ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Декабрь 2018 Том 6 № 4 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
December 2018 Vol. 6 Iss. 4 ISSN 2307-1303 http://www.itt.sut.ru

ЗАЩИЩЕННЫЙ ПРОТОКОЛ ПЕРЕДАЧИ ДАННЫХ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ НА ПРИМЕРЕ УСТРОЙСТВ RASPBERRY PI

А. В. Балуева[1], В. А. Десницкий[2*]

[1] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
[2] СПИИРАН, Санкт-Петербург, 190178, Российская Федерация
* Адрес для переписки: desnitsky@comsec.spb.ru

Аннотация
Статья посвящена исследованию и разработке защищенного протокола передачи данных в системах Интернета вещей. **Предмет исследования.** Предметом исследования являются возможные атаки на протокол передачи данных, а также методы защиты от них в условиях использования инфракрасного излучения в качестве среды передачи данных. **Метод.** Применяется методы системного анализа, а также методы обеспечения аутентичности данных в качестве защиты от возможной атаки. **Основные результаты.** Проведен анализ возможных атак на протокол передачи данных, спроектирована структура и проведена программная разработка защищенного протокола передачи данных. **Практическая значимость.** Полученные в работе результаты могут применяться для внедрения в системы умного дома в качестве аутентификации пользователей, управления устройствами или для организации защищенного обмена сообщениями между двумя пользователями.

Ключевые слова
Интернет Вещей, защищённый протокол передачи данных, инфракрасное излучение, удалённое управление.

Информация о статье
УДК 004.733
Язык статьи – русский.
Поступила в редакцию 05.11.2018, принята к печати 03.12.2018.

Ссылка для цитирования: Балуева А. В., Десницкий В. А. Защищенный протокол передачи данных в системах Интернета Вещей на примере устройств Raspberry Pi // Информационные технологии и телекоммуникации. 2018. Том 6. № 4. С. 10–20.

SECURE DATA TRANSFER PROTOCOL FOR THE INTERNET OF THINGS ON RASPBERRY PI EXAMPLE

A. Balueva[1], V. Desnitsky[2*]

[1] SPbSUT, St. Petersburg, 193232, Russian Federation
[2] SPIIRAS, St. Petersburg, 199178, Russian Federation
* Corresponding author: desnitsky@comsec.spb.ru

Abstract—The paper encompasses research and development of a secure data transfer protocol in the Internet of Things systems. **Research subject.** The subject of research comprises possible attacks on the data transfer protocol, as well as methods of protection against them, if infrared radiation is used as a data transmission medium. **Method.** Methods of sys-tem analysis as well as authenticity provision methods as a defense against possible attacks. **Core results.** Possible attacks on the data transfer protocol has been analyzed, the protocol structure has been designed and software development of the protected data transfer protocol has been constructed. **Practical relevance.** The results obtained in this paper can be used for implementation in smart home systems as user authentication, device management or for exchanging messages between two users.

Keywords—Internet of Things, secure data transfer protocol, infrared, remote control.

Article info
Article in Russian.
Received 05.11.2018, accepted 03.12.2018.

For citation: Balueva A., Desnitsky V.: Secure Data Transfer Protocol for the Internet of Things on Raspberry Pi Example // Telecom IT. 2018. Vol. 6. Iss. 4. pp. 10–20 (in Russian).

Введение

Интернет вещей представляет перспективную технологию, позволяющую, автоматизировать процессы управления домом и городскими инфраструктурами с использованием унифицированных интерфейсов управления. Цель работы – совершенствование технологий и протоколов сбора и передачи данных в системах Интернета Вещей с использованием беспроводных протоколов передачи данных. Задачи данной работы включают разработку и реализацию защищённого протокола передачи данных с использованием инфракрасных каналов (ИК, *InfraRed Data Association*, IrDA) связи в рамках систем Интернета вещей. Для корректной передачи информации предлагается определённая структура пакета данных, а в качестве защиты в структуру пакета включена хеш-сумма и метка времени, что позволяет обеспечить защиту протокола от некоторых видов атак. Актуальность поставленных цели и задач обосновываются важностью вопросов безопасности и надежности сетевых коммуникаций между устройствами Интернета вещей, в том числе с использованием инфракрасных каналов. К важнейшим результатам работы относятся, в частности, работоспособный протокол передачи данных, испытанный в рамках примера системы Интернета вещей с использова-

нием устройств платформы Raspberry Pi и языка программирования Python. Обоснованности полученных результатов подтверждается проведенным анализом литературы в предметной области исследования.

1 Обзор литературы

Применение ИК-излучения для системы умного дома, в частности для управления физическими механизмами защиты, приводится в статье [1]. Система интеллектуальной блокировки дверей (SDL) предназначена для обеспечения безопасности от вторжения несанкционированных пользователей и упрощения доступа для жильцов/сотрудников. В отличие от предшествующих решений SDL, использующих биометрию и сжатый радиочастотный спектр, авторы предлагают новую систему управления, основанную на ИК и БОКС (беспроводной оптический канал связи) с использованием ИК-светодиода и смартфонов. По результатам проведённых экспериментов, разработанная система потребляет меньшее количество энергии по сравнению с Wi-Fi или Bluetooth, что позволяет увеличить время автономной работы системы.

В [2] представлены базовые принципы взаимодействия между передатчиком информации и сенсором. Эта работа содержит описание основных протоколов и технологий умного дома, таких как ИК-протокол, Bluetooth и SPI (последовательный периферийный интерфейс). При этом описывается существующий ИК-протокол передачи информации NEC для удалённого управления, структура пакета и способ кодировки битов информации. Отличительной особенностью статьи реализация механизма распознавания разновидности протокола дистанционного управления. При этом IrDA включает в себя спецификации физического уровня IrPHY и протокольные спецификации IrLAP (протокол второго уровня, соответствующий канальному уровню сетевой модели OSI), IrLMP (протокол третьего уровня, соответствующий сетевому уровню сетевой модели OSI).

В [3] предложены усовершенствования протокола в структуре первых уровней IrDA. В частности, рассматривается технология внутренних инфракрасных сетей нового поколения (*Next-Generation Indoor Infrared LANs*), а также проблемы реализации и подходы к их решению. Спецификации IrPHY определяет условия функционирования протокола физического уровня для коротковолновых полудуплексных линий с несколькими скоростями передачи. Лежащий в основе Протокол IrMAC осуществляет контроль доступа к среде между устройствами, тогда как протокол IrLC включает контроль доступа к ссылкам. Протокол IrLAP используется для асинхронной передачи данных, высокоуровневого управления каналом передачи данных (HDLC) и отвечает за контроль доступа, поиск расположенный вблизи пользователей, установление и поддержку двунаправленного соединения (согласование скорости передачи данных), обмен данными и распределение первичной и вторичной ролей среди устройств.

В [4] представлены результаты проектирования и реализации ИК-протокола для работы системы внутреннего позиционирования (IPS). Использование инфракрасных протоколов передачи данных позволяет создавать низковольтную линию связи между светодиодными передатчиками и встроенным инфракрасным приемником. Отличие разработанного в данной статье протокола состоит в скорости позиционирования – существующие протоколы, которые предназначены для двухточечных соединений, показывают довольно высокое время позициони-

рования (3–4,5 секунды). Такие значения для позиционирования в реальном времени не подходят, поэтому представленный в статье протокол разрабатывался в первую очередь для уменьшения времени позиционирования и последующей возможности применения системы позиционирования в реальном времени без задержек.

2 Подход к разработке протокола

В наше время происходит быстрое развитие информационных технологий. Современные мобильные устройства становятся всё более многофункциональными. Скорость и объем данных, которые они могут обрабатывать, быстро растут, и в то же время стоимость этих технологий снижается. Одной из областей развития информационных технологий является Интернет вещей, предназначенный для облегчения повседневных дел и устранения необходимости контроля человеком.

Первым концепцию Интернета вещей в 1999 году представил Кевин Эштон [5], соучредитель и исполнительный директор Auto-IDCenter в Массачусетском технологическом институте. По сути, Интернет вещей представляет модульный подход к интеграции датчиков (RFID, IR, GPS, лазерных сканнеров и др.) в повседневные объекты и их подключение через Интернет через специальные протоколы обмена информацией и сообщениями, что приводит к появлению систем интеллектуального распознавания, отслеживания местоположения, систем мониторинга и управления. Большинство домашних приборов имеют процессоры, которые автоматизируют их работу, что является предпосылкой для создания унифицированной системы исполнения с микроуправлением всеми устройствами.

Инфракрасное дистанционное управление (ИКДУ) является неотъемлемой частью Интернета вещей и применяется практически во всей бытовой электронной аппаратуре. ИКДУ было выбрано для массового использования по достаточно понятным причинам – на то время (1970-е годы) ИК было одним из самых надежных и самым дешёвым видом беспроводной односторонней связи на короткие расстояния. Прежде всего, ИКДУ использовалось в бытовых телевизорах. И так как каждая компания-производитель разрабатывала свой проприетарный ИКДУ-протокол, на данный момент существует уже несколько десятков протоколов на разных частотах модуляции. Как правило, большинство современных нотаций для описания ИКДУ-протоколов предполагают нотацию, при которой, когда сигнал передаётся, это называют «Pulse», когда передача отсутствует – «Space».

Для связи и обмена информацией по сети между пользователями, помимо организации канала связи, необходимо также и соблюдение совместимых технологий при отправлении и приёме данных. Для этого существуют протоколы передачи данных, и они должны отвечать определённым требованиям для подтверждения корректной и безопасной передачи данных. К таким требованиям относят требования на (1) оперативность; (2) надёжность; (3) защищённость от возможных действий нарушителя.

Технология Интернета Вещей предполагает в основном использование сенсоров и датчиков, поэтому передача первичной информации будет происходить по беспроводным каналам (или в какой-либо другой среде передачи), при этом

протокол передачи данных не должен ориентироваться на требования к стандартным сетевым протоколам передачи данных. Требования для системы Интернета Вещей по каждой из характеристик представлены ниже.

Требования оперативности. Датчики должны быть достаточно чувствительными для получения информации, также на приёме важно максимально быстро обрабатывать информацию, чтобы полученные данные до пользователя доходили своевременно.

Требования надёжности. Так как датчики Интернета Вещей и приемники, как правило, должны находиться в одном помещении, то нужно исходить из того, что между передатчиком и приёмником могут возникать препятствия в виде тумана, яркого света и других факторов. В таком случае необходимо правильно рассчитать силу исходящего сигнала, чтобы помехи, вызванные особенностями окружающей среды (изменение плотности и влажности воздуха, солнечные лучи, блики) не смогли воспрепятствовать передаче данных и не произошло сбоя и потери информации.

Требования защищённость. В условиях систем Интернета Вещей важно учитывать, что данные могут быть перехвачены и видоизменены третьим лицом, поэтому защита должна строиться в первую очередь от атак типа MITM (атаки типа «человек посередине»). По сути MITM представляет атаку, при которой нарушитель нелегитимно подключается к каналу связи между двумя пользователями или устройствами и ретранслирует проходящую по каналу информацию, вмешиваясь в протокол передачи и нарушая целостность и достоверность передаваемых данных. Также атака типа MITM может включать анализ трафика (*sniffing*), и даже при отсутствии модификации структуры пакетов и полезной нагрузки, нарушитель может преследовать цели получения информации о передаваемых данных без нарушения их целостности.

Возможной вариацией атаки типа MITM является атака повторного воспроизведения (*replay*-атака), при которой нарушитель записывает проходящие сообщения и в дальнейшем воспроизводит их целиком, либо частично. Таким образом, любая неизменная информация (идентификаторы пользователей и устройств, пароли и др.) могут быть записаны и позднее использованы для компрометации процесса аутентификации. Для того чтобы защититься от поступления скомпрометированной информации, необходимо, чтобы в протоколе содержалось подтверждение того, что сообщение не было изменено. Подтверждением в данном случае может быть корректно построенная хеш-сумма. Другим способом, который противостоит атакам типа «человек посередине», является добавление временной метки (*timestamp*) в структуру пакета. Надёжность метки времени, сопровожденной средствами обеспечения целостности пакета данных, определяется тем, что ни правомерный пользователь, ни нарушитель, не может модифицировать данные таким образом, чтобы целостность при этом не нарушилась.

3 Реализация и эксперименты

Принцип действия ИКДУ основан на передаче управляющих команд с помощью модулированного инфракрасного излучения от пульта дистанционного управления (ДУ) до ИК-датчика. Существует разнообразие протоколов передачи данных, так как зачастую каждый производитель создаёт свой собственную реа-

лизацию протокола передачи данных. Для кодировки битов информации используются различные комбинации «pulse» и «space», где «pulse» задает время, когда светодиод включён и посылает сигнал на определённой частоте, а «space» – это время, когда датчик инфракрасного излучения не детектирует сигнал. Существует три основных типа модуляции [6]: двухфазное кодирование (ДФК); модуляция длительностью пауз (МДП); модуляция длительностью импульса (МДИ).

В настоящей работе используется модуляция длительностью пауз (МДП). При кодировании битов длительностью пауз логические единица и ноль определяются длительностью времени «space». Длительность импульса является постоянной, короткая пауза считается как 0, а длинная как 1. Используя различную длину сигнала «pulse», отправление битов будет выглядеть следующим образом (рис. 1):

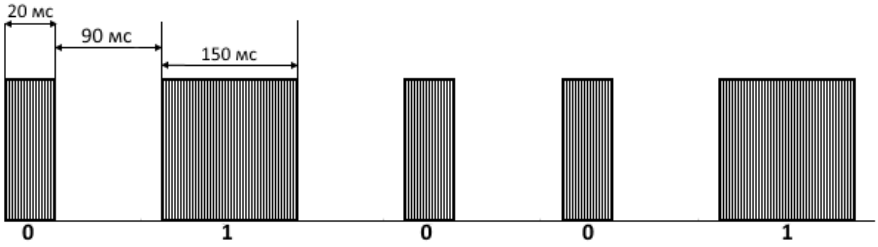

Рис. 1. Отправление сигнала

При выполнении практической реализации были использованы следующие устройства: микрокомпьютер RaspberryPi 3 model B и комплектующие – монитор, клавиатура, мышь; макетная плата, провода «папа-мама»; инфракрасный светодиод; ИК-приёмник. Собранная схема показана на рис. 2.

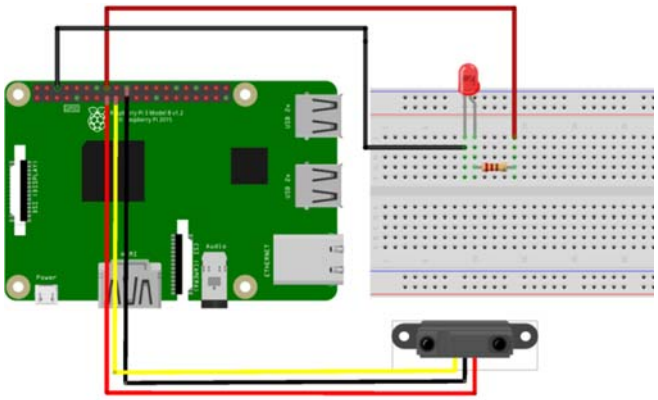

Рис. 2. Схема подключения светодиода

Для работы с интерфейсом ввода/вывода общего назначения (GPIO) использовался микрокомпьютер Raspbian Pi с использованием библиотеки RPi.GPIO для управления цифровыми контактами устройства[1]. Использовались следующие основные возможности RPi.GPIO: (1) считывание состояния каналов, сконфигу-

[1] RPi.GPIO – работа с входами, выходами и прерываниями в RaspberryPi, простые примеры [электронный ресурс]. – URL: https://ph0en1x.net/106-rpi-gpio-installation-working-with-inputs-outputs-interrupts.html

рированных на вход; (2) реакция на прерывания, инициируемые любым из каналов в режиме input; (3) управление состоянием каналов, сконфигурированных на выход; (4) широтно-импульсная модуляция на каналах в режиме output (PWM); (5) получение информации о платформе и конфигурации пинов.

Чтобы отправить бит на приёмник, светодиод включается на определённое время, то есть на приёмник поступает импульс. «1» – сигнал длительностью 150 мс, «0» – длительностью 20 мс. После отправления нуля или единицы формируется «пауза» в 90 мс, питание на светодиод не поступает и происходит разделение пришедших битов данных. Таким образом, приёмник получает импульсы разной длительности и записывает их как набор нулей и единиц. После определения способа кодирования битов можно переходить к созданию структуры пакета данных. Для корректной работы, обеспечения максимальной оперативности и защиты предлагается следующая структура пакета данных (рис. 3).

Рис. 3. Предложенная структура пакета данных

В каждом поле пакета находится определенное количество семизначных двоичных чисел, и таким образом, становится возможным отправлять символы ASCII в двоичной форме. Разработанная структура пакета данных содержит шесть полей, описание которых приведено ниже.

Поля 1 и 6: *S* и *E* – стартовая и конечная комбинации, которые содержат по одному символу – «*s*» и «*e*», соответственно. Поле идентификатора пакета *i* состоит из одного массива длиной 7 бит и содержит длину сообщения для дальнейшей обработки. Поле payload содержит полезную нагрузку сообщения. Поле timestamp – последовательность символов, показывающая точное время создания пакета. Поле *H* создаётся следующим образом: поле payload хешируется и полученный хеш складывается с меткой времени timestamp и снова хешируются 128-битным алгоритмом MD5, в итоге выходная хешированная строка составляет 32 символа. Итоговая длина пакета составляет от 287 до 1169 бит в зависимости от длины передаваемого сообщения.

Для обеспечения защиты при передаче данных встроен следующий алгоритм проверки целостности и достоверности полученного пакета:

1) Проверка корректности использования стартового и финального символов *«s»* и *«e»,* соответственно.

2) Расчёт хеш-суммы конкатенации сообщения и метки времени.

3) Сравнение исходного хеша с рассчитанным.

Таким образом, проверка на целостность пакета происходит на первом шаге алгоритма. Если пакет дошёл не полностью, то последний символ будет искажён и будет ясно, что целостность пакета нарушена. Подобная проверка не предоставляет универсальной защиты от атак злоумышленника, но помогает следить за надёжностью передачи данных.

Шаги 2 и 3 приведенного алгоритма обеспечивают защиту от таких видов атак, как атака модификации/подмены сообщения и replay-атака. Нарушитель подключается к каналу связи и перехватывает сообщение, либо для изменения данных (частично или полностью), либо для повторного воспроизведения позже

с целью получить доступ (например, аутентифицироваться) или выполнить какое-либо действие со стороны получателя данных.

Для отражения подобных атак происходит проверка хеш-суммы, а также проверка корректности меток времени. Для этого считываются поля payload и timestamp, вычисляется хеш-сумма сообщения payload, затем считается хеш для сложения хеш-суммы сообщения и метки времени и сравнивается с тем, что находится внутри пакета. Несовпадение исходного хеша, созданного на стороне отправителя и рассчитанного хеша на стороне получателя говорит о том, что на канал связи и полученный пакет была совершена атака. При любом несовпадении обработка пакета прерывается.

Программная реализация разработанного протокола передачи данных состоит из нескольких частей (рис. 4):

1) Создание пакета с описанной выше структурой на стороне отправителя.
2) Отправления сгенерированного пакета данных.
3) Приём битов информации получателем.
4) Обработка битов и проверка целостности и достоверности полученных данных.

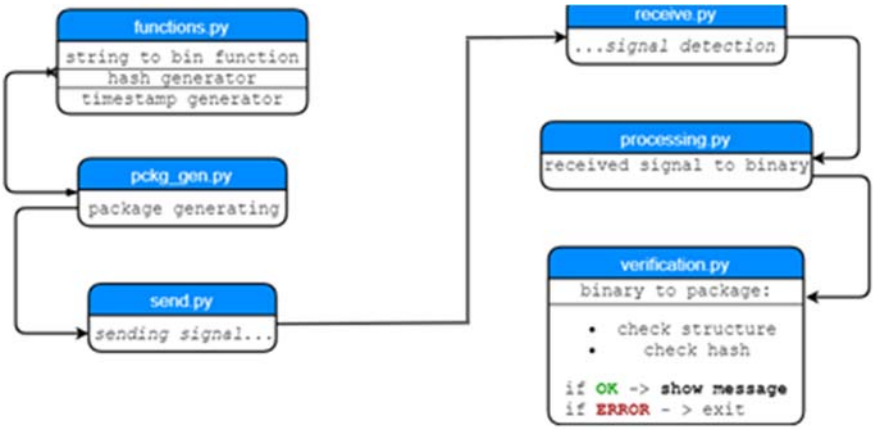

Рис. 4. Схема программной реализации протокола

На рис. 5 показан фрагмент программного интерфейса средства управления процессом передачи данных с использованием разработанного протокола. В случае если при верификации полученных данных не возникло ошибок на стороне получателя, то будет выдано сообщение о корректности передачи данных.

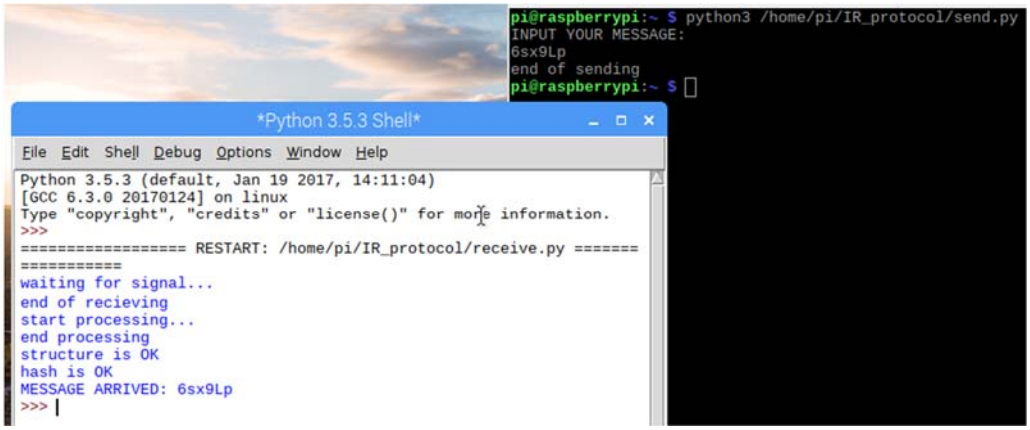

Рис. 5. Скриншот работы протокола передачи данных

Проведена оценка протокола на предмет выполнимости установленных требований. Оперативность определяет, по сути, характеристику скорости передачи данных. Так как вес пакета зависит от длины сообщения и кодировки символов, то в рамках эксперимента было принято взять пятнадцать разных сообщений отличающейся длины. Также в протокол передачи данных была добавлена функция вывода времени выполнения программы. По результатам проведенных экспериментов средняя скорость передачи данных составила 4,8 бит/сек.

В контексте проведенного эксперимента надёжность понимается как отсутствие ошибок при передаче данных. Подтверждением целостности полученных данных в данном протоколе является проверка корректности структуры и правильности хеш-суммы. На рис. 6 проиллюстрированы результаты эксперимента, в котором данные искажены из-за отсутствия сигнала – приёмник на некоторое время был убран из области распространения сигнала. В данном примере видно, что повреждённый пакет не может пройти проверку и пользователь не будет дезинформирован неверными данными.

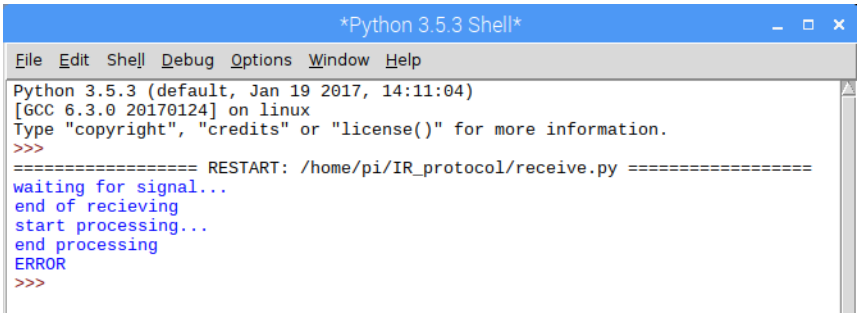

Рис. 6. Передача повреждённого пакета

Оценка защищённости представляет анализ возможности проведения атаки на протокол, в который не встроены функции защиты. В данном случае в качестве защиты выступает хеш-сумма и метка времени *timestamp*. Для начала рассматривается вариант протокола, в котором отсутствует хеш-сумма, а, следовательно, и метка времени. Так, как при такой структуре протокола отсутствует какая-либо проверка на достоверность сообщения, то получателю поступит изменённое сообщение, и таким образом, переданные ему данные будут скомпрометированы. Альтернативный вариант атаки – атака повторного воспроизведения, то есть нарушитель перехватывает сообщение и эксплуатирует его некоторых целях позже [7]. Хеширование не спасает от такой атаки, так как нет подтверждения, что пакет был отправлен в момент создания. Метка времени удостоверяет создание сообщения в момент отправления и таким образом доказывает отсутствие несанкционированного третьего лица в канале связи.

3 Выводы

Проведены разработка и оценка защищенного беспроводного протокола передачи данных для систем Интернета вещей. Для начала были изучены источники литературы в предметной области, и приведен их анализ. Проведен анализ понятий Интернета вещей и дистанционного управления на основе инфракрасных каналов. Сформулированы требования к беспроводному протоколу в системах Интернета вещей, показаны возможные атаки на протокол передачи данных, а также проанализированы возможные средства защиты от них. В практической

части предлагается структура пакета данных для разработанного протокола, приведен перечень устройств и описание программ, написанных на языке Python, необходимых для корректной работы протокола передачи данных.

Согласно полученным оценкам, разработанный протокол соответствует всем установленным требованиям, предъявляемым к нему. В частности, протокол поддерживает максимальную для данного оборудования скорость передачи данных, канал связи работает без перебоев, и вся информация корректно доходит от отправителя к получателю. Также реализованы средства защиты, которые препятствуют при несанкционированном доступе к каналу связи третьим лицом (нарушителем) осуществлять модификацию данных или их повторно отправку нарушителем.

Заключение

Технологии Интернета Вещей предполагают использование множеств современных программно-аппаратных узкоспециализированных устройств. Использование ИК-канала, а также множества различных датчиков и исполнительных механизмов позволяет реализовать автоматизацию и дистанционное управление между различными системами в доме, офисе, производственном помещении, что повышает уровень комфорта, безопасность, энергоэффективности и другие характеристики.

Протокол, построенной в ходе данной работы предоставляет широкий спектр возможностей для развития в сфере Интернета вещей, которую можно и нужно совершенствовать для последующего внедрения в системы умного дома для аутентификации санкционированных пользователей и защиты от злоумышленников. Так, при наличии более производительного оборудования можно увеличить скорость отправления информации, объем отправляемых данных, увеличить дистанцию между источником и детектором инфракрасного излучения. К возможным усовершенствованиям можно также отнести сквозное шифрование для обеспечения конфиденциальности данных, а также усложнение структуры пакетов данных и их обработку для применения инфракрасного канала связи не только в целях аутентификации, но и в целях комплексного мониторинга устройств системы. Также можно реализовать обмен сообщениями по ИК-каналу в обе стороны, т. е. построить защищённый канал обмена сообщениями для двух пользователей. Или, например, создать охранную систему обнаружения вторжений на заданный периметр.

Технические возможности инфракрасных каналов связи увеличиваются, и его относительная дешевизна, малое энергопотребление и простота в использовании способствуют созданию «лёгкого», и недорогой в реализации протокола передачи данных, помогающий в управлении умным домом, что немаловажно, так как Интернет Вещей является динамично развивающейся и актуальной технологией.

Литература

1. Dhondge K., Ayinala K., Choi B.-Y., Song S. Infrared Optical Wireless Communication for Smart Door Locks Using Smartphones // Mobile Ad-Hoc and Sensor Networks (MSN). 2016. № 12. pp. 251–257. DOI: 10.1109/MSN.2016.46.

2. Starkova O., Herasymenko K., Babailova Y. Remote Control Systems of Household Appliances // Scientific-Practical Conference Problems of Infocommunications. Science and Technology. 2017. № 4. pp. 585–588.

3. Ozugur T., Copeland J. A., Naghshineh M., Kermani P. Next-Generation Indoor Infrared LANs: Issues and Approaches // IEEE Personal Communications. 1999. N 6. pp. 6–19. DOI: 10.1109/98.813818.

4. Popoola O. R., Popoola W. O., Ramirez-Iniguez R., Sinanović S. Design of improved IR protocol for LED indoor positioning system // Wireless Communications and Mobile Computing Conference (IWCMC). 2017. N 13. pp. 882–887.

5. Ashton K. That "Internet of Things" Thing [Electronic resource]. URL: http://www.rfidjournal.com/articles/view?4986

6. Жирнова Л. В., Мошкин В. В. Анализатор сигналов инфракрасного пульта дистанционного управления // Технические науки: проблемы и перспективы. 2011. С. 52–55.

7. Desnitsky V., Kotenko I., Chechulin A. An abstract model for embedded systems and intruders // 19th International Euromicro Conference on Parallel, Distributed, and Network-Based Processing (PDP 2011). 2011. pp. 25–26.

References

1. Dhondge, K., Ayinala, K., Choi, B.-Y., Song S. Infrared Optical Wireless Communication for Smart Door Locks Using Smartphones // 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN). 2016. pp. 251–257.

2. Starkova, O., Herasymenko, K., Babailova, Y. Remote Control Systems of Household Appliances // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). 2017. pp. 585–588.

3. Ozugur, T., Copeland, J. A., Naghshineh, M., Kermani, P. Next-Generation Indoor Infrared LANs: Issues and Approaches // IEEE Personal Communications. 1999. Vol. 6. Iss. 6. pp. 6–19.

4. Popoola, O. R., Popoola, W. O., Ramirez-Iniguez, R., Sinanović, S. Design of Improved IR Protocol for LED Indoor Positioning System // 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017. pp. 882–887.

5. Ashton, K. That 'Internet of Things' Thing. URL: http://www.rfidjournal.com/articles/view?4986

6. Zhirnova, L. V., Moshkin, V. V. Infrared Remote Control Signal Analyzer // International Scientific Conference "Technical Science: Problems and Prospects" 2011. pp. 52–55.

7. Desnitsky, V., Kotenko, I., Chechulin, A. An Abstract Model for embedded Systems and Intruders // 19th International Euromicro Conference on Parallel, Distributed, and Network-Based Processing (PDP). 2011. pp. 25–26.

Балуева Анастасия Владимировна – студентка, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, _tonys_@mail.ru

Десницкий Василий Алексеевич – кандидат технических наук, старший научный сотрудник, СПИИРАН, Санкт-Петербург, 199178, Российская Федерация, desnitsky@comsec.spb.ru

Balueva Anastasia – Student, SPbSUT, St. Petersburg, 193232, Russian Federation, _tonys_@mail.ru

Desnitsky Vasily – Candidate of Engineering Sciences, Senior Research Officer, SPIIRAS, St. Petersburg, 199178, Russian Federation, desnitsky@comsec.spb.ru