УДК 004.738
DOI https://doi.org/10.32838/2663-5941/2020.1-1/07

Переверзєв О.А.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Гумен Т.Ф.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Трапезон К.О.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ СТВОРЕННЯ СИСТЕМИ БЕЗПЕКИ БУДИНКУ НА ОСНОВІ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

Наведено опис архітектури системи Інтернету речей через розгляд основних налаштувань елементів, які є ключовими при проектуванні системи домашньої безпеки типового приміського житлового будинку. Запропоновано підхід, за яким існуючі рівні концепції Інтернету речей можна використати при створенні нової системи безпеки житлового будинку, яка буде вирізнятись надійністю, автономністю та широким спектром індивідуальних функцій охорони приміщення, починаючи від пасивних інфрачервоних датчиків на вікнах чи на дверях і закінчуючи віддаленим управлінням системою безпеки будинку, її окремими елементами через «хмарний сервіс» у будь-якій точці, де є підключення до мережі Інтернет.

Визначено склад системи безпеки, де основну роль присвячено пасивному інфрачервоному датчику як одному з ключових елементів в архітектурі системи безпеки об'єкту на основі концепції Інтернету речей. Зазначено, що через особливості роботи таких сенсорів у будинку можна забезпечити значну зону безпеки за периметром приміщення. Сформульовано основні переваги та недоліки інфрачервоних датчиків руху і зазначено, що одним із обмежень роботи останнього і спрацювання його на сигнал тривоги є ситуація, коли об'єкт вторгнення в будинок, який охороняється має одяг, покритий матеріалом, що не пропускає інфрачервоне випромінювання.

Окремо розглянуто технологію LoRaWAN як базову при підключенні пасивних інфрачервоних датчиків у складі системи безпеки будинку. Визначено технічні особливості цієї технології і зазначено, що вона базується на основі відкритого протоколу ALOHA, для якого не передбачено за стандартом методів мультиплексування. Натомість усі дані, які передаються між кінцевими пристроями, повинні бути зашифровані. Доведено, що ця технологія є простою, але вирізняється тим, що дані переважно передаються лише в одну сторону від пристроїв до шлюзів у не ліцензованому діапазоні частот. Колізія можлива лише за ситуації, коли пристрої при підключенні використовують один частотний канал.

Ключові слова: *сенсор, безпека, технологія, архітектура, сигнал тривоги, система, будинок, LoRaWAN.*

Постановка проблеми. Класичні підходи, функціональні схеми проектування систем безпеки приміщень, а саме налаштування звукових систем сигналізації за типом, наприклад замикання-розмикання магнітного контакту, окреме використання контактів за типом «геркону» вже не можуть повністю забезпечити суцільну надійну охорону приміщення. Це пояснюється тим, що у зловмисників наявні спеціальні засоби та відповідне обладнання, яке дозволяє нейтралізувати сигнали тривоги існуючих систем безпеки. Крім цього, при проектуванні системи безпеки необхідно у розрізі стрімкого розвитку інформаційних технологій забезпечити контроль елементів охорони в режимі реального часу і цілодобово, адже при зовнішньому вторгненні у приміщення саме час реакції відіграє головну роль.

Слід враховувати, що спроектована система охорони повинна мати низький відсоток хибного спрацювання і високу надійність роботи у будь-яких умовах, наприклад у форс-мажорній ситуації, коли будинок тимчасово відключено від споживання електроенергії, або відбулась певна аварія в комунікаціях будинку. Основною проблемою при створенні системи безпеки приміщення є те, аби система була прозора і контрольована на

відстані, працювала автономно, незалежно, мала високу надійність і певний захист від зовнішнього зламу. Розв'язання окреслених проблем можливе на основі підходів і принципів концепції Інтернету речей.

Постановка завдання. Використання технологій, підходів, принципів які закладено в поняття «розумний» будинок можна долучити при створенні системи безпеки будинку. Враховуючи, що концепція Інтернету речей має певну архітектуру і правила, які визначають взаємодію елементів архітектури, елементи захисту будинку повинні відповідати саме цій концепції.

Основним завданням статті можна визначити те, що спроектована система безпеки будинку повинна вирізнятися тим, що її елементи повинні відповідати стандартизованим технологіям і рівням концепції Інтернету речей. В цьому контексті слід забезпечити цю взаємодію елементів безпеки на нижньому рівні архітектури Інтернету речей, адже спрацювання системи безпеки, створення сигналу безпеки, його передавання у хмарний сервіс або службу відіграє ключову роль у ефективності роботи всієї системи.

Метою статті є визначення особливостей, які слід враховувати при проектуванні на нижньому рівні системи безпеки житлового будинку на основі підходів і правил концепції Інтернету речей. Додатково необхідно визначити особливості, які слід враховувати при підключенні інфрачервоних сенсорів до системи безпеки будинку.

Виклад основного матеріалу дослідження. Нині актуальною проблемою для людства залишається забезпечення безпеки власного нерухомого майна. Технології XXI століття дають можливість захистити свій будинок за допомогою автономних охоронних систем, тим самим піднімаючи охорону та безпеку на новий рівень. Сучасні телекомунікаційні та інформаційні технології значно розширили функціональні можливості охоронних систем завдяки збільшенню швидкості передачі інформації та зниженню вартості телекомунікаційних послуг. Інтернет Речей (Internet of Things, IoT) [1] дає можливість «підняти» на новий рівень ці системи, використовуючи різні канали зв'язку, залежно від потреб користувача, але для будь-якої системи необхідний певний спосіб передачі інформації. Для передачі даних може бути використана будь-яка з існуючих технологій. У разі використання бездротових мереж особливу увагу потрібно приділяти підвищенню надійності передачі даних.

Кожна система IoT за своїм призначенням може відрізнятися між собою, проте основа для кожної архітектури Інтернету речей, а також її загальний потік обробки даних є приблизно однаковими. Архітектуру на основі Інтернету речей можна описати за рівнями. На рисунку 1 наведено ключові рівні архітектури Інтернету речей. Так, вона побудована з речей, які є об'єктами, підключеними до мережі Інтернет. За допомогою вбудованих датчиків і виконавчих механізмів вони здатні сприймати навколишнє середовище і збирати інформацію, яка потім передається на шлюзи IoT. Цю особливість можна використати при створенні системи безпеки будинку.

Рис. 1. Рівні архітектури IoT

В якості основи для кожної системи IoT визначають підключені пристрої, які відповідають за забезпечення сутності Інтернету речей, а саме даних. Щоб отримати фізичні параметри з зовнішнього світу або з самого об'єкта потрібні датчики. Вони можуть бути або вбудованими в пристрої, або реалізованими як окремі об'єкти для вимірювання та збору даних телеметрії.

Ще одним обов'язковим елементом цього рівня є виконавчі механізми. Перебуваючи в тісній зв'язці з датчиками, вони можуть перетворювати дані, які генеруються інтелектуальними об'єктами, у фізичні дії. Це важливо, адже підключені об'єкти повинні не тільки підтримувати зв'язок з відповідними шлюзами або системами збору даних, але й мати можливість розпізнавати і спілкуватися один з одним для збору та обміну інформацією, спільної роботи в режимі реального часу.

Наступним етапом роботи системи на основі концепції Інтернету речей можна вважати збір даних IoT і використання шлюзів, які отримують величезну масу необроблених даних, задля подальшого їх перетворення в цифрові потоки з відповідною обробкою та аналізом. Шлюзи полегшують зв'язок між датчиками й іншою частиною системи, перетворюючи дані датчиків у формати, які легко переносяться і можуть використовуватися іншими компонентами системи. Більш того, вони можуть контролювати, фільтрувати і вибирати дані, щоб мінімізувати обсяг інформації, яка повинна бути передана в «хмару», що позитивно впливає на вартість передачі по мережі і час відгуку. Таким чином, шлюзи забезпечують місце для локальної

попередньої обробки даних датчика, які стискаються в пакети і є готовими для подальшої обробки.

Третій рівень архітектури можна представити через периферійні пристрої, які відповідають за подальшу обробку і розширений аналіз даних. На цьому рівні також можуть з'явитися технології візуалізації і машинного навчання. Оскільки швидкість аналізу даних є ключовою в деяких промислових додатках Інтернету речей, останнім часом різко зросла популярність периферійних обчислень серед таких екосистем. В умовах обмеженої доступності та швидкості передачі даних хмарних платформ IoT проміжні системи можуть забезпечити більш швидкий час відгуку і велику гнучкість при обробці й аналізі даних IoT.

Після цього інформація передається в центри обробки даних, які можуть бути хмарними або встановленими локально. Саме тут дані зберігаються, обробляються й аналізуються для більш глибокого аналізу. На відміну від периферійних рішень, центр обробки даних або хмарна система призначені для зберігання, обробки та аналізу величезних обсягів даних для більш глибокого розуміння з використанням потужних механізмів аналізу даних і механізмів машинного навчання, які проміжні системи ніколи не зможуть підтримувати. Володіючи все більш широким упровадженням протягом останніх років, хмарні обчислення сприяють підвищенню продуктивності, скороченню незапланованих простоїв, енергоспоживанню і багатьом іншим перевагам для бізнесу, які допомагають людям взаємодіяти з системою, контролювати її, а також приймати обґрунтовані рішення на основі звітів, інформаційних панелей і даних, які переглядаються в режимі реального часу.

Безпека будинку – це місце, де можна розкрити потенціал розглянутої архітектури IoT. Його використовують для створення недорогої системи безпеки як для будинку, так і для промислового використання. Система повідомить власнику про будь-яке несанкціоноване проникнення або про те, що двері відкриті, відправивши повідомлення. Після того, як користувач отримає повідомлення, він може вжити необхідних заходів.

Система охорони та її складники

Всі системи домашньої безпеки працюють за одним принципом захисту точок входу, таких як двері і вікна, а також внутрішнього простору, яка включає такі цінності, як предмети мистецтва, комп'ютери, зброю і колекції монет. Незалежно від розміру будинку або кількості дверей і вікон, внутрішніх приміщень, які домовласник вирішує захистити, єдина реальна відмінність полягає в кількості компонентів безпеки, розгорнутих по всьому будинку, які відслідковуються панеллю керування. У такому випадку йдеться про системи домашньої безпеки, які є мережами інтегрованих електронних пристроїв, що працюють разом із центральною панеллю керування для захисту від грабіжників і інших потенційних домашніх зловмисників.

Типова система домашньої безпеки включає в себе:

- панель управління, яка є основним контролером системи безпеки будинку;
- дверні та віконні датчики;
- датчики руху (як внутрішні, так і зовнішні);
- дротові або бездротові камери безпеки;
- сирену або сигнал тривоги;
- наліпки на вікна.

Системи домашньої безпеки працюють за простою концепцією захисту точок входу в будинок за допомогою датчиків, які обмінюються даними з панеллю керування або командним центром, встановленим у зручному місці десь у будинку.

Датчики зазвичай встановлюються у дверях, які ведуть у будинок і з нього, а також у легко доступні вікна, особливо ті, які відкриваються, особливо на рівні землі. Перевагою є можливість віддаленого управління будинком. При цьому господар можете ставити і знімати з охорони свою систему безпеки з будь-якої точки світу через вебпристрій, відстежувати, хто прибуває і залишає будинок. Часто використовуються в системах сигналізації PIR датчики. Ці датчики малі за габаритами, недорогі, споживають мало енергії, легкі в експлуатації, практично не схильні до зносу.

PIR-сенсори і їх реалізація в системі охорони

PIR Sensor – це скорочення від пасивного інфрачервоного датчика, яке застосовується для проєктів, у яких необхідно виявляти рух людини або частинок в певному діапазоні. Його також можна назвати датчиком PIR (руху) або IR-датчиком (рисунок 2).

Рис. 2. PIR-сенсор [2]

Пасивна інфрачервона сигналізація не випромінює енергію в оточуючий простір, а базується на отриманні інфрачервоного випромінювання від людського тіла для подачі сигналу тривоги. Будь-який об'єкт із температурою постійно випромінює інфрачервоні промені у зовнішній світ. Тобто дія інфрачервоного датчика заснована на аналізі теплового (інфрачервоного) випромінювання. Пасивний інфрачервоний датчик при цьому не випускає ніякого випромінювання, а лише аналізує вхідні теплові промені.

Основні недоліки інфрачервоних датчиків руху:

− можливість помилкових спрацювань. Внаслідок того, що датчик реагує на будь-які інфрачервоні (теплові) випромінювання, можливі випадкові локальні спрацювання навіть на теплому повітрі, яке надходить із кондиціонера, радіаторів опалення тощо;

− знижено точність роботи на вулиці через вплив оточуючих факторів (пряме сонячне світло, опади тощо);

− відносно низький діапазон робочих температур;

− не виявляє об'єкти, які одягнені / покриті, які не пропускають інфрачервоне випромінювання.

Основні переваги інфрачервоних датчиків руху:

− можливість досить точного регулювання дальності і кута виявлення рухомих об'єктів;

− зручний у використанні поза приміщеннями, оскільки реагує лише на об'єкти, які мають власну температуру;

− при роботі абсолютно безпечні для здоров'я людини або домашніх тварин, працюють як «приймач», нічого не випромінюючи.

Пасивні інфрачервоні сигнали тривоги можуть бути класифіковані на інфрачервоні датчики і секції контролю сигналів тривоги [3–4]. Найбільш розповсюдженим є піроелектричний детектор, який використовується в якості датчика для перетворення інфрачервоного випромінювання людини в електричний сигнал. Якщо людське інфрачервоне випромінювання безпосередньо вплине на детектор, воно викличе зміну температури для формування сигналу, але при цьому відстань виявлення не буде значною. Щоб збільшити дальність виявлення детектора, необхідно додати до конструкції датчика оптичну систему для збору інфрачервоного випромінювання. Це, як правило, пластикова оптична система відображення або лінза Френеля, виготовлена із пластику, як система фокусування для інфрачервоного випромінювання.

У зоні виявлення енергія інфрачервоного випромінювання людського тіла через одяг сприймається лінзою детектора і фокусується на піроелектричному датчику. Коли людське тіло (зловмисник) рухається в цьому режимі спостереження, воно послідовно входить у певне поле зору і потім виходить із нього. Піроелектричний датчик деякий час бачить рухомий об'єкт, а потім не бачить його. Інфрачервоне випромінювання постійно змінює температуру піроелектричного матеріалу, тому що він видає відповідний сигнал, який є сигналом тривоги (рис. 3).

Для підключення PIR сенсорів можна використовувати технологію LoRaWAN, яка отримала широке поширення в роботі операторів стільникового зв'язку. LoRaWAN – це відкритий асинхронний протокол управління доступом до середовища (MAC) для глобальних мереж на базі протоколу

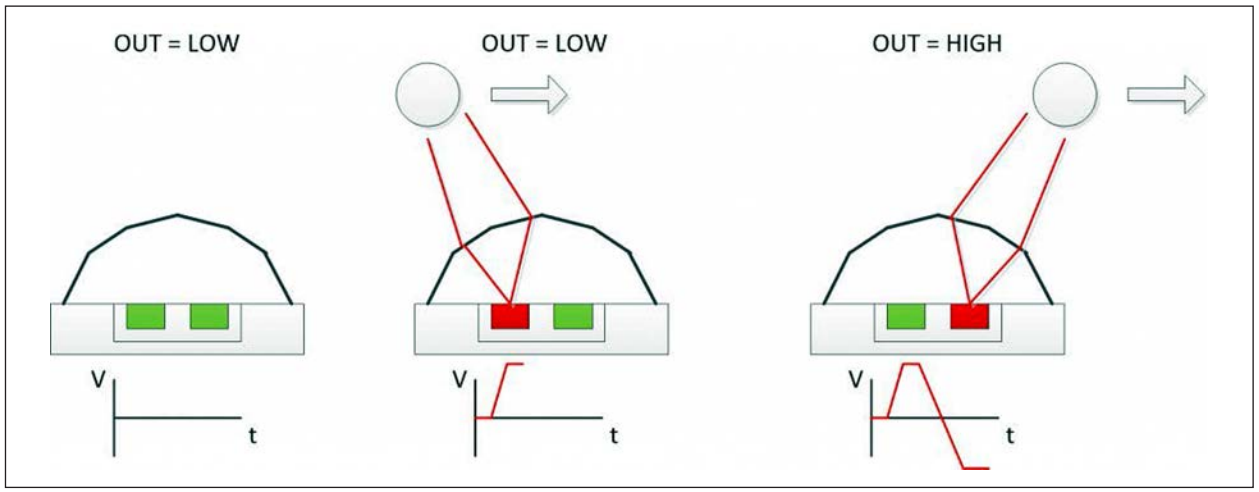

Рис. 3. Принцип роботи датчика

ALOHA. Він призначений для того, щоб пристрої з низьким енергоспоживанням могли обмінюватися даними з підключеними до інтернету додатками по бездротових з'єднаннях на значні відстані. LoRaWAN може бути зіставлений з другим і третім рівнями моделі OSI. Він реалізований поверх модуляції LoRa або FSK у промислових, наукових і медичних (ISM) радіодіапазонах. Перевага LoRaWAN полягає в можливості дальньої дії. Один шлюз або базова станція можуть покривати цілі міста або сотні квадратних кілометрів. LoRaWAN працює в неліцензійному радіочастотному спектрі. На рисунку 4 наведено архітектуру LoRaWAN, де:

− end node – об'єкт з убудованим малопотужним пристроєм зв'язку;

− gateway – антени, які приймають широкомовні повідомлення від кінцевих пристроїв і відправляють дані назад на кінцеві пристрої;

− network server – сервери, які направляють повідомлення від кінцевих пристроїв до потрібного додатка і назад;

− application – це частина програмного забезпечення, яка працює на сервері.

Дані між елементами архітектури є зашифрованими на основі моделі AES із 128 розрядним кодом. В архітектурі при передаванні даних між датчиками та шлюзом (хабом) не використовуються методи мультиплексування. Шлюз, отримуючи дані, забезпечує ретрансляцію пакетів у «хмарний» сервіс, розташований в мережі Інтернет. За такої організації колізії при передаванні можуть виникати лише тоді, коли дані від датчиків передаються в одному частотному каналі. Кінцевий вузол може бути пов'язаний за протоколом LoRaWAN відразу з декількома шлюзами.

Завдяки надійним і масштабованим опціям фізичного рівня LoRaWAN може забезпечувати енергоефективний зв'язок на значні відстані. Протоколи канального і мережевого рівнів забезпечують масштабовані та ефективні мережі, дозволяють вибирати і регулювати ключові параметри для оптимізації енергоспоживання. Технологія має досить просту конструкцію (рис. 4), яка дозволяє використовувати кінцеві пристрої з дуже низькою вартістю, забезпечуючи достатню пропускну здатність і досить низьку затримку для підтримки нетривіальних додатків IoT і ключових допоміжних сценаріїв зв'язку (оновлення вбудованого програмного забезпечення по повітрю).

Висновки. Майбутнє концепції Інтернету речей практично необмежене завдяки прогресу технологій і бажанням споживачів інтегрувати

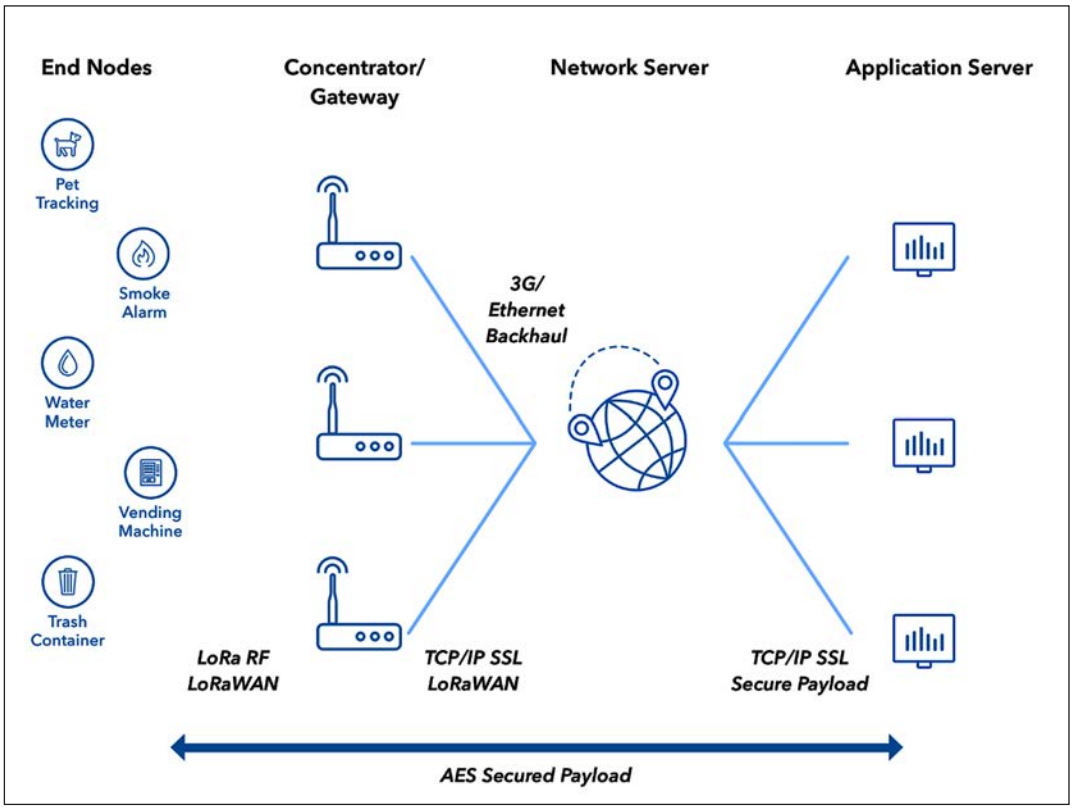

Рис. 4. Варіант архітектури за рівнями LoRaWAN

пристрої, такі як смартфони, з побутовою технікою в будинку. Тим самим є можливість значно вдосконалити систему охорони, невід'ємним елементом для якої є набір певних сенсорів. Хоча існує ряд технологій для виявлення руху, включаючи датчики ультразвукового і мікрохвильового випромінювання, інфрачервоний датчик популярний завдяки своїй простоті налаштування і високій продуктивності. Такі датчики коштують недорого і споживають мало енергії.

Для об'єднання датчиків можна використовувати LoRaWAN, яка є ключовою технологією для Інтернету речей. Її простота і здатність підтримувати недорогі, малопотужні кінцеві пристрої зі зв'язком на відстані означає, що вона добре підходить для використання в ряді стаціонарних і мобільних додатків IoT.

Список літератури:

1. Ли П. Архитектура интернета вещей. Москва : «ДМК Пресс», 2019. 454 с.
2. Муромцев Д.И., Шматков В.Н. Интернет вещей: введение в программирование на Arduino. Санкт-Петербург : «ИТМО», 2018. 36 с.
3. Jerker D. IoT Automation: Arrowhead Framework, Great Britain : CRC Press, 2017. 366 p.
4. McEwen A. Designing the Internet of Things, USA : Publishing NT, 2013. 336 p.

Pereverziev O.A., Humen T.F., Trapezon K.O. RESEARCH FEATURES OF CREATING A HOUSEHOLD SECURITY SYSTEM BASED ON THE CONCEPT OF THE INTERNET OF THINGS

A description of the architecture of the Internet of Things system is given, considering the basic settings of the elements that are key in designing a home security system for a typical suburban home. An approach is proposed whereby existing levels of the Internet of Things concept can be used to create a new home security system that will be characterized by the reliability, autonomy and wide range of individual room security features, ranging from passive infrared sensors to windows or doors and door and door controls home, its individual elements through the "cloud service" at any point where there is an Internet connection.

The structure of the security system is defined, where the main role is devoted to the passive infrared sensor, as one of the key elements in the security system architecture of the object based on the concept of the Internet of Things. It is noted that due to the peculiarities of the operation of such sensors in the house, it is possible to provide a significant safety zone beyond the perimeter of the room. The main advantages and disadvantages of infrared motion sensors have been formulated and it is noted that one of the limitations of the operation of the infrared sensor is the situation when the object of invasion of the protected house has clothing covered with material that does not transmit infrared radiation.

Separately, we consider the technology LoRaWAN as a base when connecting passive infrared sensors in the home security system. The technical features of this technology have been identified and noted that it is based on the open ALOHA protocol, which is not provided with the standard of multiplexing methods. Instead, all data transmitted between the end devices must be encrypted. It is proven that this technology is simple but characterized in that the data is preferably transmitted only one way from the devices to the gateways in the unlicensed frequency range and collision is possible only when the devices use the same frequency channel when connecting.

Key words: *sensor, security, technology, architecture, alarm, system, home, LoRaWAN.*