УДК 004.89

АНАЛІЗ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ ЗА ТЕХНОЛОГІЄЮ LORAWAN

Міночкін Д.А., Рибак О.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: alex96.rybak@gmail.com

The analysis of security Internet of Things on technology LoRaWAN

The theme of security is topical in almost any area of the Internet, Internet of Things (IoT) and Industrial Internet of Things (IIoT). Security has not always been taken into account when developing products. This is a big problem that deserves attention. Some IoT products come with outdated operating systems in their embedded form. Thus, all the benefits of new technologies should be achieved only in a safe environment.

Стек протоколів LoRaWAN представлений на рисунку 1. Схема складається з прикладного рівня, MAC рівня і фізичного рівня [1]. Дані з прикладного рівня відображаються в корисне навантаження MAC. Рівень MAC створює кадр MAC з використанням корисного навантаження MAC. Корисне навантаження MAC містить заголовок кадру (що містить адресу джерела і призначення, а також лічильник кадрів), порт кадру і корисне навантаження кадру (що містять дані додатків). Порт кадру використовується для визначення, чи містить кадр тільки команди MAC. Нарешті, рівень PHY використовує кадр MAC як корисне навантаження PHY і створює кадр PHY після вставки преамбули, заголовка PHY.

Рис. 1. Стек протоколу LoRaWAN.

Оскільки для будь-якої бездротової мережі вкрай важливо забезпечити безпеку, LoRaWAN використовує два рівня безпеки, один для мережі і один для прикладного рівня. Безпека мережевого рівня забезпечує справжність пристрою в мережі. Безпека на рівні додатків гарантує, що оператор мережі не має доступу до даних кінцевого користувача. Кінцевий пристрій (вузол) має бути

активовано, перш ніж сенсор зможе обмінюватися даними в мережі LoRaWAN. У мережах LoRaWAN доступні два методи активації: OTAA і ABP.

Активація по повітрю (OTAA). Цей метод заснований на бездротових повідомленнях про приєднання. Кожний кінцевий пристрій (вузол) розгортається з 64-біт DevEUI, 64-біт AppEUI і 128-біт AppKey. DevEUI є унікальним ідентифікатором для пристрою, який має 64-розрядний адрес, який можна порівняти з MAC-адресою для пристрою TCP/IP. AppKey використовується для криптографічного підпису запиту на приєднання, також AppKey використовується, коли вузол відправляє повідомлення запиту на з'єднання, як показано на рисунку 2. Вузол відправляє повідомлення запиту на з'єднання, що складається з його AppEUI і DevEUI. Крім того, він відправляє DevNonce, який є унікальним, випадково згенерованим двобайтовим значенням, використовуваним для запобігання атак [2].

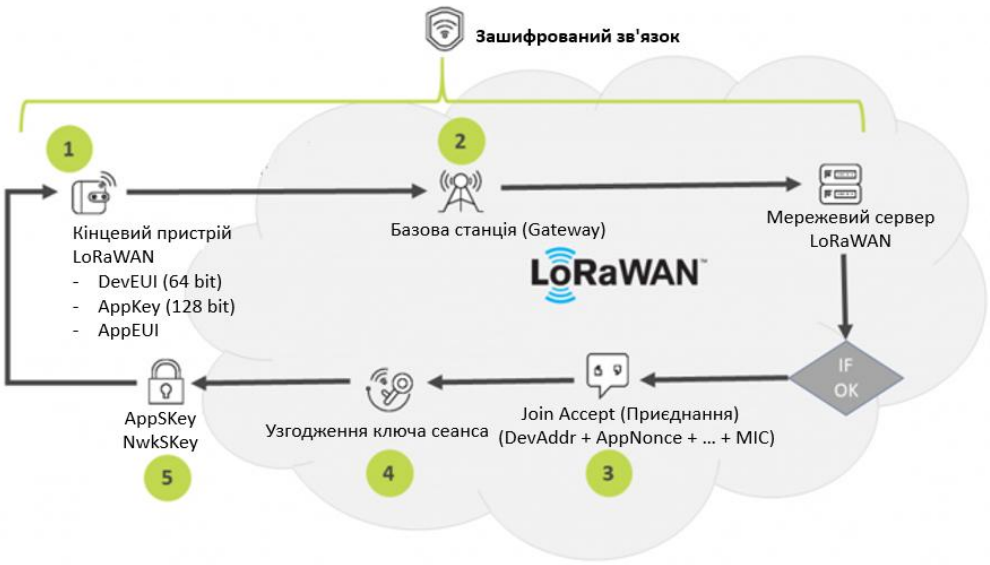

Рис. 2. Метод OTAA в LoRaWAN.

Ці три значення підписані 4-байтовим MIC (код цілісності повідомлення) з використанням AppKey пристрою. Сервер приймає запити на приєднання тільки від пристроїв з відомими значеннями DevEUI і AppEUI при перевірці MIC за допомогою AppKey.

Рис. 3: Елементи повідомлення LoRaWAN.

Якщо сервер приймає запит на приєднання, то відповідається пристрою повідомленням про приєднання. Сервери додатків і мережі обчислюють два 128-бітних ключа вузла: ключ сеансу додатка (AppSKey) і ключ сеансу мережі (NwkSKey) відповідно. Вони розраховуються на основі значень, відправлених в повідомленні запиту на приєднання від кінцевого пристрою (вузла), крім того, сервер додатків генерує своє власне одноразове значення: AppNonce. Це ще одне унікальне, випадкове згенероване значення. Відповідь Join Accept включає в себе AppNonce, NetID і адреса кінцевого пристрою (DevAddr), а також дані конфігурації для затримок RxDelay і використовуваних каналів (CFList). Join Accept є 32-бітовим ідентифікатором, який є унікальним в мережі. При отриманні даних назад, дані шифруються за допомогою AppKey. Потім вузол використовує AppKey для дешифрування даних і отримує AppSKey і NwkSKey, використовуючи значення AppNonce, отримане у відповіді Join Accept.

Активація методом персоналізації (ABP). Цей метод відрізняється від OTAA тим, що вузли поставляються з DevAddr і обома сеансовими ключами (NwkSKey і AppSKey), які повинні бути унікальними для вузла. Оскільки вузли вже мають необхідну інформацію і ключі, вони можуть почати зв'язок з сервером без необхідності обміну повідомленнями про приєднання. Після того, як вузол приєднався до мережі LoRaWAN - через OTAA або ABP - всі майбутні повідомлення будуть зашифровані та підписані з використанням комбінації ключа мережевого сеансу (NwkSKey) та ключа сеансу додатка (AppSKey). Ці два сеансових ключа (NwkSKey і AppSKey) є унікальними для кожного пристрою і для кожного сеансу. Якщо пристрій динамічно активується (OTAA), ці ключі відновлюються при кожній активації. Якщо пристрій статично активовано (ABP), ці параметри залишаються незмінними до тих пір, поки вони не будуть змінені вручну [3].

Висновок. Стандарт LoRaWAN вже містить порівняно високий ступінь безпеки та з кожним роком стає все більш досконалим завдяки LoRa Alliance, який постійно працює над поліпшенням стандарту. В цій статті було представлено, якими способами можна зареєструвати кінцеві пристрої (вузли) в мережі Інтернету Речей за технологією LoRaWAN та яким чином відбувається шифрування. LoRa Alliance - це некомерційна асоціація організацій, які працюють разом для стандартизації мереж LPWAN [4].

Література

1. Security in LoRaWAN Applications (2018). [Online]. Available: https://smartmakers.io/en/ security-in-lorawan-applications/, Accessedon: Oct. 9,2018.
2. R. Miller. (2016, June). LoRa Security Building a Secure LoRa Solution. Presented at BSides 2016 Conference. [Online]. Available: http://bit.ly/ mwr-lora-security, Accessed on: Jun. 5, 2017.
3. J. Daemen, V. Rijmen, The Design of Rijndael, AES - The Advanced Encryption Standard. Springer-Verlag, Berlin, Heidelberg, Germany, 2002.
4. LoRa specification provided by LoRa Alliance (2015). [Online]. Available: http://bit.ly/LoRaWAN-specification,Accessedon:Jun.1,2017.