

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

<b>Введение</b>	<b>3</b>
<b>1 Анализ литературы</b>	<b>5</b>
1.1 Технологии Интернета вещей . . . . .	5
1.2 Используемые протоколы . . . . .	6
1.2.1 ZigBee . . . . .	6
1.2.2 Z-Wave . . . . .	9
1.2.3 Wi-Fi . . . . .	11
<b>2 Безопасность сетевых протоколов IoT</b>	<b>12</b>
2.1 ZigBee . . . . .	12
2.2 Z-Wave . . . . .	14
2.3 Wi-Fi . . . . .	14
<b>3 Криптографические угрозы и атаки</b>	<b>15</b>
<b>4 Модификация алгоритмов и протоколов</b>	<b>16</b>
<b>Заключение</b>	<b>17</b>
<b>Список использованных источников</b>	<b>18</b>

# 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, визуализируя 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 сделан 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: ближнего, 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 ZigBee, 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 система 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 обмениваться 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 удорожания качественного сигнала и быстрой передачи данных для лучшего соединения и надёжности. Несмотря на это Wi-Fi является ключевой технологией в развитии и распространении IoT.

## 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 перво-степенной 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 длиной 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

## Глава 3

# Криптографические угрозы и атаки

## Глава 4

# Модификация алгоритмов и протоколов



# Заключение

# Литература

- [1] List of ZigBee certified products. -Mode of access:  
[https://zigbeealliance.org/product\\_type/certified\\_product/](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.