DOI: 10.18372/2225-5036.29.17871

ЗАСТОСУВАННЯ ЗБИТКОВИХ LDPC КОДІВ В СТАНДАРТІ LORAWAN

Сергій Погасій

Національний технічний університет "Харківський політехнічний інститут", Україна

ПОГАСІЙ Сергій Сергійович, к.е.н., доц.
Рік та місце народження: 1978, Харків, Харківська область, Україна.
Освіта: Харківський національний економічний університет, 1999. Посада: доцент кафедри кібербезпеки Національного технічного університету "Харківський політехнічний інститут", Україна Наукові інтереси: захист інформації у кіберфізичних системах.
Посада: доцент кафедри кібербезпеки та інформаційних технологій.
Наукові інтереси: захист інформації у кіберфізичних системах.
Публікації: більше 32 наукових публікацій, включаючи монографії, підручники, статті та патенти.
E-mail: spogasiy1978@gmail.com.
Orcid ID: 0000-0002-4540-3693.

Анотація. *В умовах зростання технологій Інтернет-речей, актуальною проблемою стає забезпечення безпеки інформації. Визначено, що найбільш перспективною бездротовою мережею зв'язку для Інтернету речей (IoT) на даний час є LoRaWAN. Однак пропрієтарна технологія модуляції та шифрування LoRa, "закрита" патентом Semetech, що приводить до кіберінцидентів з вилучення ключів із пристрою за допомогою реверс-інжинірингу; зламування мережі за допомогою облікових даних за замовчуванням або через вразливість та викрадення ключів із сервера. В якості засобу вдосконалення існуючого алгоритму пропонується інтеграція у існуючу апаратну частину IoT пристрою додаткового мікроконтролеру (засіб криптографічного захисту інформації) з вбудованими алгоритмами крипто-кодових конструкцій Мак-Еліса та Нідеррейтера на модифікованих LDPC кодах в для посилення алгоритмів шифрування технології LoRaWAN що застосовуються при передачі даних в середині мережі та для забезпечення безпеки зовнішнього контуру пропонується використовувати розроблений сервер, який фізично розміщується у місці де буде знаходитися шлюз з виходом до зовнішнього каналу зв'язку мережі інтернет.*

Ключові слова: *LoRaWAN, засіб криптографічного захисту інформації, крипто-кодові конструкції, збиткові LDPC коди.*

Постановка проблеми

Розвиток технологій Інтернету речей (IoT) з низьким споживанням енергії та високим покриттям є однією з ключових тенденцій у сфері IoT. Ця область технологій продовжує еволюціонувати і розвиватися, і наступні напрямки її розвитку особливо актуальні:

Подальше зменшення споживання енергії є основною метою в розвитку IoT. Розробники працюють над новими методами ефективного використання енергії, включаючи оптимізацію роботи мікроконтролерів, використання низькоенергетичних радіочастотних модулів і підтримку спеціалізованих акумуляторів та батарей. Мережі з низькими витратами енергії (LPWAN) використовують технології LoRaWAN, C-UNB і NB-IoT, набувають та все більшої популярності через їх велику покриття і низькі витрати енергії. Вони дозволяють підключити велику кількість пристроїв з довгим терміном служби батарей.

Розширення мереж IoT підвищує важливість боротьби зі загрозами безпеки та забезпечення конфіденційності даних. Розробники працюють над заходами безпеки на рівні пристроїв, мереж та даних.

Безпека в системах Інтернету речей (IoT) є критичним аспектом, оскільки ці системи зазвичай працюють з великою кількістю даних, комунікують з численними пристроями та впливають на реальний світ. Недотримання стандартів безпеки може призвести до вразливостей і ризиків для конфіденційності, цілісності та доступності даних. Важливо переконатися, що всі пристрої, які підключені до мережі IoT, відомі і автентифіковані перед тим, як отримати доступ до системи. Для кожного пристрою повинні бути налаштовані відповідні права доступу до ресурсів мережі. Для захисту конфіденційності даних, які передаються між пристроями і мережею, дані необхідно шифрувати. IoT-системи повинні бути захищені від різних типів атак, таких як атаки на внедрення, атаки на відмову в обслуговуванні (DoS) і атаки на видалений запуск коду. Захищеність системи має бути високою пріоритетом.

Забезпечення приватності особистих даних користувачів є надзвичайно важливим аспектом.

Дані повинні бути анонімізованими і захищеними від несанкціонованого доступу. Забезпечення безпеки в системах IoT вимагає комплексного підходу та постійного вдосконалення, оскільки загрози і технології постійно змінюються.

Задачі які будуть вирішенні в рамках даної роботи наступні:

- проаналізувати основні енергозберігаючі технології передачі даних на великі відстані;
- визначити найбільш перспективну бездротову мережу зв'язку для Інтернету речей (IoT) «останньої мілі»;
- дослідити можливість впровадження крипто-кодових конструкцій Мак-Еліса та Нідеррейтера на модифікованих LDPC кодах в алгоритми шифрування визначеної IoT технології.

Аналіз останніх досліджень і публікацій

Бездротові мережі зв'язку для Інтернету речей (IoT) грають критичну роль у забезпеченні зв'язку між IoT-пристроями і центральними системами, що дозволяє збирати, обробляти і передавати дані. Існує кілька бездротових IoT технологій, які використовуються для забезпечення споживачів Інтернету речей (IoT), і кожна з них має свої властивості та застосування (табл. 1). Ось кілька основних технологій для IoT:

Таблиця 1

Характеристика технологій бездротових мереж зв'язку (IoT)

Бездротові мережі IoT	Швидкість передачі даних	Покриття	Витрати енергії	Застосування	Діапазон роботи	Стандарт	Шифрування
Wi-Fi	54 (Mbps) до 30 (Gbps).	зона дії Wi-Fi маршрутизатора	Високі для багатьох IoT пристроїв, що працюють від батарей	Інтернет-речей в дому, офісі, завдяки високій швидкості і стабільності з'єднання	2400-2483,5 МГц	IEEE 802.11	AES
Bluetooth	1-2 Mbps	до 100 метрів	Залежить від версії Bluetooth; Bluetooth Low Energy (BLE) має низькі витрати	Зазвичай використовується для низькоресурсних пристроїв, таких як бездротові навушники, фітнес-трекери, сенсори	2402-2480 МГц.	EEE 802.15.1	алгоритм FHSS та Kinit і link key
Zigbee	2,4 ГГц - 250 Kbps 915 МГц 40 Kbps 868 МГц 20 кбіт/с	До 100 метрів розширене через маршрутизатори	Зазвичай низькі, ідеально для батарейних пристроїв	Зазвичай використовується для розумних будинків та мережі сенсорів	2,4 ГГц, 915 МГц, 868 МГц	IEEE 802.15.4	128 AES
LoRa	5 - 50(Kbps)	1—20 км	Дуже низькі	Далекий моніторинг і керування віддаленими об'єктами, такими як сільське господарство або моніторинг стану інфраструктури	ISM-діапазони (170, 433, 868 , 915 МГц)	LoRaWAN	128 AES: AES-CMAC, AES-CCM
NB-IoT	20-200 (Kbps).	покриття на основі LTE 4G	дуже низькі, ідеально для батарейних пристроїв	глобальне IoT-з'єднання для різних застосувань, включаючи моніторинг, віддалену команду і вимірювання	B20 (800МГц), B8(900МГц, B3(1800МГц)	3GPP (3	LTE-шифрування
C-UNB	До 20 (Kbps)	1-40	низькою споживаною енергією	моніторинг активів, логістика, сільське господарство.	ISM- 868 МГц до 869 МГц.	пропрієтарні технології	(AES) або симетричні методи шифрування
EC-GSM	200 (bps) до 1 (Mbps),	існуюча мережа GSM,	споживає більше енергії порівняно з іншими, базується на існуючому стандарті GSM	місця зі слабким сигналом, такі як внутрішні приміщення або важкодоступні області.	існуючий діапазон GSM	розширення стандарту GSM	A5/1, A5/2 та A5/3 шифрування

Як бачимо з даних таблиці 1 найбільш привабливими варіантами є чотири основні види технологій LPWAN: C-UNB, LoRa, EC-GSM і NB-CIoT, що відповідають поставленим завданням. З рисунку 1 можна визначити, що обсяг ринку цих технологій продовжує зростати і оцінюється на мільярди доларів. Важливо враховувати, що точні цифри можуть варіюватися в залежності від джерела і регіону, а також враховувати обсяги обладнання, послуг і платформ, пов'язаних із сегментом IoT. Загалом, ринок IoT продовжує демонструвати стабільний ріст, і ці технології займають важливу позицію в екосистемі IoT, надаючи різнобарвні можливості підключення для різних застосувань і галузей (рис. 1).

За обсягом ринку лідируючи позиції у цьому сегменті виробництва абонентських пристроїв утримає LoRaWAN та NB-IoT. Хоча обидві мережі зазвичай підтримують геолокацію приблизно з однаковим ступенем, між ними є деякі відмінності. LoRaWAN споживає менше енергії, ніж NB-IoT, що робить його

ідеальним для будь-якого проекту, що потребує високої частоти оновлення. Батарея його пристроїв може тривати до п'ятнадцяти років, порівняно з десятьма роками NB-IoT. Однак останній має кращу пропускну здатність, ніж перший [3].

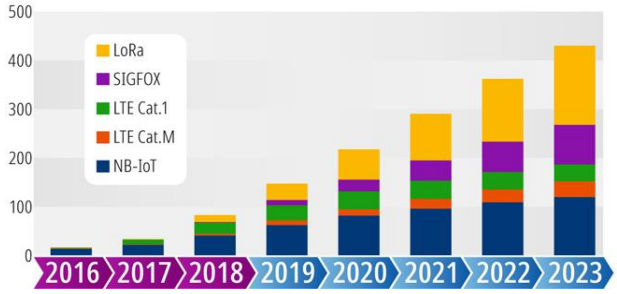

Рис.1. Статистика и прогноз поставок абонентських пристроїв IoT (млн шт.) [1, 2]

Мета та постановка завдання

Головна мета статті – визначити найбільш ефективну бездротову енергозберігаючу технології передачі даних (IoT) на великі відстані, для подальшого вдосконалення її механізма безпеки за допомогою шифрування каналів передачі даних на основі модифікованих LDPC кодах.

Виклад основного матеріалу дослідження

На основі аналізу останніх досліджень і публікацій, ми дійшли висновку, що використання протоколу LoRaWAN у світі Інтернету речей (IoT) є одним найбільших на ринку енергозберігаючих бездротових технологій, завдяки здатності забезпечувати дальній та ефективний бездротовий зв'язок для IoT-пристроїв.

Однією з головних переваг LoRaWAN є здатність працювати на великій відстані від базової станції, що робить його ідеальним для використання в віддалених областях на низьких потужностях. Мережі LoRaWAN легко масштабуються для обслуговування великої кількості пристроїв, що робить його підходящим для масштабних IoT-проектів у сфері розумних міст, промислового виробництва і транспорту. Для створення цих мереж не потрібно великої інфраструктури або дорогої обладнання. Це робить його вигідним з економічної точки зору.

Однак відкритий стандарт LoRaWAN приводить до того, що стандартні пристрої можуть працювати в різних мережах LoRaWAN , це сприяє інтероперабельності та вибору між різними постачальниками обладнання та мережевих послуг і в той же самий час несе загрозу безпеці як самих пристроїв так і каналів зв'язку у середині мережі.

Конструкція безпеки LoRaWAN відповідає принципам: використання стандартних, перевірених алгоритмів та наскрізної безпеки, фундаментальні властивості, системі безпеки включають:

- взаємна автентифікація;
- захист цілісності;
- захист конфіденційності.

Архітектура мережі LoRaWAN забезпечує конфіденційність даних. Вона зберігається у процесі проходження всього ланцюжка задіяних пристроїв.

Вміст пакета даних на всіх стадіях процесу залишається доступним тільки відправнику (кінцевому пристрої) та одержувачу (додатку), якому він призначається.

У мережі IoT LoRaWAN використовується багаторівнева система безпеки передачі даних. Загальна схема безпеки даних у мережі LoRaWAN представлена на рис. 2.

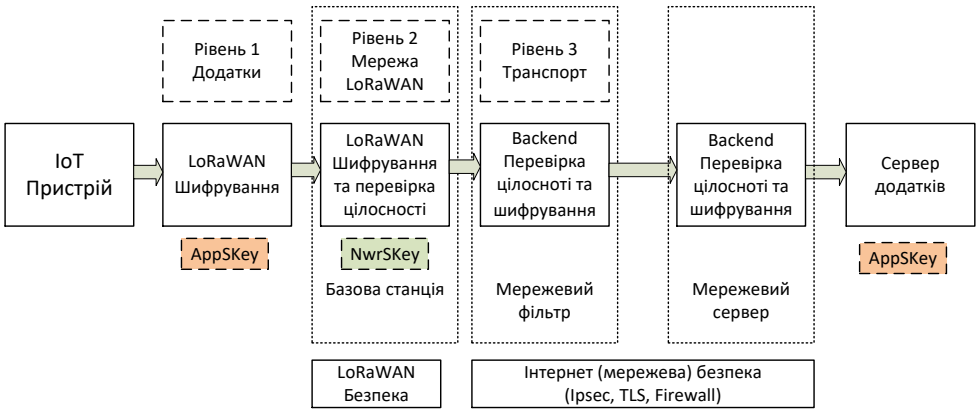

Рис.2. Загальна схема безпеки даних у мережі LoRaWAN [4]

Перший рівень має AES-шифрування на рівні програми (між абонентським терміналом та сервером додатків) за допомогою 128 бітного змінного сесійного ключа Application Session Key (AppSKey) Цей ключ шифрування зберігається в абонентському терміналі та на сервері програм і недоступний оператору мережі (доступ до AppSKey є тільки у клієнта-власника сервера програм). Формування сесійного ключа AppSKey відбувається паралельно в абонентському терміналі та на стороні мережі під час процедури активації терміналу, а через ефір AppSKey не передається.

Другий рівень передбачає AES-шифрування та перевірку цілісності повідомлень на мережному рівні

(між абонентським терміналом та мережним сервером) за допомогою 128 бітного змінного сесійного ключа Network Session Key (NwkSKey) Цей ключ шифрування також зберігається в абонентському терміналі та на мережевому сервері і недоступний клієнту (доступ до NwkSKey є лише у оператора мережі-власника мережного сервера). Формування сесійного ключа NwkSKey також відбувається паралельно в абонентському терміналі та на стороні мережі під час процедури активації терміналу, а через ефір NwkSKey не передається.

Третій рівень включає стандартні методи аутентифікації та шифрування інтернет-протоколу (IPsec, TLS тощо) під час передачі даних по транспортній мережі між вузлами мережі (базова станція, мережевий сервер, join-сервер, сервер додатків).

Мережевий сервер працює з даними у виключно зашифрованому вигляді. Сервер здійснює аутентифікацію та перевіряє цілісність кожного пакета, але при цьому не має доступу до інформації від підключених сенсорів. Виняток становить лише застосування нерекомендованих сценаріїв. Вони шифрування корисного навантаження виконує мережевий сервер з допомогою ключа NwkSKey, а чи не сервер додатків. Але ми не розглядатимемо такий спосіб обробки даних.

Доступно два режими активації кінцевих пристроїв, а саме:

- повітряна активація – Over-The-Air Activation (OTAA);

- активація персоналізацією - Activation by Personalization (ABP).

Активація по повітрю – Over-The-Air Activation (OTAA) При активації повітрям кінцеві пристрої LoRa не прив'язані жорстко до якоїсь конкретної мережі (рис. 3). На кінцевих пристроях LoRa прописуються ідентифікатор пристрою (DevEUI), ідентифікатор програми (AppEUI) та ключ програми (AppKey). Кінцевий пристрій під час активації ініціює JOIN процедуру. Ключі шифрування (AppSKey і NwkSKey), необхідні передачі інформації, обчислюються самим кінцевим пристроєм. Такий метод активації рекомендований для використання. Він забезпечує високий рівень безпеки.

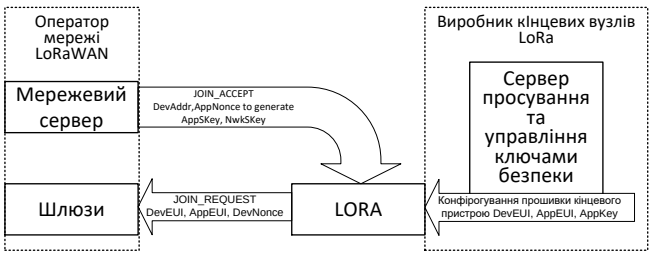

Рис.3. Активація по повітрю (OTAA)

Активація персоналізацією – Activation by Personalization (ABP) При активації персоналізацією кінцеві пристрої жорстко прописуються до роботи у конкретній мережі оператора (рис. 4).

Рис.4 Активація персоналізацією ABP

Кінцеві пристрої прошиваються з певними мережевим ключем (NwkSKey) та ключем програми (AppSKey). Такий метод активації не рекомендується використовувати для комерційних мереж. Це пояснюється низьким рівнем безпеки даних та складністю реалізації.

За командою програми чи мережевого сервера у будь-який момент можливий перехід на нову сесію з генерацією нового комплекту ключів шифрування, що робить непотрібними старі ключі шифрування. Також є можливість встановити періодичну генерацію нового комплекту ключів NwkSKey та AppSKey.

Однак, як виявили дослідники, зловмисник може отримати ключі шифрування LoRaWAN для здійснення DDoS-атак та відправлення мереж підроблених даних. Більше того, в даний час організації ніяк не можуть дізнатися, чи знаходяться їх мережі LoRaWAN під атакою, і чи були скомпрометовані ключі шифрування, що суттєво ускладнює захист.

Дослідники виявили кілька способів отримання ключів LoRaWAN шифрування. Сюди входять: вилучення ключів із пристрою за допомогою реверс-інжинірингу; отримання ключів із тегів, що відображають код, який адміністратор забув видалити перед розгортанням пристрою; отримання вихідного коду пристрою із відкритих репозиторіїв або сайту виробника; отримання ключів шляхом перебору; зламування мережі за допомогою облікових даних за замовчуванням або через вразливість та викрадення ключів із сервера.

Інші способи включають: компрометацію систем виробника пристрою, відповідального за встановлення прошивки; зламування комп'ютера фахівця, відповідального за розгортання пристрою, де можуть зберігатися ключі шифрування; отримання ключів із флеш-накопичувачів або електронних листів виробника або його клієнтів; отримання AppKey за допомогою брутфорсу.

Отримавши ключі шифрування, зловмисники можуть здійснити низку атак, здатних призвести до серйозних наслідків. Оскільки в даний час способів виявлення атак на LoRaWAN не існує, пропонується впровадити додаткові засобів кодування (шифру-

вання) при передачі повідомлень, що буде використовуються в стандарті LoRaWAN рівні шифрування AES-128 можуть бути доповнені одним із алгоритмів на основі ССС Мак-Еліса та Нідеррайтера на LDPC-кодах [4]. Для цього пропонується при виробництві абонентських терміналів LoRaWAN встановлювати в пристрої додатковий мікроконтролер СКЗІ (засіб криптографічного захисту інформації), В якості такого мікроконтролера можуть бути використані мікропроцесори ESP-WROOM-32 , що мають невеликі розміри та мале енергоспоживання і може виконувати роль шлюзу з пристроями WiFi 802.11. Нижче представлено схему безпеки даних у мережі LoRaWAN з додатковим рівнем СКЗІ (рис. 5).

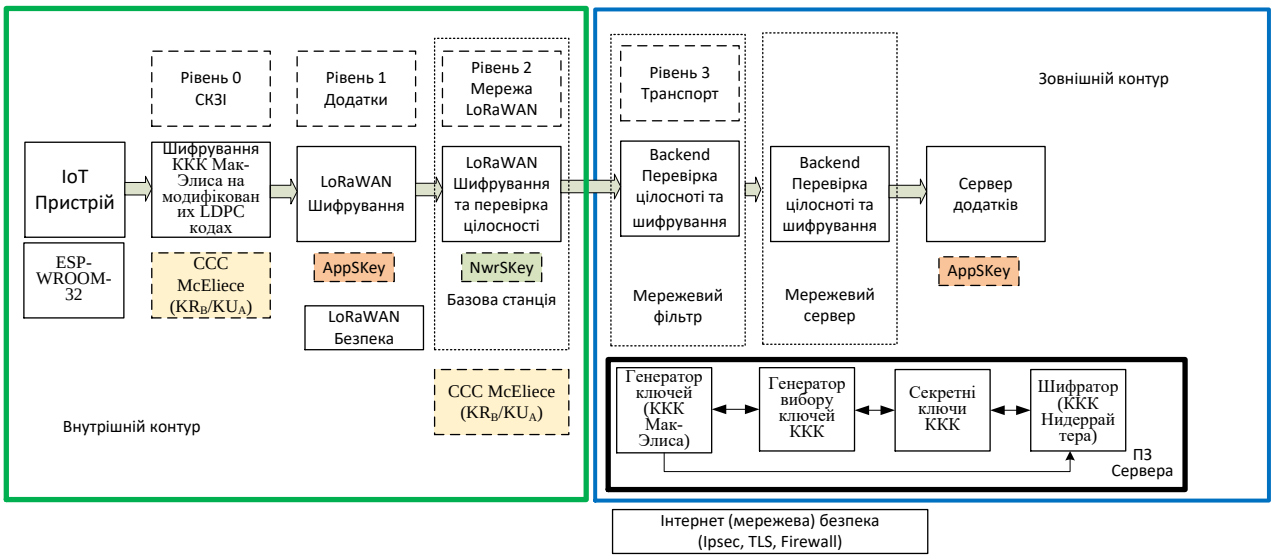

Рис.5. Схема безпеки даних у мережі LoRaWAN з додатковим рівнем СКЗІ

Ключ шифрування рівня СКЗІ SubSKey прошивається в абонентський термінал LoRaWAN при виробництві, так само як і кореневий ключ першого і другого рівнів шифрування LoRaWAN, або впроваджується в термінал разом з мікроконтролером СКЗІ при (використовуючи спеціальний слот). Дешифрація даних рівня СКЗІ проводиться на території замовника сервером програм після дешифрації рівня програми сесійним ключем AppSKey. Ключ шифрування SubSKey передає клієнту разом із датчиком безпосередньо виробник абонентського терміналу, і цей ключ недоступний співробітникам оператора мережі LoRaWAN.

Додатковий мікроконтролер СКЗІ забезпечує шифрування цифрового повідомлення на основі ССС Мак-Еліса. Після цього зашифроване повідомлення передається через LoRa-каналдо базової станції. При цьому використовуються стандартні протоколи LoRaWAN. Це дозволяє забезпечувати конфіденційність передачі даних без урахування вимог каналу зв'язку, вимог виробників чіпсету LoRa, не враховувати їх модифікації та технології Інтернет.

Крім цього, використання програмно-апаратної реалізації шифратора СКЗІ у вигляді чіпсету дозволяє суттєво знизити витрати на виробництво та реалізацію цього підходу. Для безпеки в IoT пристроях записується тільки сеансовий пароль залежно від ролі (відправник, одержувач), які записуються з мобільного додатка.

Після закінчення сеансу вони видаляються. При цьому в чіпсеті СКЗІ реалізується шифратор ССС Мак-Еліса. Забезпечення безпеки передачі ключових даних між програмою та сервером забезпечується ССС Нідеррайтера. Для забезпечення безпеки серверної частини після генерації ключів для передачі даних IoT та їх передачі відправнику та одержувачу проводиться обнулення ВП сервера, що забезпечує тунелювання каналу між користувачами. Секретні ключі крипто-кодових конструкцій Мак-Еліса та Нідеррайтера змінюються з різними проміжками часу і є OTP-ключами (сеансовими ключами).

Використання постквантових несиметричних криптосистем забезпечить необхідний рівень захищеності при забезпеченні послуг безпеки. Використання кодів LDPC дозволяє без істотних змін використовувати мобільні бездротові технології на основі стандартів LoRaWAN. Кіберфізична система управляє комплексом автономних систем, кожна з яких управляє певними IoT пристроями в, поєднуючи їх загальну кіберфізичну систему. Однак для забезпечення безпеки зовнішнього контуру (системи керування та зберігання інформації) пропонується використовувати розроблений сервер, який фізично розміщується у місці де буде знаходитися шлюз з виходом до зовнішнього каналу зв’язку мережі інтернет.

Кожна система відправляє пакет даних на локальний сервер, що дозволяє управляти Загальною кіберфізічною системою без інтернету, перебуваючи в тій

же локальній мережі (будучи підключеним до Базової станції Lora). Інформація в мережі кіберфізичної системи передається відкритими бездротовими каналами з шифруванням на основі ССС Мак-Еліса і Нідеррайтера на LDPC-кодах [5, 6].

Такий підхід забезпечує послуги безпеки, а за рахунок використання локального сервера управління забезпечує зниження ймовірності цільових атак на отримання несанкціонованого доступу до rs,thaspbxyj] cbcntvb. Також підхід забезпечує необхідний рівень безпеки при використанні мобільних програм управління, на основі використання ССС Мак-Еліса і Нідеррайтера на LDPC-кодах. Для забезпечення безпеки бази даних можуть використовуватись ССС Мак-Еліса та Нідеррайтера на ЄС (МЕС), що значно ускладнить можливість реалізації кібератак класу R2L (Remote to Local (user) Attack – віддалена атака на локального користувача) [7, 8].

Висновки. В роботі проаналізовано основні енергозберігаючі технології передачі даних на великі відстані в результати чого визначено, що найбільш перспективною бездротовою мережею зв'язку для Інтернету речей (IoT) на даний час є LoRaWAN. Ця мережа має велику дальність передачі радіосигналу, порівняно з іншими бездротовими технологіями, що застосовуються для телеметрії, сягає 10-20 км. Низьке енергоспоживання кінцевих пристроїв, завдяки мінімальним витратам енергії на передачу невеликого пакету даних. Висока здатність радіосигналу, що особливо проникає, що особливо важливо в міській забудові, за рахунок використання частот субгігагерцового діапазону. Висока масштабованість мережі на великих територіях. Відсутність необхідності отримання частотного дозволу та плати за радіочастотний спектр внаслідок використання неліцензованих частот (ISM band). Однак ця технологія має ряд недоліків - відносно низька пропускна здатність. Вона варіюється в залежності від технології передачі даних на фізичному рівні і становить від декількох сотень біт/с до декількох десятків кбіт/с.

Певна затримка передачі даних від датчика до кінцевої програми, пов'язана з часом передачі радіосигналу. Період затримки може становити від кількох до кількох десятків секунд. Відсутність єдиного стандарту, який визначає фізичний шар та керування доступом до середовища для бездротових LPWAN-мереж. Ризики шуму спектру неліцензованого діапазону частот. Пропрієтарна технологія модуляції та шифрування LoRa, "закрита" патентом Semetech, що приводить до інтендантів з вилучення ключів із пристрою за допомогою реверс-інжинірингу; отримання ключів із тегів, що відображають код, отримання вихідного коду пристрою із відкритих репозиторіїв або сайту виробника; отримання ключів шляхом перебору; зламування мережі за допомогою облікових даних за замовчуванням або через вразливість та викрадення ключів із сервера.

На основі отриманої інформації було запропоновано встановлювати в пристрої додатковий мікроконтролер СК3І(ESP-WROOM-32) з вбудованими алгоритмами крипто-кодових конструкцій Мак-Еліса та Нідеррейтера на модифікованих LDPC кодах в алгоритми шифрування технології LoRaWAN для передачі даних в середині мережі та для забезпечення безпеки зовнішнього контуру пропонується використовувати розроблений сервер, який фізично розміщується у місці де буде знаходитися шлюз з виходом до зовнішнього каналу зв′язку мережі інтернет.

Список літератури

[1]. Y. Feng, W. Wang, Y. Weng and H. Zhang, "A Replay-Attack Resistant Authentication Scheme for the Internet of Things," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2017, pp. 541-547, DOI: 10.1109/CSE-EUC.2017.101.

[2]. Singh, S., Sharma, P.K., Moon, S.Y. et al. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput (2017). https://doi.org/10.1007/s12652-017-0494-4.

[3]. 3GPP Release 13 Specification //https://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/.

[4]. LoRaWAN® Is Secure (but Implementation Matters)//https://lora-alliance.org/resource_hub/lorawan-is-secure-but-implementation-matters/.

[5]. Jan Broul´ım. LDPC codes - new methodologies / PhD thesis, University of West Bohemia, August 2018, p. 127.

[6]. Hai Zhu, Liqun Pu, Hengzhou Xu, and Bo Zhang. Construction of Quasi-Cyclic LDPC Codes Based on Fundamental Theorem of Arithmetic / Wireless Communications and Mobile Computing, Volume 2018, Article ID 5264724, 9 pages. https://doi.org/10.1155/2018/5264724.

[7]. S. Yevseiev, H. Kots, and Y. Liekariev, "Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system", Eastern-European Journal of Enterprise Technologies, 6/4(84), 2016, pp. 11-23.

[8]. S. Yevseiev, S. Pohasii, V. Khvostenko. Development of a protocol for a closed mobile internet channel based on post-quantum algorithms. Системи обробки інформації. 2021. № 3(166). С. 35-40. https://doi.org/10.30748/soi.2021.166.03.

УДК 681.32:007.5

Pohasii S. Application of harmful ldpc codes in the lorawan standard

***Abstract**. In the conditions of the growth of Internet of Things technologies, ensuring information security is becoming an urgent problem. It has been determined that LoRaWAN is currently the most promising wireless communication*

network for the Internet of Things (IoT). However, the proprietary LoRa modulation and encryption technology is "covered" by Semetech's patent, leading to cyber-incidents of reverse-engineering keys from the device; hacking the network using default credentials or vulnerability and stealing keys from the server. As a means of improving the existing algorithm, it is proposed to integrate into the existing hardware part of the IoT device an additional microcontroller (a means of cryptographic protection of information) with built-in algorithms of McEliece and Niederreiter crypto-code structures on modified LDPC codes in order to strengthen the encryption algorithms of LoRaWAN technology used in data transmission in the middle of the network and to ensure the security of the external circuit, it is suggested to use a developed server, which is physically located in the place where the gateway with access to the external communication channel of the Internet will be located.
***Key words**: LoRaWAN, means of cryptographic protection of information, crypto-code structures, loss-making LDPC codes.*

Погасій Сергій Сергійович, кандидат економічних наук, доцент кафедри кібербезпеки та інформаційних технологій Національного технічного університету "Харківський політехнічний інститут".

Serhii Pogasii, candidate of economic sciences, associate professor of the department of cyber security and information technologies of the National Technical University "Kharkiv Polytechnic Institute".

Отримано 4 *липня 2023 року*, затверджено редколегією *28 серпня 2023 року*