УДК 004.056.5

Шестопал Р.В.
Салієва О.В.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ IOT-МЕРЕЖ

Вінницький Національний Технічний Університет

Анотація

В даній роботі проаналізовано такі методи захисту IoT-мереж як DTLS, PSK, OSCORE, PKI, хешування та цифровий підпис. Наведено їх особливості, переваги та недоліки.

Ключові слова: Захист, IoT-мережа, автентифікація, шифрування.

Abstract

This paper analyzes such methods of protecting IoT networks as DTLS, PSK, OSCORE, PKI, hashing, and digital signature. Their features, advantages, and disadvantages are presented.

Key words: Protection, IoT-network, authentication, encryption.

Вступ

Забезпечення безпеки в IoT-мережах є однією з ключових задач сучасних досліджень, оскільки ці системи характеризуються високою вразливістю до кібератак через обмежені ресурси пристроїв та їхню масштабованість. У даній роботі проведено аналіз основних методів захисту IoT-мереж із урахуванням їхніх характеристик безпеки, ресурсоспоживання, сфер застосування та недоліків, що дозволяє визначити оптимальні підходи для різних сценаріїв використання.

Дослідження

DTLS (Datagram Transport Layer Security) є протоколом, який забезпечує шифрування, автентифікацію та цілісність даних у мережах, де використовується небезпечний транспортний рівень, наприклад, UDP (User Datagram Protocol). Основна ідея DTLS полягає в адаптації механізмів захисту протоколу TLS (Transport Layer Security) до умов ненадійних з'єднань, характерних для IoT-середовищ, де важливі як захист даних, так і низька затримка передачі. DTLS підтримує автентифікацію клієнта та сервера, шифрування повідомлень та перевірку цілісності шляхом використання криптографічних алгоритмів. Ці можливості роблять його одним із найпоширеніших протоколів безпеки для IoT-систем.

Протокол DTLS є ефективним у забезпеченні захищеного обміну даними, але його впровадження в IoT-пристрої супроводжується певними обмеженнями. Високе ресурсоспоживання, особливо під час встановлення з'єднання, створює значне навантаження на процесор і пам'ять пристроїв з обмеженими обчислювальними можливостями. Це може призводити до збільшення затримок, що є критичним у системах реального часу. Крім того, процес повторного встановлення сесії при втраті пакету є складним, оскільки він вимагає додаткових обчислень для підтримки цілісності даних та їх захисту.

Незважаючи на обмеження, DTLS широко використовується в IoT-середовищах завдяки його універсальності та можливості інтеграції з різними типами пристроїв. Його застосування виправдане в системах, де пріоритетом є захист даних, навіть якщо це супроводжується підвищеними вимогами до ресурсів. Наприклад, у медичних IoT-системах DTLS забезпечує безпечну передачу чутливих даних, таких як результати моніторингу пацієнта, що є критично важливим для підтримки конфіденційності та точності інформації. У промислових мережах DTLS використовується для захисту даних, що передаються між сенсорами та центральними контролерами, забезпечуючи безперервність роботи системи навіть у випадку виникнення атак на рівні мережі.

Таким чином, DTLS є важливим інструментом для забезпечення безпеки IoT-мереж, особливо в критичних системах. Його ефективність обумовлена широким набором функцій безпеки, хоча високе ресурсоспоживання залишається основним недоліком для його використання в системах з обмеженими можливостями. Подальший розвиток і оптимізація протоколу можуть розширити його застосування у різноманітних сферах людської діяльності [1].

PSK (Pre-Shared Key) є одним із найпростіших та найефективніших методів забезпечення безпеки в IoT-мережах, де використовується попередньо встановлений ключ для автентифікації та шифрування даних між пристроями. Цей підхід базується на тому, що всі учасники обміну мають доступ до одного секретного ключа, який заздалегідь розповсюджується серед пристроїв. Основною перевагою PSK є його низьке ресурсоспоживання, що робить його особливо привабливим для IoT-пристроїв із

обмеженими обчислювальними та енергетичними можливостями. Метод PSK дозволяє забезпечити швидку та ефективну автентифікацію, уникаючи складних криптографічних обчислень, характерних для інших методів захисту.

PSK знаходить широке застосування у невеликих IoT-мережах, таких як сенсорні мережі або пристрої для домашньої автоматизації, де кількість учасників обміну є обмеженою. У таких системах використання попередньо встановлених ключів є практичним, оскільки мінімізується потреба в управлінні складними сертифікатами чи динамічними механізмами генерації ключів. Завдяки своїй простоті, PSK легко інтегрується в системи з мінімальними витратами часу та ресурсів на впровадження. Крім того, низькі вимоги до обчислювальної потужності дозволяють використовувати цей метод навіть у пристроях із найменшими ресурсами, таких як прості сенсори чи актуатори.

Однак основним недоліком PSK є труднощі управління ключами у масштабованих мережах. У великих системах із багатьма пристроями оновлення або заміна попередньо встановлених ключів стає складним завданням, особливо якщо пристрої розташовані у віддалених або важкодоступних місцях. Крім того, використання одного ключа для багатьох пристроїв підвищує ризик компрометації, оскільки компрометація одного пристрою може призвести до розкриття секретного ключа для всієї мережі. У таких випадках необхідність заміни ключа в усій системі створює значні організаційні та технічні труднощі [1].

Застосування PSK є обґрунтованим у невеликих IoT-системах, де ключ може бути розповсюджений вручну або за допомогою безпечного каналу. Для більших мереж із високими вимогами до безпеки PSK зазвичай використовується в комбінації з іншими методами, такими як протоколи управління ключами або більш складні схеми автентифікації. Попри свої обмеження, PSK залишається важливим методом захисту, особливо для простих і ресурсно обмежених IoT-пристроїв, де його простота та ефективність є вирішальними перевагами.

OSCORE (Object Security for Constrained RESTful Environments) є спеціалізованим механізмом безпеки, розробленим для забезпечення end-to-end шифрування та автентифікації у системах IoT із обмеженими ресурсами. На відміну від традиційних протоколів захисту транспортного рівня, таких як TLS або DTLS, OSCORE працює на рівні додатків, що дозволяє захищати лише певні частини повідомлення, залишаючи інші доступними для обробки проміжними вузлами. Це підвищує ефективність і зменшує затримки, що є критично важливим для IoT-середовищ.

Основною перевагою OSCORE є його здатність забезпечувати конфіденційність, цілісність і автентифікацію повідомлень між кінцевими пристроями незалежно від проміжної інфраструктури. Шифрування на рівні додатка дозволяє уникнути необхідності створення захищених каналів на транспортному рівні, що знижує обчислювальні витрати та навантаження на мережу. OSCORE підтримує різні криптографічні алгоритми для шифрування та перевірки автентичності, забезпечуючи гнучкість і можливість адаптації до специфічних вимог IoT-мереж [2].

OSCORE активно використовується у великих IoT-системах, зокрема в промислових мережах, сенсорних мережах із високими вимогами до безпеки та системах з великою кількістю вузлів. Його перевага полягає у мінімізації обчислювальних витрат і використанні наявних протоколів, таких як CoAP, що дозволяє інтегрувати OSCORE у вже існуючі системи без значних змін у їхній архітектурі. Протокол також підтримує захист від атак на повторення (replay attacks) через використання механізмів збереження стану сесії.

Однак OSCORE має певні недоліки. Одним із них є складність інтеграції в існуючі системи, що може вимагати значних зусиль на етапах впровадження та налаштування. Крім того, хоча OSCORE забезпечує ефективний захист на рівні додатка, для повного захисту всієї системи його часто необхідно поєднувати з іншими методами захисту транспортного рівня, такими як DTLS. Ресурсоспоживання залежить від конкретної реалізації протоколу, що може створювати додаткові труднощі для пристроїв із мінімальними ресурсами.

Застосування OSCORE є виправданим у сценаріях, де потрібен захист даних між кінцевими пристроями в умовах обмежених ресурсів. Це рішення забезпечує високу гнучкість і ефективність, дозволяючи зберігати баланс між безпекою та продуктивністю. Незважаючи на складнощі інтеграції, OSCORE є перспективним методом захисту для IoT-систем, де end-to-end шифрування є ключовою вимогою [2].

PKI (Public Key Infrastructure) є потужним криптографічним підходом, що забезпечує автентифікацію, цілісність і конфіденційність даних через використання асиметричної криптографії. У контексті IoT-мереж PKI є основним механізмом для створення та управління сертифікатами, які

дозволяють ідентифікувати пристрої, користувачів або служби. Цей підхід базується на концепції пари ключів: приватного, який використовується для підпису даних, та публічного, який доступний для перевірки підпису або шифрування даних [3].

PKI забезпечує надійну автентифікацію пристроїв у масштабованих IoT-мережах, таких як промислові системи або розподілені сенсорні мережі. Сертифікати, які видаються центром сертифікації (CA), містять інформацію про ідентифікацію пристрою, його публічний ключ та термін дії сертифіката. Використання сертифікатів у PKI дозволяє створювати безпечні канали зв'язку між пристроями, навіть якщо вони не мали попередніх взаємодій. Це робить підхід PKI особливо корисним у великих системах із динамічно змінними пристроями, де ручне управління ключами є недоцільним.

Попри свою ефективність, PKI має певні обмеження, пов'язані з ресурсоспоживанням. Перевірка сертифікатів та виконання криптографічних операцій із використанням асиметричних ключів потребують значних обчислювальних ресурсів, що може бути проблемою для пристроїв із низькою потужністю. Крім того, управління сертифікатами в масштабованих системах, таких як IoT-мережі, може стати складним завданням. Зокрема, необхідність періодичного оновлення сертифікатів, відкликання скомпрометованих сертифікатів або забезпечення надійного доступу до центру сертифікації вимагає додаткових організаційних та технічних зусиль [4].

PKI є незамінним у критичних IoT-системах, де безпека даних є пріоритетом. Наприклад, у промислових мережах PKI дозволяє захищати взаємодію між сенсорами, контролерами та серверами, забезпечуючи надійний обмін даними. У системах «розумного міста» PKI використовується для захисту транспортних мереж, енергетичних систем і систем громадської безпеки. У медичних IoT-системах PKI забезпечує конфіденційність даних пацієнтів і захищає доступ до медичних пристроїв.

Таким чином, PKI є потужним інструментом для забезпечення безпеки IoT-мереж, який поєднує гнучкість і масштабованість із високим рівнем захисту. Проте його використання вимагає врахування обмежень ресурсів пристроїв і складності управління сертифікатами. Завдяки своїй здатності підтримувати автентифікацію, шифрування та цілісність даних, PKI залишається одним із найважливіших механізмів захисту в масштабованих IoT-системах із високими вимогами до безпеки.

У таблиці 1 відображено порівняння методів захисту IoT-мереж.

Таблиця 1 – Порівняння методів захисту IoT-мереж

Метод захисту	Характеристики безпеки	Ресурсоспоживання	Застосування	Недоліки
DTLS (Datagram Transport Layer Security)	Шифрування, автентифікація, цілісність даних	Високе, особливо під час встановлення з'єднання	Критичні IoT-системи (медичні, промислові)	Додаткові затримки та навантаження на ресурси
PSK (Pre-Shared Key)	Автентифікація та шифрування через попередньо встановлений ключ	Низьке	Невеликі та обмежені мережі IoT (сенсорні)	Труднощі управління ключами в масштабованих мережах
OSCORE (Object Security for Constrained RESTful Environments)	End-to-end шифрування та автентифікація на рівні додатка	Середнє, залежить від реалізації	Великі IoT-системи, промислові та захищені сенсорні мережі	Вимоги до ресурсів, складність інтеграції
Хешування та цифровий підпис	Цілісність і автентифікація даних	Може бути як середнє, так і високе, залежить від алгоритму	Критичні IoT-системи (медичні, промислові)	Ресурсомісткість, можливі затримки
PKI (Public Key Infrastructure)	Сертифікатна автентифікація	Високе, особливо для перевірки сертифікатів	Великі мережі IoT (розподілені системи, промислові мережі)	Складне управління сертифікатами

Аналіз методів захисту IoT-мереж показав, що вибір технології залежить від специфіки системи та її обмежень. Методи, такі як DTLS і PKI, забезпечують високий рівень безпеки для критичних і масштабованих систем, але потребують значних ресурсів. Натомість PSK і OSCORE є ефективними для малих і обмежених мереж, проте мають свої обмеження у масштабованості та інтеграції. Хешування та цифровий підпис є універсальними, але їхня ресурсомісткість може бути викликом для IoT-пристроїв із низькою потужністю. Таким чином, оптимальним рішенням є адаптація методів залежно від конкретних вимог та ресурсів мережі.

Висновок

У роботі проведено аналіз основних методів захисту IoT-мереж, включаючи DTLS, PSK, OSCORE, хешування та цифровий підпис, а також PKI. Отримані результати демонструють, що кожен із розглянутих методів має свої переваги та обмеження, які визначають доцільність їхнього використання залежно від специфіки IoT-системи.

DTLS і PKI забезпечують високий рівень безпеки, що робить їх придатними для критичних застосувань і великих масштабованих мереж, проте вони потребують значних обчислювальних ресурсів. PSK та OSCORE відзначаються низьким ресурсоспоживанням і простотою впровадження, що робить їх ефективними для малих і обмежених IoT-мереж, але вони менш підходять для великих систем через труднощі управління ключами та складність інтеграції. Хешування та цифровий підпис забезпечують універсальність і високий рівень безпеки, але їхня ефективність залежить від обраного алгоритму та доступних ресурсів.

Таким чином, вибір методу захисту IoT-мереж повинен враховувати особливості системи, рівень загроз і доступні ресурси пристроїв. Успішне поєднання різних методів у багаторівневій архітектурі безпеки дозволить створити ефективну стратегію захисту, адаптовану до сучасних викликів у сфері IoT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. RIVEST R., SHAMIR A., ADLEMAN L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems [Електронний ресурс] / RONALD RIVEST, ADI SHAMIR, LEONARD ADLEMAN. – 1978. – Режим доступу до ресурсу: https://people.csail.mit.edu/rivest/Rsapaper.pdf.
2. IoT Security Foundation. Best Practices for IoT Security [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.iotsecurityfoundation.org/best-practices/.
3. ALPERN B. PKI Overview and Use Cases [Електронний ресурс] / BRUCE ALPERN. – 2020. – Режим доступу до ресурсу: https://pki-solutions.com/wp-content/uploads/2020/PKI-Overview.pdf.
4. SCHNEIER B. Applied Cryptography: Protocols, Algorithms, and Source Code in C [Електронний ресурс] / BRUCE SCHNEIER. – 1996. – Режим доступу до ресурсу: https://www.schneier.com/books/applied_cryptography/.

Шестопал Роман Валерійович– студент групи КІТС-23М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: sestopalroma5@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Shestopal Roman – student of KITS-23M group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: sestopalroma5@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com