УДК 004.056.5

Р. В. Бачинський, А. В. Купецький
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ BLUETOOTH ЗВ’ЯЗКУ МІЖ ПРИСТРОЄМ ІНТЕРНЕТУ РЕЧЕЙ ТА МОБІЛЬНИМ ОБЧИСЛЮВАЛЬНИМ ПРИСТРОЄМ

Розглянуто захист каналу зв’язку між пристроями інтернету речей та пристроїв на базі ОС iOS. Проаналізовано способи шифрування каналу та розподіл спільних ключів у незахищеному середовищі. Описано та розроблено систему для захисту такого каналу.

Ключові слова: шифрування, iOS, Bluetooth, автентифікація.

Bluetooth communication channel protection for IOT devices and IOS based devices considered in the article. Channel encryption and shared key distribution in unsaved environment analyzed. The proposed protection system is developed and described.

Key words: cypher, iOS, Bluetooth, authentification.

Вступ

Сьогодні темпи та масштаби діяльності суспільства значно зросли, порівняно з попереднім століттям. Основною з причин такого стрімкого росту є бурхливий розвиток сфери інформаційних технологій (IT). Останніми роками, завдяки швидкому розвитку мобільності обчислювальних систем, активно розвивається одна зі сфер вищезгаданих технологій – автоматизація процесів у звичайному житті людини, таких як приготування обіду, налаштування температури й освітлення у кімнаті, інакше кажучи – інтернет речей.

Це поняття почало активно розвиватися з кінця XX ст., а саме 1982 р., коли з’явилась модифікована машина для “Кока-коли”, яка за потреби охолоджувала напої [1]. Концепція інтернету речей набула популярності в 1999 р., коли маркування товарів різноманітними мітками, такими як RFID, NFC, QR-коди, баркоди, стало звичним явищем та дещо автоматизувало процес покупки та індексування товарів [2].

Будь-який пристрій, що містить на борту модуль провідного чи безпровідного зв’язку, пристрій накопичення і перетворення даних, а також її передавання за допомогою вищезгаданого модуля, може використовуватись як основна частина цієї системи.

Основною перевагою таких пристроїв є їхня мобільність, сумісність із поточними комп’ютерними мережами, проведеними у будинках чи на вулицях. Використання таких систем дає змогу людині як споживачеві оминути часто повторювані, рутинні операції, а також забезпечити постійний моніторинг системи загалом.

Стан проблеми

Перед будь-яким пристроєм, що передає дані, постає основна проблема – захист каналу зв’язку між пристроями від зловмисників. Оскільки кількість пристроїв інтернету речей невпинно зростає, з такою ж швидкістю підвищується рівень небезпеки. Доволі часто у виробників, що займаються апаратною частиною пристроїв, недостатньо знань щодо програмної частини, а також сфери захисту даних. Через такі проблеми заводи випускають пристрої, що важко, а то й неможливо захистити [3].

Цю проблему вирішували декілька десятків років, і над нею продовжують працювати. Інформацію у таких системах можна перехопити за допомогою перехоплення або підбору ключів, якими шифрують корисну інформацію, що навіть сьогодні є ресурсозатратним завданням та не вкладається у розумні часові межі (для криптостійких алгоритмів – від кількох років до тисячоліття). Можливі також атаки посередників (Man-In-The-Middle attack). У системах

криптографічного захисту ПК і серверів для захисту від таких атак основним джерелом “довіри” є третя особа – центр авторизації (Certification Authority), що дає змогу сторонам впевнитись в істинності їх намірів спілкування [4].

Логічно, що всі сучасні надбання для криптографічного захисту можна застосувати і для обміну даними між мобільним обчислювальним пристроєм та пристроєм інтернету речей, проте це не завжди так.

Проблемою пристроїв інтернету речей є те, що апаратні засоби, на яких вони побудовані, не є обчислювально потужними, а також не мають постійного стабільного зв’язку з інтернетом, а також достатньо складного програмного забезпечення, щоб отримати доступ до центрів авторизації.

Іншим вузьким місцем Bluetooth каналу, а саме технології Bluetooth Low Energy (далі BLE), є розмір пакетів, у якому максимальний розмір даних не перевищує 27 байтів для Bluetooth версії 4.0-4.1 та до 251 у версії 4.2. Такий розмір є достатнім для передавання зашифрованих ключів та сервісних даних, проте потребує розділення на підпакети на вищому рівні абстракції, якщо дані великого розміру.

Проблема захисту каналу Bluetooth зв’язку актуальна, оскільки це один з найпопулярніших та широковживаних каналів для обміну інформацією з іншими пристроями, наприклад, смартфонами, через які часто передається цінна інформація про власника – його місцезнаходження, різноманітні паролі, персональні дані та інша важлива інформація.

Постановка задачі

Розробити систему криптографічного захисту Bluetooth каналу між пристроєм інтернету речей та мобільним обчислювальним пристроєм на платформі iOS. Описати спосіб шифрування пакетів, що передаються між пристроями. Розробити структурну схему системи, алгоритм її роботи та діаграму класів. Проаналізувати швидкодію пристроїв інтернету речей під час розрахунку різних алгоритмів шифрування, доцільність їх використання.

Розв’язання задачі

Для розв’язання цієї задачі було вирішено взяти за основу декілька алгоритмів – протокол обміну ключами Діффі–Хельмана, алгоритм DSA для створення цифрового підпису даних, необхідних для вищезгаданого протоколу, а також алгоритм AES з різними режимами шифрування для автентифікації та симетричного шифрування даних. Вибір вищезгаданих протоколів пояснюється взаємною компенсацією проблемних місць у протоколах. Наприклад, AES потребує ключ шифрування, однаковий для двох сторін, адже використовується як для зашифровування даних, так і навпаки. Цю проблему вирішує протокол Діффі–Хельмана, проте кожна зі сторін повинна впевнитись у тому, що вона створює спільний ключ із кінцевим користувачем, а не зловмисником, що діє як посередник. Цю проблему вирішує алгоритм DSA. Опис вищезгаданих компонентів надано нижче.

Протокол обміну ключами Діффі–Хельмана дає змогу створити спільний приватний ключ, який можна надалі використати для шифрування пакетів у незахищеному каналі зв’язку [5].

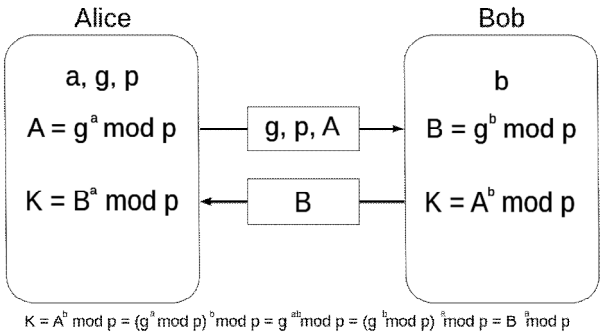

Рис. 1. Схематичне представлення роботи протоколу Діффі–Хельмана

Протокол працює так: Аліса створює для Боба деякі ключі g і p, де p – просте велике число, а g – первісний корінь за модулем p (також просте число), а також розраховує $A = g^a mod\, p$ та відправляє їх Бобу. Боб натомість надсилає Алісі число В: $B = g^b mod\, p$. Після операції обміну Боб та Аліса виконують обчислення значення К: $K = g^{ab} mod\, p$, що являє собою спільний для них другий ключ, який можна використати для подальшої комунікації.

Криптостійкість цього алгоритму полягає у теоретичній складності розрахунку спільного ключа $K = A^b mod\, p = B^a = g^{ab} mod\, p$. Власне розрахунок g^{ab} є доволі складним і має власну назву – проблема Діффі–Хельмана. Також Аліса та Боб повинні використовувати різні генератори випадкових чисел, оскільки існує ймовірність, що результат обох користувачів не буде повністю випадковим.

У протоколі зазначено, що він призначений лише для створення спільного ключа у незахищеному каналі зв'язку, проте не гарантує авторизації користувачів між собою, тобто протокол у стандартному виконанні є вразливим до атак "людина посередині". Ймовірна така ситуація, що у спілкування Аліса та Боба втрутиться прослуховувач Мелорі, яка матиме спільний приватний ключ для Аліси, а також ключ для розмови з Бобом. Отже, вона зможе без будь-яких проблем отримати від Аліси пакет з даними, розшифрувати їх, зашифрувати ключем Боба та відправити дані йому, і навпаки.

Для вирішення цієї проблеми використано асиметричний алгоритм створення та перевірки цифрового підпису DSA (Digital Signature Algoritm). Алгоритм часто називають DSS (Digital Signature Standard), оскільки цей документ являє собою американський стандарт, що описує принцип роботи і застосування DSA. Використання цього алгоритму дає змогу однозначно підтвердити достовірність даних, необхідних для створення спільного ключа.

Оскільки розмір пакета для передавання даних фіксований і досить малий, а також зважаючи на продуктивність системи, доцільно вибрати одну з реалізацій вищезгаданих алгоритмів, що ґрунтуються на використанні еліптичних кривих. Такий підхід дає змогу зменшити розмір даних для шифрування/дешифрування, а також, за наявності апаратних блоків шифрування, пришвидшити розрахунок алгоритмів.

Алгоритм цифрового підпису даних на еліптичних кривих використовуватиме множину кривої, рекомендовану Національним інститутом стандартів і технологій (NIST), що має назву secp256r1.

Для шифрування даних, що передаються між складовими системи, вибрано блоковий симетричний алгоритм шифрування AES. Це криптостійкий алгоритм, що пропонує Агентство національної безпеки США для шифрування цінної інформації з використанням ключа розміром 128 бітів.

Для цієї системи використовується режим шифрування CCM, що рекомендують застосовувати разом із алгоритмом AES.

CCM поєднує режим шифрування CBC-MAC, що будує аутентифікаційний ключ повідомлення (Message Authentification Code, MAC), із шифруванням у режимі лічильника (CTR), що перетворює його на потоковий алгоритм шифрування [6].

Використання двох вищезгаданих аспектів шифрування даних дає змогу розробити систему, що не вимагатиме підтвердження від довіреної "особи" для автентифікації користувачів, що скоротить час роботи між пристроями та кількість необхідних для їх функціонування ресурсів.

Оскільки кожна зі сторін матиме свій приватний набір публічних та приватних ключів, що застосовуються для шифрування та верифікації повідомлень, зловмиснику потрібно розшифрувати всі приватні ключі, для того щоб система вийшла з ладу, а це забезпечує її стійкість.

Така система може працювати у складі інших систем, до прикладу, в застосунку користувача, що створений для роботи з пристроями інтернету речей.

Структура програмної системи (рис. 2) містить блок встановлення Bluetooth з'єднання та передавання даних між пристроєм, блок шифрування даних, а також блок отримання та перетворення даних у бінарний формат та навпаки.

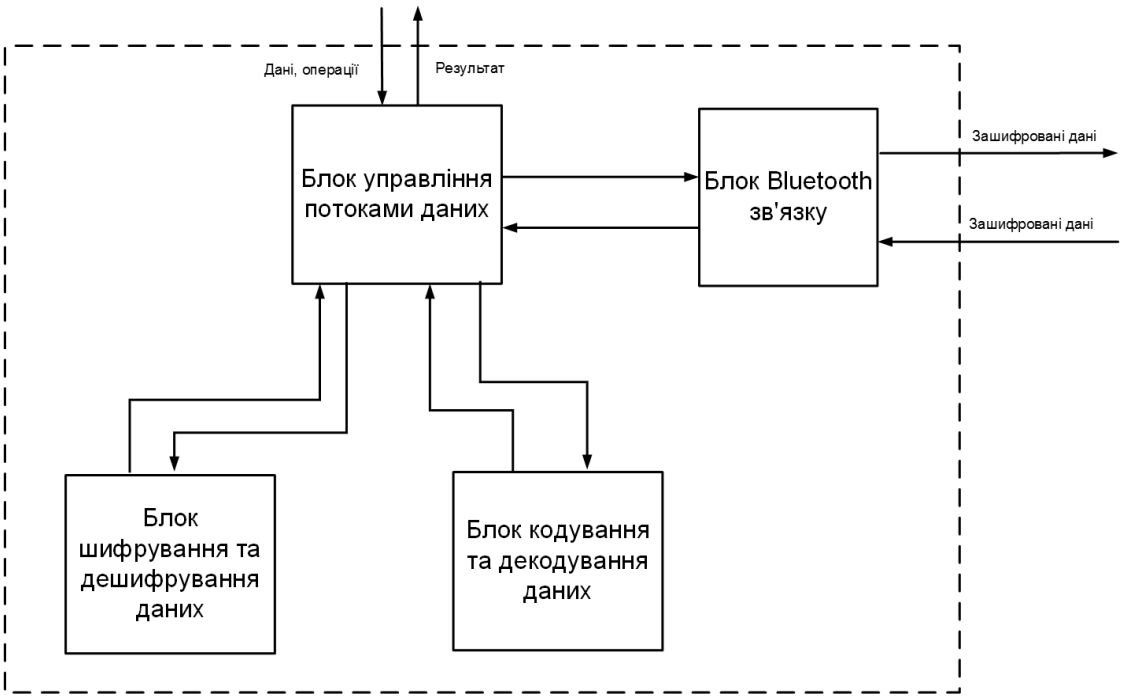

Рис. 2. Структурна схема системи криптографічного захисту Bluetooth зв'язку між пристроєм інтернету речей та мобільним обчислювальним пристроєм

Алгоритм роботи системи складається із таких кроків: встановлення з'єднання з BLE пристроєм, початок створення приватних та публічних ключів, створення публічних простих чисел для протоколу Діффі–Хельмана, передавання їх периферійному пристрою.

Після цього етапу потрібно здійснити обчислення числа, що буде передано пристрою для розрахунку спільного ключа. Після отримання іншого числа від пристрою система розраховує спільний приватний ключ, після чого вона готова до передавання шифрованих даних між пристроями.

Варто зазначити, що невиконання будь-якого кроку однією зі сторін призводить до негайного припинення сеансу роботи та потребує повторного виконання алгоритму. Так система забезпечує стабільність та захищеність від завад чи зловмисників. Ціною захищеності є затрати часу на встановлення, автентифікацію та шифрування даних для передавання.

Для створення цієї програмної системи вирішено вибрати об'єктно- та протоколо-орієнтовану мову програмування Swift, що підтримується ОС iOS, а також використати бібліотеки, що надає ОС, – Core Foundation, Core Bluetooth, UIKit, CommonCrypto та інші. Під час її проектування було отримано діаграму класів, наведену на рис. 3. Основними класами цієї системи є: BTTransportService – клас, що відповідає за з'єднання системи із периферійним пристроєм через Bluetooth канал. BTCypherService – клас, відповідальний за успішне виконання алгоритму отримання спільного приватного ключа, та його використання блоковим алгоритмом AES-CCM для шифрування та дешифрування одержаного повідомлення. Як допоміжні класи створено BTPeripheralDevice – клас, що містить у собі список всіх доступних сервісів та характеристик у периферійному пристрої, а також їх екземпляри, активні в цей момент. Також створено BTDataMarshaller, єдиним завданням якого є перетворення вхідних даних будь-якого формату на масив байтів та навпаки. Також доцільно згадати клас, що містить у собі всі константи під час роботи з Bluetooth периферією, а саме – унікальні ідентифікатори (UUID) периферійного пристрою, сервісів та характеристик.

Як пристрій інтернету речей можна використати будь-який пристрій, що ґрунтується на RISC процесорі Cortex M0/M0+. Цей процесор вирізняється енергоефективністю та потужністю, достатньою для виконання поставлених перед ним завдань, зокрема оброблення і відправлення даних, отриманих за допомогою Bluetooth. Практично всі пристрої, побудовані на цьому процесорі,

придатні для шифрування/дешифрування переданих даних різноманітними алгоритмами. Нижче наведемо результати тестування продуктивності розрахунку вищезгаданих алгоритмів (ECDHE, ECDSA) у табл. 1, а у табл. 2 – швидкодію симетричних алгоритмів для шифрування даних.

Рис. 3. Алгоритм роботи системи криптографічного захисту Bluetooth зв'язку між пристроєм інтернету речей та мобільним обчислювальним пристроєм

Таблиця 1

Результати тестування алгоритмів авторизації та отримання спільного ключа

Тип алгоритму	Час виконання, мс
ECDHE (secp256r1)	1672
ECDSA, операція підпису даних	459
ECDSA, операція перевірки даних	1759

Тестування здійснено на рекомендованій NIST множині кривої secp256r1.

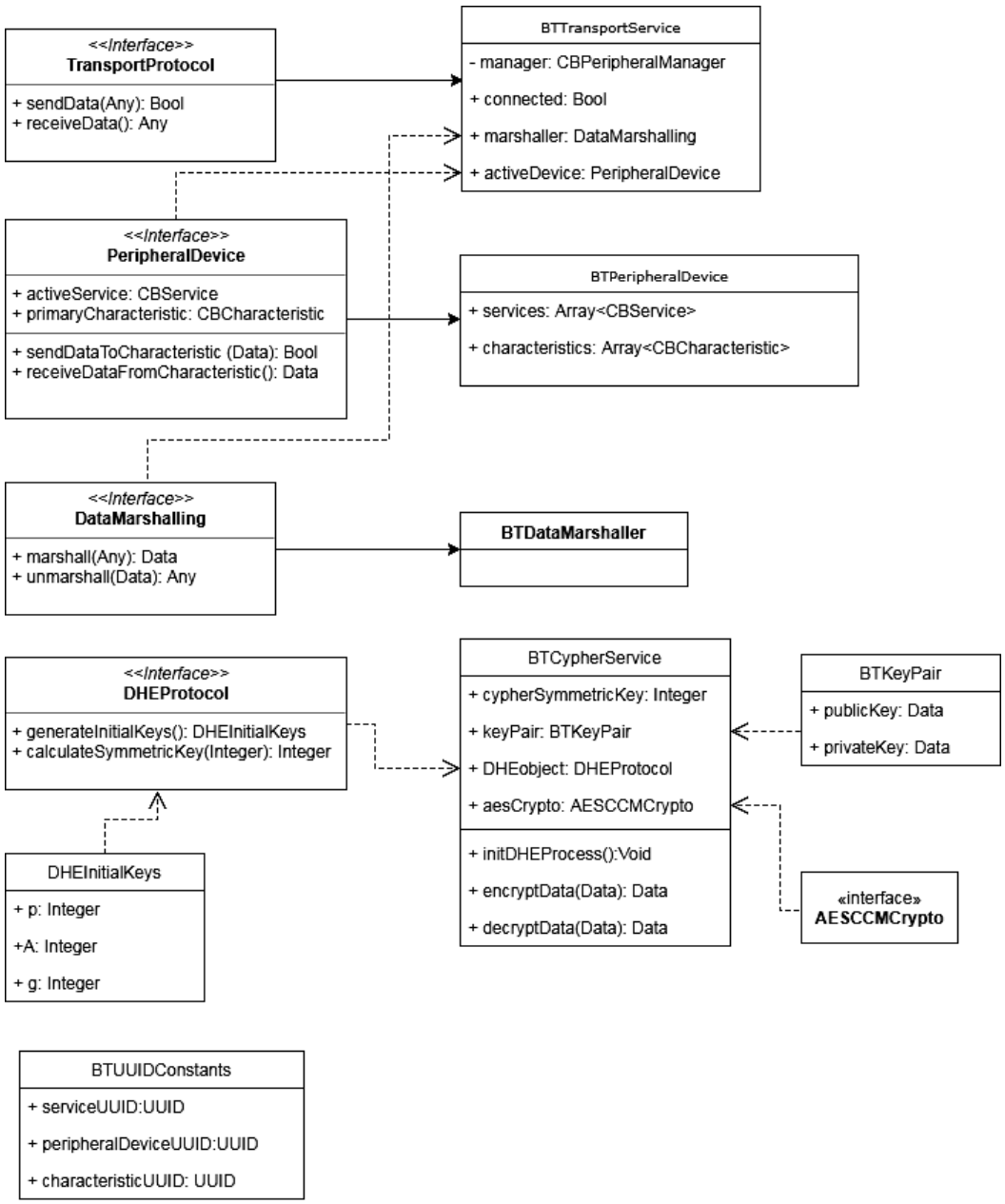

Рис. 4. Діаграма класів системи криптографічного захисту Bluetooth зв'язку між пристроєм інтернету речей та мобільним обчислювальним пристроєм

Таблиця 2

Результати тестування алгоритму симетричного шифрування даних AES у різних режимах роботи та з різними розмірами ключа

Режим роботи	Час виконання, мс
AES-CCM-128	1320
AES-CCM-256	1540
AES-CBC-128	2201
AES-CBC-256	2584

Тестування здійснено на даних розміром 1 Кб.

Оцінюючи дані, наведені вище, можна сказати що більшість пристроїв на базі ARM Cortex M0/M0+ прийнятні для шифрування та автентифікації даних користувача.

Висновки. В ході виконання цієї роботи було розроблено систему криптографічного захисту Bluetooth зв'язку між пристроєм інтернету речей та мобільним обчислювальним пристроєм на платформі iOS. Також описано спосіб шифрування пакетів, що передаються між пристроями. Розроблено структурну схему системи, алгоритм її роботи та діаграму класів. Проаналізовано швидкодію пристроїв інтернету речей під час розрахунку різних алгоритмів шифрування, доцільність їх використання.

1. Internet of Things Done Wrong Stifles Innovation // InformationWeek, July 2014. 2. Magrassi P. Why a Universal RFID Infrastructure Would Be a Good Thing. 2 of May, 2002. 3. Feamster, Nick. Mitigating the Increasing Risks of an Insecure Internet of Things. Freedom to Tinker. 2017 8 of August, 2017. 4. Kirk Hall. Standards and Industry Regulations Applicable to Certification Authorities. Trend Micro, April 2013. 5. RFC 2631 – Diffie–Hellman Key Agreement Method. E. Rescorla. June 1999. 6. Dworkin, Morris, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality (PDF) (Technical report). NIST Special Publications, May 2004.