim Lounis, Mohammad Zulkernine. Bluetooth Low Energy Makes ”Just Works” Not Work. Cyber Security in Networking Conference, Oct 2019, Quito, Ecuador. ffhal-02528877: Онлайн: https://hal.science/hal-02528877/document
8. Zhang, Jiansong, Zeyu Wang, Zhice Yang, and Qian Zhang. "Proximity based IoT device authentication." In IEEE INFOCOM 2017-IEEE conference on computer communications, pp. 1-9. IEEE, 2017: Онлайн: https://ieeexplore.ieee.org/abstract/document/8057145.