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:

1. объекты, или «вещи»;
2. данные, которыми они обмениваются;
3. 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.

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). Первоначальная спецификация была признана стандартом IEEE в 2003 года, а первые модули, совместимые с ZigBee, появились в массовой продаже в начале 2006 года.

ZigBee был разработан как стандарт для радиосетей с ячесистой (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. 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.

1.2.2 Z-Wave

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.

Глава 2

Безопасность сетевых протоколов IoT

Глава 3

Криптографические угрозы и атаки

Глава 4

Модификация алгоритмов и протоколов

Заключение

Литература