ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.05

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ УМНОГО ДОМА Z-WAVE, ZIGBEE И THREAD

Ермаков Ярослав Владиславович
Студент группы ИУК5-61Б
Калужский филиал Московского государственного технического университета имени Н.Э. Баумана
ermakovyav@student.bmstu.ru

Ткаченко Анастасия Владимировна
Аспирант кафедра ИУК5 «Системы обработки информации»
Калужский филиал Московского государственного технического университета имени Н.Э. Баумана
tkachenko_av@bmstu.ru

Фадеев Вячеслав Олегович
Студент группы ИУК5-61Б
Калужский филиал Московского государственного технического университета имени Н.Э. Баумана
fadeevvo@student.bmstu.ru

Аннотация

В данной статье были рассмотрены наиболее распространенные беспроводные технологии используемые в IoT с фокусом на их применимости в контексте умного дома. Также представлен анализ их отказоустойчивости, энергопотребления, помехоустойчивости и безопасности.

Ключевые слова: IoT, беспроводные технологии, распределенные сенсорные сети, умный дом.

COMPARATIVE ANALYSIS OF Z-WAVE, ZIGBEE AND THREAD SMART HOME PROTOCOLS

Yaroslav V. Ermakov
Student of group IUK5-61B
Bauman Moscow State Technical University (Kaluga Branch)
ermakovyav@student.bmstu.ru

Anastasiya V. Tkachenko
Postgraduate student of the Department of IUK5 "Information Processing Systems"
Bauman Moscow State Technical University (Kaluga Branch)

tkachenko_av@bmstu.ru

Vyacheslav O. Fadeev
Student of group IUK5-61B
Bauman Moscow State Technical University (Kaluga Branch
fadeevvo@student.bmstu.ru

ABSTRACT

This article reviewed the most common wireless technologies used in IoT with a focus on their applicability in the context of a smart home. An analysis of their fault tolerance, energy consumption, noise immunity and safety is also presented.

Keywords: IoT, wireless technologies, distributed sensor networks, smart home.

Введение

Развитие Интернета вещей (IoT) и концепции умного дома привело к бурному росту беспроводных технологий связи, призванных обеспечить взаимодействие устройств и создание распределенных сенсорных сетей. Однако многообразие доступных протоколов, каждый из которых обладает уникальными характеристиками, создает сложности при выборе оптимальной технологии для конкретных приложений IoT.

Обзор основных беспроводных технологий используемых в IoT

Z-Wave

Одной из целей компании Zensys было предложить упрощенный беспроводной протокол, который бы с достаточной надежностью передавал сообщения в пределах жилого здания. Стек Z-Wave состоит из необходимого минимума (как показано на рис. 1): физический/канальный уровень – для контроля доступа к радиочастотный среде передачи данных, транспортный уровень, на котором осуществляется проверка целостности пакетов данных, подтверждения и ретрансляции, и сетевой уровень, отвечающий за маршрутизацию и интерфейсы приложений.

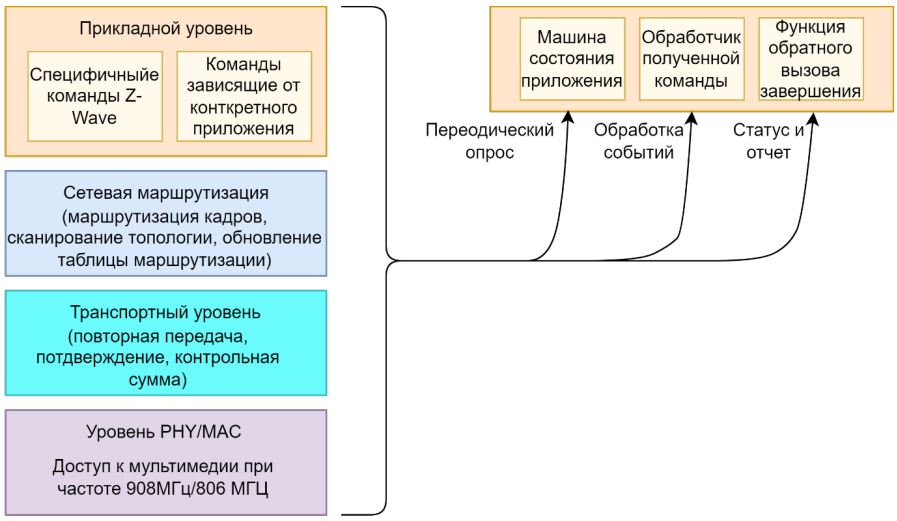
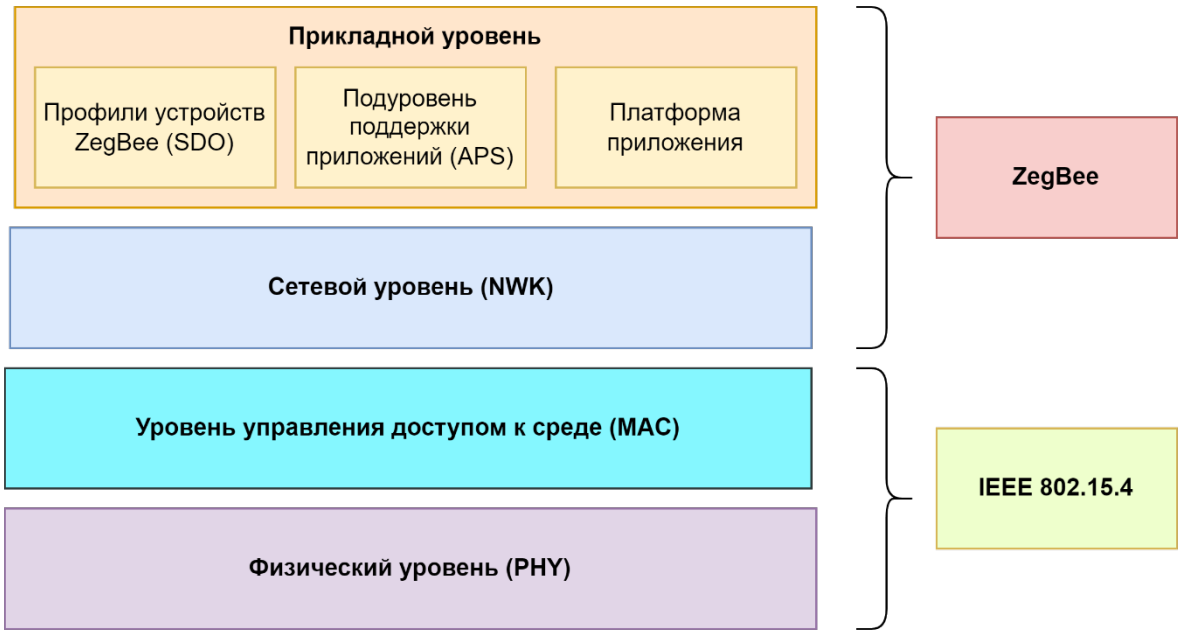


Рисунок 1. Стек протокола Z-Wave и его применение [6]

ZigBee

Стандарт ZigBee разработан для обеспечения низкой стоимости, низкой скорости передачи данных и низкой мощности беспроводной сенсорной сети, как показано на рисунке 2. Протокол нижнего уровня PHY и MAC напрямую использует стандарт IEEE



802.15.4, и предусмотрены дополнительные спецификации сетевого уровня (NWK), уровня поддержки приложений (APS), платформы AP и объекта устройства ZigBee (ZDO). Это также применимо к беспроводным системам мониторинга для промышленной автоматизации, интеллектуального дома, медицинского обслуживания, военного применения и обеспечения безопасности. В ZigBee определены три типа объектов устройств: ZC (координатор ZigBee), ZR (маршрутизатор ZigBee) и ZED (конечное устройство ZigBee).[7]

Рисунок 2. Стек протокола ZigBee

Thread

Стек Thread – это сетевой протокол на основе IPv6, разработанный для маломощных устройств Интернета вещей в беспроводной ячеистой сети IEEE 802.15.4-2006, обычно называемой беспроводной персональной сетью (WPAN).Он разработан специально для подключенных домашних приложений , где требуется подключение к сети на основе IP и в стеке могут использоваться различные прикладные уровни (рис. 3) [5].

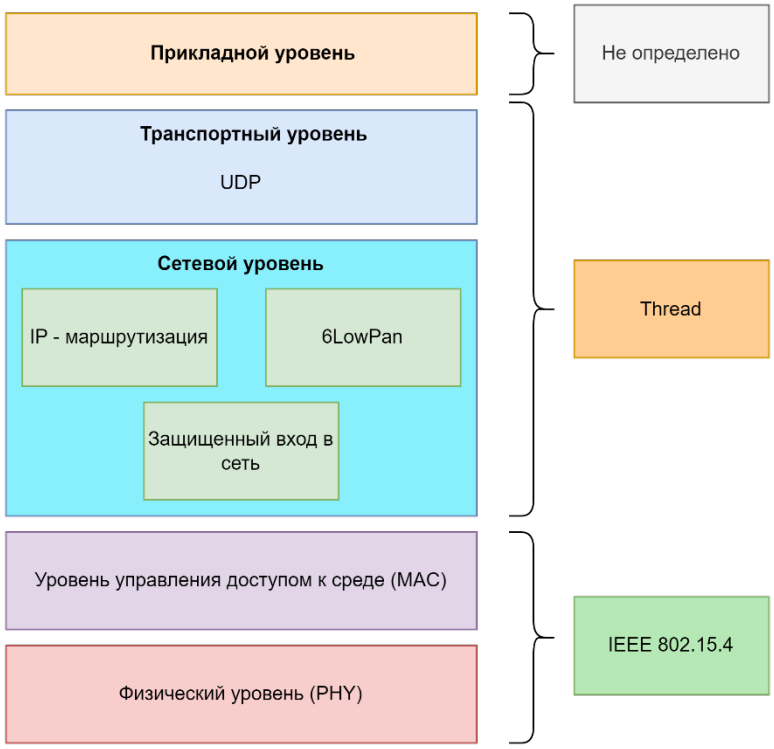


Рисунок 3. Стек протокола Thread

Сравнение протоколов Z-Wave, ZigBee, Thread

Энергопотребление

Протокол Z-Wave использует маршрутизацию с низким энергопотреблением – это позволяет устройствам спать большую часть времени и просыпаться только для передачи данных. Также Z-Wave оптимизирован для минимизации количества передач данных, что также помогает снизить энергопотребление.

В свою очередь устройства ZigBee также могут переходить в спящий режим, что бы сэкономить энергию. Также как и Z-Wave, ZigBee использует протокол маршрутизации с низким энергопотреблением для эффективной передачи данных.

Thread как и Z-Wave с ZigBee позволяет устройствам переходить в спящий режим, а также он использует протокол обмена данными который минимизирует нагрузку на сеть что экономит энергию.

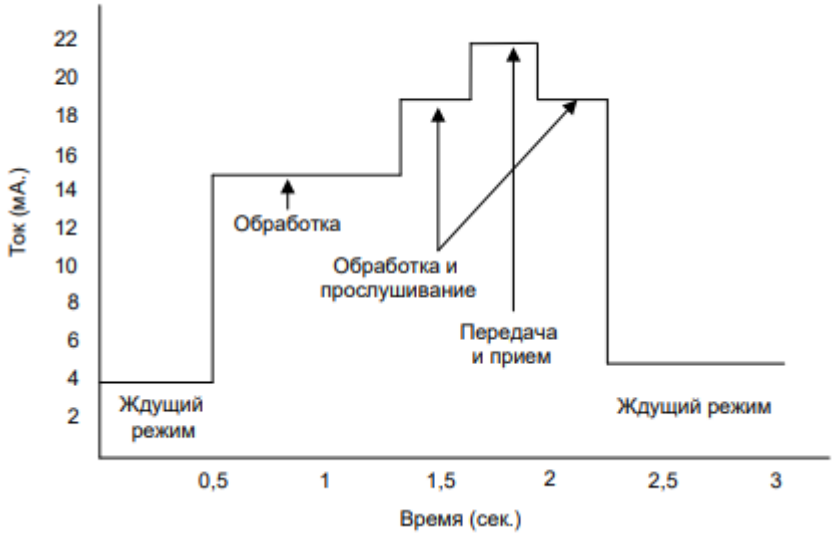


Рис. 4. Потребление тока узлом.[4]

Отказоустойчивость

Протокол Z-Wave обладает функцией практически мгновенного восстановления сети при неполадках в работе узлов. Это достигается за счет использования процедуры Explorer Frame, которая автоматически запускается для определения всех доступных рабочих маршрутов и восстановления работоспособности сети в течение считанных секунд. Дополнительно, функция ассоциации между устройствами позволяет одному устройству напрямую отправлять команды другому устройству, минуя центральный контроллер, что повышает отказоустойчивость и улучшает быстродействие сети Z-Wave.

ZigBee использует механизм повторителей сигнала который позволяет устройствам передавать информацию через несколько узлов (ретрансляторов) в сети. Это обеспечивает надежную доставку данных даже в случае возникновения проблем с прямым соединением между отправителем и получателем. Устройства Zigbee регулярно отправляют подтверждения о получении данных, что позволяет обнаруживать и компенсировать потерю пакетов данных. В случае неудачной передачи данных, протокол автоматически повторяет отправку пакетов для обеспечения доставки.

Thread менее зависим от стандарта 802.15.4, чем ZigBee. Кроме того, Thread предоставляет безопасное сетевое решение, основанное на IP, с возможностью самовосстановления в mesh-сети. Это облегчает подключение устройств к Интернету для доступа к облачным сервисам без необходимости использования специального IP-шлюза, как в случае с ZigBee. Поддержка стандарта 6LoWPAN позволяет взаимодействовать с IP-сетями, используя протокол IPv6 поверх сетей стандарта IEEE 802.15.4.

Помехоустойчивость

Протокол Z-Wave известен своей высокой помехоустойчивостью, которая обеспечивается несколькими механизмами. Один из ключевых факторов - использование радиочастотного диапазона 868,42 МГц в Европе и 908,42 МГц в Северной Америке, что позволяет избежать интерференции с другими устройствами, работающими на более распространенных частотах. Кроме того, применение механизмов маршрутизации и повторения сигналов позволяет обеспечить надежную передачу данных даже в условиях ослабленного сигнала или временных помех. Такие функции как динамическое выбор канала и автоматическое повторное подключение также способствуют повышению надежности и помехоустойчивости сети Z-Wave.

ZigBee работает в сверхзагруженном диапазоне 2,4 МГц. ZigBee плохо справляется с ситуациями, когда в зоне действия сети существуют сильные помехи, создаваемые другими устройствами. Будучи одноканальным решением, ZigBee далеко не всегда может эффективно бороться с помехами, которые часто встречаются в перегруженной полосе 2,4 ГГц, совместно используемой протоколом с такими технологиями, как Wi-Fi или Bluetooth.

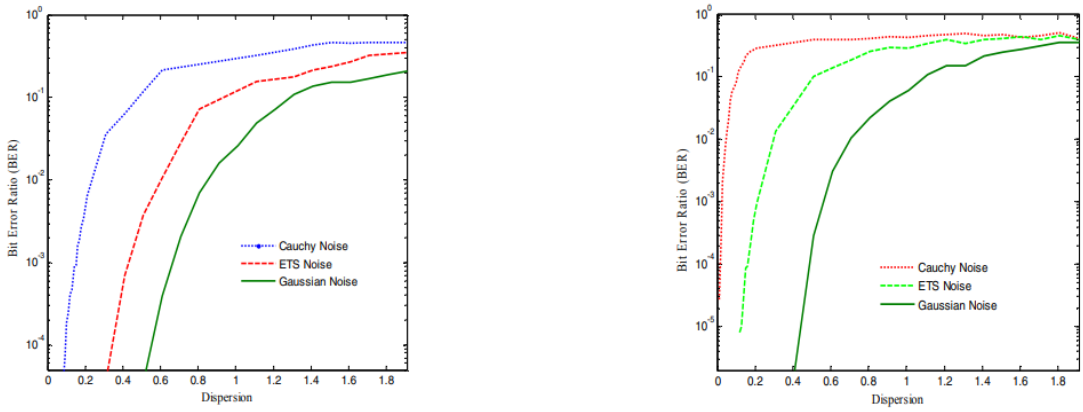


Рис. 5. Смоделированы рабочие характеристики Zigbee в присутствии помех Коши (α = 1), измеренных (α = 1,40) и Гаусса (α = 2) для диапазонов (a) 868/915 и (b) 2,4 ГГц.[3]

Thread так же как и ZigBee работает в безлицензионном радиодиапазоне 2,4 ГГц, но имеет ряд механизмов для минимизации влияния помех. Thread использует адаптивную

частотную модуляция (AFH) для динамического переключения на менее загруженные частотные каналы, избегая помех. Так же он использует автоматический выбор канала (ACS): ACS позволяет устройствам Thread автоматически выбирать оптимальный канал связи с наименьшим уровнем помех.

Безопасность

Протокол Z-Wave принимает серьезные меры для обеспечения безопасности своих сетей умного дома. Одним из ключевых элементов безопасности является использование шифрования AES-128 для защиты передаваемых данных. Этот стандартный протокол шифрования обеспечивает высокий уровень конфиденциальности, делая данные недоступными для несанкционированного доступа.

Дополнительным механизмом безопасности в протоколе Z-Wave является система S2 (Security 2) (рис. 6). S2 представляет собой дополнительный уровень защиты, который обеспечивает аутентификацию и шифрование на более высоком уровне, чем предыдущие версии протокола. Он включает в себя различные методы аутентификации, такие как использование уникальных ключей для каждого устройства и дополнительные методы защиты от взлома.

Система S2 также включает в себя защиту от повторных атак и механизмы обнаружения взлома, что делает протокол Z-Wave более устойчивым к различным видам кибератак.

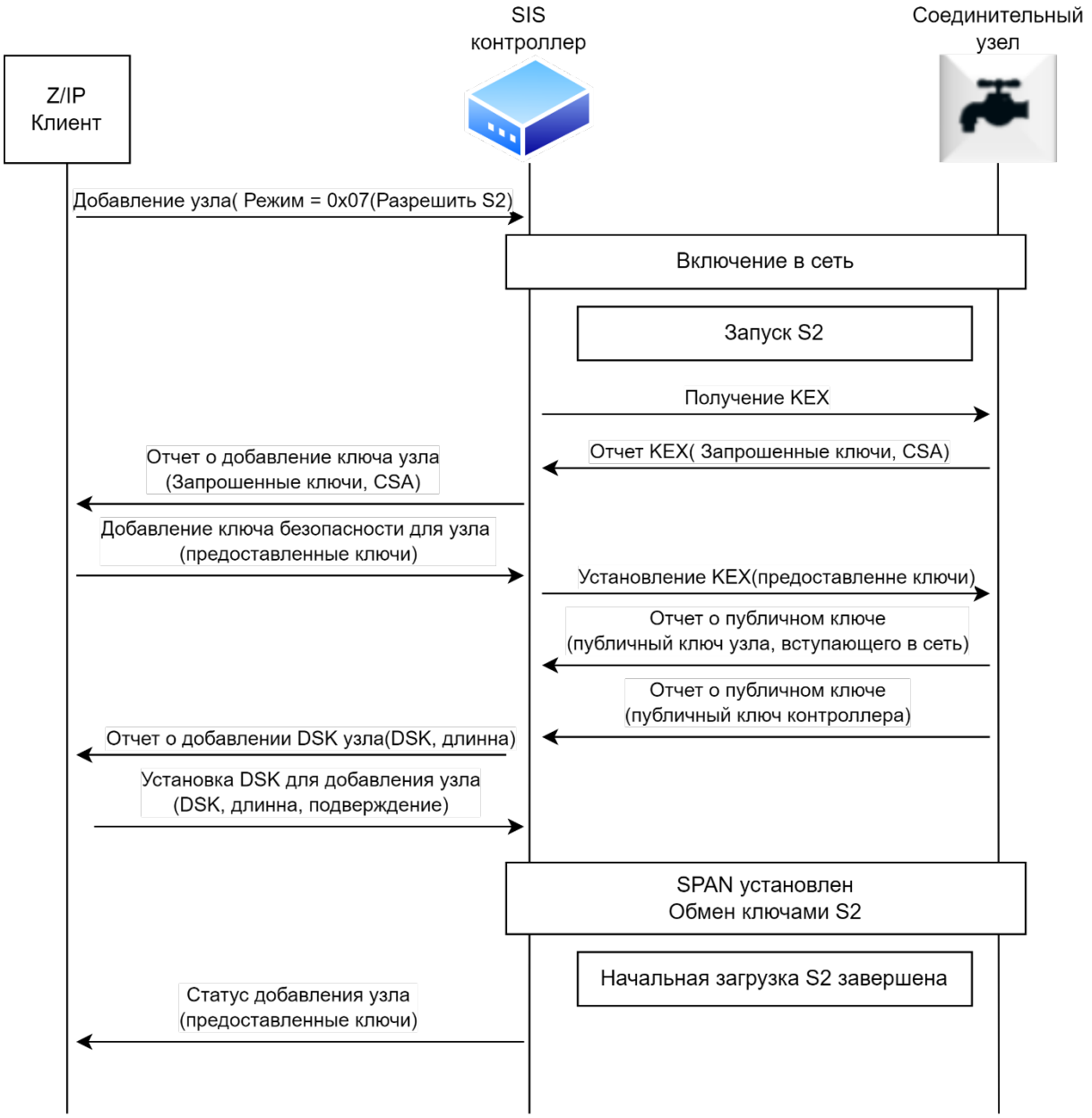


Рис. 6. Включение узла с помощью SIS/Primary контроллера [1]

Zigbee использует 128-битный симметричный ключ для шифрования всех передач на сетевом уровне с использованием AES-128. Сетевые и вспомогательные заголовки отправляются в открытом виде, но аутентифицируются, в то время как сетевая полезная нагрузка аутентифицируется и шифруется. AES-128 используется для создания хэша всей сетевой части сообщения (заголовка и полезной нагрузки), который добавляется в конец сообщения. Этот хэш известен как код целостности сообщения (MIC) и используется для аутентификации сообщения путем проверки его на предмет изменений. Получающее устройство хэширует сообщение и проверяет вычисленное значение MIC по отношению к значению, добавленному к сообщению. Изменения в сообщении аннулируют MIC, и получающий узел полностью отбрасывает сообщение.

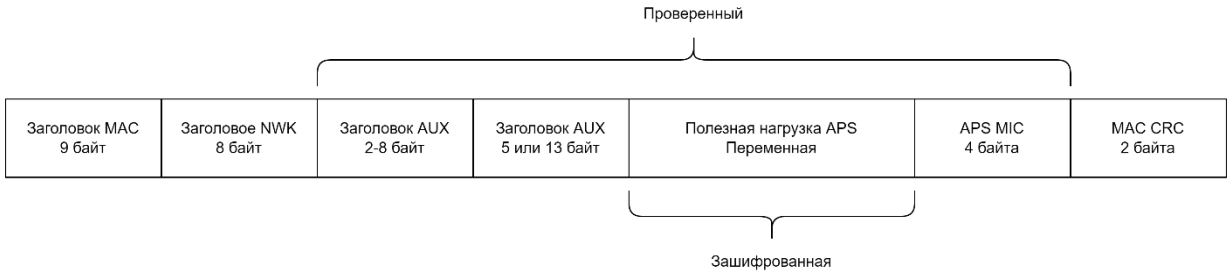


Рис. 7. Безопасность пакета APS [2]

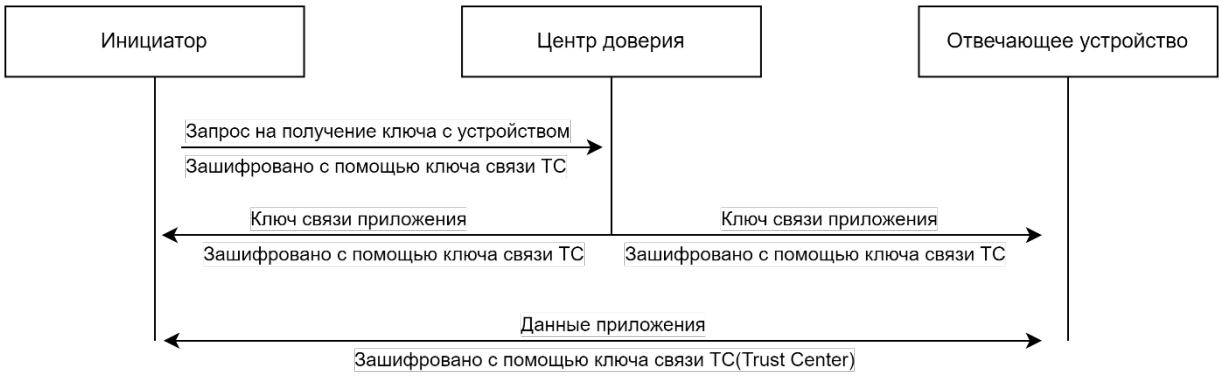


Рис. 8. Установка ключа приложения [2]

Протокол Thread обеспечивает безопасность своей сети с помощью нескольких механизмов. В частности, он использует современные криптографические алгоритмы для шифрования и аутентификации данных. Управление ключами безопасности осуществляется специальными механизмами, позволяющими периодически обновлять или перераспределять ключи. Протокол также включает механизмы аутентификации узлов, защиту от различных видов атак и средства контроля доступа к сети.

Заключение

Исследование этих трех протоколов умного дома позволило провести сравнительный анализ их ключевых характеристик, включая безопасность, помехоустойчивость, энергопотребление и отказоустойчивость.

С точки зрения безопасности, все три протокола демонстрируют высокий уровень защиты данных и устройств в сети, хотя подходы к реализации безопасности могут немного различаться.

В отношении помехоустойчивости, каждый из протоколов имеет механизмы, способные справиться с внешними воздействиями и обеспечить стабильную работу сети умного дома даже в условиях электромагнитных помех или перегрузок сети, но так как Z-Wave работает в нелицензируемой части диапазона, то помехоустойчивость у него будет выше.

Вопрос энергопотребления является ключевым для умных домов, особенно для устройств с батарейным питанием. Исследование показало, что протоколы Z-Wave, Zigbee и Thread предлагают эффективные механизмы управления энергопотреблением, что позволяет продлить срок службы батарей и снизить общие затраты на эксплуатацию системы.

Наконец, отказоустойчивость является критически важным аспектом для систем умного дома, поскольку непредвиденные сбои могут привести к нарушению нормального функционирования системы и угрозам безопасности. Сравнительный анализ показал, что Z-Wave, Zigbee, Thread имеют ячеистую топологию сети, а так же свои методы для поддержания работы сети, что обеспечивает высокую отказоустойчивость системы в целом.

Список литературы:

1. Z/IP and Z-Wave Traffic Analysis [Электронный ресурс] URL: https://docs.silabs.com/z-wave/1.0.0/z-wave-training-docs/gateway-session3-traffic-analysis (дата обращения 01.03.2024)
2. AN1233: Zigbee Security [Электронный ресурс] URL: https://www.silabs.com/documents/public/application-notes/an1233-zigbee-security.pdf (дата обращения 01.03.2024)
3. Vulnerability of Zigbee to Impulsive Noise in Electricity Substations [Электронный ресурс] URL: https://www.ursi.org/proceedings/procGA11/ursi/E07-4.pdf (дата обращения 01.03.2024)
4. Проблемы энергоэффективности и защиты данных в беспроводных сенсорных сетях [Электронный ресурс] URL: https://www.elibrary.ru/item.asp?id=26847534 (дата обращения 01.03.2024)
5. Thread Stack Fundamentals [Электронный ресурс] URL: https://www.threadgroup.org/Portals/0/documents/support/ThreadOverview_633_2.pdf (дата обращения 01.03.2024)
6. Application oriented wireless sensor network communication protocols and hardware platforms A survey [Электронный ресурс] URL: https://www.researchgate.net/publication/224327774_Application-oriented_wireless_sensor_network_communication_protocols_and_hardware_platforms_A_survey (дата обращения 01.03.2024)
7. Reliable Data Broadcast for Zigbee Wireless Sensor Networks [Электронный ресурс] URL: https://www.researchgate.net/publication/267375044_Reliable_data_broadcast_for_zigbee_wireless_sensor_networks (дата обращения 01.03.2024)

References:

1. Z/IP and Z-Wave Traffic Analysis [Electronic resource] URL: https://docs.silabs.com/z-wave/1.0.0/z-wave-training-docs/gateway-session3-traffic-analysis (accessed 03/01/2024)
2. AN1233: Zigbee Security [Electronic resource] URL: https://www.silabs.com/documents/public/application-notes/an1233-zigbee-security.pdf (accessed 03/01/2024)
3. Vulnerability of Zigbee to Impulsive Noise in Electricity Substations [Electronic resource] URL: https://www.ursi.org/proceedings/procGA11/ursi/E07-4.pdf (accessed 03/01/2024)
4. Problems of energy efficiency and data protection in wireless sensor networks [Electronic resource] URL: https://www.elibrary.ru/item.asp?id=26847534 (accessed 03/01/2024)
5. Thread Stack Fundamentals [Electronic resource] URL: https://www.threadgroup.org/Portals/0/documents/support/ThreadOverview_633_2.pdf (accessed 03/01/2024)
6. Application oriented wireless sensor network communication protocols and hardware platforms A survey [Electronic resource] URL: https://www.researchgate.net/publication/224327774_Application-

oriented_wireless_sensor_network_communication_protocols_and_hardware_platforms_A_survey (accessed 03/01/2024)

7. Reliable Data Broadcast for Zigbee Wireless Sensor Networks [Electronic resource] URL: https://www.researchgate.net/publication/267375044_Reliable_data_broadcast_for_zigbee_wireless_sensor_networks (accessed 03/01/2024).