КЕРУВАННЯ КЛЮЧАМИ ШИФРУВАННЯ У БЕЗПРОВІДНІЙ MESH МЕРЕЖІ

Влах-Вигриновська Г.І., к.т.н., доцент, Рудий Ю.П., аспірант,
Національний університет "Львівська політехніка", Україна,
e-mail: halyna.i.vlakh-vyhrynovska@lpnu.ua

https://doi.org/10.23939/istcmtm2024.04.037

Анотація. Метод перевірено на чіпі LoRa EBYTE SX1262 з ESP-WROOM-32. Використовувалися алгоритми прогнозування часу оновлення. Бездротові мережі MESH важливі для забезпечення зв'язку в умовах, коли інфраструктура зв'язку обмежена або відсутня. У таких мережах управління ключами шифрування відіграє важливу роль у забезпеченні безпеки передачі даних. У роботі аналізуються існуючі підходи до управління ключами шифрування в бездротових мережах і пропонується метод оптимального оновлення ключів.

Ключові слова**.** Ключ, Бездротові сітчасті мережі, LoRa, Esp32, Криптографія

1. Вступ

Бездротові мережі MESH стають все більш важливими в сучасному світі, особливо в умовах, коли традиційна комунікаційна інфраструктура обмежена або повністю відсутня. Ці мережі дозволяють спілкуватися у віддалених районах, під час надзвичайних ситуацій, а також у ситуаціях військового конфлікту. Враховуючи відкритий характер бездротового каналу зв'язку та можливість будь-якого пристрою брати участь у комунікаціях, забезпечення безпеки передачі даних є критично важливим завданням [1-3].

Ключовим компонентом безпеки в таких мережах є ефективне керування ключами шифрування. Це включає створення, розповсюдження, зберігання та оновлення ключів. Ці ключі необхідні для захисту даних від несанкціонованого доступу та забезпечення цілісності інформації. Незважаючи на численні дослідження та розробки в цій галузі, існуючі підходи все ще мають низку недоліків, таких як висока обчислювальна складність, необхідність частого оновлення ключів та обмежені ресурси пристроїв, що використовуються в мережах MESH [4-7].

2. Недоліки

У поточних реалізаціях керування ключами в бездротових мережах MESH є кілька недоліків:

– Деякі методи вимагають частого оновлення ключів для підтримки безпеки, що може призвести до значного збільшення мережевого трафіку та додаткового навантаження на її компоненти.

– Пристрої, що використовуються в мережах MESH, часто мають обмежені ресурси, такі як пам'ять і потужність обробки, що ускладнює використання складних криптографічних алгоритмів і процедур керування ключами.

– Відкритий характер каналів бездротового зв'язку та широко відомі протоколи роблять мережі MESH вразливими до різних типів атак, таких як перехоплення, підробка та відтворення повідомлень.

– У децентралізованих мережах MESH немає центрального контролюючого органу, що ускладнює процес централізованого керування ключами та моніторингу безпеки мережі.

Побудова ефективних схем маршрутизації для зменшення завантаження каналу зв'язку є складним завданням, особливо в умовах динамічних змін мережі [7].

3. Мета

Метою цієї роботи є розробка та впровадження оптимізованої системи керування ключами шифрування для бездротових мереж MESH, яка відповідає сучасним вимогам безпеки та продуктивності.

4. Керування ключами шифрування у безпровідній MESH мережі

Бездротові мережі використовують як симетричні, так і асиметричні криптографічні алгоритми для забезпечення безпеки передачі даних.

Симетричні криптографічні алгоритми використовують один і той же ключ як для шифрування, так і для дешифрування даних. Це означає, що обидві сторони, які беруть участь в обміні даними, повинні мати доступ до одного секретного ключа. AES є найпоширенішим симетричним алгоритмом, який використовується в бездротових мережах завдяки високому рівню безпеки та ефективності. AES підтримує ключі довжиною 128, 192 і 256 біт [8].

Асиметричні криптографічні алгоритми використовують пару ключів: відкритий ключ для шифрування даних і закритий ключ для їх дешифрування. Відкритий ключ може бути відомий кожному, а закритий ключ зберігається в секреті.

ECC (Elliptic Curve Cryptography) забезпечує подібний рівень безпеки, як і RSA, але використовує менші ключі, що робить його більш ефективним для пристроїв з обмеженими ресурсами. Він використовується для шифрування даних, обміну ключами та цифрових підписів у бездротових сенсорних мережах та IoT.

Крипточіпи ATAES132A від Microchip Technology є важливим компонентом у забезпеченні безпеки пристроїв Інтернету речей (IoT) [9-12].

Ці чіпи розроблені для безпечної автентифікації, шифрування даних і керування ключами, що робить їх ідеальними для використання в різних додатках IoT. ATAES132A використовує унікальні секретні ключі для аутентифікації пристрою, забезпечуючи захист від втручання (рис.1). Чіп підтримує різні криптографічні операції, такі як HMAC (Hash-based Message Authentication Code) для автентифікації повідомлень. Чіп підтримує AES-128, який забезпечує високий рівень шифрування для захисту конфіденційності даних у режимах CTR (Counter) і CBC (Cipher Block Chaining).

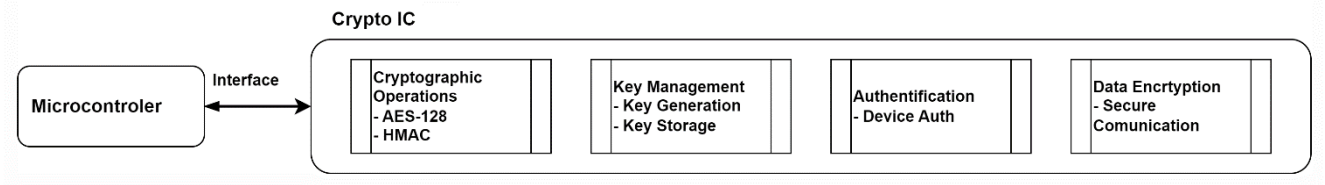

fig.1. Крипточіп ATAES132A

Крипточіп ATECC608A від Microchip Technology є потужним інструментом для забезпечення безпеки пристроїв Інтернету речей (IoT). Він забезпечує високий рівень безпеки завдяки використанню апаратних криптографічних можливостей, включаючи автентифікацію, шифрування даних і керування ключами. Чіп підтримує криптографічні операції ECC (Elliptic Curve Cryptography) для безпечної автентифікації, AES-128 і AES-256 для шифрування даних і SHA256 для генерації хеш-функцій, які забезпечують цілісність даних. Вбудовані алгоритми автентифікації дозволяють перевіряти автентичність пристроїв, що підключаються до мережі IoT, запобігаючи підключенню неавторизованих пристроїв.

Використання крипточіпів дозволяє реалізувати контроль доступу до ресурсів мережі на основі криптографічно захищених ідентифікаторів.

ATECC608A генерує пару ключів (приватний і відкритий) за допомогою ECC. Закритий ключ зберігається всередині чіпа і ніколи його не покидає, забезпечуючи високий рівень захисту. Відкритий ключ можна надіслати в CA (Certificate Authority) для видачі сертифіката. Інші пристрої в мережі можуть перевірити автентичність пристрою за допомогою сертифіката, виданого ЦС. ECDSA (Elliptic Curve Digital Signature Algorithm) використовується для цифрових підписів, які підтверджують автентичність повідомлень, надісланих пристроєм. ECDH (Elliptic Curve Diffie-Hellman) використовується для встановлення безпечних сеансів між пристроями, що забезпечує безпечний обмін даними.

Розглянемо системи сигналізації Ajax - одну з найбільш технологічно передових систем безпеки, яка використовує сучасні криптографічні методи для забезпечення високого рівня захисту даних і безпеки зв’язку між пристроями. Ajax використовує алгоритм AES-128 (Advanced Encryption Standard) для шифрування даних, що передаються між датчиками та центральним блоком (хабом). AES-128 забезпечує високий рівень безпеки завдяки складності алгоритму та довжині ключа. Шифрування виконується в режимі Cipher Block Chaining (CBC), що підвищує стійкість до криптографічних атак за рахунок залежності кожного блоку шифротексту від усіх попередніх блоків [13].

Для первинного обміну ключами між пристроями використовується асиметричний алгоритм RSA (Rivest-Shamir-Adleman). RSA дозволяє безпечно обмінюватися ключами шифрування без необхідності передачі фізичного ключа [14].

Після первинного обміну ключами RSA система може використовувати ECDH для обміну ключами сеансу, забезпечуючи швидкий і безпечний обмін ключами з меншими обчислювальними витратами. Для перевірки цілісності та автентичності повідомлень, що передаються між пристроями, Ajax використовує HMAC. Це гарантує, що повідомлення не було змінено під час передачі.

Передача нового ключа шифрування, зашифрованого індивідуальним ключем одержувача, використовується для забезпечення безпечного обміну ключами між відправником і конкретним одержувачем. Основна ідея полягає в тому, що новий ключ шифрування шифрується індивідуальним (відкритим) ключем одержувача, гарантуючи, що лише одержувач може його розшифрувати. Відправник генерує новий ключ шифрування сеансу (наприклад, AES-128). Новий ключ шифрування шифрується за допомогою відкритого ключа одержувача (наприклад, за допомогою RSA або ECC). Новий зашифрований ключ передається одержувачу по каналу зв'язку. Одержувач отримує зашифрований ключ і розшифровує його за допомогою свого закритого ключа. Тепер одержувач може використовувати новий ключ сеансу для шифрування та дешифрування наступних повідомлень.

Передача нового ключа шифрування, зашифрованого за допомогою ключа оновлення групи, використовується для оновлення ключів шифрування в групі пристроїв у Mesh-мережі (див. Малюнок 2). Новий ключ шифрування шифрується за допомогою ключа оновлення групи, який відомий усім пристроям у групі. Це дозволяє одночасно оновлювати ключі шифрування для всіх пристроїв у групі. Адміністратор або центральний пристрій генерує новий ключ шифрування сеансу. Новий ключ шифрування шифрується за допомогою ключа оновлення групи, який відомий усім пристроям у групі. Новий зашифрований ключ передається на всі пристрої в групі через безпечний канал зв’язку. Кожен пристрій у групі отримує зашифрований ключ і розшифровує його за

допомогою своєї копії ключа оновлення групи. Тепер пристрої можуть використовувати новий сеансовий ключ для шифрування та дешифрування наступних повідомлень.

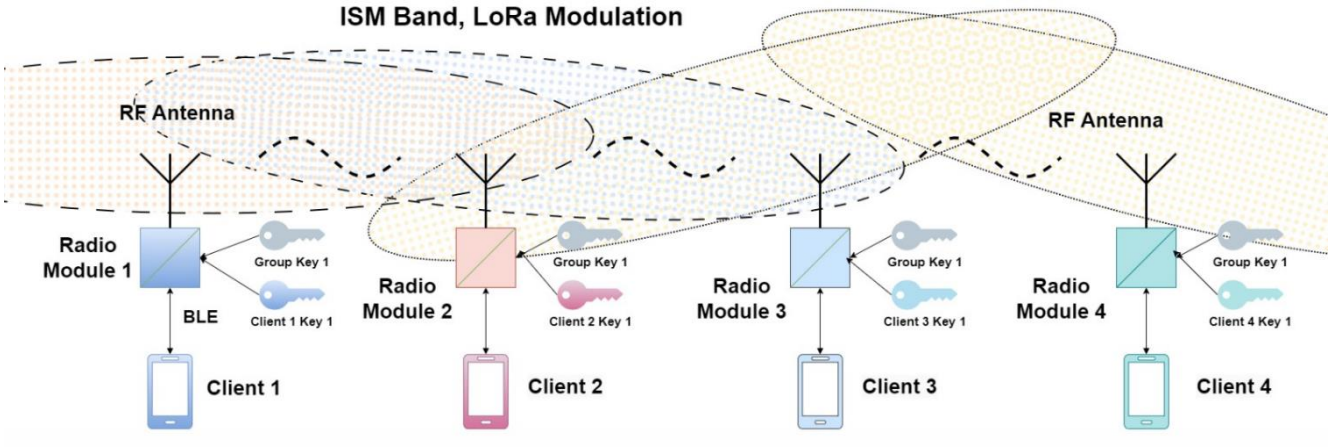

fig.2. Mesh network

При поширенні ключів шифрування ми можемо зіткнутися з проблемою радіочастотного шуму в певних областях мережі (рис.3). Це може бути наслідком як випадкових перешкод, так і наслідків свідомого придушення радіочастот засобами радіоелектронної боротьби. Щоб збільшити ймовірність доставки пакетів даних усім учасникам мережі, ми можемо ввести коефіцієнт повторної передачі, а також пріоритетність повідомлень. Також можуть бути використані методи псевдовипадкової стрибкоподібної зміни частоти.

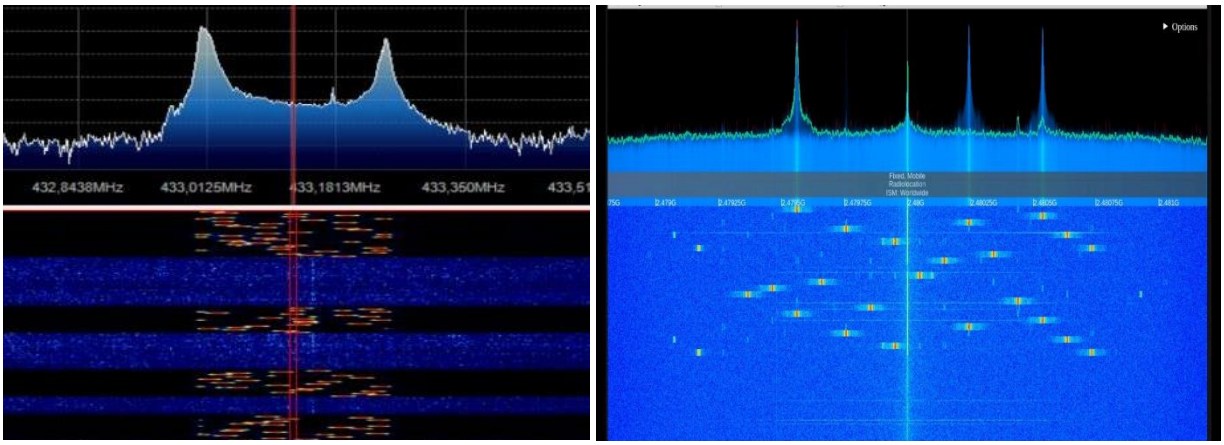

fig 3. Normal frequrency vs hopping

Для тестування алгоритмів за основу було використано програмне забезпечення з відкритим кодом Meshtastic [15]. Апаратна платформа складається з ESP32 Wroom, радіомодуля EBYTE E22 400M30S з трансивером SX1268 і приймача GPS (рис.4).

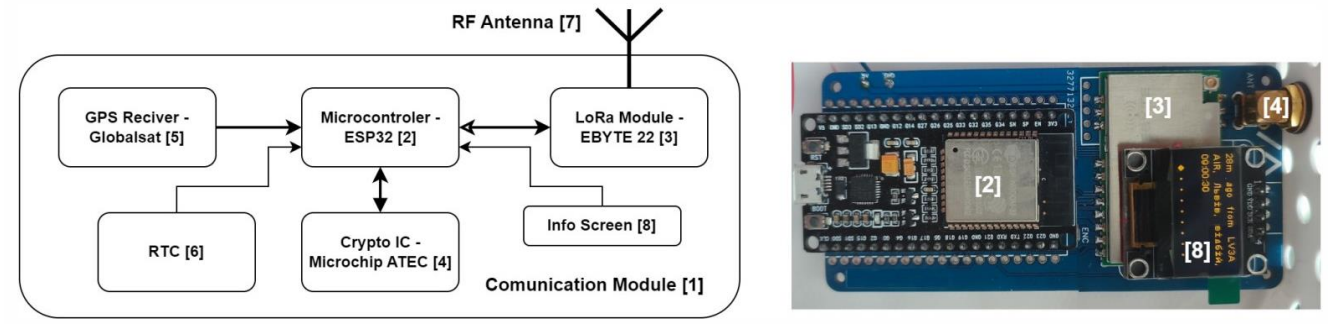

fig. 4. Тестова апаратна платформа

Важливу роль у цій схемі відіграє точна синхронізація часу всіх нод. GPS надає дуже точні мітки часу, що дозволяє всім вузлам у мережі мати узгоджений час. Це критично важливо для координації таких дій, як передача даних, оновлення ключів і виконання криптографічних операцій. Мітки часу використовуються для визначення моментів оновлення ключів шифрування. Це дозволяє автоматично та синхронно оновлювати ключі в мережі, забезпечуючи високий рівень безпеки. Розроблений сервіс дозволяє: переглядати список усіх пристроїв, їх стан, наявність живлення, параметри збережених ключів, час останнього обміну та рівень сигналу.

У меню керування ключами ми бачимо поточний мережевий ключ, термін дії та додаткові ключі, які

почнуть діяти через певний час.

Можна сформулювати запит на новий ключ, вказати тривалість його дії, умову, чи потрібне додаткове підтвердження готовності всієї мережі працювати з новими ключами (потрібно у випадках, коли деякі ноди не отримали новий ключ).

Також вказати рівень безпеки, а саме: чи повинен ключ передаватися зашифрованим груповим ключем або індивідуальним ключем (це необхідно в разі втрати або компрометації однієї із нод). У перехідний період, коли відбувається перехід на нові ключі шифрування, зберігається можливість розшифровки повідомлень старим ключем. Час не повинен перевищувати 5 секунд. Після цього старий ключ знищується в сховищі

Після підтвердження від усіх вузлів щодо оновлення ключів шифрування мережа може перейти на нові ключі.

Переваги системи:

1. Віддалене оновлення ключів шифрування повідомлень
2. Встановлення часових рамок дії ключа
3. Підтвердження оновлень від кінцевих вузлів
4. Протоколювання всіх подій
5. Рентабельність: зменшення витрат, пов'язаних зі змінами, відсутність фізичного підключення до кінцевих пристроїв і скорочення людино-годин для обслуговуючого персоналу».

Розглянемо процес безпечного керування ключами в малопотужних мережах IoT.

Оновлення ключів шифрування в LoRaWAN [7].

LoRaWAN (Long Range Wide Area Network) - це специфікація малопотужного бездротового зв'язку, яка використовує технологію LoRa для забезпечення широкого покриття. Оновлення ключів шифрування в LoRaWAN є важливим для підтримки безпеки мережі [16].

Основні типи ключів в LoRaWAN включають AppKey (Application Key), який відповідає за генерацію інших ключів під час процесу активації пристрою; NwkSKey (Network Session Key), який використовується для забезпечення цілісності та автентичності даних на мережевому рівні, і AppSKey (Application Session Key) для шифрування даних на прикладному рівні.

Процес оновлення ключів шифрування в LoRaWAN зазвичай відбувається під час реєстрації пристрою або під час використання процесу повторної активації. Існує два основних методи активації пристрою в LoRaWAN, кожен з яких має власний механізм оновлення ключа:

Метод Activation by Personalization (ABP) передбачає, що ключі встановлюються вручну та залишаються статичними протягом усієї роботи пристрою.

ABP має обмеження у безпеці, оскільки ключі ніколи не оновлюються, що може призвести до їх компрометації. У випадку компрометації ключів адміністратор мережі повинен вручну змінити ключі на пристрої та сервері.

Метод Over-the-Air Activation (OTAA) передбачає, що під час активації пристрій ініціює процес підключення до мережі через повідомлення Join Request. Пристрій надсилає повідомлення Join Request, яке містить DevEUI, AppEUI та DevNonce. Мережевий сервер відповідає повідомленням Join Accept, яке зашифровано за допомогою AppKey.

Після успішної активації за допомогою AppKey генеруються NwkSKey і AppSKey. Ці ключі використовуються для захисту подальших комунікацій між пристроєм і сервером. Ключі можуть бути автоматично оновлені під час повторної активації пристрою через OTAA, що забезпечує високу безпеку.

Регулярна повторна активація пристроїв за допомогою OTAA забезпечує часте оновлення ключів, що знижує ризик компрометації. DevNonce — це унікальний номер, який використовується під час кожної активації OTAA, щоб запобігти повторному використанню старих повідомлень Join Request. Ключі мають зберігатися в надійному місці на пристрої, наприклад у безпечній пам'яті або криптографічному модулі, який забезпечує додатковий рівень захисту від фізичних атак.

Керування ключами у NB-IoT.

NB-IoT (Narrow Band Internet of Things) є стандартом стільникового зв'язку, який пропонує надійний спосіб з'єднання багатьох малопотужних пристроїв на великих відстанях, дозволяючи їм обмінюватися невеликими обсягами даних [17].

У NB-IoT керування ключами має велике значення для безпечного зв'язку між пристроями та мережею. Процес складається з кількох етапів, починаючи з автентифікації пристрою та генерації ключа.

На першому етапі кожен пристрій NB-IoT ідентифікується за допомогою унікального IMSI (International Mobile Subscriber Identity), який зберігається на SIM-карті або eSIM.

Далі процес автентифікації пристрою виконується за допомогою Центру автентифікації оператора мережі (AuC), який підтримує IMSI разом із відповідними ключами Ki.

Ki (ключ автентифікації абонента), необхідний для генерації ключів автентифікації та шифрування, зберігається як на SIM-карті пристрою, так і в AuC.

Під час процесу автентифікації мережа надсилає на пристрій випадкове число, відоме як RAND (Random Number).

Використовуючи Ki та RAND, мережа генерує відповідь автентифікації (XRES) разом із ключем шифрування (CK) і ключем цілісності (IK).

Автентифікація.

Мережа надсилає RAND та запит на автентифікацію пристрою.

Пристрій використовує K_i та RAND для обчислення відповідей XRES, CK, IK за допомогою алгоритму.

Пристрій надсилає XRES назад у мережу.

Мережа обчислює очікуваний XRES та порівнює його з отриманим від пристрою. Якщо вони співпадають, пристрій аутентифікований.

Шифрування даних.

Ключ K_ASME (Access Security Management Entity Key) генерується з CK та IK і використовується для подальшої генерації ключів захисту рівня доступу.

Ключ K_eNB (eNodeB Key) генерується з K_ASME і використовується для захисту даних, що передаються між пристроєм та базовою станцією.

Ключ KRRC (Radio Resource Control Key) використовується для шифрування сигналізації на рівні RRC.

Ключ KUPenc (User Plane Encryption Key) використовується для шифрування даних користувача.

Ключі можуть оновлюватися періодично або за запитом оператора мережі для забезпечення додаткової безпеки. Оновлення ключів можна виконати за допомогою процесу повторної аутентифікації, що усуває необхідність повторно генерувати RAND і обчислювати нові ключі.

Можна сказати, що процес безпечного управління ключами в малопотужних мережах IoT є надзвичайно важливим для захисту даних і підтримки конфіденційності. Це включає регулярне оновлення ключів і автентифікацію пристроїв, що допомагає запобігти компрометації.

5. Висновки

Керування ключами для шифрування в бездротових мережах MESH є критично важливим аспектом забезпечення безпеки та надійності мережевого зв'язку. Розглянуті в статті методи та рекомендації підкреслюють необхідність комплексного підходу до генерації, обміну, зберігання та відновлення ключів. Можливість дистанційного оновлення певного кінцевого пристрою з підтвердженням є важливим елементом гнучкості та керованості мережі. Це дозволяє оперативно реагувати на потенційні загрози та забезпечує актуальність криптографічного захисту.

Групове оновлення через трансляцію на всі кінцеві пристрої з підтвердженням оновлення є ефективним методом масового оновлення ключа. Це забезпечує синхронізацію всіх пристроїв у мережі, підвищуючи загальну безпеку.

Встановлення терміну служби ключів і їх оновлень на основі GPS-синхронізації дозволяє підтримувати високу точність і постійність оновлень. Дослідження перехідних етапів оновлення ключів безпеки допомагає уникнути втрати даних і забезпечує безперервність роботи мережі.

Використання криптографічно безпечних алгоритмів, таких як RSA, ECC або DH, є основою надійного шифрування. Ключі повинні бути достатньо довгими, щоб запобігти атакам грубої сили, що підвищує загальний рівень безпеки.

Безпечне зберігання ключів на вузлах є критично важливим для захисту від фізичних атак. Використання апаратних модулів для зберігання ключів може значно підвищити рівень безпеки.

У цій статті розглядаються різні аспекти керування ключами шифрування в бездротових мережах MESH і надаються рекомендації щодо їх використання, наголошуючи на важливості надійного та ефективного керування ключами для забезпечення безпеки та надійності мережевого зв'язку.

Подяка

Автори висловлюють вдячність співробітникам кафедри інформаційно-вимірювальних технологій за допомогу в роботі.

Конфлікт інтересів

Автори не мають претензій один до одного.

Список літератури

[1] Hoa, L. V., & Vinh, T. Q. Real-time Key Management for Wireless Mesh Network. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), Vol. 10 No. 2-6, 2018, pp.13–18. Retrieved from https://jtec.utem.edu.my/jtec/article/view/4362

[2] Gianni D'Angelo, Francesco Palmieri. A hound-inspired pre-hybridized genetic approach for router placement in wireless mesh networks. Applied Soft Computing. Vol 166, 2024, p.112159, doi.org/10.1016/j.asoc.2024.112159

[3] R. Imam, Q.M. Areeb, A. Alturki, F. Anwer Systematic and critical review of RSA based public key cryptographic schemes: past and present status. IEEE Access, 9, 2021, pp. 155949-155976, doi.org/10.1109/ACCESS.2021.3129224

[4] Abdmeziem, M. R., & Ahmed Nacer, A., & Deroues, N.M (2024). Group key management in the Internet of Things: Handling asynchronicity. Future Generation Computer Systems, Volume 152, pp. 273-287, doi.org/10.1016/j.future.2023.10.023

[5] Bruno Ramos-Cruz , JavierAndreu-Perez, Luis Martínez. The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. Neurocomputing. Volume 581, p.1274277, 2024, doi.org/10.1016/j.neucom.2024.127427
[6] Osama A. Khashan a, Rami Ahmad b, Nour M. Khafajah. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad Hoc Networks. Vol 115, 2021, p. 102448, doi.org/10.1016/j.adhoc.2021.102448
[7] Abdmeziem, M. R., & Ahmed Nacer, A., & Deroues, N.M (2024). Group key management in the Internet of Things: Handling asynchronicity. Future Generation Computer Systems, Volume 152, pp. 273-287, doi.org/10.1016/j.future.2023.10.023
[8] Xueping Yan, Lin Tan, Hong Xu, Wenfeng Qi. Improved mixture differential attacks on 6-round AES-like ciphers towards time and data complexities. Journal of Information Security and Applications,Volume 80, 2024, p. 103661, doi.org/10.1016/j.jisa.2023.103661
[9] Miguel Antonio Caraveo-Cacep a b 1, Rubén Vázquez-Medina a 1, Antonio Hernández Zavala. A survey on low-cost development boards for applying cryptography in IoT systems. Internet of Things. Vol 22, 2023, p. 100743, doi.org/10.1016/j.iot.2023.100743.
[10] Antonio Muñoz, Ruben Ríos, Rodrigo Román, Javier López. A survey on the (in) security of trusted execution environments. Computers & Security. Vol 129, 2023, 103180, doi.org/10.1016/j.cose.2023.103180
[11] Kendall Niles a, Jason Ray a, Kenneth Niles a, Andrew Maxwell a, Anton Netchaev. Monitoring for Analytes through LoRa and LoRaWAN Technology. Procedia Computer Science. Vol 185, 2021, pp. 152-159, doi.org/10.1016/j.procs.2021.05.041
[12] Inc, Atecc608a, secure element to secure authentication. Accessed on 27.10.2022. www.microchip.com/en-us/product/ATECC608A
[13] Yasmeen Shaher Alslman1, Ashraf Ahmad1, Yousef AbuHour. Enhanced and authenticated cipher block chaining mode. Bulletin of Electrical Engineering and Informatics. Vol.12(4), 2023, pp. 2357-2362 doi:10.11591/beei.v12i4.5113
[14] R. Imam, Q.M. Areeb, A. Alturki, F. Anwer Systematic and critical review of RSA based public key cryptographic schemes: past and present status. IEEE Access, 9, 2021, pp. 155949-155976, doi.org/10.1109/ACCESS.2021.3129224
[15] Nil Llisterri Giménez, Joan Miquel Solé, Felix Freitag. Embedded federated learning over a LoRa mesh network. Pervasive and Mobile Computing. Vol 93, 2023, p.101819, doi.org/10.1016/j.pmcj.2023.101819
[16] Kun-Lin Tsai, Li-Woei Chen, Fang-Yie Leu, Chuan-Tian Wu. Two-Stage High-Efficiency Encryption Key Update Scheme for LoRaWAN Based IoT Environment. Computers, Materials and Continua.
Vol 73, №1, 2022, pp. 547-562, doi.org/10.32604/cmc.2022.026557
[17] S. Anbazhagan, R.K. Mugelan. Next-gen resource optimization in NB-IoT networks: Harnessing soft actor–critic reinforcement learning. Computer Networks. Vol 252, 2024,p. 110670, doi.org/10.1016/j.comnet.2024.110670