УДК 004.056.523:004.7

РОЗГЛЯД МЕТОДІВ ШИФРУВАННЯ ТА АУТЕНТИФІКАЦІЇ ДЛЯ БЕЗПЕЧНИХ БЕЗПРОВІДНИХ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Стрименешенко О.С.,
Науковий керівник – д. т. н., проф. Агеєв Д. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії ім.Поповського В.В.,
e-mail: oleksandr.strymeneshenko@nure.ua

In recent decades, we have seen an exponential growth in the number of devices that connect to the Internet. From home devices and smart gadgets to industrial sensors and medical devices, the Internet of Things is becoming not only an integral part of our daily lives, but also a key foundation for innovation and development of modern society. However, along with this, the threat to the security and confidentiality of this data is also increasing. Each new connected device in the Internet of Things network opens up a new potential attack vector for attackers. From misuse of devices to leakage of personal information, the risks are growing as the number of connected devices grows. Therefore, the importance of ensuring data security and privacy in wireless Internet of Things networks is becoming more and more important.

Шифрування в безпровідних мережах Інтернету речей (IoT) відіграє ключову роль у забезпеченні конфіденційності даних, переданих через мережу. Призначенням шифрування є перетворення звичайного тексту у нерозбірливий шифрований текст за допомогою криптографічних алгоритмів. Це робить дані незрозумілими для будь-якого, хто не має відповідного ключа для розшифрування.[1]

Одним із найпоширеніших і найбільш ефективних методів шифрування для безпровідних мереж є протокол WPA2 (Wi-Fi Protected Access 2). WPA2 використовує стандартний криптографічний протокол AES (Advanced Encryption Standard), який вважається одним з найбільш безпечних методів шифрування. AES забезпечує високий рівень захисту, що робить його надійним і відповідним для захисту важливих даних в безпровідних мережах IoT.

Наступним важливим аспектом є питання обміну ключами. Під час встановлення безпровідного зв'язку, пристрої взаємодіють, щоб обмінятися ключами, необхідними для шифрування та розшифрування даних. Забезпечення безпеки обміну ключами є критичним, оскільки недостатня захищеність може призвести до компрометації всієї мережі. Також важливо регулярно змінювати ключі шифрування для запобігання можливим атакам на злам.

Загалом, шифрування є невід'ємною частиною забезпечення безпеки в безпровідних мережах IoT. Використання надійних методів шифрування, таких як WPA2 з AES, в поєднанні з правильним обміном ключами та регулярною зміною ключів, є важливими стратегіями для захисту конфіденційності даних у мережі IoT.

Іншими важливим елементом захисту є аутентифікація у безпровідних мережах Інтернету речей (IoT), оскільки вона визначає, чи може пристрій отримати доступ до мережі. Цей процес полягає в перевірці ідентичності користувача чи пристрою, що намагається підключитися до мережі, перш ніж надавати йому доступ до ресурсів.

Один із популярних методів аутентифікації у безпровідних мережах IoT - це використання протоколу EAP (Extensible Authentication Protocol). EAP дозволяє використовувати різні методи аутентифікації, що робить його дуже гнучким та адаптивним до різних потреб і сценаріїв застосування. Наприклад, метод EAP-TLS (Transport Layer Security) використовує сертифікати для аутентифікації, тоді як EAP-TTLS (Tunneled Transport Layer Security) створює захищений тунель для передачі аутентифікаційних даних.

Крім того, важливо враховувати різні фактори аутентифікації для підвищення рівня безпеки. Наприклад, використання біометричних даних, таких як відбиток пальця або розпізнавання обличчя, може забезпечити додатковий рівень впевненості у тому, що лише власник має доступ до пристрою. Одноразові паролі або токени також можуть бути використані для створення унікальних і тимчасових ідентифікаторів, які надаються користувачеві лише на певний час або за певних умов.

Загалом, використання надійних методів аутентифікації та врахування різних факторів аутентифікації є ключовими для забезпечення безпеки у безпровідних мережах IoT. Це дозволяє уникнути несанкціонованого доступу та забезпечити захист конфіденційності даних, які передаються через ці мережі.

Поза шифруванням та аутентифікацією, існують інші методи забезпечення безпеки в безпровідних мережах IoT. Наприклад, використання вогнепровідних стін та систем виявлення вторгнень може допомогти вчасно виявляти та відвертати загрози. Також важливо постійно оновлювати програмне забезпечення пристроїв та мережевого обладнання для закриття виявлених вразливостей.

Список використаних джерел:

1. Savelyev A. V., Кібербезпека в інтернеті речей. Безпека бізнесу. – 2019. – № 2 (46). – С. 45–51.