

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В СУПУТНИКОВІЙ СИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ НА БАЗІ ПРОТОКОЛУ LoRaWAN

¹Новіцька А.О., ¹Капштик С.В., ²Наритник Т.М.

¹Національний центр управління та випробувань космічних засобів, Україна

²Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: s.kapshtyk@spacecenter.gov.ua; director@mitris.com

FEATURES OF INFORMATION SECURITY IN THE SATELLITE INTERNET OF THINGS SYSTEM BASED ON THE LoRaWAN PROTOCOL

Features of the Internet of Things satellite systems design using the LoRaWAN protocol are considered. The prospects of transferring the key element of the system - the LoRaWAN gateway to the space segment are shown. The proposals for the distribution of LoRaWAN information security tools have been developed, taking into account the peculiarities of the low-Earth-orbit satellite system. The advantages of inter-satellite-links introducing to the architecture of the Internet of Things satellite system constellation based on the LoRaWAN protocol for the implementation of information protection mechanisms in the LoRaWAN satellite system are shown.

Важливою складовою частиною діяльності щодо впровадження систем та послуг Інтернету речей [1-3] є формування телекомунікаційної інфраструктури, необхідної для передачі інформації від сенсорів – пристроїв Інтернету речей, призначених для перетворення фізичних параметрів контрольованих процесів в електричні сигнали і формування інформаційних посилок, та до актуаторів – пристроїв Інтернету речей, що забезпечують формування керуючих впливів на підставі отриманих інформаційних посилок – команд керування.

Завдяки своїм перевагам технологія мережі передачі повідомлень Інтернету речей LoRaWAN [4] активно застосовується в супутникових низькоорбітальних системах Інтернету речей, що в переважній більшості створюються із використанням космічних апаратів класу куб-сат (масою 1-10 кг) [5]. Зокрема, компанія SWARM розробляє супутникову систему, що буде побудована із використанням куб-сатів, і буде використовувати протокол LoRaWAN [6]. Але недоліком такого підходу є використання супутникового сегменту в якості радіоподовжувача, тобто пристрою, який приймає та перевипромінює радіосигнали, які випромінюються передавальними пристроями в межах зони радіобачення космічного апарату.

Підвищити ефективність супутникової системи, яка функціонує на базі протоколу LoRaWAN, можливо шляхом перенесення до космічного сегменту системи пристроїв зі складу інфраструктури системи LoRaWAN, які здійснюють об'єднання в єдиному потоці інформації від окремих сенсорів.

На рис.1 наведена структурна схема супутникової мережі, що побудована із використанням протоколу LoRaWAN. На відміну від запропонованих раніше рішень, до складу корисного навантаження космічних апаратів введено шлюз LoRaWAN. Космічний апарат приймає інформацію від усіх пристроїв Інтернету речей, які знаходяться в межах зони радіобачення космічного апарату, формує єдиний інформаційний потік, який передає до наземної станції спряження провайдера послуг Інтернету речей. Управління ресурсом супутникової системи здійснює центр управління мережею LoRaWAN, який виконує функції оператора мережі, і який має окрему станцію спряження мережі. Зважаючи на особливості спрямування інформаційних потоків в мережі LoRaWAN можливо розглядати варіант використання спільної станції спряження, яка обслуговує центр управління послугами Інтернету речей, тобто провайдера послуг Інтернету речей, та центр управління мережею, тобто оператора мережі.

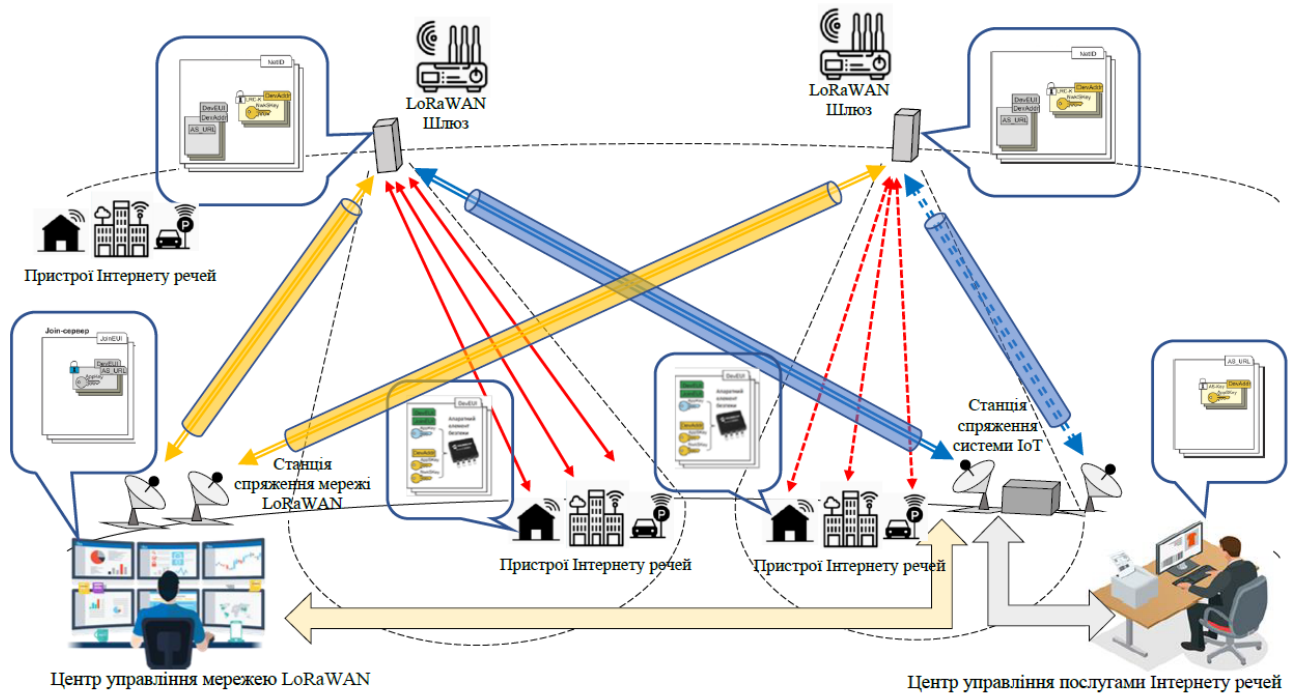


Рис. 1. Супутникова система Інтернету речей на базі протоколу LoRaWAN.

Протокол LoRaWAN передбачає використання вбудованих ефективних методів захисту інформації, які побудовані на базі алгоритму блочного шифрування AES (Advanced Encryption Standard) [7]. На мал.1 показано розподіл елементів захисту інформації по складових частинах супутникової системи. Зокрема, в кінцевому пристрої Інтернету речей (сенсори та актуатори) зберігаються ключі, що застосовуються для шифрування інформації на рівні додатків AppSKey та на рівні мережі NwkSKey. В шлюзі, який розташований у складі корисного навантаження космічного апарату, зберігається ключі доступу до мережі NwkSKey, в центрі управління мережею LoRaWAN розташований Join-сервер. Ключі рівня додатків AppSKey зберігаються в сервері додатків, який розташований в центрі управління послугами Інтернету речей.

Особливістю архітектури супутникової системи, наведеної на мал.1, є відсутність з'єднань між космічними апаратами. В наслідок цього, пристрої Інтернету речей контролюють наявність зв'язку із космічним апаратом шляхом контролю за надходженням повідомлень по лінії «до низу» у вікнах **приймання** повідомлень від шлюзу. В разі відсутності підтвердження від шлюзу кінцевий пристрій переходить в режим очікування і ініціює процедуру запиту доступу до мережі чергового космічного апарату, який заходить до зони радіобачення пристрою Інтернету речей. Кінцевий пристрій LoRa ініціює JOIN процедуру. Спочатку до супутника передається запит для приєднання JOIN_REQUEST, який складається з ідентифікатора додатку (AppEUI), ідентифікатора пристрою (DevEUI) і випадкового числа (DevNonce), що використовується при розрахунку ключів NwkSKey і AppSKey. Після підтвердження запиту, шлюз і кінцевий пристрій генерують однакові ключі за допомогою DevNonce. В результаті кінцевий пристрій передає повідомлення JOIN_ACCEPT. Така архітектура супутникової системи представляє систему як сукупність мікро радіомереж LoRaWAN, що сформовані окремими космічними апаратами. Керування інформаційним обміном та безпекою таких мікро радіомереж LoRaWAN здійснюється із застосуванням технології тунелювання IP-трафіку між станціями спряження та шлюзами LoRaWAN окремо для кожного космічного апарату.

Введення до складу космічного сегменту супутникової системи ліній зв'язку між космічними апаратами дозволяє підвищити гнучкість системи, подовжити строк використання розрахованих ключів, скоротити частоту виконання процедури запиту на входження до мережі LoRaWAN кінцевих пристроїв Інтернету речей (рис.2).

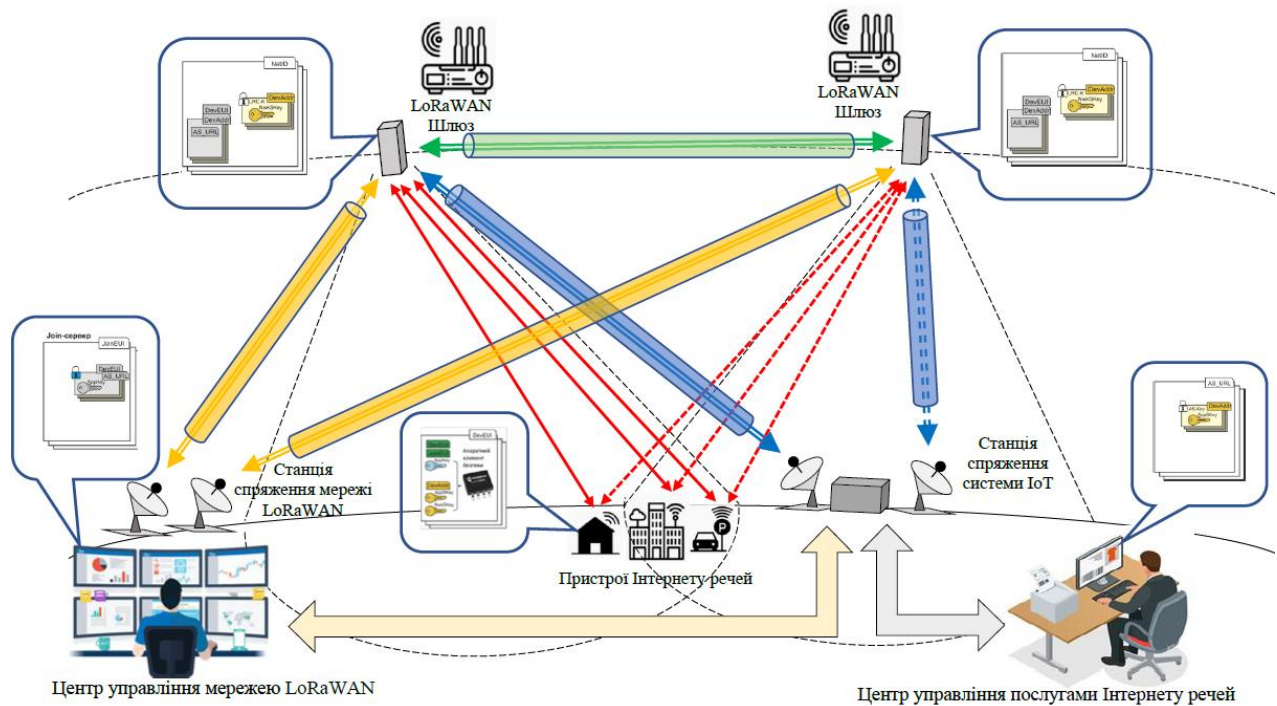


Рис.2. Модифікована супутникова система Інтернету речей на базі протоколу LoRaWAN.

По лінії зв'язку між супутниками може передаватись масив інформації, який містить вихідні дані, що використовувались при реалізації процедури доступу кінцевих пристроїв до мережі LoRaWAN: ідентифікатор додатку (AppEUI), ідентифікатор пристрою (DevEUI), випадкове число (DevNonce). Космічний апарат, який забезпечує передачу інформації на пристрої Інтернету речей, передає до сусіднього космічного апарату, який рухається за ним, масив інформації про усі пристрої Інтернету речей, які знаходяться в межах його зони обслуговування, і які приймають участь і інформаційному обміні в мережі LoRaWAN (тобто за винятком непрацюючих пристроїв). На підставі отриманого масиву даних космічний апарат, що входить в зону радіобачення пристрою Інтернету речей, має можливість розрахувати дублікат мережевого ключа, що виключає необхідність використання процедури запиту доступу до мережі.

Ініціатива передачі управління від космічного апарату, що виходить із зони радіобачення, до космічного апарату, який входить до зони радіобачення кінцевого пристрою Інтернету речей, належить космічному апарату. Космічний апарат контролює радіоінтерфейс до кінцевих пристроїв. В разі виявлення факту отримання сигналу від кінцевого пристрою, інформаційна посилка до якого пройшла перевірку на цілісність, космічний апарат повідомляє про це попередній космічний апарат. Попередній космічний апарат надсилає кінцевому пристрою Інтернету речей інформацію про передачу управління до наступного космічного апарату. Кінцевий пристрій Інтернету речей передає тестове повідомлення до обох космічних апаратів, оскільки ще знаходиться на перетині зон обслуговування обох космічних апаратів, що рухаються один за одним. В разі отримання підтвердження від космічних апаратів про цілісність прийнятих тестових повідомлень кінцевий пристрій та шлюз космічного апарату приймають рішення про актуальність мережевого ключа та продовжують інформаційний обмін. Про вдале завершення процедури передачі тестового повідомлення та про підтвердження актуальності мережевого ключа шлюз повідомляє оператора мережі та провайдера послуг.

З метою підвищення інформаційної безпеки системи та мережі LoRaWAN, супутникова система може запроваджувати процедуру примусового виконання процедури запиту доступу до мережі для кінцевих пристроїв Інтернету речей. Період такої процедури може становити відрізок часу, кратний періоду орбіти системи, оскільки із врахуванням обертання Землі на наступному витку орбіти космічні апарати починають обслуговувати іншу ділянку – смугу

обслуговування на поверхні Землі. Таким чином до зони обслуговування космічних апаратів потрапляють інші кінцеві пристрої Інтернету речей, а до зони радіобачення кінцевих пристроїв Інтернету речей в свою чергу заходять інші космічні апарати (зі складу сусідньої орбітальної площини орбітального угруповання).

Підвищити ефективність супутникової системи, яка функціонує на базі протоколу LoRaWAN, можливо шляхом використання запропонованої схеми розподілу засобів інформаційної безпеки в супутниковій системі Інтернету речей та перенесення до космічного сегменту системи пристроїв зі складу інфраструктури системи LoRaWAN, які здійснюють об'єднання в єдиному потоці інформації від окремих сенсорів.

Введення до складу космічного сегменту супутникової системи ліній зв'язку між космічними апаратами і періодичність примусового застосування процедури запиту доступу до мережі дозволяє покращити гнучкість системи, подовжити строк використання розрахованих ключів, скоротити частоту виконання процедури запиту на входження до мережі LoRaWAN кінцевих пристроїв Інтернету речей.

В матеріалах доповіді, визначено умови застосування процедур розрахунку ключів додатків та доступу до мережі. Визначено місце реалізації процедур та методів захисту інформації зі складу протоколу LoRaWAN в супутниковій системі. Запропоновано два варіанти розподілу засобів захисту інформації для архітектури орбітального угруповання без та із лініями зв'язку між космічними апаратами.

Література

1. The computing load balancing through the orbital computer network of the internet of things (2020) / Ilchenko, M., Narytnik, T., Prisyazhny, V., Kapshtyk, S., Matvienko, S. / Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 79 (4), pp. 343-352. / Електронний ресурс. Режим доступу: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085244112&doi=10.1615%2fTelecomRadEng.v79.i4.70&partnerID=40&md5=73f400a98bc0fa4ae5c25074171c5593> / DOI: 10.1615/TelecomRadEng.v79.i4.70.
2. The solution of the problem of the delay determination in the information transmission and processing in the LEO satellite internet of things system (2019) / Ilchenko, M., Narytnik, T., Prisyazhny, V., Kapshtyk, S., Matvienko, S. / 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, стаття № 9061350, pp. 419-425. / Електронний ресурс. Режим доступу: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083638366&doi=10.1109%2fPICST47496.2019.9061350&partnerID=40&md5=7768787b80c0fd34e7417001cecc231b> / DOI: 10.1109/PICST47496.2019.9061350.
3. Ільченко М.Ю., Наритник Т.М., Присяжний В.І., Капштик С.В., Матвієнко С.А. Низькоорбітальна супутникова система Інтернету речей на базі розподіленого супутника. Космічна наука і технологія. 2020. 26. №4 (125). С.57-85. <https://doi.org/10.154307/knit.2020.04.057>.
4. Інтернет вещей: LoRa устройства от Mikrotik / Електронний ресурс. Режим доступу: <https://lanmarket.ua/stats/internet-veshchey-lora-ustroystva-ot-mikrotik/>
5. Semtech and Swarm Deliver Satellite Communications With LoRa® / Електронний ресурс. Режим доступу: <https://www.semtech.com/company/press/semtech-and-swarm-deliver-satellite-communications-with-lora>.
6. Our Technology. See how Swarm works and what makes us unique / Електронний ресурс. Режим доступу: <https://swarm.space/our-technology/>
7. Обзор технологии LoRa / Електронний ресурс. Режим доступу: <https://itechinfo.ru/content/%D0%BE%D0%B1%D0%B7%D0%BE%D1%80-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8-lora>.