УДК 004.056.5:004.78

А. С. Мосєвніна

МЕТОД ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ГОЛОСОВОГО ЗВ'ЯЗКУ В СИСТЕМАХ SMART-БУДИНКУ

Вінницький національний технічний університет;

Анотація

У роботі розглянуто проблему забезпечення безпеки голосового зв'язку в системах Smart-будинку, які активно використовують мережеві IoT-пристрої та голосові інтерфейси. Запропоновано метод забезпечення конфіденційності та цілісності голосових даних на основі використання криптографічних алгоритмів шифрування та цифрових підписів. Розглянуто основні етапи передачі захищених голосових повідомлень і визначено функціональні модулі програмної системи, що реалізує безпечну комунікацію між пристроями Smart-будинку.

Ключові слова: Smart-будинок; захищений голосовий зв'язок; IoT; криптографія; шифрування; цифровий підпис.

Abstract

The paper considers the problem of ensuring secure voice communication in smart home systems that actively use networked IoT devices and voice interfaces. A method for ensuring the confidentiality and integrity of voice data based on cryptographic encryption algorithms and digital signatures is proposed. The main stages of secure voice message transmission are analyzed, and the functional modules of the software system that provides secure communication between smart home devices are defined.

Keywords: smart home; secure voice communication; IoT; cryptography; encryption; digital signature.

Вступ

Системи Smart-будинку є важливою складовою сучасної концепції Інтернету речей (IoT) та передбачають інтеграцію різноманітних пристроїв, які взаємодіють між собою через мережу для автоматизації повсякденних процесів. Одним із напрямів розвитку таких систем є використання голосових інтерфейсів, що дозволяють користувачам керувати пристроями та отримувати інформацію за допомогою голосових команд або голосового зв'язку між компонентами системи.

Разом із розширенням функціональності голосових сервісів зростає і потреба у забезпеченні безпеки передавання голосових даних. Передача аудіоповідомлень через мережу може супроводжуватися ризиками перехоплення інформації, підміни даних або несанкціонованого доступу до системи. Тому важливим завданням є розробка методів забезпечення конфіденційності та цілісності голосового зв'язку в системах Smart-будинку.

Актуальність

Актуальність дослідження зумовлена стрімким розвитком технологій Інтернету речей (IoT) та широким впровадженням систем Smart-будинку, які інтегрують різноманітні пристрої для автоматизації та підвищення комфорту користувачів. Значну роль у таких системах відіграють голосові інтерфейси та засоби голосового зв'язку, що дозволяють взаємодіяти з пристроями без використання традиційних засобів керування. Разом із тим передача голосових даних через мережу створює низку ризиків, пов'язаних із можливістю перехоплення інформації, підміни повідомлень або несанкціонованого доступу до системи.

У сучасних умовах зростання кількості IoT-пристроїв проблема забезпечення конфіденційності та цілісності голосових даних стає особливо важливою. Недостатній рівень захисту комунікацій може призвести до витоку персональної інформації або компрометації системи Smart-будинку. Тому актуальним є розроблення ефективних методів захисту голосового зв'язку, що забезпечують безпечну передачу даних між пристроями та користувачами із застосуванням сучасних криптографічних механізмів.

Метод забезпечення захищеного голосового зв'язку

Системи Smart-будинку активно використовують голосові сервіси для взаємодії користувача з пристроями та для передачі голосових повідомлень між компонентами системи. Такі системи функціонують у середовищі Інтернету речей, де велика кількість пристроїв обмінюється даними через мережу, що створює нові виклики у сфері інформаційної безпеки [1]. Проте передача голосових даних через мережу може супроводжуватися ризиками перехоплення інформації, підміни повідомлень або

несанкціонованого доступу до системи. У зв'язку з цим виникає необхідність забезпечення захисту голосового трафіку з використанням сучасних криптографічних механізмів [2].

Для забезпечення захисту голосового трафіку застосовуються різні криптографічні методи, серед яких найбільш поширеними є симетричне та асиметричне шифрування, а також цифрові підписи [3]. Симетричні алгоритми, зокрема AES, широко використовуються для захисту переданих даних завдяки високій швидкодії та ефективності при обробці потокової інформації. Асиметричні алгоритми, такі як RSA або ECC, застосовуються переважно для безпечного обміну ключами та автентифікації пристроїв у мережі [4].

Для вирішення цієї задачі пропонується метод забезпечення захищеного голосового зв'язку, який передбачає використання алгоритмів шифрування та цифрового підпису. Основна ідея методу полягає у шифруванні голосових даних перед передачею мережею та перевірці їх цілісності на стороні отримувача. Подібні підходи активно досліджуються у сучасних роботах, присвячених безпечним комунікаціям у середовищі IoT [5].

Процес передачі захищеного голосового повідомлення включає кілька основних етапів:

1) захоплення голосового сигналу за допомогою аудіопристрою;
2) перетворення аудіосигналу у цифровий формат;
3) шифрування даних за допомогою криптографічного алгоритму;
4) формування цифрового підпису повідомлення;
5) передача зашифрованих даних через мережу;
6) перевірка цифрового підпису на стороні отримувача;
7) дешифрування даних та відтворення голосового повідомлення.

Застосування криптографічних методів дозволяє забезпечити захист голосових даних на різних рівнях передачі інформації. Найбільш поширені методи захисту голосового трафіку наведено у таблиці 1.

Таблиця 1. Порівняння методів захисту голосових даних

Метод	**Основне призначення**	**Переваги**	**Недоліки**
Симетричне шифрування (AES)	Захист конфіденційності даних	Висока швидкість обробки	Потребує безпечного обміну ключами
Асиметричне шифрування (RSA)	Обмін ключами та захист даних	Високий рівень безпеки	Нижча швидкодія
Цифровий підпис	Перевірка цілісності та автентичності	Гарантує автентичність даних	Збільшує обсяг переданих даних
Захищені протоколи (TLS, SRTP)	Комплексний захист передачі	Підтримка стандартів безпеки	Складність реалізації

На основі аналізу існуючих підходів запропоновано архітектуру програмного модуля захищеного голосового зв'язку для систем Smart-будинку. Основні функціональні модулі системи наведено у таблиці 2.

Таблиця 2. Основні модулі системи захищеного голосового зв'язку

Модуль	**Функції**
Модуль захоплення аудіо	Отримання голосового сигналу з мікрофона
Модуль обробки аудіоданих	Перетворення та підготовка сигналу до передачі
Модуль шифрування	Захист конфіденційності голосових даних
Модуль цифрового підпису	Забезпечення цілісності та автентичності даних
Мережевий модуль	Передача зашифрованих повідомлень через мережу
Модуль дешифрування	Відновлення вихідного голосового повідомлення

Запропонований підхід може бути реалізований у вигляді програмного модуля, інтегрованого до системи Smart-будинку. Реалізація такого модуля дозволяє підвищити рівень безпеки голосових комунікацій між пристроями та користувачами, а також забезпечити захист конфіденційної інформації.

Висновки

У роботі розглянуто проблему забезпечення безпеки голосового зв'язку в системах Smart-будинку, що функціонують у середовищі Інтернету речей. Проведений аналіз показав, що передача голосових даних через мережу супроводжується ризиками перехоплення інформації, підміни повідомлень та несанкціонованого доступу до системи. Для підвищення рівня безпеки запропоновано метод забезпечення захищеного голосового зв'язку, який передбачає використання криптографічних алгоритмів шифрування та цифрових підписів.

Запропонований підхід дозволяє забезпечити конфіденційність і цілісність голосових повідомлень під час їх передачі між пристроями Smart-будинку. Також визначено основні функціональні модулі програмної системи, що реалізує безпечну передачу голосових даних. Отримані результати можуть бути використані при розробці програмних засобів захищених комунікацій у IoT-системах та можуть слугувати основою для подальших досліджень методів проєктування безпечних систем голосового зв'язку[6].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Silva C., Cunha V., Barraca J., Aguiar R. «Analysis of the Cryptographic Algorithms in IoT Communications», DOI: 10.1007/s10796-023-10383-9, 2023. URL: https://www.researchgate.net/publication/370532591_Analysis_of_the_Cryptographic_Algorithms_in_IoT_Communications
2. Dargaoui S., Azrour M., El Allaoui A. «Internet of Things Authentication Protocols: Comparative Study», DOI: 10.32604/cmc.2024.047625, 2024. URL: https://www.researchgate.net/publication/379421064_Internet_of_Things_Authentication_Protocols_Comparative_Study
3. Krasnowski P., Lebrun J., Martin B. «Introducing an experimental distortion-tolerant speech encryption scheme for secure voice communication», 2021. URL: https://www.researchgate.net/publication/349492835_Introducing_an_experimental_distortion-tolerant_speech_encryption_scheme_for_secure_voice_communication
4. Kumar S., Hu Y., Andersen M. «JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT», DOI: 10.48550/arXiv.1905.13369, 2019. URL: https://www.researchgate.net/publication/333563873_JEDI_Many-to-Many_End-to-End_Encryption_and_Key_Delegation_for_IoT
5. Dumitrache C., Anghelescu P. «Design and Implementation of a Secure Communication Architecture for IoT Devices», 2025. URL: https://www.mdpi.com/2224-2708/14/4/64
6. Sarwar N., Alharthi R., Mujlid H. «Enhancing IoT communication in fog computing: a lightweight remote user authentication and key management scheme utilizing ECC», DOI: 10.1186/s13677-025-00816-y, 2025. URL: https://www.researchgate.net/publication/397970540_Enhancing_IoT_communication_in_fog_computing_a_lightweight_remote_user_authentication_and_key_management_scheme_utilizing_ECC

Мосєвніна Аліна Сергіївна - студентка групи 1ПІ-25м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: mosievninaaa@gmail.com

Науковий керівник: Ліщинська Людмила Броніславівна - д-р техн. наук, професор, професор кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: llb@vntu.edu.ua

Mosievnina Alina Sergiivna - student of group 1PI-25m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: mosievninaaa@gmail.com

Academic supervisor: Lishchynska Lyudmyla Bronislavivna - Dr. Sc. (Eng.), Full Professor, Professor of Program Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: llb@vntu.edu.ua261