

ПРОТОКОЛЫ И АРХИТЕКТУРЫ ДЛЯ БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ В ИНТЕРНЕТЕ ВЕЩЕЙ С НИЗКИМ ЭНЕРГОПОТРЕБЛЕНИЕМ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ LPWAN-ТЕХНОЛОГИЙ

А.М. Тюнина, В.В. Кондусова, Д.С. Кукуева, Сахаров С.Л.

ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

В статье проводится комплексный анализ протоколов и архитектур для обеспечения безопасного и энергоэффективного взаимодействия в сетях Интернета Вещей (IoT). Основное внимание уделяется сравнительному исследованию LPWAN-технологий, в частности протоколов LoRaWAN и NB-IoT. Детально рассматриваются их сетевые стеки, механизмы безопасности, включая системы шифрования AES-128 и методы аутентификации, рабочие диапазоны частот, а также типовые сценарии применения в различных отраслях. Представлен анализ архитектурных решений LoRaWAN, включая компоненты конечных устройств, шлюзов, сетевого сервера и сервера приложений. Проведено сравнение ключевых параметров LPWAN-технологий по дальности связи, скорости передачи данных, энергопотреблению и безопасности. Результаты исследования демонстрируют компромиссы между энергоэффективностью, стоимостью развертывания и уровнем безопасности в различных IoT-сценариях, что позволяет выбрать оптимальную технологию для конкретных применений.

Ключевые слова: LPWAN, LoRaWAN, NB-IoT, Интернет Вещей, IoT безопасность, энергопотребление, протоколы связи, OTA-обновления, сквозное шифрование, AES-128, LTE Cat-NB1, сетевые уязвимости, диапазоны частот, IoT архитектура.

PROTOCOLS AND ARCHITECTURES FOR SECURE INTERACTION IN THE INTERNET OF THINGS WITH LOW POWER CONSUMPTION: A COMPARATIVE ANALYSIS OF LPWAN TECHNOLOGIES

A.M. Tyunina, V.V. Kondusova, D.S. Kukueva, Sakharov S.L.

Voronezh State University of Forestry and Technologies named after G.F. Morozov

The article provides a comprehensive analysis of protocols and architectures to ensure secure and energy-efficient interaction in the Internet of Things (IoT) networks. The main focus is on the comparative study of LPWAN technologies, in particular the LoRaWAN and NB-IoT protocols. Their network stacks, security mechanisms, including AES-128 encryption systems and authentication methods, operating frequency ranges, as well as typical application scenarios in various industries are discussed in detail. The analysis of LoRaWAN architectural solutions, including components of end devices, gateways, network server and application server, is presented. The key parameters of LPWAN technologies in terms of communication range, data transfer rate, energy consumption and security are compared. The results of the study demonstrate the trade-offs between energy efficiency, cost of deployment, and level of security in various IoT scenarios, which allows choosing the optimal technology for specific applications.

Keywords: LPWAN, LoRaWAN, NB-IoT, Internet of Things, IoT security, power consumption, communication protocols, OTA updates, end-to-end encryption, AES-128, LTE Cat-NB1, network vulnerabilities, frequency ranges, IoT architecture.

Быстрое развитие Интернета Вещей (IoT) сопровождается серьезными вызовами в области безопасности и энергоэффективности. Уникальные характеристики IoT-устройств, включая ограниченные вычислительные ресурсы, длительную автономную работу от батарей и работу в неконтролируемых средах, создают принципиально новые угрозы безопасности. Традиционные подходы к защите информации оказываются неприменимыми в условиях ограниченных ресурсов IoT-устройств, что требует разработки специализированных протоколов и архитектур. Проблема усугубляется разнородностью IoT-экосистемы, включающей устройства с различными требованиями к дальности связи, скорости передачи данных и энергопотреблению. Особую сложность представляет обеспечение безопасности в LPWAN-сетях, где крайне ограниченные ресурсы устройств сочетаются с требованиями многолетней автономной работы. Существующие протоколы безопасности часто оказываются слишком ресурсоемкими для IoT-устройств, что приводит к компромиссам между уровнем защиты и продолжительностью работы. В связи с этим возникает необходимость в комплексном анализе современных LPWAN-технологий с точки зрения их способности обеспечивать баланс между энергоэффективностью, безопасностью и функциональностью в различных сценариях применения IoT.

Главным принципом IoT является автономное взаимодействие физических объектов без прямого участия человека для повышения эффективности процессов и создания новой ценности. Примером может служить автоматизация фермы: датчики влажности почвы автоматически

активируют систему полива, метеодатчики предсказывают заморозки и включают обогрев, а платформа аналитики оптимизирует расход ресурсов без участия агронома. Этот принцип коренным образом отличает IoT от традиционных систем, где человек всегда выступает в роли оператора или контроллера процессов.

Экосистема Интернета Вещей предъявляет уникальные требования к сетевым технологиям: обеспечение многолетней автономной работы устройств от батарей при одновременной гарантии безопасности передаваемых данных. Технологии LPWAN (Low-Power Wide Area Network) предлагают сбалансированное решение, сочетающее дальность связи, энергоэффективность и безопасность.

Сеть LoRaWAN включает в себя следующие основные компоненты: конечные устройства, шлюзы, сетевой сервер и сервер приложений.

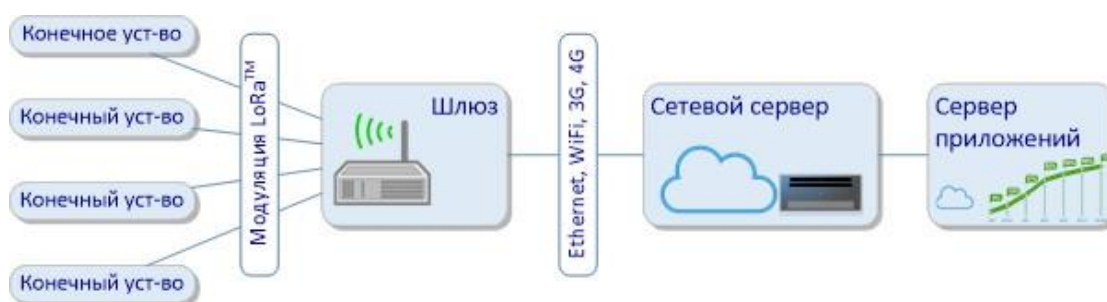


Рисунок 1 – Архитектура LoRaWAN

Конечное устройство представляет собой элемент сети, предназначенный для выполнения измерительных и/или управляющих функций. Оно оснащается необходимыми сенсорными и исполнительными модулями, обеспечивающими сбор данных и реализацию управляющих воздействий в соответствии с поставленными задачами.

Шлюз выполняет функцию промежуточного узла, осуществляющего приём данных от конечных устройств по радиоканалу и их последующую передачу в транзитную сеть. В качестве транзитной среды могут использоваться проводные (Ethernet) или беспроводные (Wi-Fi, сотовые сети) каналы связи. Конечные устройства и шлюз формируют топологию типа звезда (star-of-stars), при которой все конечные устройства взаимодействуют непосредственно со шлюзом. Шлюз, как правило, оснащён многоканальными

приёмопередатчиками, что позволяет ему одновременно обрабатывать сигналы в нескольких радиоканалах или принимать несколько сигналов в одном канале. Совокупность шлюзов формирует радиопокрытие сети и обеспечивает прозрачную двунаправленную передачу данных между конечными устройствами и сетевым сервером.

Сетевой сервер осуществляет централизованное управление сетью LoRaWAN. Его функции включают организацию расписания обмена данными, адаптацию скоростных параметров связи (ADR — Adaptive Data Rate), а также хранение, обработку и маршрутизацию поступающих сообщений.

Сервер приложений выполняет роль верхнего уровня архитектуры, обеспечивая взаимодействие с прикладными сервисами. Он осуществляет удалённый контроль и управление конечными устройствами, а также сбор, обработку и интерпретацию данных, поступающих из сети.

Архитектура сети LoRaWAN реализует иерархическую звездообразную топологию с четким разделением функциональных ролей. Конечные устройства взаимодействуют со шлюзами через радиоканалы, образуя периферийный сегмент сети. Шлюзы функционируют как прозрачные мосты, обеспечивая агрегацию трафика и его передачу на центральный сетевой сервер через транспортные сети. Сетевой сервер выполняет функции координации работы сети, управления подключениями и обработки данных. Модель владения инфраструктурой предполагает, что оператор сети управляет шлюзами и сетевым сервером, в то время как абоненты владеют конечными устройствами. Данная архитектура обеспечивает сквозную защищенную двунаправленную передачу данных между абонентскими устройствами и сетевыми сервисами. Криптографическая защита реализуется на уровне приложений с использованием алгоритмов симметричного шифрования.

Операторская модель обеспечивает централизованное управление сетевыми ресурсами, соблюдение регуляторных требований и снижение эксплуатационных затрат абонентов. При этом сохраняется полная прозрачность передачи данных для пользователей и гарантируется изоляция трафика различных абонентов.

Таблица 1 – Сравнение компонентов

Параметр	LoRaWAN	NB-IoT	Sigfox	LTE-M
----------	---------	--------	--------	-------

Диапа зоны частот	Нелиценз ируемые (868 МГц EU, 915 МГц US)	Лиценз ируемые (LTE bands)	Нелиценз ируемые (868 МГц EU)	Лиценз ируемые (LTE bands)
Дальн ость связи	10-15 км (город), до 40 км (сельская местность)	1-10 км	10-15 км (город), до 50 км (сельская местность)	1-11 км
Ско рость передачи	0.3-50 кбит/с	50- 200 кбит/с	100 бит/с	1 Мбит/с
Потр ебление	Очень низкое (10+ лет)	Низкое (5-10 лет)	Крайне низкое (15+ лет)	Умерен ное(2-5 лет)

Безопасность в IoT требует комплексного подхода, сочетающего корректный выбор протокола связи, реализацию надежных механизмов аутентификации и шифрования, а также разработку эффективных стратегий обновления устройств. Понимание компромиссов между энергоэффективностью, стоимостью и безопасностью позволяет создавать устойчивые IoT-системы, способные противостоять современным киберугрозам.

Перспективы развития безопасных и энергоэффективных решений для IoT связаны с созданием адаптивных систем безопасности, способных динамически регулировать уровень защиты в зависимости от контекста и доступных ресурсов. Особый потенциал демонстрируют подходы, основанные на постквантовой криптографии для защиты от будущих угроз и lightweight-алгоритмах шифрования, оптимизированных для устройств с ограниченными ресурсами. Дальнейшие исследования должны быть направлены на разработку стандартизированных фреймворков безопасности для IoT, обеспечивающих интероперабельность между различными протоколами и платформами. Важным направлением является также создание эффективных механизмов OTA-обновлений, гарантирующих безопасное обновление прошивок даже в условиях нестабильного соединения. Учитывая растущее распространение IoT в критически важных инфраструктурах, особую актуальность приобретают исследования в области resilience-архитектур, способных сохранять работоспособность при частичных отказах и кибератаках. Развитие технологий машинного обучения на edge-устройствах открывает новые возможности для

обнаружения аномалий и проактивного реагирования на угрозы непосредственно на уровне IoT-устройств, снижая зависимость от облачных сервисов и уменьшая задержки при принятии решений

Список литературы

1. Кононенко, А. А. Сети связи "Интернета вещей" - старт стратегических проектов / А. А. Кононенко // Цифровая экономика. – 2020. – № 2(10). – С. 71-76. – DOI 10.34706/DE-2020-02-07. – EDN ENKBTA.
2. Павлова, И. Д. Алгоритм доступа к каналу с прослушиванием несущей для снижения задержки в сетях NB-Fi / И. Д. Павлова, Д. В. Банков // Информационные технологии и системы 2023 (ИТиС 2023) : Сборник трудов 47-й междисциплинарной школы-конференции ИППИ РАН, Огниково, 17–21 сентября 2023 года. – Москва: Институт проблем передачи информации им. А.А. Харкевича РАН, 2023. – С. 287-295. – DOI 10.53921/itas2023_287. – EDN SLBHBFB.
3. Барсков, А. Сети для IoT: LPWAN / А. Барсков // Журнал сетевых решений LAN. – 2016. – № 11. – С. 11-15. – EDN XWQAPX.
4. Нгуен, Д. К. Разработка метода взаимодействия узлов сети LPWAN на базе ячеистой топологии / Д. К. Нгуен, Р. В. Киричек // Интернет вещей и 5G, Санкт-Петербург, 07 декабря 2016 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. – С. 42-46. – EDN XGGXNJ.
5. LPWAN технологии, применяемые в мире интернета вещей / М. Г. Старичихин, Н. С. Графова, С. Д. Храпов, О. О. Латипов // Современные тенденции развития науки и технологий. – 2016. – № 12-4. – С. 76-78. – EDN XHQNTV.
6. Князев, Н. С. Сравнительный анализ стандартов беспроводных сетей LPWAN / Н. С. Князев, В. А. Чечеткин, Д. А. Летавин // Системы синхронизации, формирования и обработки сигналов. – 2017. – Т. 8, № 2. – С. 109-112. – EDN ZWBPOR.

References

1. Kononenko, A. A. Communication networks of the Internet of Things - the start of strategic projects / A. A. Kononenko // Digital Economy. – 2020. – № 2(10). – Pp. 71-76. – DOI 10.34706/DE-2020-02-07 . – EDN ENKBTA.
2. Pavlova, I. D. An algorithm for accessing a channel with listening to a carrier to reduce latency in NB-Fi networks / I. D. Pavlova, D. V. Bankov // Information Technologies and Systems 2023 (ITiS 2023) : Proceedings of the 47th Interdisciplinary School-conference of the IPPI RAS, Ognikovo, September 17-21, 2023. Moscow: A.A. Kharkevich Institute of Information Transmission Problems of the Russian Academy of Sciences, 2023. pp. 287-295. – DOI 10.53921/itas2023_287. – EDN SLBHBFB.
3. Barskov, A. Networks for IoT: LPWAN / A. Barskov // Journal of LAN network Solutions. – 2016. – No. 11. – pp. 11-15. – EDN XWQAPX.
4. Nguyen, D. K. Development of a method for the interaction of LPWAN network nodes based on mesh topology / D. K. Nguyen, R. V. Kirichek // Internet of Things and 5G, St. Petersburg, December 07, 2016. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruевич, 2016. – pp. 42-46. – EDN XGGXHJ.
5. LPWAN technologies used in the world of the Internet of Things / M. G. Starichikhin, N. S. Grafova, S. D. Khrapov, O. O. Latipov // Modern trends in the development of science and technology. – 2016. – No. 12-4. – pp. 76-78. – EDN XHQNTV.
6. Knyazev, N. S. Comparative analysis of LPWAN wireless network standards / N. S. Knyazev, V. A. Chechetkin, D. A. Letavin // Signal synchronization, generation and processing systems. – 2017. – Vol. 8, No. 2. – pp. 109-112. – EDN ZWBPOR.