АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В БЕЗДРОТОВІЙ МЕРЕЖІ LORAWAN

Болінова М.М.
Науковий керівник – доц. Ликов Ю. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. КРіСТЗІ, тел. (057) 702-14-30)
e-mail: maryna.bolinova@nure.ua

This article is devoted to the importance of data security in the LoRaWAN network. This report describes the principles of encrypting session keys using the AES algorithm, over-the-air activation and activation by personalization.

LoRa – одна з перших технологій сучасних мереж LPWA, яка призначена для обслуговування IoT-пристроїв. LoRa - це частотне розширення спектра, яке було запатентовано в 2008 році компанією Cycleo (Франція) [1].

Безпека є основним завданням для будь-якого масового розгортання IoT, а специфікація LoRaWAN визначає два рівня криптографії:

Унікальний 128-розрядний ключ мережевого сеансу, яким користуються між кінцевим пристроєм та сервером (NwkSKey)

Унікальний 128-бітний ключ сеансу додатка (AppSKey), яким користуються на рівні додатку [2].

NwkSKey – ключ мережевого сеансу, який використовується для взаємозв'язку між вузлом і мережевим сервером. Його задача – провірити достовірність повідомлень (перевірка MIC).

Ключ AppSKey використовується для шифрування і дешифрування корисного навантаження. Корисне навантаження повністю зашифроване між вузлом і компонентом обробника/сервера додатків Інтернету речей (який можна запустити на своєму власному сервері).

До початку OTAA активації в кінцевому вузлі вже повинні зберігатися такі дані:

DevEUI – (8-ми байтовий, EUI64) глобально унікальний ідентифікатор пристрою (End-device identifier). Може бути присвоєний виробником пристрою, в обмеженій кількості може бути отриманий з доступного пулу ідентифікаторів оператора, або отриманий власником вузла в складі пулу в IEEE.

AppEUI – (8-ми байтовий, EUI64) глобально унікальний ідентифікатор додатка для маршрутизації отриманих даних сервером мережі (Network Server)

AppKey – унікальний (16-ти байтовий, AES-128) ключ шифрування, згенерований сервером додатків (AppServer) саме для цього пристрою.[3]

ABP (Activation by Personalization) - спрощена процедура, при якій сесійні ключі відразу зашиваються в радіомодуль і відразу ж прописані з

серверної сторони [4].

Надійність шифрування залежить від сесійних ключів мережевого сервера і сервера додатку. Спрощений алгоритм шифрування наступний: шифроване повідомлення розбивається на 128-бітові блоки. Кожен блок шифрується окремо AES-ключем. Причому, при шифруванні другого блоку, крім ключа, використовується результат шифрування першого. А при шифруванні третього - результат другого і (опосередковано) першого. Такий чином ланцюг ускладнюється [5].

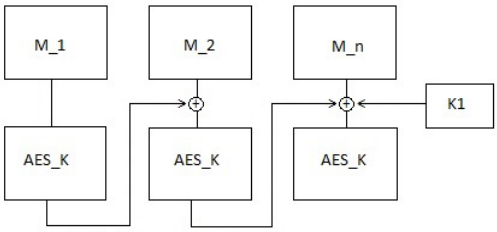

Рисунок 1 – Принцип шифрування AES-CMAC

Будь-які дані в мережі LoRaWAN надійно захищені від несанкціонованого доступу. Такий рівень безпеки став можливим завдяки шифруванню унікальних AES-ключів на мережевому и прикладному рівнях. Шифрування виконується відповідно до RFC-4493. Важливі дані (payload) шифруються безпосередньо на кінцевому вузлі (end-node) і проходять весь шлях від відправника до одержувача в зашифрованому вигляді.

Для того, щоб зламати систему знадобиться велика вибірка пакетів, в кілька тисяч. Але на практиці за 10 років невдалих спроб зі сторони хакерів-зловмисників, стало зрозуміло, що проблема зламу більш теоретична.

Представлена технологія шифрування двома різними AES-128 ключами дозволяє уникнути спотворення, або підміни даних, перехоплення повідомлень в LoRaWAN мережі також втрачає сенс для зловмисників.

Абсолютно безпечних способів передачі даних не існує, але концепції безпеки протоколу LoRaWAN, роблять злам практично неможливим, обчислювальні потужності здатні підібрати комплект з двох AES-128 ключів за оптимальний час з'являться ще дуже не скоро.

Перелік посилань:

1. http://orion-m2m.kz/ru/news/lorawan-shirokie-vozmozhnosti-seti-dal-nego-radiusa/

2. https://deps.ua/knowegable-base-ru/spravochnaya-informatsiya /item/6-6633.html

3. https://www.thethingsnetwork.org/docs/lorawan/security.html

4. http://lo-ra.ru/lorawan-end-node-activation-and-security/

5. https://habr.com/ru/post/413105/