УДК

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ НА ОСНОВЕ ТЕХНОЛОГИИ LORA

Коронец В.Г, студент гр.241301

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лапцевич А.А. – канд. физ.-мат. наук

Аннотация. В работе рассматривается проблема обеспечения информационной безопасности *IoT*-сетей на базе технологии *LoRa*. Предложена архитектура системы многоуровневой верификации, комбинирующая криптографическую защиту с анализом физических характеристик сигнала (частотный отпечаток, *RSSI, SNR*). Обосновано применение топологии *Point-to-Point* и концепции граничных вычислений на базе микроконтроллера *ESP32* и трансивера *SX1278* для обеспечения прямого доступа к прецизионным PHY-метаданным. Успешно реализована компенсация температурного дрейфа кварцевого генератора, повышающая точность аппаратной идентификации узлов. Доказано, что данный подход формирует надежную эшелонированную защиту, устойчивую к подмене устройств, анализу трафика и подавлению радиоканала.

Ключевые слова. Интернет вещей, *LoRa*, информационная безопасность, физический уровень, аутентификация, частотный отпечаток, граничные вычисления, микроконтроллер *ESP32*.

Стремительное развитие технологий Интернета вещей (*IoT*) и расширение сферы их применения в концепциях умного города, индустриального мониторинга и автоматизированного сбора показаний приборов учета (*smart metering*) требуют создания надежных, автономных и энергоэффективных систем передачи телеметрии на большие расстояния. При выборе технологии для построения системы распределенного мониторинга необходимо учитывать множество факторов, так как на рынке беспроводной связи представлен широкий спектр решений, среди которых *Wi-Fi, Bluetooth Low Energy (BLE), ZigBee, NB-IoT и LoRa*.

Технологии *Wi-Fi* (стандарты семейства IEEE 802.11) обеспечивают высокую пропускную способность, однако обладают критически высоким энергопотреблением и ограниченной дальностью действия, которая на практике редко превышает пятьдесят метров в условиях закрытых помещений. Это делает их абсолютно непригодными для долгосрочной автономной работы на обширных территориях, где замена элементов питания затруднена. Технология *Bluetooth Low Energy (BLE)* оптимизирована для сверхнизкого энергопотребления и широко применяется в персональных носимых устройствах, однако ее радиус действия также ограничен несколькими десятками метров, что исключает ее использование в качестве магистрального канала передачи телеметрии распределенных объектов. Стандарт *ZigBee (IEEE 802.15.4*) опирается на сложную ячеистую топологию (*mesh*), требующую постоянного наличия множества активных узлов-маршрутизаторов для поддержания связности сети. Выход из строя ключевых маршрутизаторов может привести к фрагментации сети, а процесс ретрансляции данных неизбежно увеличивает задержки. Альтернативным вариантом выступают сети сотовой связи для *IoT*, такие как *NB-IoT*. Они обеспечивают превосходное покрытие и высокое качество связи, однако жестко привязывают архитектуру к платной инфраструктуре провайдеров. Необходимость использования SIM-карт и регулярной оплаты абонентских тарифов для каждого датчика многократно увеличивает капитальные и операционные расходы, а также делает систему зависимой от внешнего оператора связи.

В свою очередь, технология *LoRa*, базирующаяся на проприетарной модуляции с расширением спектра (*Chirp Spread Spectrum, CSS*), занимает уникальную нишу. Основной физический принцип данной модуляции заключается в том, что частота несущего радиосигнала непрерывно и линейно изменяется во времени в пределах жестко заданной полосы пропускания. Такой подход обеспечивает феноменальную устойчивость канала связи к узкополосным интерференционным помехам, эффекту Доплера и многолучевому замиранию сигнала, характерному для плотной городской застройки. Технология позволяет организовать бесперебойную связь на дистанциях до 10–15 километров в условиях прямой видимости при сохранении сверхнизкого энергопотребления периферийных узлов, способных функционировать от одного литий-ионного элемента питания на протяжении нескольких лет.

Ключевыми конфигурационными параметрами, определяющими характеристики *LoRa*-передачи, выступают коэффициент расширения спектра (*Spreading Factor, SF*), полоса пропускания радиоканала (*Bandwidth, BW*) и коэффициент избыточности помехоустойчивого кодирования (*Coding Rate, CR*). Варьирование этих параметров предоставляет инженерам исключительную гибкость. Коэффициент расширения спектра определяет количество бит информации, кодируемых одним символом (чирпом), и может принимать значения от семи до двенадцати. Увеличение данного коэффициента на единицу экспоненциально увеличивает продолжительность нахождения сигнала в эфире, что позволяет приемнику накапливать больше энергии и успешно демодулировать полезный сигнал даже тогда, когда его уровень находится значительно ниже уровня фонового шума (вплоть до минус двадцати децибел). Оптимальным выбором полосы пропускания для диапазона 433 мегагерц является значение 125 килогерц, которое обеспечивает наилучший компромисс между чувствительностью приемного тракта и скоростью передачи

данных. Кодирование с избыточностью, например, со значением четыре пятых, добавляет служебные биты к полезной нагрузке, предоставляя приемнику возможность математически восстанавливать поврежденные в эфире фрагменты информации без необходимости запроса повторной передачи пакета.

При разработке систем беспроводной связи критически важно учитывать нормативно-правовую базу, регулирующую использование радиочастотного спектра. В Республике Беларусь использование диапазона 433–434 МГц относится к категории лицензионно-свободных частот индустриального, научного и медицинского назначения (*ISM*). Это кардинально упрощает процесс внедрения и масштабирования разрабатываемой системы, так как избавляет от необходимости прохождения сложных бюрократических процедур получения индивидуальных разрешений на использование частот. Единственным строгим нормативным ограничением является соблюдение лимита на максимальную эффективную излучаемую мощность передатчика (до 10 мВт), что неукоснительно соблюдается при программной конфигурации используемых радиомодулей. К тому же радиоволны в субгигагерцовом диапазоне обладают значительно меньшим коэффициентом затухания в свободном пространстве и лучшей проникающей способностью сквозь бетонные и кирпичные перекрытия по сравнению со стандартом 2.4 ГГц.

Несмотря на очевидные физические преимущества, трансляция данных в открытом радиоэфире обуславливает высокую уязвимость канала связи к злонамеренным воздействиям. Угрозы информационной безопасности в сетях *LoRa* можно классифицировать по векторам воздействия на конфиденциальность, целостность и доступность. К наиболее опасным видам кибератак относятся пассивное прослушивание эфира, активный спуфинг, повторное воспроизведение пакетов и целенаправленное глушение радиоканала. Пассивное прослушивание подразумевает использование злоумышленником *SDR*-приемника для сбора трафика. Даже в случае стойкого шифрования данных простой анализ метаданных эфира (время передачи, размер пакетов, частота выхода на связь) позволяет выявить поведенческие паттерны системы и подготовить плацдарм для более сложных вторжений. Атака подмены данных (*Spoofing*) заключается во внедрении в сеть клонированного узла, который, используя украденные идентификаторы, передает фальсифицированную телеметрию, что может привести к принятию критически неверных решений в системах автоматики. Атака повторного воспроизведения (*Replay Attack*) использует запись легального, валидного пакета данных с его последующей многократной ретрансляцией. Глушение канала (*Jamming*) представляет собой генерацию высокомощного шумового или тонального сигнала на рабочей частоте, что приводит к переполнению приемного тракта легитимного шлюза и вызывает полный отказ в обслуживании (*DoS*). Также злоумышленники могут использовать направленные помехи для истощения батарей конечных узлов (атака "отказ в сне"), вынуждая их постоянно пытаться переподключиться к сети.

Традиционные методы защиты, опирающиеся исключительно на прикладную или сетевую криптографию, демонстрируют ограниченную эффективность перед лицом перечисленных угроз. Бесспорно, симметричное шифрование по алгоритму AES-128 и расчет криптографического кода аутентификации сообщения (*MIC*) являются обязательным фундаментом, гарантирующим конфиденциальность и защиту пакета от несанкционированной модификации во время его нахождения в эфире. Строгий контроль монотонно возрастающих счетчиков пакетов (*Sequence Number*) отсекает любые попытки атак повторного воспроизведения. Однако классическая криптография обладает серьезным концептуальным ограничением: она защищает информацию, но не способна достоверно подтвердить аппаратное происхождение радиосигнала. Если злоумышленнику удастся извлечь секретные сессионные ключи из физической памяти одного из датчиков, он сможет сгенерировать программный клон, который будет формировать математически безупречные криптограммы. Сетевой сервер расшифрует их и примет фальшивые данные как легитимные, поскольку не обладает инструментами для верификации самого физического источника.

Понимание этих фундаментальных уязвимостей приводит к необходимости создания гибридных систем многоуровневой верификации, объединяющих строгую математическую криптографию с анализом уникальных физических характеристик приемопередатчиков (методы *PHY-level security*). Анализ существующих отраслевых решений демонстрирует, что доминирующая на рынке стандартизированная архитектура *LoRaWAN* обладает существенными архитектурными ограничениями для реализации таких методов защиты. В классической сети *LoRaWAN* структура разделена на конечные узлы, промежуточные шлюзы и централизованный облачный сетевой сервер. В этой парадигме шлюзы выполняют роль простых ретрансляторов, а основная вычислительная нагрузка и проверка безопасности вынесены в облако. Проблема заключается в том, что стандарт строго регламентирует формат взаимодействия, и прецизионные радиочастотные метаданные, собираемые на приемной антенне шлюза, сильно абстрагируются или вовсе отбрасываются при упаковке пакета для передачи через IP-сеть на сервер.

Для решения данной проблемы в рамках проводимого исследования была разработана специализированная архитектура на основе топологии *Point-to-Point (P2P*), реализующая концепцию периферийных граничных вычислений (*Edge Computing*) непосредственно на самом приемном шлюзе. Отказ от жестких рамок стандарта *LoRaWAN* позволил предоставить управляющему микроконтроллеру шлюза прямой, низкоуровневый доступ к регистрам радиомодуля по высокоскоростной шине SPI. Это открыло возможность извлекать "сырые", неискаженные метаданные физического уровня сразу в момент демодуляции радиопакета.

В качестве единой аппаратной платформы как для периферийных узлов, так и для центрального шлюза обработки был выбран тандем из высокопроизводительного двухъядерного микроконтроллера ESP32 и радиочастотного трансивера *SX1278*. Микроконтроллер *ESP32*, оперирующий на тактовой частоте 240 мегагерц и обладающий 520 килобайтами оперативной памяти, фундаментально решает классическую проблему нехватки вычислительных ресурсов, свойственную традиционным восьмибитным *IoT*-устройствам. Исключительно важным фактором выбора *ESP32* стало наличие встроенного кремниевого сопроцессора для аппаратного ускорения криптографических операций. Бенчмарки показывают, что аппаратная реализация алгоритма шифрования *AES-128* на чипе *ESP32* выполняется в 10–20 раз быстрее по сравнению с программными библиотеками. Это позволяет осуществлять потоковое шифрование и расшифровку плотного потока сообщений от множества датчиков в режиме реального времени без возникновения программных задержек, сохраняя при этом общую энергоэффективность системы. Радиомодуль *SX1278*, в свою очередь, обеспечивает высочайшую чувствительность (вплоть до минус 137 децибел к милливатту) и предоставляет точные метрики состояния канала: индикатор уровня сигнала (*RSSI*), логарифмическое отношение сигнал/шум (*SNR*) и, что самое главное, ошибку несущей частоты (*Frequency Error*). Для обеспечения полной энергонезависимости шлюз спроектирован для работы от литий-ионного аккумулятора повышенной емкости, что позволяет ему функционировать автономно в полевых условиях до полугода.

Комплексный контур безопасности разработанной системы выстраивается в несколько эшелонов, где каждый последующий уровень компенсирует уязвимости предыдущего. На криптографическом уровне конфиденциальность защищается аппаратным *AES-128*, а целостность — проверкой MIC. Параллельно с этим, на физическом уровне, система противодействует пассивному анализу трафика с помощью адаптивного управления мощностью излучения и алгоритмов частотного *хоппинга* — псевдослучайного переключения рабочих частот по криптографически защищенному закону, известному только доверенным узлам. Атаки повторного воспроизведения (*Replay*) блокируются не только проверкой счетчика пакетов, но и строгим таймингом: шлюз анализирует временные интервалы поступления сигналов, отвергая пакеты, пришедшие с аномальной задержкой.

Главным инновационным элементом аппаратной аутентификации выступает анализ смещения несущей частоты, известного как радиочастотный отпечаток (*RF Fingerprint*). Природа этого явления кроется в физическом несовершенстве компонентов. Каждый радиопередатчик тактируется от собственного кварцевого резонатора. Вследствие микроскопических допусков при заводском выращивании и огранке пьезоэлектрических кристаллов, реальная частота генерации каждого чипа имеет уникальное, неповторимое отклонение от идеального номинала, заданного в прошивке (*Carrier Frequency Offset*). Трансивер шлюза SX1278 способен измерять это микроскопическое отклонение для каждого принимаемого пакета путем считывания специального внутреннего регистра. Таким образом, во время фазы инициализации шлюз собирает статистику и формирует уникальный биометрический паспорт для каждого доверенного периферийного датчика. В рабочем режиме каждый входящий пакет, даже если он обладает валидной криптографической подписью, проходит физическую сверку. Если система фиксирует аномальное смещение частоты, не совпадающее с эталонным профилем конкретного узла, устройство идентифицируется как программный клон, и пакет блокируется до его передачи на уровень приложения.

Реализация метода радиочастотных отпечатков сталкивается с серьезной инженерной проблемой: нелинейной температурной нестабильностью самих кварцевых кристаллов. При эксплуатации датчиков в реальных климатических условиях индустриального диапазона (от минус двадцати до плюс шестидесяти градусов Цельсия) резонансная частота кристалла может подвергаться дрейфу величиной в один-два килогерца. Эта температурная погрешность по своей амплитуде значительно превосходит уникальную аппаратную разницу между различными модулями, что неизбежно ведет к массовым ложным срабатываниям системы безопасности. Для нивелирования этого негативного фактора в системе применена сложная адаптивная программно-математическая фильтрация. Каждый периферийный узел оснащен подпрограммой, которая извлекает данные со встроенного в кристалл *SX1278* кремниевого датчика температуры и интегрирует эти показания в зашифрованную полезную нагрузку пакета. На приемной стороне высокопроизводительный процессор *ESP32* в режиме реального времени применяет полиномиальные калибровочные кривые. Анализируя полученную температуру узла, шлюз динамически сдвигает окно ожидаемого эталонного значения частоты, тем самым полностью компенсируя влияние климатических факторов и восстанавливая кристальную достоверность частотного отпечатка.

Помимо прецизионной температурной компенсации, процессор граничного шлюза реализует алгоритмы непрерывного статистического мониторинга качества радиоэфира для защиты сети от атак глушения (*Jamming*). В основе этого механизма лежит анализ отношения сигнал/шум (*SNR*) — показателя, представляющего собой разность между логарифмическими значениями мощности принимаемого полезного сигнала и средней мощности фонового шума в анализируемой полосе частот. Использование концепции скользящего окна (*Sliding Window*) позволяет шлюзу сглаживать кратковременные естественные флуктуации эфира и точно фиксировать начало преднамеренной узкополосной помехи, избегая при этом ложных срабатываний и излишних переконфигураций сети. В штатных условиях эксплуатации, при чистом эфире, периферийные узлы используют минимальный коэффициент расширения спектра, что позволяет передавать данные на высокой скорости и экстремально экономить ресурс батарей. Однако при фиксации резкого и стабильного падения отношения сигнала к шуму, что

является неоспоримым признаком начала атаки глушения, интеллектуальный алгоритм шлюза инициирует протокол выживания сети. По резервному каналу шлюз отправляет доверенным узлам экстренную команду на синхронное увеличение коэффициента расширения спектра до максимального значения. Такой адаптивный переход радикально, экспоненциально повышает чувствительность приемного тракта. Несмотря на то, что время нахождения пакета в эфире возрастает многократно, модуляция *CSS* позволяет шлюзу успешно "вытаскивать" телеметрию из-под мощного слоя белого шума, генерируемого злоумышленником. Таким образом, система гарантированно сохраняет свою функциональность и способность доставлять критически важные данные даже в самых агрессивных условиях радиоэлектронного подавления.

Список использованных источников:

1.Semtech Corporation. SX1276/77/78/79 Datasheet. Rev. 7, 2023.
2.Espressif Systems. ESP32 Technical Reference Manual. Rev. 3.6, 2023.
3.LoRa Alliance. LoRaWAN Specification v1.0.4. 2020.
4.RadioLib Library Documentation. GitHub Repository, 2024.

INFORMATION PROCESSING SYSTEMS BASED ON LORA TECHNOLOGY

Koronets V.G.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Laptsevich A.A.- PhD in Physics and Mathematics

Annotation. The paper considers the problem of ensuring information security of IoT networks based on LoRa technology. The architecture of a multi-level verification system is proposed, combining cryptographic protection with analysis of the physical characteristics of the signal (frequency fingerprint, RSSI, SNR). The application of the Point-to-Point topology and the concept of edge computing based on the ESP32 microcontroller and the SX1278 transceiver to provide direct access to precision PHY metadata is substantiated. The quartz oscillator temperature drift compensation has been successfully implemented, increasing the accuracy of hardware node identification. It is proved that this approach forms a reliable layered protection that is resistant to device substitution, traffic analysis, and radio channel suppression.

Keywords. Internet of Things, LoRa, information security, physical layer, authentication, frequency fingerprint, edge computing, ESP32 microcontroller.