МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математического моделирования и анализа данных

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ В IoT СИСТЕМАХ

Курсовая работа

Шиляева Ивана Владимировича
студента 4 курса, 9 группы
специальность
«компьютерная безопасность»

Научный руководитель:
ассистент
М.А. Казловский

Минск, 2021

Оглавление

Введение

Термин «Интернет вещей» («Internet of Things») появился более 20 лет назад, а история развития технологии насчитывает почти два столетия. Среди множества определений термина можно выделить следующее: интернет вещей — это глобальная сеть объектов, подключённых к интернету, которые взаимодействуют между собой и обмениваются данными без вмешательства человека.

Основными компонентами IoT систем являются:

- объекты, или «вещи»;
- данные, которыми они обмениваются;
- инфраструктура, с помощью которой осуществляется взаимодействие.

К последнему пункту можно отнести разнообразные виды соединения и каналы связи, программные средства и протоколы. Инфраструктура и её криптографический аспект представляют собой наибольший практический интерес и составляют предметную область данной работы.

Говоря о практическом применении Интернета вещей, многие отрасли выигрывают при использовании этой технологии. И в каждой из этих отраслей необходимо думать о безопасности и защите данных. В связи с этим возникают задачи актуализации знаний об алгоритмах и протоколах, применяемых в данной сфере, их сравнении и реализации в рамках программного обеспечения, а также рассмотрения вариантов модификации и улучшения этих протоколов с применением белорусской криптографии. Эти задачи и легли в основу данной работы. В соответствии с задачами были поставлены следующие цели:

1. Изучить сетевые протоколы, применяемые в сфере IoT, и провести их сравнительный анализ;
2. Разобрать криптографический аспект описанных в первой главе сетевых протоколов в контексте используемых в них криптографических протоколов и алгоритмов;

3. Описать уязвимости и угрозы используемых решений;

4. Проанализировать возможность модификации криптографических протоколов и алгоритмов с внедрением элементов белорусской криптографии.

Данная работа состоит из 4 глав, в которых последовательно раскрываются все перечисленные выше вопросы.

Глава 1

Анализ литературы

1.1 Технологии Интернета вещей

IoT включает в себя бесчисленное количество технологий и решений, и чтобы понять их все, необходимо потратить немало времени. Однако в целях упрощения существует возможность разбить весь IoT стек на четыре базовых технологических уровня, которые позволяют функционировать всему Интернету вещей.

Аппаратное обеспечение устройств является первым из этих уровней. Устройства — это те самые «вещи» в аббревиатуре IoT. Выступая в роли интерфейса между реальным и цифровым миром, они могут принимать разные формы и размеры, а также иметь разные уровни технологической оснащённости в зависимости от выполняемой задачи. Практически любой предмет может быть подключен к Интернету и оснащён необходимым инструментарием (сенсорами, датчиками и т.д.) в целях измерения и сбора данных. Единственным существенным ограничением может быть реальный практический сценарий использования.

Программное обеспечение является элементом, который делает девайсы по-настоящему «умными». Программы ответственны за коммуникацию с облаком, сбор данных, взаимодействие между устройствами, а также анализ данных в реальном времени. Более того, программное обеспечение помогает взаимодействовать с IoT системами на уровне приложения конечному пользователю, визуализирую обработанные данные для него.

Уровень коммуникации (или сообщения) тесно связан с программным и аппаратным обеспечением, однако необходимость рассматривать его отдельно является ключевой. Этот уровень содержит средства для обмена информацией между умными устройствами и основным IoT миром. Он включает в себя как физическое соединение, так и специальные протоколы, на которых будет сделать акцент в данной работе. Выбор правильного решения

для обмена сообщениями является ключевым при построении каждой системы. Технологии отличаются в зависимости от способа передачи данных и управления устройствами.

Благодаря программному и аппаратному обеспечению девайсы могут считывать, что происходит вокруг, и коммуницировать с пользователями по специальным каналам связи. **IoT платформа** — это место, в котором все собранные данные обрабатываются, анализируются и представляются пользователю в удобном виде. Её достоинством является извлечение полезных данных из большого объёма информации, который передаётся от устройств по каналам связи.

1.2 Используемые протоколы

Существует множество разнообразных способов взаимодействия умных устройств между собой. Поэтому при выборе протоколов для Интернета вещей часто возникает вопрос о том, есть ли реальная необходимость разработки новых решений, в то время как хорошо зарекомендовавшие себя протоколы сети Интернет уже используются повсеместно десятилетиями. Причина для этого кроется в том, что существующие протоколы часто оказываются недостаточно эффективными и слишком энергоёмкими для работы с возникающими IoT технологиями. Поэтому речь пойдёт об альтернативных решениях, посвящённых именно IoT системам.

Одна из возможных классификаций разбивает все протоколы на три группы: близкого, среднего и дальнего действия. Наиболее ярким представителем первой группы является Bluetooth, который несмотря на свою повсеместную распространённость остаётся далеко не лучшим решением, особенно при передаче больших объёмов данных. К последней группе относят такие протоколы как NB-IoT, LTE Cat-M1, LoRa WAN и SigFox. Эти решения являются весьма современными и продвинутыми, однако используются часто в масштабах предприятий. Наша же цель заключается в изучении решений, применимых к простым пользователям IoT систем, поэтому данный раздел будет преимущественно сконцентрирован вокруг второй группы, а именно протоколов средней зоны действия.

1.2.1 ZigBee

Этот популярный стандарт беспроводных сетей находит свое наиболее частое применение в системах управления дорожным движением, бытовой электронике и машиностроении. Созданный на базе стандарта IEEE 802.15.4,

Zigbee поддерживает высокую отказоустойчивость, низкое энергопотребление, безопасность и надежность.

Протокол ZigBee описывает беспроводные персональные сети (Wireless personal area network, WPAN). Технология, определённая спецификацией Zig-Bee, подразумевает более дешёвое производство по сравнению с другими беспроводными персональными сетями, такими как Bluetooth, или более общими технологиями, такими как Wi-Fi. ZigBee обычно используется в решениях, требующих долгого времени работы (например, от батареи), и безопасной передачи данных. Индивидуальные устройства в подобной сети могут работать на одной батарее до двух лет. Сети на основе ZigBee характеризуются довольно низкой пропускной способностью (до 250 Кбит/с) и дальностью связи между узлами до 100 метров (на открытой местности это значение может достигать 200 метров). Протокол был задуман в 1998 году. Первоначальная спецификация была признана стандартом IEEE в 2003 году, а первые модули, совместимые с ZigBee, появились в массовой продаже в начале 2006 года [1].

Существует три класса устройств Zigbee:

1. Координатор Zigbee (ZC). Он образует корень сетевого дерева и может соединяться с другими сетями, являясь самым функциональным устройством. В каждой сети есть только один координатор Zigbee, поскольку именно это устройство является создателем сети. Однако спецификация Zigbee LightLink позволяет работать без координатора, что делает её более пригодной для использования в готовых домашних продуктах. Координатор хранит информацию о сети, выполняя в том числе функции удостоверяющего центра и хранилища ключей безопасности.

2. Маршрутизатор Zigbee (ZR). Помимо выполнения функции приложения, маршрутизатор может выступать в качестве промежуточного звена, передавая данные от других устройств.

3. Конечное устройство Zigbee (ZED). Содержит достаточно функций, чтобы общаться с координатором или маршрутизатором и не может передавать данные от других устройств. Такое взаимодействие позволяет узлу находиться в спящем состоянии значительную часть времени, что обеспечивает длительное время автономной работы. ZED требует наименьшего объема памяти и поэтому может быть дешевле в производстве, чем координатор или маршрутизатор.

Посмотрим на классы устройств ZigBee на примере беспроводного выключателя света. Узел Zigbee на лампе способен постоянно принимать сигнал,

так как он подключён к электрической сети. В то же время выключатель, работающий от батарейки, будет находиться в спящем режиме большую часть времени: до тех пор, пока его состояние не будет изменено. В этом случае выключатель просыпается, посылает команду лампе, дожидается подтверждения и возвращается в спящий режим. В подобной сети узел лампы должен быть по меньшей мере маршрутизатором сети, узел выключателя обычно является конечным устройством.

ZigBee был разработан как стандарт для радиосетей с ячеистой (mesh) топологией, предназначенных для использования в системах телеметрии, для связи между различными типами датчиков, устройств мониторинга, а также для беспроводного считывания результатов измерений с приборов учета энергии, тепла и т.д. Кроме того, ZigBee поддерживает сети с топологией «звезда» и «дерево». В каждой сети должно быть одно устройство-координатор. В сетях с топологией «звезда» координатор должен быть центральным узлом. Как древовидные, так и ячеистые сети позволяют использовать маршрутизаторы Zigbee для расширения связи на сетевом уровне. Стандарт ZigBee представляет собой относительно простой, устойчивый к ошибкам связи и несанкционированному считыванию, пакетный протокол обмена данными, который часто реализуется в устройствах с относительно небольшими требованиями, таких как микроконтроллеры, датчики и т.д.

ZigBee легко устанавливать и обслуживать, поскольку он основан на самосборке и самовосстанавливающейся топологии сети. Он также легко масштабируется до тысяч узлов, а максимальное число узлов в подобной сети может достигать 65000. В настоящее время существует множество поставщиков, предлагающих устройства, поддерживающие этот открытый стандарт.

Устройства, использующие ZigBee, преимущественно включают в себя беспроводные лампочки и выключатели света, системы управления дорожным движением и другое потребительское и промышленное оборудование. Типичными сферами применения являются:

- домашняя автоматизация;
- промышленные системы управления;
- сбор медицинских данных;
- оповещение о задымлении и несанкционированном проникновении;
- автоматизация зданий.

Zigbee Alliance — это группа компаний, которые поддерживают и публикуют стандарт Zigbee [2]. Название Zigbee является зарегистрированной

торговой маркой этой группы и представляет из себя не просто технический стандарт. Организация публикует материалы, которые позволяют производителям создавать совместимые продукты. Связь между IEEE 802.15.4 и Zigbee похожа на связь между IEEE 802.11 и Wi-Fi Alliance.

За годы существования альянса его членами стали более 500 компаний, включая Comcast, Ikea, Legrand, Samsung SmartThings и Amazon. Zigbee Alliance имеет три уровня членства. Члены первой группы имеют доступ к готовым спецификациям и стандартам Zigbee, а члены второй — право голоса, играя роль в развитии Zigbee и имея ранний доступ к спецификациям и стандартам для разработки продуктов.

1.2.2 Z-Wave

Z-Wave — это протокол беспроводной связи, используемый в основном для домашней автоматизации. Он применяется преимущественно для управления бытовой техникой и другими устройствами, такими как освещение, охранные системы, термостаты, окна, замки, бассейны и открыватели гаражных дверей. Как и другие протоколы, предназначенные для рынка автоматизации дома и офиса, система Z-Wave может управляться через Интернет со смартфона, планшета или компьютера, а также локально через умную колонку или хаб, настенную панель со шлюзом Z-Wave или центральным устройством управления. Z-Wave обеспечивает совместимость на прикладном уровне между системами управления домом различных производителей, входящих в её альянс. Число совместимых продуктов Z-Wave значительно растёт, к 2019 году их количество составляло более 2600 [3].

Протокол Z-Wave был разработан датской компанией Zensys, расположенной в Копенгагене, в 1999 году. В этом же году была представлена потребительская систему управления светом. Набор микросхем серии 100 был выпущен в 2003 году, а серии 200 — в мае 2005 года. Микросхема серии 500, также известная как Z-Wave Plus, была выпущена в марте 2013 года, с увеличенным в четыре раза объемом памяти, улучшенным радиусом действия беспроводной связи и увеличенным временем автономной работы. Технология начала распространяться в Северной Америке примерно в 2005 году, когда пять компаний приняли Z-Wave и сформировали Z-Wave Alliance, целью которого является продвижение использования технологии Z-Wave [4]. При этом все продукты компаний, входящих в альянс, должны быть совместимы. В том же 2005 году технология получила первые инвестиции.

В настоящее время Z-Wave Alliance насчитывает более 700 производителей. Основными членами альянса являются ADT Corporation, Assa Abloy, Jasco, Leedarson, LG Uplus, Nortek Security & Control, Ring, Silicon Labs,

SmartThings, Trane Technologies и Vivint.

Взаимодействие Z-Wave на уровне приложений обеспечивает обмен информацией между устройствами и позволяет всем аппаратным и программным средствам Z-Wave работать вместе. Технология беспроводной ячеистой сети (аналогичная с ZigBee) позволяет любому узлу напрямую или косвенно общаться с соседними узлами, управляя любыми дополнительными узлами. Узлы, находящиеся в радиусе действия, общаются друг с другом напрямую. Если они не находятся в радиусе действия, они могут связаться с другим узлом, который расположен в зоне действия обоих узлов, чтобы получить доступ и обменяться информацией.

Z-Wave разработан для обеспечения надёжной передачи небольших пакетов данных с низкой задержкой на скорости до 100 кбит/с. Пропускная способность составляет 40 кбит/с и подходит для приложений управления и датчиков, в отличие от Wi-Fi и других систем беспроводных локальных сетей на базе IEEE 802.11, которые предназначены в основном для высокой скорости передачи данных. Расстояние связи между двумя узлами составляет около 40 метров.

Z-Wave функционирует в диапазоне частот до 1 ГГц. Этот диапазон конкурирует с некоторыми беспроводными телефонами и другими устройствами бытовой электроники, но позволяет избежать помех в виде Wi-Fi, Bluetooth и других систем, работающих в переполненном диапазоне 2,4 ГГц.

Z-Wave использует архитектуру ячеистой сети с маршрутизацией от источника. Устройства могут связываться друг с другом, используя промежуточные узлы для активной маршрутизации и обхода бытовых препятствий или мертвых зон. Таким образом, сеть Z-Wave может охватывать гораздо большее расстояние, чем радиус действия одного узла. Однако при наличии нескольких таких переходов может возникнуть небольшая задержка между управляющей командой и желаемым результатом.

Простейшая сеть представляет собой одно управляемое устройство и первичный контроллер. Дополнительные устройства могут быть добавлены в любое время, как и вторичные контроллеры,включая приложения для смартфонов и ПК, разработанные для управления и контроля сети Z-Wave. Сеть может включать до 232 устройств, а при необходимости увеличения количества устройств возможно объединение сетей.

Каждой сети Z-Wave назначается идентификатор, а каждое устройство содержит идентификатор узла. Идентификатор сети (Home ID) — это общая идентификация всех узлов, принадлежащих к одной логической сети Z-Wave. Сетевой ID имеет длину 4 байта и присваивается каждому устройству первичным контроллером, когда устройство добавляется в сеть. Узлы с разными сетевыми идентификаторами не могут взаимодействовать друг с другом.

Идентификатор узла — это адрес одного узла в сети. Идентификатор узла имеет длину 1 байт и является уникальным в своей сети.

Чип Z-Wave оптимизирован для устройств, работающих от батарей, и большую часть времени находится в режиме энергосбережения, чтобы потреблять меньше энергии, просыпаясь только для выполнения своей функции. В ячеистых сетях Z-Wave каждое устройство в доме распространяет беспроводные сигналы по всему дому, что приводит к низкому энергопотреблению, позволяя устройствам работать годами без необходимости замены батарей. Чтобы устройства Z-Wave могли передавать сторонние сообщения, они не должны быть в спящем режиме. Поэтому устройства, работающие от батарей, не предназначены для использования в качестве ретрансляторов.

1.2.3 Wi-Fi

Построенный на базе стандарта IEEE 802.11, Wi-Fi остаётся самым распространённым и наиболее известным беспроводным протоколом взаимодействия. Его широкое использование в мире IoT в основном ограничено энергопотреблением выше среднего по причине удержание качественного сигнала и быстрой передачи данных для лучшего соединения и надёжности. Несмотря на это Wi-Fi является ключевой технологией в развитии и распространении IoT.

Для создания сети Wi-Fi требуются устройства, способные передавать беспроводные сигналы, то есть такие устройства, как телефоны, компьютеры или маршрутизаторы. В домашних условиях маршрутизатор используется для передачи интернет-соединения из общественной сети в частную домашнюю или офисную сеть. Wi-Fi обеспечивает подключение к Интернету близлежащих устройств, находящихся в определенном радиусе действия. Другой способ использования Wi-Fi — создание точки доступа.

Wi-Fi использует радиоволны, которые передают информацию на определенных частотах. Двумя основными частотами являются 2,4 ГГц и 5 ГГц. Оба частотных диапазона имеют ряд каналов, по которым могут работать различные беспроводные устройства, что помогает распределить нагрузку таким образом, чтобы индивидуальные соединения устройств не прерывались. Это в значительной степени предотвращает переполнение беспроводных сетей.

Диапазон в 100 метров является типичным для стандартного Wi-Fi соединения. Однако чаще всего радиус действия ограничивается 10-35 метрами. На эффективное покрытие влияет мощность антенны и частота передачи. Дальность и скорость Wi-Fi подключения к Интернету зависит от окружающей среды и от того, обеспечивает ли оно внутреннее или внешнее покрытие.

Технология Wi-Fi была создана в 1998 году. В 2018 году Wi-Fi Alliance [5] ввёл упрощенную нумерацию поколений Wi-Fi для обозначения оборудования, поддерживающего Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac) и Wi-Fi 6 (802.11ax). Эти поколения имеют высокую степень обратной совместимости с предыдущими версиями. Альянс заявил, что уровень поколения 4, 5 или 6 может быть указан в пользовательском интерфейсе при подключении, наряду с уровнем сигнала.

Generation	IEEE Standard	Bands	Max data rate	Year
Wi-Fi 0	802.11	2.4 GHz	2 Mbit/s	1997
Wi-Fi 1	802.11b	2.4 GHz	11 Mbit/s	1999
Wi-Fi 2	802.11a	5 GHz	54 Mbit/s	1999
Wi-Fi 3	802.11g	2.4 GHz	54 Mbit/s	2003
Wi-Fi 4	802.11n	2.4/5 GHz	600 Mbit/s	2008
Wi-Fi 5	802.11ac	5 GHz	6933 Mbit/s	2014
Wi-Fi 6	802.11ax	2.4/5 GHz	9608 Mbit/s	2019
Wi-Fi 6E	802.11ax	6 GHz	9608 Mbit/s	2020

Таблица 1.1: Основные поколения Wi-Fi

Основные поколения Wi-Fi представлены в Таблице 1.1. Однако для технологии IoT особый интерес представляют только некоторые из этих поколений, а именно:

- IEEE 802.11b/g/n. Эти стандарты отличаются относительно небольшим радиусом действия. Они функционируют в полосе частот 2400—2483,5 МГц. В стандарте IEEE 802.11n, выпущенном в 2008 году, скорость соединения была существенно увеличена. Однако новая скорость может быть достигнута лишь в одном из трёх режимов работы, в котором не поддерживается обратная совместимость со стандартами IEEE 802.11b/g. Данные стандарты являются весьма популярными в устройствах для домашней автоматизации, где не всегда нужны огромные скорости передачи данных или большой радиус покрытия, а существенным параметром является энергоэффективность.

- IEEE 802.11ah. Этот протокол беспроводных сетей был опубликован в 2017 году под названием Wi-Fi HaLow. Он использует освобожденные от лицензий полосы частот 900 МГц для обеспечения сетей Wi-Fi с увеличенной дальностью действия по сравнению с обычными сетями Wi-Fi, работающими в диапазонах 2,4 ГГц и 5 ГГц. Он также отличается более низким энергопотреблением, что позволяет создавать большие

группы станций или датчиков, которые взаимодействуют для обмена сигналами, поддерживая концепцию Интернета вещей. Благодаря низкому энергопотреблению протокол конкурирует с Bluetooth и имеет дополнительные преимущества в виде более высокой скорости передачи данных и более широкого радиуса действия.

1.3 Сравнение протоколов

	ZigBee	Z-Wave	Wi-Fi
Standard	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.11
Max data rate	250 Kbit/s	100 Kbit/s	300+ Mbit/s
Power consumption	Low	Low	High
Bands	2.4 GHz	908.42 MHz	2.4 GHz/5 GHz
Network topology	Mesh	Mesh	Star

Таблица 1.2: Сравнение основных протоколов IoT

В Таблице 1.2 приведено сравнение основных характеристик трёх подробно рассмотренных протоколов. В сравнение не включена дальность действия: говоря о Wi-Fi, радиус непосредственного взаимодействия между двумя устройствами обычно является большим, однако сети на основе ZigBee и Z-Wave, как указано в таблице, имеют ячеистую топологию, за счёт чего они могут использовать промежуточные устройства для передачи сигнала и увеличения радиуса действия.

Говоря о технических характеристиках, отличие ZigBee от Z-Wave невелико: Z-Wave выделяется только используемой частотой. Но кроме этого существует разница в распространении устройств на основе обоих протоколов. Z-Wave получил более широкое распространение в США, в то время как ZigBee больше популярен в Европе. Существует ещё одно небольшое отличие, которое заключается в частотных диапазонах. В Северной Америке, Европе, и ряде других стран под Z-Wave и другие протоколы отводятся разные диапазоны частот. Однако в большинстве случаев это не оказывает большого влияния, поскольку вне зависимости от используемой частоты схожие устройства, как правило, обладают одинаковым функционалом.

Немало важным фактором в сравнении является стоимость конечных устройств. В данном случае она может заметно варьироваться. Говоря, например, о домашней автоматизации, стоимость устройств, поддерживающих Wi-Fi, оказывается выше. Более дешёвая цена устройства на основе ZigBee и Z-Wave достигается за счёт специализированных модулей и чипов.

Но кроме цены комплектующих влияние на стоимость оказывает способ управления конечными устройствами. Гаджеты на основе Wi-Fi могут управляться с любого смартфона, в то время как для управления ZigBee и Z-Wave сетями в подавляющем большинстве случаев требуется некоторое промежуточное устройство: хаб. Хаб позволяет преобразовывать сигналы от устройств в тот же самый Wi-Fi, добавляя возможность управления практически с любого устройства. Хаб имеет дополнительную стоимость. Устройства, совместимые с Wi-Fi, являются более дорогими, поскольку дают возможность обходиться без него.

Наконец, стоит отметить, что для каждого протокола с каждом годом появляется всё больше производителей. В связи с этим встаёт вопрос совместимости между устройствами различных производителей. Не редки случаи, когда несколько устройств не имеют возможности взаимодействия, несмотря на то, что они работают на одном протоколе. А при совместном использовании, например, ZigBee и Z-Wave, стоит быть ещё более внимательным и осторожным при выборе устройств.

Глава 2

Безопасность сетевых протоколов IoT

2.1 ZigBee

Одной из определяющих особенностей Zigbee является предоставление средства для осуществления безопасной связи, защиты создания и транспортировки криптографических ключей, шифрования кадров и управления устройствами. Данная особенность основывается на базовой структуре безопасности, определенной в стандарте IEEE 802.15.4. Эта часть архитектуры опирается на правильное управление симметричными ключами и корректную реализацию методов и политик безопасности.

Основным механизмом обеспечения конфиденциальности является защита всего ключевого материала. Доверие между сторонами предполагается при первоначальной установке ключей, а также при обработке информации о безопасности.

Проблема защита и безопасного распределения ключей является первостепенной в любой системе безопасности. Ключи никогда не должны передаваться по незащищенному каналу. В случае Zigbee кратковременное исключение из этого правила происходит на начальном этапе добавления в сеть ранее не сконфигурированного устройства. Модель сети Zigbee уделяет особое внимание соображениям безопасности, поскольку сети, формирующие свою структура «на лету» (ad-hoc сети), могут быть физически доступны для внешних устройств. Также невозможно предсказать состояние рабочей среды.

В стеке протоколов различные сетевые уровни не разделены криптографически, поэтому необходимыми являются политики доступа. Открытая модель доверия внутри устройства позволяет совместно использовать ключи,

что значительно снижает потенциальную стоимость. Если могут существовать вредоносные устройства, то каждая полезная нагрузка сетевого уровня должна быть зашифрована, чтобы несанкционированный трафик мог быть немедленно прерван. Исключением, опять же, является передача сетевого ключа, который передаёт единый уровень безопасности сети новому присоединяющемуся устройству.

Zigbee использует симметричное шифрование AES с длинной ключа 128 бит для реализации своих механизмов безопасности. Ключ может быть связан либо с сетью, что позволяет использовать его обоими уровнями Zigbee и подуровнем MAC, либо с каналом, полученным в результате предварительной установки, соглашения или транспортировки. Создание ключей канала связи основывается на использовании главного ключа. В конечном итоге, по крайней мере, главный ключ (мастер-ключ) должен быть получен через безопасную среду (с помощью защищённого канала связи или по предварительной установке), поскольку от этого зависит безопасность всей сети. Главный ключ виден только на прикладном уровне. Различные службы используют разные односторонние вариации ключа связи, чтобы избежать утечек и рисков безопасности.

В безопасной сети для распределения ключей назначается одно специальное устройство, которому доверяют другие устройства: так называемый удостоверяющий центр. При идеальном сценарии устройства должны иметь адрес удостоверяющего центра и начальный главный ключ, предварительно загруженный в них. Типичные приложения без особых требований к безопасности будут использовать для связи данный сетевой ключ, предварительно предоставленный удостоверяющим центром.

Архитектура безопасности распределена между сетевыми уровнями следующим образом:

- Подуровень MAC (уровень управления доступом к среде) способен обеспечивать надежные соединения между двумя устройствами. Как правило, уровень безопасности, который он использует, задается верхними уровнями.

- Сетевой уровень управляет маршрутизацией, обрабатывает полученные сообщения и транслирует запросы. Исходящие кадры будут использовать ключ соединения в соответствии с маршрутизацией, если он доступен; в противном случае для защиты полезной нагрузки от внешних устройств будет использоваться сетевой ключ.

- Прикладной уровень обеспечивает создание ключей и транспортные услуги как для объектов сети, так и для приложений.

2.2 Z-Wave

До 2008 года в спецификации Z-Wave не было никаких упоминаний о способах защиты каналов связи. Таким образом, все устройства Z-Wave коммуницировали открыто. Это означало, что любая сеть Z-Wave была доступна извне и взламывать её было не нужно. В 2008 в спецификацию было добавлено понятие шифрования (Z-Wave S0 Security), а в качестве алгоритма шифрования был выбран AES с длиной ключа 128 бит. Это изменение было призвано решить проблему распространения устройств Z-Wave. Однако разработчики не учли мелких деталей.

В 2013 году в спецификации Z-Wave S0 Security была обнаружена уязвимость. В момент первичной инициализации соединения перед началом сеанса передачи данных устройству отправляется ключ шифрования. На тот момент этот ключ представлял собой последовательность из 128 нулей. Таким образом, злоумышленник мог легко подслушать первичный сеанс связи, ключ которого был заранее известен. Далее не составляло труда отследить последующие изменения ключей шифрования. В результате практически каждая Z-Wave сеть оказалась уязвимой.

После этой истории репутация Z-Wave была существенно испорчена. Для решения проблемы в 2016 году появилась улучшенная версии спецификации Z-Wave S2 Security. В ней для первичной выработки ключей используется протокол Диффи-Хеллмана.

2.3 Wi-Fi

С точки зрения безопасности Wi-Fi необходимо учитывать среду передачи сигнала. В беспроводных сетях получить доступ к передаваемой информации и повлиять на канал передачи данных значительно проще. Для этого достаточно поместить соответствующее устройство в зоне действия сети. Основными протоколами защиты информации в сетях Wi-Fi являются WEP, WPA, WPA2 и WPA3.

Протокол WEP (Wired Equivalent Privacy) был разработан в 1997 году вместе с первой версией Wi-Fi Для шифрования использовался алгоритм RC4 со статическим ключом длиной 64 или 128 бит. Некоторое время протокол успешно функционировал и был способен противостоять базовым атакам типа «человек посередине». Недостатками для шифрования являлись малая длина ключа, а так же использование для шифрования непосредственно пароля, предоставленного пользователем. Wi-Fi Alliance отказался от использования WEP в 2004 году, официально объявив этот протокол небезопасным.

В 2003 году на замену WEP пришёл протокол WPA (Wi-Fi Protected Access). WPA использует протокол целостности временного ключа (TKIP) с всё той же длинной ключа 64 или 128 бит. Для шифрования использовался тот же самый алгоритм RC4, но вектор инициализации был увеличен вдвое: с 24 до 48 бит. TKIP использует ключ на каждый пакет, то есть динамически генерирует новый 128-битный ключ для каждого пакета и таким образом предотвращает типы атак, которые скомпрометировали WEP. Несмотря на все улучшения протокол WPA позиционировался как временная мера для замены уязвимого протокола WEP.

Полноценной же заменой стал протокол WPA2, который появился в использовании с 2004 года. С этого же года началась сертификация, а с 2006 по 2020 год сертификация WPA2 была обязательной для всех новых устройств с торговой маркой Wi-Fi. В качестве замены TKIP был внедрён протокол блочного шифрования с имитовставкой и режимом сцепления блоков и счётчика: CCMP. TKIP использовался только для обратной совместимости. CCMP основан на алгоритме шифрования AES с длиной ключа 128 бит. Преимуществом по сравнение со старыми версиями является генерация ключей шифрования во время соединения, а не их статическое распространение.

В январе 2018 года Wi-Fi Alliance объявил WPA3 в качестве замены WPA2. Сертификация началась в июне 2018 года. Самое крупное изменение связано с новым метод аутентификации. SAE (Simultaneous Authentication of Equals) явился заменой PSK (Pre-Shared Key), который использовал четырёхэтапное установление связи в протоколе WPA2. SAE работает на основе предположения о равноправности устройств, вместо того, чтобы считать одно устройство отправляющим запросы, а второе — предоставляющим право на подключение [6]. Кроме того, SAE обеспечивает защиту от чтения назад. 128-битное шифрование осталось минимально допустимой нормой, а для промышленных масштабов предложен вариант использования AES с длиной ключа 256 бит в режиме GCM с SHA-384 в качестве HMAC для проверки целостности информации. С выходом WPA3 появились две новые сопутствующие технологии: Easy Connect и Enhanced Open. Первая позволяет сделать процесс добавления новых устройств в сеть более простым и является весьма актуальной для домашней автоматизации. Отныне у каждого устройства будет уникальный QR-код, который сможет работать в качестве публичного ключа. Вторая технология усиливает защиту пользователей в открытых сетях. Данные технологии не зависят напрямую от WPA3, но улучшают безопасность для определённых типов сетей. Таким образом, вместо полной переработки безопасности Wi-Fi, WPA3 концентрируется на новых технологиях, которые позволят устранить уязвимости, появившиеся в WPA2.

2.4 Сравнение безопасности

Весьма схожие в техническом плане ZigBee и Z-Wave, с точки зрения безопасности так же не имеют существенных различий: оба протокола используют симметричный алгоритм блочного шифрования AES с длиной ключа 128 бит. Единственным отличием является метод распределения ключей: в Z-Wave используется протокол Диффи-Хеллмана, в то время как в ZigBee этот процесс по-прежнему доверен центру управления безопасностью.

В сетях на основе Wi-Fi безопасности уделяется значительно больше внимания в силу их повсеместного распространения. В контексте домашней автоматизации и некоторых других сфер, в которых Wi-Fi конкурирует с ZigBee и Z-Wave, отличия всё также незначительны. Для шифрования используются дополнительные надстройки и протоколы, но в основе лежит AES-128. В случае промышленного использования для Wi-Fi применяются более продвинутые технологии защиты информации.

Глава 3

Криптографические угрозы и атаки

3.1 ZigBee

Несколько вариантов атак на протокол ZigBee детально описаны в [7]. Среди прочих атак интерес вызывает так называемая атака повторной отправки сообщения, при которой в случае отсутствия в сети удостоверяющего центра или использования статического ключа шифрования злоумышленнику удаётся получить управления над конечными устройствами. Стоит отметить, что при правильной конфигурации сети устройства на основе ZigBee не подвержены атакам, направленным на этап присоединения нового устройства в сеть. Поскольку во всех трёх решения (ZigBee, Z-Wave, Wi-Fi) в том или ином виде используется алгоритм AES, шифрование данных оказывается весьма надёжным. И именно этап установки соединения является наиболее уязвимым. В отличие от ZigBee, подобным атакам оказываются подвержены два других решения, о чём пойдёт речь ниже.

3.2 Z-Wave

Домашняя автоматизация на сегодняшний день предлагает на рынке огромный выбор устройств. Некоторые из них потенциально не несут никакой угрозы, даже в случае взлома. Однако другие влияют напрямую на нашу безопасность. К таким устройствам можно отнести, например, автоматизированные дверные замки. В случае их компрометации последствия могут оказаться весьма неудачными. И такой случай имел место быть. В зашифрованных алгоритмом AES дверных замках на основе протокола Z-Wave была обнаружена ранняя уязвимость. Использую её, злоумышленник получал воз-

можность удалённо отпирать двери без знания ключей шифрования. А после изменения ключей последующие сетевые сообщения, например, «дверь открыта», игнорировались установленным контроллером сети. Уязвимость не была связана с недостатком в спецификации Z-Wave, а являлась ошибкой в реализации, допущенной производителем дверного замка.

Безопасность протокола Z-Wave была улучшена в 2016 году с появлением спецификации Z-Wave S2 Security. Однако из-за обратной совместимости с предыдущей версией спецификации S0 устройства оказались по-прежнему уязвимы в процессе подключения. В Z-Wave S0 Security использовался статический первичный ключ, состоящий из 128 нулей, из-за чего дальнейший взлом и управление устройствами оказывались весьма тривиальными. В качестве улучшения в S2 для первичной выработки ключей используется протокол Диффи-Хеллмана, а также дополнительно может потребоваться ввод 5-символьного кода устройства. Но в 2018 году была обнародована атака, которая позволяла понижать версию спецификации с S2 до S0 и эксплуатировать старые уязвимости.

Рассмотрим более подробно процесс понижения версии. Первые шаги при сопряжении устройства и контроллера в спецификация S0 и S2 аналогичны и заключаются в следующем:

1. На контроллере (управляющем устройстве) необходимо выбрать режим добавления нового устройства.

2. Далее пользователь нажимает кнопку (или последовательность кнопок) на присоединяемом устройстве.

3. После этого новое устройство посылает в сеть информацию о себе (Node info).

4. Контроллер получает эту информацию и приступает к процессу выработки ключей.

Единственным отличием в полезной нагрузке Node info для устройств на основе S2 Security является поддержка класса команды 0x9F – COMMAND_ _CLASS_SECURITY_2. Стоит отметить, что вся информация в Node info является незашифрованной. Таким образом, активный атакующий может убрать соответствующую команду из Node info и отправить подделанные данные контроллеру. Контроллер посчитает, что устройство не поддерживает спецификацию S2 Security, и будет выбрана уязвимая к атакам спецификация S0. Справедливо заметить, что в этом случае контроллер должен выдать предупреждение пользователю об использовании более ранней версии, однако

данное предупреждение, как правило, игнорируется. Подделанный Node info должен содержать тот же home ID, что и у оригинального устройства. Поле home ID не является константным, а генерируется каждый раз при добавлении или перезагрузке устройства. Это значит, что злоумышленник сперва должен завладеть home ID. Эта задача выполнима и требует лишь пересчитывания длины и чексуммы после удаления команды о поддержке S2.

Резюмирую, можно сказать, что данная атака подчёркивает проблему множества протоколов, а именно проблему улучшения безопасности при необходимости поддерживать старые устройства. Стоит отметить, что уже подключённые в сеть с использование S2 Security и успешно функционирующие устройства находятся в относительной безопасности, однако новые устройства остаются подверженными уязвимости.

3.3 Wi-Fi

WPA2 являлся основным стандартом шифрования для Wi-Fi на протяжении 14 лет: с 2004 по 2018 год. Однако в 2016 году на WPA2 была разработана атака с переустановкой ключа (Key Reinstallation Attack, Krack). Krack — это атака повторного воспроизведения [8]. Многократно сбрасывая одноразовый код, передаваемый на третьем этапе установки соединения WPA2, злоумышленник может постепенно сопоставить зашифрованные пакеты, сохранённые ранее, и узнать ключ шифрования. Уязвимость проявляется в самом стандарте Wi-Fi и не связана с ошибками реализации. В связи с этим любая корректная реализация WPA2 вероятнее всего является уязвимой. Уязвимость затрагивает все основные программные платформы.

При подключении нового клиента к сети Wi-Fi с защитой по WPA2 общий ключ шифрования согласуется за 4 этапа. Данный ключ служит для шифрования всех пакетов данных. Однако, из-за потери отдельных сообщений точка доступа (роутер) может повторно отправлять сообщения третьего этапа до получения подтверждение о его получении. Каждый раз при получении подобного сообщения клиент устанавливает уже имеющийся ключ шифрования. На практике злоумышленник заставляет жертву выполнить переустановку ключа.

Благодаря повторному использованию ключа шифрования появляется возможность воспроизведение пакетов, расшифрования и подделки содержания. При определённых условиях злоумышленник способен осуществлять атаки типа «человек посередине».

С появлением стандарта WPA3 данная уязвимость была устранена благодаря введению SAE (Simultaneous Authentication of Equals).

Глава 4

Модификация алгоритмов и протоколов

Заключение

Литература

[1] List of ZigBee certified products. -Mode of access: https://zigbeealliance.org/product_type/certified_product/. -Date of access: 11.12.2021.

[2] ZigBee Alliance. -Mode of access: https://zigbeealliance.org/solution/zigbee/. -Date of access: 11.12.2021.

[3] List of Z-Wave certified products. -Mode of access: https://products.z-wavealliance.org. -Date of access: 11.12.2021.

[4] Z-Wave Alliance. -Mode of access: https://z-wavealliance.org/. -Date of access: 11.12.2021.

[5] Wi-Fi Alliance. -Mode of access: https://www.wi-fi.org/. -Date of access: 11.12.2021.

[6] 802.11-2016 - IEEE Standard for Information technology. -Mode of access: https://ieeexplore.ieee.org/document/7786995. -Date of access: 11.12.2021.

[7] Ján Ďurech, Mária Franeková: Security attacks to ZigBee technology and their practical realization. SAMI, Herl'any, Slovakia, 2014.

[8] Common Vulnerabilities and Exposures: WPA2 reinstallation key. -Mode of access: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13077. -Date of access: 11.12.2021.