

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОГО СЕНСОРНОГО УЗЛА НА БАЗЕ ТЕХНОЛОГИИ LORA

Гребешков А.Ю.¹, Дараев Д.М.²

¹ Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ

² Акционерное общество «Инфосистемы Джет», Самара, РФ

E-mail: grebeshkov-ay@psuti.ru

Для сбора, обработки и передачи сенсорных данных возможно применение различных радиотехнологий сетей доступа с использованием как лицензионной части радиочастотного спектра, так и в области нелицензионного радиочастотного спектра. Одновременно требуется обеспечить защищенность информационного обмена между оконечным узлом и шлюзом беспроводной сенсорной сети. Оконечное устройство, используя принцип программно определяемого радио, позволяет применять современные средства управления сбором и обработкой информации. В результате сенсорный узел в зависимости от программных настроек может выполнять функции оконечного устройства или функции шлюза при однотипном аппаратном обеспечении и с поддержкой требуемых протоколов безопасности. Для повышения эффективности передачи целесообразно использование управляемой ориентируемой антенны с выбором оптимального направления приема-передачи между оконечным узлом и шлюзом-сервером. В статье описан результат разработки сенсорного узла на базе стандарта LoRaWAN, выполнен анализ методов и способов обеспечения информационной безопасности в сетях LoRa, разработан алгоритм калибровки антенны для выбора лучшего, чем существующее, направления передачи между оконечным устройством и шлюзом.

Ключевые слова: сенсорный узел, шлюз сенсорной сети, LPWAN, LoRa, LoRaWAN, SDR, Sigfox

Введение

В цифровой экономике [1] для сбора и передачи сенсорных данных требуются интеллектуальные сетевые элементы, обеспечивающие требуемые параметры обмена данными с учетом условий передачи. Особое значение имеет телекоммуникационная инфраструктура для «последней мили», которая должна обеспечить передачу с требуемым качеством и защищенностью, например в рамках эволюции стандарта LTE-Advanced [2]. Однако для передачи телеметрии целесообразно рассмотреть альтернативные решения в виде радиотехнологий маломощных глобальных радиосетей LPWAN (Low Power Wide Area Network) [3]. Далее в настоящей статье рассматривается разработка прототипа сенсорного узла LPWAN, способного в зависимости от программного обеспечения выполнять как функции шлюза, так и функции оконечного устройства.

Анализ технологий маломощной беспроводной связи

В связи с развитием технологий Интернета вещей IoT, межмашинного взаимодействия M2M существенно увеличивается объем передачи телеметрической информации. Для этого требуется сравнительно дешевая с точки зрения затрат, оперативно разворачиваемая радиолиния доступа с функциями «последней мили». В рамках развития стандарта LTE-Advanced для решения рассматриваемой задачи предлагаются

«узкополосные» сети Интернета вещей NB-IoT (NarrowBand Internet of Things), которые поддерживаются существующей инфраструктурой базовых станций сотовых сетей связи в частотных диапазонах 700...2,2 ГГц, 452,5...467,5 МГц со скоростью передачи до 200 Кбит/с. Технология узкополосного Интернета вещей NB-IoT была разработана Партнерством третьего поколения (3GPP). NB-IoT развернут в лицензируемом диапазоне радиочастотного спектра (РЧС) и использует существующие сотовые (мобильные) сети GSM, защитные полосы несущей LTE или неиспользуемые блоки в диапазоне LTE. Трансиверы NB-IoT имеют выходную мощность до 23 дБм и чувствительность входа 135 дБм [4].

Для случаев, когда инфраструктура сотовых сетей не обеспечивает требуемого покрытия либо при разворачивании беспроводных сетей Интернета вещей в условно-свободных от лицензирования диапазонах нет требуемой интеллектуальной инфраструктуры когнитивных сетей, можно использовать альтернативные технологические решения в виде маломощных радиосетей с широким покрытием LPWAN (Low Power Wide Area Network) [5–9], которые не требуют специального частотного выделения и не привязаны к базовым станциям сетей 3G/4G/5G. Среди технологий, использующих нелицензируемый диапазон РЧС, рассмотрим Sigfox и LoRaWAN.

Технология Sigfox использует ультразвуковую полосу РЧС (Ultra-Narrow Band, UNB) с двухпозиционной или двоичной фазовой модуляцией

Таблица. Данные для выбора технологии LPWAN

Показатель технологии	LoRaWAN	Sigfox
Частота несущей, МГц	433, 868	868, 902–920
Чувствительность приемника	–148 дБм	–130 дБм
Скорость передачи	37,5 кбит/с	600 бит/с
Максимальная длина пакета	255 байт	12 байт

BPSK (Binary Phase Shift Keying). В Европе Sigfox использует диапазон ISM 868 МГц, а в остальных странах выделяется полоса частот в диапазоне 902...920 МГц. Максимальная выходная мощность составляет 14 дБм, а максимальная скорость передачи данных указана 600 бит/с. Такая скорость считается достаточной для большинства применений датчиков и телеметрии. Возможны сообщения как по условно восходящим, так и нисходящим каналам, в результате чего интервалы для нисходящей линии связи для конечных устройств указываются непосредственно после отправки сообщения на шлюз.

К технологиям LPWAN также относится технология LoRaWAN, которая предложена альянсом производителей LoRa (LoRa Alliance) и предусматривает создание оконечных приёмопередающих узлов и шлюзов сбора данных. Оконечные узлы подразделяются на узлы класса А с дуплексной асинхронной передачей с минимальной мощностью; на узлы класса В с дуплексной передачей с синхронизацией с сетью, с проверкой наличия входящего трафика; узлы класса С с дуплексной передачей с наименьшей задержкой, поскольку средство связи постоянно находится в режиме приема.

Для передачи радиосигнала в LoRa применяется модуляция с расширенным спектром и вариацией линейной частотной модуляции CSS (Chirp Spread Spectrum) с применением прямой коррекции ошибок FEC (Forward Error Correction). В результате в LoRa значительно увеличивается чувствительность приемника и существует возможность использования всей доступной ширины полосы пропускания канала. Другим достоинством LoRa следует считать устойчивость к канальным шумам и достаточная инертность в отношении девиаций, обусловленных расстройкой частот опорных кварцевых резонаторов.

Дальность связи при использовании LoRa составляет для пары корреспондирующих узлов до 3–5 км в городе со среднеэтажной застройкой,

и до 15 км в равнинных местностях согласно частотному плану RU868, то есть в условно-свободном (нелицензируемом) диапазоне радиочастот 867,8...869,2 МГц и в аналогичном диапазоне 866...868 МГц. Для ширины полосы пропускания канала в 125 кГц скорость передачи данных составляет до 50 кбит/с.

Возможность использования LoRaWAN в сравнении с технологиями-аналогами для передачи телеметрии особенно выигрышна для минимизации затрат на поддержку беспроводной инфраструктуры Интернета вещей с возможностью организации надежного радиосоединения при условии наличия препятствий на пути распространения сигнала.

Международный опыт показывает возможность использования LoRa на коротких и длинных дистанциях, в условиях чрезвычайных ситуаций, для поддержки инфраструктуры Интернета вещей с надежным радиосоединением и с возможностью преодоления препятствий на пути распространения сигнала [10; 11].

Структура и схема сетей Sigfox и LoRa одинаковы, причем конечные узлы LPWAN не привязаны к конкретным шлюзам. Таким образом, несколько шлюзов могут получать и пересылать сообщения с помощью сервера или серверного программного обеспечения, которое отвечает за фильтрацию одинаковых сообщений, пересылаемых несколькими шлюзами – оконечными устройствами. Такой подход увеличивает надежность сети.

Наиболее существенные характеристики для конструирования сенсорного узла и выбора программного обеспечения управления представлены в таблице.

По результатам анализа далее для создания лабораторного прототипа интеллектуального сенсорного узла в качестве базовой технологии радиодоступа выбирается технология LoRaWAN.

Шлюзы LoRa взаимодействуют с сетевым шлюзом-сервером с использованием протокола IP. Шлюзы сети LoRa могут быть территориально совмещены с базовой станцией сотовой сети, если это соответствует требованиям электромагнитной совместимости.

Сетевой сервер сети LoRa управляет трафиком, устраняет дубликаты пакетов, управляет расписанием передачи и адаптирует скорость передачи данных. Применение принципов программно определяемого радио SDR позволяет реализовать оконечное устройство и шлюз на одной аппаратной основе.

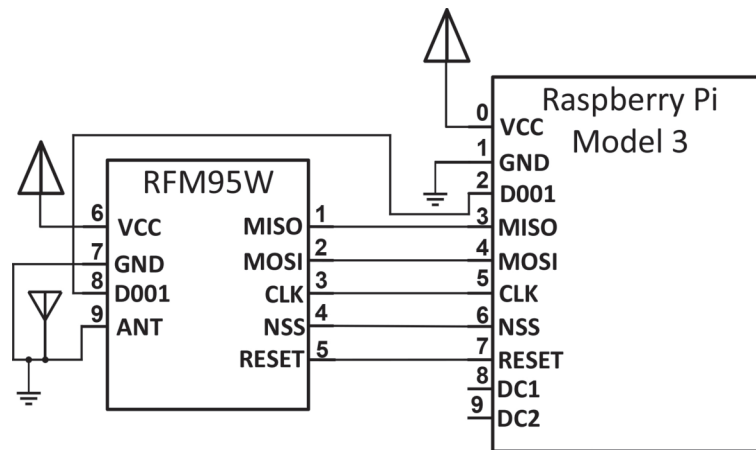


Рисунок 1. Функциональная схема интеллектуального сенсорного узла «ЛоРа-С»

Разработка конструкции сенсорного узла с технологией LoRa и защитой трафика

Для изучения на практике возможностей технологии LoRaWAN, проведения экспериментов для определения помехоустойчивости, защищенности и дальности действия технологии авторами в инициативном порядке был разработан экспериментальный прототип сенсорного узла под шифром «ЛоРа-С».

Устройство собрано из готовых серийных компонент, включает мобильную вычислительную платформу (бортовой компьютер) Raspberry Pi3 и радиомодуль LoRa RFM95W (см. рисунок 1). В компоновку входит съемный аккумулятор в виде батареи для автономной работы в режиме класса A/B/C. Для стабилизации электропитания и использования режима энергоэффективности применяется микроконтроллер, позволяющий использовать различные типы съемных аккумуляторов, в том числе батареи от ноутбуков, включая режим снижения электропотребления в нерабочем режиме.

С помощью дополнительных адаптеров WiFi 802.11n и Bluetooth 4.1 Low Energy (BLE) есть техническая возможность собирать данные от 10 до 100 сенсоров различного назначения в радиусе до 50 м без дополнительных средств связи, обрабатывать эти данные и передавать их корреспондирующему устройству/шлюзу в режиме «точка – точка», «точка – много точек», ячеистая сеть, ad-hoc сеть.

Разработка практически может использоваться компаниями со множеством удаленных объектов, поскольку снижаются затраты на сбор первичных данных за счёт низкой себестоимости готового решения, особенно при массовой установке узлов, в том числе в удаленных и труднодоступных районах. Разработка может применяться,

если требуется организовать контроль и мониторинг состояния производственных помещений и зданий непромышленного назначения.

Общий вид размещения и монтажа компонент узла представлен на рисунке 2. Разработка при использовании влаго- и ударопрочных корпусов может использоваться в полевых условиях, для организации связи «по требованию» без дополнительных затрат на развертывание сети, в том числе при стихийных бедствиях, для дистанционного обслуживания и контроля больных и маломобильных граждан.

Узел «ЛоРа-С» использует свободно распространяемое программное обеспечение, Raspbian или Debian Linux. Для настройки программного обеспечения «ЛоРа-С» достаточно подключить только дисплей и клавиатуру. В целом лабораторный прототип «ЛоРа-С» имеет открытую и масштабируемую программно-аппаратную архитектуру, способную к развитию, расширению и изменению функциональности за счет программного управления.

Преимуществом решения является комплексирование радиомодулей и микрокомпьютера для сбора и передачи информации вместе с автономным источником электропитания и программным обеспечением для сбора, анализа и защиты сенсорных данных.

Основной задачей исследования с помощью комплекса из двух и более конечных узлов «ЛоРа-С» и сервера на базе «ЛоРа-С» являются определение и выбор оптимальных режимов защищенных приема-передачи сенсорной информации в сетях LoRaWAN для городских и полевых условий.

Одновременно проводятся эксперименты по выбору типа приема-передающей антенны с контролируемым направленным и ненаправленным (всесторонним) излучением и определение

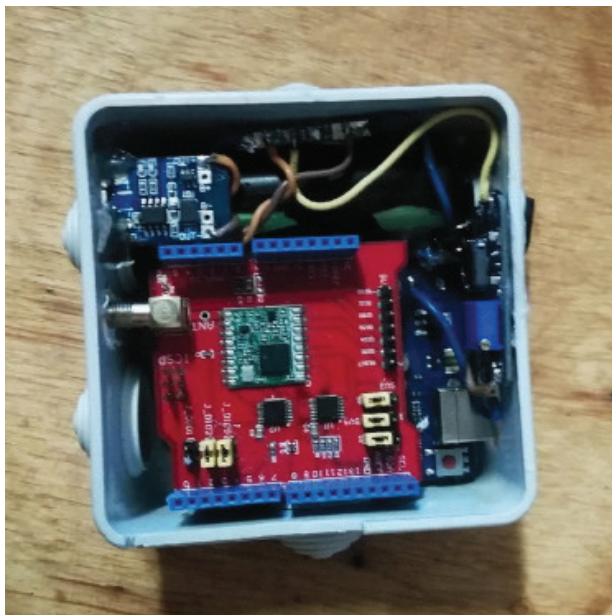


Рисунок 2. Компоновка оконечного интеллектуального сенсорного узла «LoRa-S»

рекомендуемого типа антенны для конкретных условий применения. Также с помощью «LoRa-S» можно исследовать применение различных способов защиты информации, поскольку при использовании технологии LoRaWAN и разработанного узла применяются различные протоколы безопасности для аутентификации, обеспечения конфиденциальности, предотвращения сетевых атак, обнаружения вредоносных узлов и обеспечения бесперебойной IP-сессии.

С точки зрения безопасности контур защиты технологии LoRaWAN и разработанного узла можно описать следующим образом [12; 13].

1. Контур защиты устройства – здесь обеспечивается доступ к устройству LoRaWAN только для приложений авторизованного пользователя, в том числе для подконтрольного изменения данных устройства пользователя.

2. Контур доверенного доступа к сети обеспечивает функционирование в сети только авторизованных устройств. Сетевые службы будут доступны только авторизованным узлам, где под узлом понимаются шлюз, узел-координатор, или оконечный сенсорный узел. В пределах контура доверенного доступа к сети сохраняются конфиденциальность и целостность данных сети LoRa.

3. Контур сети предназначен для обеспечения безопасности сетевой инфраструктуры в целом, включая IP-обмен низкоскоростным трафиком между устройствами, безопасность межсетевых стыков, например при передаче данных из сети LoRaWAN в магистральную сеть.

4. Контур IP-приложений обеспечивает работу на узле только безопасных и доверенных прило-

жений, в результате чего информационный обмен становится безопасным.

Обеспечение защищенной связи для узлов LoRaWAN является сложной задачей, поскольку в рамках стандарта имеются относительно ограниченные возможности обработки данных, достаточно низкая пропускная способность каналов и ограниченная доступная мощность батарей электропитания. В этой связи на перспективу рассматривается вариант конструкции сенсорного узла с возможностью использования солнечных батарей.

В целом с точки зрения безопасности в сети LoRaWAN потенциально возможны следующие модели безопасности.

1. Модель без специальных мер защиты, которая используется в тех случаях, когда сеть LoRaWAN работает в высоконадежной и защищенной зоне безопасности, например с использованием виртуальной частной сети VPN (Virtual Private Network) или аппаратного шифрования. При этом режиме на канальном уровне не должно быть нарушений услуг безопасности обмена и защиты информации, но кадры при этом передаются без проверки целостности или контроля доступа.

2. Модель со списком контроля доступа, когда такой список создается на каждом устройстве LoRaWAN и предотвращает доступ неавторизованных устройств к сетевым ресурсам и данным. Этот режим допускает прием кадра только теми устройствами, которые внесены в список доступа. В результате услуги безопасности характеризуются как ограниченные, поскольку криптографическая защита в этом режиме не используется.

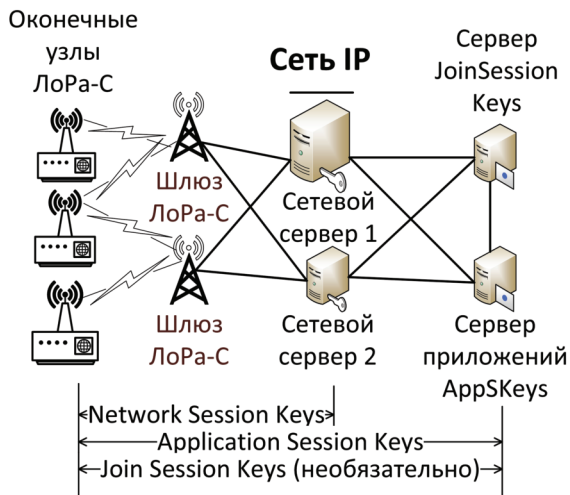


Рисунок 3. Использование предлагаемой конструкции сенсорного узла «ЛоРа-С» с учетом защищенности [12]

3. Модель безопасности с ключом безопасности, например с AES с 128-битным шифрованием, который используется для защиты данных перед их передачей в сети. В этом режиме на устройстве может быть включена любая из служб безопасности в зависимости от критичности приложения.

С точки зрения рассмотренных подходов далее применяется базовая архитектура безопасности на основе модели с ключом безопасности и шифрованием. Для подключения к сети LoRaWAN каждое оконечное устройство должно быть распознано и активировано.

Активация производится двумя способами: либо через активацию по беспроводному интерфейсу ОТАА (Over-The-Air Activation), либо персонализированная активация АВР (Activation By Personalization). Каждое устройство LoRa использует 64-битный расширенный уникальный идентификатор сети (EUI64) для обеспечения безопасности на сетевом уровне, 64-битный расширенный уникальный идентификатор для обеспечения безопасности на уровне приложений и собственный 128-битный уникальный идентификатор, как это показано на рисунке 3.

Для осуществления ОТАА может использоваться специальный сервер участия в сети, Join Server, который осуществляет функцию регистрации устройства LoRaWAN, прежде всего шлюза, в сети LoRa с помощью специального идентификатора JoinEUI. Также возможна идентификация оконечного устройства LoRaWAN с помощью идентификатора EUI128. Указанные идентификаторы могут быть заменены иными идентификационными признаками, которые потенциально могут использоваться для уникального обозначения узлов LoRaWAN.

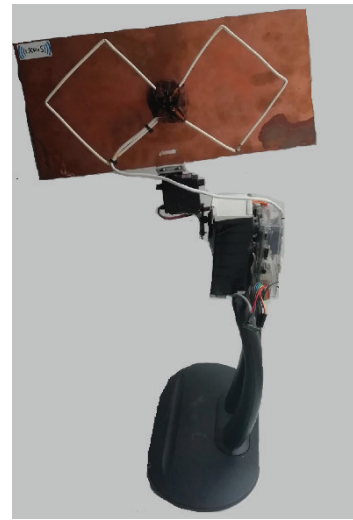


Рисунок 4. Использование управляемой ориентируемой антенны для сенсорного узла «ЛоРа-С»

Разработка алгоритма калибровки приемо-передающей антенны «ЛоРа-С»

Для обеспечения применения комплекса «ЛоРа-С» в полевых и близких условиях, в отличие от штыверной антенны [14], разработана управляемая ориентируемая антенна, показанная на рисунке 4.

За основу конструкции была взята антенна Харченко «двойной биквадрат» из двух квадратов, соединенных в одной из их вершин разомкнутыми сторонами. Электропитание антенны осуществляется из пунктов соединения квадратов. В точке соединения квадратов друг с другом входное сопротивление антенны 50 Ом. В качестве отражателя используется лист омедненного текстолита.

Подвижная конструкция реализуется на двухшаговых сервоприводах MG995, в активном режиме способных выдерживать нагрузку, для 4,8 В равную 8,5 кг/см, либо 6 В с нагрузкой 10 кг/см. В данном случае стабильная работа сервоприводов достигается на 4,8 В. Угол поворота составляет до 120°. Двигатели закрепляются относительно друг друга по двум осям с целью организации поворотного механизма и сканирования пространства для поиска наилучшего направления передачи на узел-сервера LoRa по двум плоскостям. Алгоритм функционирования данного решения показан на рисунке 5.

Каждый из моторов сервопривода выполняет цикл калибровки, после прохождения которого выполняется смещение в каждой плоскости 10 градусов. После прохождения всех циклов калибровки А и Б сервоприводы автоматически устанавливаются в положение, где соотношение

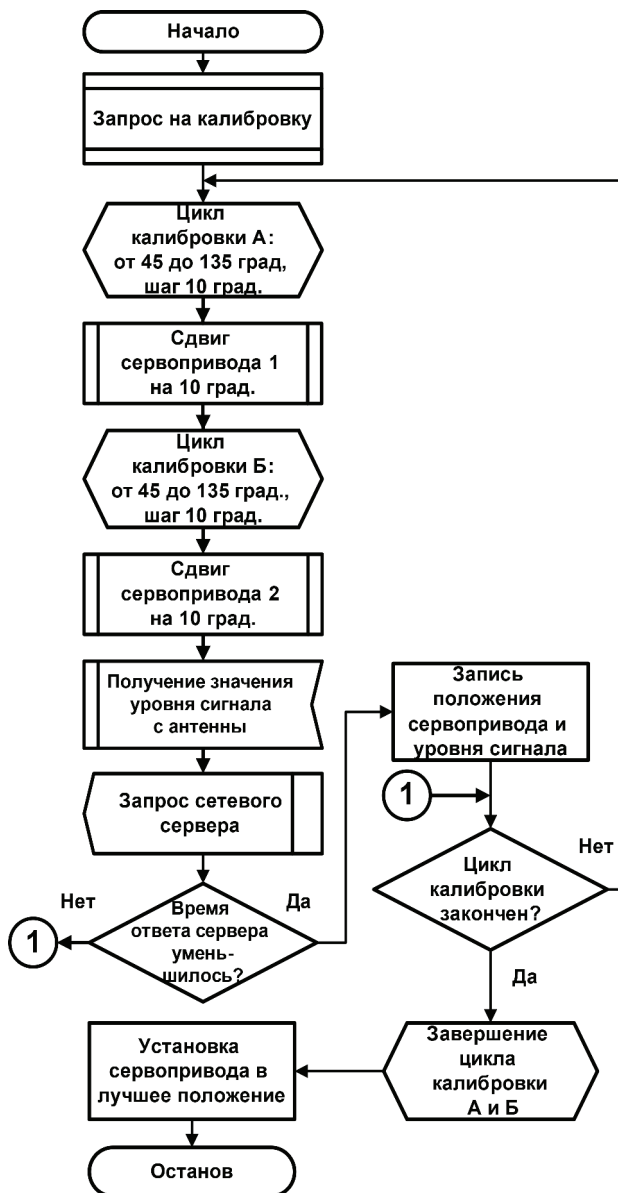


Рисунок 5. Алгоритм калибровки ориентируемой антенны комплекса «ЛоРа-С»

сигнал/шум обеспечивает минимальное время отклика сервера LoRa на рисунке 3.

Начальные эксперименты показали выигрыш от применения антенны на рисунке 4 на расстоянии до 100 м для оконечного узла составляет до 10 дБ и в направлении на сервер.

Заключение

Представлен лабораторный прототип сенсорного узла на базе технологии LoRa с ориентируемой антенной. Сенсорный узел поддерживает протоколы безопасности и является платформой для проведения дальнейших исследований беспроводных сенсорных сетей.

Публикация подготовлена при поддержке Фонда содействия инновациям (договор № 166ГУЦЭС8-D3/56235 от 24.12.2019)

Литература

1. Национальная программа «Цифровая экономика Российской Федерации» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. URL: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (дата обращения: 04.04.2020).
2. Концепция создания и развития сетей 5G/IMT-2020 в Российской Федерации // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. URL: <https://digital.gov.ru/uploaded/files/proekt-kontseptsii-sozdaniya-i-razvitiya-setej-5g-imt-2020-v-rossijskoj-federatsii.pdf> (дата обращения: 04.04.2020).
3. Кумаритова Д.Л., Киричек Р.В. Обзор и сравнительный анализ технологий LPWAN сетей // Информационные технологии и телекоммуникации. 2016. Т. 4, Вып. 4. С. 33–48.
4. Тихвинский В.О., Бочечка Г.С., Коваль В.Н. Технология LoRa: перспективы внедрения на сетях IoT // Первая миля. 2016. № 6. С. 43–49.
5. Выдрин Д.Ф., Ситдииков Д.Р. Основные параметры беспроводной технологии LORAWAN // Academy. 2019. № 2 (41). С. 22–24.
6. Сабко А.Н., Грудковский Н.А. Технология LoRa // Телекоммуникационные системы и сети: материалы 53-й научной конференции. Минск: БГУИР, 2017. С. 85–86.
7. Верхулевский К. Технология LoRa в вопросах и ответах // Беспроводные технологии. 2016. № 1. С. 20–23. URL: <https://rucont.ru/efd/411223> (дата обращения: 04.04.2020).
8. Internet of Things (IoT) using LoRa technology / A. Zourmad [et al.] // Proc. IEEE International conference on automatic control and intelligent systems (I2CASIS). Malaysia: IEEE, 2019. P. 324–330. DOI: 10.1109/I2CASIS.2019.8825008.
9. Гребешков А.Ю., Дараев Д.В. Обмен данными сенсоров с помощью программно-аппаратного комплекса ЛоРа-С // Материалы XXVII Росс. науч.-техн. конф. проф.-препод. состава, науч. сотр. и аспиранта. Самара, ПГУТИ, 2020. С. 24–25.
10. Knoll M., Breitegger P., Bergmann A. Low-power wide-area technologies as building block for smart sensors in air quality measurements // Elektrotechnik and Informationstechnik. 2018. Vol. 135, № 6. P. 416–422.
11. LPWAN technologies for IoT and M2M applications / B.S. Chaudhari [et al.]. London:

- Academic Press is an imprint of Elsevier, 2020. 325 p.
12. Butun I., Pereira N., Gidlund M. Security risk analysis of LoRaWAN and future directions // *Future Internet*. 2019. Vol. 11, № 3. p. 22. DOI: 10.3390/fi11010003.
 13. Мамиллов Б.Е. К вопросу о противостоянии системы LoRa внешним радиопомехам // *Вестник Казахской академии транспорта и коммуникаций*. 2017. Вып. 102, № 3. С. 94–101.
 14. On the performance of LoRaWAN in smart city: end-device design and communication coverage / D. Poluektov [et al.] // 22nd International conference Distributed computer and communication networks (DCCN 2019): revised selected papers. LNCS 11965. Moscow: Springer Cham, 2019. P. 15–29. DOI: 10.1007/978-3-030-36614-8_2.

Получено 04.12.2020

Гребешков Александр Юрьевич, д.т.н., доцент, профессор кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 846 339-11-97. E-mail: grebeshkov-ay@psuti.ru

Дараев Денис Михайлович, специалист по информационной безопасности АО «Инфосистемы Джет» сервисного отделения в г. Самара. 443070, Российская Федерация, г. Самара, ул. Партизанская, 88, офис 2-6. Тел. +7 846 339-11-97. E-mail: d.daraev@yandex.ru

DESIGN OF AN INTELLIGENT SENSOR NODE BASED ON LORA TECHNOLOGY

Grebeshkov A.Y.¹, Daraev D.M.²

¹ *Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation*

² *Jet Infosystems Joint-Stock Company, Samara, Russian Federation*

E-mail: grebeshkov-ay@psuti.ru

These days it is possible to apply different radio technologies for a long-range access and use the radio frequency spectrum as in the licensed part of spectrum as an unlicensed radio frequency. LoRa technology is a register trademark and title of radio access technology for design of low power wide area network at the unlicensed radio frequency spectrum 866 MHz. This paper presents a laboratory prototype of the LoRa-based sensor node device with special oriented motile antenna for the transmission of sensor data. Designed sensor node is ensure to the security requirements for data exchange between the end-node and the LoRa gateway. Designed LoRa sensor node base on the principles of software-defined radio and allows to use the open-source software and off-the-shelf hardware for data processing. As a result, the sensor node, depending on the software settings, can perform the functions of a terminal device or a gateway or server with security protocols supporting. For an increasing of the transmission stability, it is supposed to use a spatially oriented program-control antenna with the possibility of the optimal direction choose for a sensor data transmission. The article describes the result of the development of a sensor node based on the LoRaWAN standard, analyzes the methods and methods of ensuring information security in LoRa networks, and developed an antenna calibration algorithm to select the transmission direction between the terminal device and the gateway.

Keywords: *sensor node, sensor network gateway, LPWAN, LoRa, LoRaWAN, Sigfox, SDR*

DOI: 10.18469/ikt.2021.19.2.06

Grebeshkov Alexander Yuryevich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Professor of Telecommunications Network and Systems Department, Doctor of Technical Science / System, Networks and Telecommunications Devices. Tel. +7 846 339-11-97. E-mail: grebeshkov-ay@psuti.ru

Daraev Denis Mikhaylovich, Join-Stock company «Jet Infosystems» service office at Samara, 88, Partizanskaya Street, office 2-6, Samara, 443070, Russian Federation; Specialist for Information Security. Tel. +7 846 339-11-97. E-mail: d.daraev@yandex.ru

References

1. National program «Digital Economy of the Russian Federation». Ministry of Digital Development, Communications and Mass Media of the Russian Federation: official website. URL: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifro-vaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (accessed: 04.04.2020). (In Russ.)
2. Concept of creation and development of 5G / IMT-2020 networks in the Russian Federation. Ministry of Digital Development, Communications and Mass Media of the Russian Federation: official website. URL: <https://digital.gov.ru/uploaded/files/proekt-kontseptsii-sozdaniya-i-razvitiya-setej-5g-imt-2020-v-rossijskoj-federa-tsii.pdf> (accessed: 04.04.2020). (In Russ.)
3. Kumaritova D.L., Kirichek R.V. Review and comparative analysis of LPWAN network technologies. *Informatsionnye tehnologii i telekommunikatsii*, 2016, vol. 4, no. 4, pp. 33–48. (In Russ.)
4. Tihvinskij V.O., Bochechka G.S., Koval' V.N. LoRa technology: prospects for implementation on IoT networks. *Pervaja milja*, 2016, no. 6, pp. 43–49. (In Russ.)
5. Vydrin D.F., Sitdikov D.R. Basic parameters of LORAWAN wireless technology. *Academy*, 2019, no. 2 (41), pp. 22–24. (In Russ.)
6. Sabko A., Grudkovskij N.A. LoRa technology. *Telekommunikatsionnye sistemy i seti: materialy 53-j nauchnoj konferentsii*. Minsk: BGUIR, 2017, pp. 85–86. (In Russ.)
7. Verhulevskij K. LoRa technology in questions and answers. *Besprovodnye tehnologii*, 2016, no. 1, pp. 20–23. URL: <https://rucont.ru/efd/411223> (accessed: 04.04.2020). (In Russ.)
8. Zourmad A. et al. Internet of Things (IoT) using LoRa technology. *Proc. IEEE International conference on automatic control and intelligent systems (I2CASIS)*. Malaysia: IEEE, 2019, pp. 324–330. DOI: 10.1109/I2CACIS.2019.8825008.
9. Grebeshkov A.Ju., Daraev D.V. Sensor data exchange using the LoRa-S software and hardware complex. *Materialy XXVII Ross. nauch.-tehn. konf. prof.-prepod. sostava, nauchn. sotr. i aspir.* Samara, PGUTI, 2020, pp. 24–25. (In Russ.)
10. Knoll M., Breitegger P., Bergmann A. Low-power wide-area technologies as building block for smart sensors in air quality measurements. *Elektrotechnik and Informationstechnik*, 2018, vol. 135, no. 6, pp. 416–422.
11. Chaudhari B.S. et al. *LPWAN technologies for IoT and M2M applications*. London: Academic Press is an imprint of Elsevier, 2020, 325 p.
12. Butun I., Pereira N., Gidlund M. Security risk analysis of LoraWAN and future directions. *Future Internet*, 2019, vol. 11, no. 3, pp. 22. DOI: 10.3390/fi11010003.
13. Mamilov B.E. To the question of the resistance of the LoRa system to external radio interference. *Vestnik Kazahskoj akademii transporta i kommunikatsij*, 2017, no. 102, pp. 94–101. (In Russ.)
14. Poluektov D. et al. On the performance of LoRaWAN in smart city: end-device design and communication coverage. *22nd International conference Distributed computer and communication networks (DCCN 2019): revised selected papers*. LNCS 11965. Moscow: Springer Cham, 2019, pp. 15–29. DOI: 10.1007/978-3-030-8_2.

Received 04.12.2020