

УДК 004.056

Розломій І.О., канд. техн. наук, доцент
Черкаський державний технологічний університет, inna-roz@ukr.net
Науменко С.В., аспірант
Михайловський П.В., аспірант
Черкаський національний університет ім. Б. Хмельницького,
naumenko.serhii1122@vu.cdu.edu.ua

ФОРМУВАННЯ СЕАНСОВИХ КЛЮЧІВ У СЕНСОРНИХ ПРИСТРОЯХ З ОБМЕЖЕНИМ ОБСЯГОМ ПАМ'ЯТІ НА ОСНОВІ ЧАСОВИХ ТОКЕНІВ

Зростання популярності сенсорних пристроїв, що є частиною архітектури Інтернету речей (IoT), супроводжується актуалізацією питань конфіденційності та цілісності переданих даних. Забезпечення інформаційної безпеки в таких пристроях ускладнюється через їхні обмеження щодо обчислювальних ресурсів, енергоспоживання та доступної пам'яті [1]. Традиційні підходи до управління ключами часто є непридатними для впровадження в сенсорних вузлах, оскільки вимагають значного обсягу пам'яті або складних обчислювальних процедур. Крім того, багато сенсорних пристроїв працюють у нестабільному середовищі з переривчастим живленням, що унеможливує збереження ключів у довготривалій пам'яті без ризику втрати. Це зумовлює необхідність використання динамічних схем генерації ключів у режимі реального часу.

Одним з перспективних напрямів є застосування часових токенів (time-based tokens), які дають змогу формувати динамічні сеансові ключі без збереження довготривалих секретів або проведення складних криптографічних операцій [2]. Такий підхід дозволяє ефективно використовувати наявні ресурси сенсорного пристрою, мінімізуючи ризик компрометації ключа.

Метою дослідження є розробка моделі формування сеансових ключів на основі часових токенів, адаптованої до умов сенсорних пристроїв з обмеженим обсягом пам'яті.

У контексті сенсорних IoT-пристроїв, що функціонують в умовах обмеженої пам'яті, обчислювальних ресурсів та енергоспоживання, виникає потреба в механізмах формування криптографічних ключів, які реалізуються без постійного зберігання конфіденційних ключових параметрів. Одним з таких механізмів є генерація сеансових ключів на основі часових токенів, яка передбачає створення тимчасових кодів, синхронізованих за годинниковими мітками на обох кінцях каналу зв'язку.

Запропонований підхід ґрунтується на використанні алгоритму TOTP (Time-based One-Time Password), адаптованого до обмежених умов сенсорних пристроїв [3]. На відміну від стандартної реалізації, яка потребує зберігання секретного ключа для кожного пристрою, запропонована модель передбачає генерацію тимчасового токена шляхом обчислення геш-функції від комбінації поточного часу та ідентифікатора пристрою. Таким чином, у пам'яті пристрою зберігається лише одна константа (наприклад, загальний системний seed або пристроєвий UID), що суттєво знижує вимоги до обсягу пам'яті. Сеансовий ключ K_{sess} визначається за формулою:

$$K_{sess} = HMAC_{SHA1}(UID||T),$$

де UID – унікальний ідентифікатор сенсорного пристрою, T – поточне значення часу, округлене до фіксованого інтервалу (наприклад, 30 секунд), а $HMAC_{SHA1}$ – функція хешування з ключем. Такий ключ залишається дійсним лише в межах заданого тимчасового інтервалу, після чого автоматично змінюється, знижуючи ризики перехоплення або повторного використання.

Для синхронізації часу між вузлами мережі пропонується використовувати полегшені протоколи типу SNTP (Simple Network Time Protocol) або обмежене число звернень до

базової станції чи шлюзу. Архітектуру взаємодії сенсорних пристроїв із базовою станцією з урахуванням часової синхронізації та вікна толерантності представлено на рис. 1.

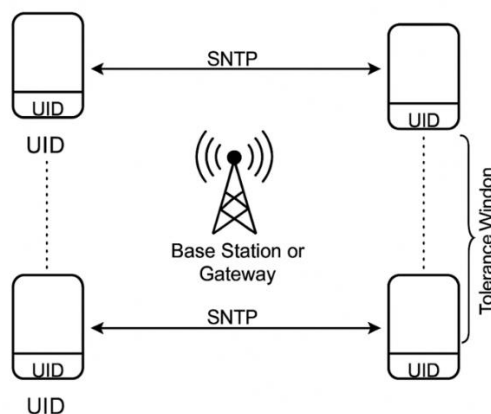


Рис. 1 – Архітектура часової синхронізації сенсорів і шлюзу через SNTP

З рис. 1. видно сенсорні пристрої з унікальними ідентифікаторами (UID), які взаємодіють із базовою станцією через полегшений протокол SNTP. Для забезпечення точності формування сеансових ключів на основі часових токенів критичною є синхронізація годинників. Протокол SNTP дозволяє підтримувати актуальний часовий стан із мінімальним енергоспоживанням, а використання вікна толерантності ± 1 інтервал дозволяє уникнути збоїв у зв'язку при незначних відхиленнях часу. Такий підхід забезпечує баланс між безпекою, енергоефективністю та простотою реалізації.

Запропоновану модель доцільно використовувати в таких сценаріях: при побудові сеансів автентифікації між сенсором і шлюзом у медичних пристроях; для шифрування тимчасових каналів зв'язку між компонентами розподіленої сенсорної мережі на промислових об'єктах; у безпілотних сенсорних платформах, які функціонують із переривчастим живленням та не можуть зберігати ключі постійно.

Для оцінки ефективності було проведено моделювання формування сеансових ключів у пристроях з 32 КБ оперативної пам'яті. Результати засвідчили, що застосування часових токенів не призводить до значного навантаження на систему й не потребує додаткових апаратних засобів.

Моделювання виконувалося в середовищі Arduino IDE з використанням мікроконтролера типу ATmega328P, який широко застосовується в сенсорних IoT-платформах. Алгоритм генерації часових токенів реалізовано з використанням адаптованої функції HMAC-SHA1 із лінійним доступом до пам'яті та обмеженою кількістю циклічних операцій. Тестування проводилося в умовах симуляції енергозалежного живлення з обмеженим циклом оновлення ключів (кожні 30 секунд) та часовим вікном толерантності ± 1 інтервал.

Аналіз результатів показав стабільну генерацію ключів без затримок, пікове споживання оперативної пам'яті не перевищувало 21 КБ, а середній час генерації одного сеансового ключа становив менше 15 мс. Це підтверджує придатність підходу для вбудованих систем із жорсткими обмеженнями ресурсів.

Список посилань

1. Rozlomi, I., Naumenko, S., Mykhailovskyi, P., & Monarkh, V. (2024, October). Resource-Saving Cryptography for Microcontrollers in Biomedical Devices. In 2024 IEEE 5th KhPI Week on Advanced Technology (KhPIWeek) (pp. 1-5). IEEE.
2. Nakamura, S., Enokido, T., & Takizawa, M. (2021). Information flow control based on capability token validity for secure IoT: implementation and evaluation. *Internet of Things*, 15, 100423.
3. Nakami, A. H., & Elmedany, W. (2022, December). Secure authentication framework based on one-time password for internet of things. In *IET Conference Proceedings CP824* (Vol. 2022, No. 26, pp. 451-457). Stevenage, UK: The Institution of Engineering and Technology.