Безопасность в протоколах и технологиях IoT: обзор

Ж.С. Каженова, Ж.Е. Кенжебаева

***Аннотация*—IoT открывает обширную область для творческих приложений, которые изменят мир и человеческие жизни. Небольшие чувствительные устройства, подключенные к Интернету, сделают возможными всеохватывающие вычисления. В этой статье описаны широко распространенные технологии и стандарты для сетей IoT, делается обзор наиболее известных протоколов и технологий безопасности, доступных в настоящее время для принятия в IoT, на разных уровнях типичного стека связи. В первом разделе представлены существующие технологии и протоколы безопасности интернета вещей. Во втором разделе обзора обсуждается технологии и протоколы используемые в IoT. В следующем разделе дается краткий обзор протоколов и механизмы безопасности в IoT. В последнем разделе обсуждаются проблемы безопасности и решения, показано сравнение протоколов, которые ранее обсуждались в предыдущих разделах. В будущей работе авторы стремятся построить модель безопасности взаимосвязанных вычислительных устройств на основе облегченной и безопасной схемы аутентификации для Интернета вещей. Данная работа облегчит правильно ориентироваться в стэке протоколов безопасности интернета вещей.**

***Ключевые слова*— интернет вещей, устройства, передача данных, стек, частная информация.**

I. Введение

Интернет вещей (IoT) – это сеть подключенных устройств, каждое из которых автоматически собирает и обменивается данными по сети, то есть, интернет вещей – это взаимодействие между несколькими устройствами, вещами и объектами. Концепция этой новой технологии заключается в том, чтобы автоматизировать работу и подключать устройства через Интернет которые используются во многих секторах и отраслях, таких как потребительские приложения, бизнес-приложения, правительственные приложения. Количество устройств интернет вещей во всем мире в настоящее время исчисляется миллиардами.

Устройства интернет вещей могут обладать интеллектуальными возможностями для сбора, анализа и даже принятия решений без вмешательства человека, поэтому в системе интернет вещей безопасность является высшим требованием. Во первых, известные угрозы безопасности, уязвимости и атаки традиционных систем информационных технологий (ИТ) естественным образом наследуются. Во вторых, многие дополнительные векторы атак безопасности включены против более простых устройств IoT. Большинство устройств будут напрямую подключены к Интернету, чтобы быть непосредственно доступными, и это также делает их непосредственно подверженными нескольким видам атак безопасности, особенно отказу в обслуживании (DoS). Типичная локальная сеть будет включать в себя значительно большее количество устройств с ограниченными ресурсами. Это не только делает большой набор устройств IoT значительно более уязвимым и менее способным справляться с атаками безопасности, но также приводит к дополнительным трудностям при разработке и внедрении решений безопасности, которые также доступны по цене для устройств IoT с ограниченными возможностями.

В сетевых устройствах, таких как камеры, было обнаружено много недостатков, например, жестко закодированные учетные данные, открытые порты Telnet и классические ошибки, такие как внедрение команд SQL (Structured Query Language). В случае неправильного использования вредоносные агенты могут привести к таким катастрофам, как атака DDoS (Distributed Denial of Service) ботнетом Mirai [1]. На Рисунке 1 показано как могут распространяться скрытые уязвимости.

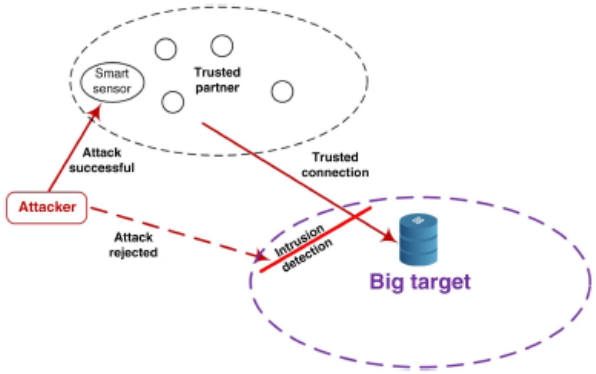

Рис. 1. Косвенная атака.

Вредоносное программное обеспечение может получить контроль над доступным сетевым устройством. Очевидно, это зависит от того, насколько защищена система и насколько умен злоумышленник. Владелец этой системы может недооценивать риск атаки

Статья получена 4 ноября 2021.

Жанар Сабыртаевна Каженова, Казахский агротехнический университет имени Сакена Сейфуллина (kazhenova7138-1@murdoch.in)

Жанат Елубаевна Кенжебаева, Казахский агротехнический университет имени Сакена Сейфуллина (kenzhebayeva@lund-univer.eu)

и экономить средства, необходимые для защиты периферийной системы. Эта, периферийная система возможно, не является целью атаки, но, будучи надежным партнером этой системы, она может служить трамплином и способствовать косвенной атаке на большую цель. Очевидно, что атакованная компания может повысить чувствительность своей системы обнаружения вторжений, но это может привести к блокировке необходимого доверенного соединения при каждом ложном событии [2].

В сетевой системе, взаимодействующей с несколькими партнерами, которая не контролирует все элементы, такой риск будет существовать. Система контроля стратегической инфраструктуры должна быть построена в кругах безопасности, и все слабые места должны быть определены. В сети Интернет используются стандартизованные протоколы для обеспечения безопасности и надежности связи между разнородными устройствами. Стандартные протоколы определяют правила и форматы, которые устройства используют для создания сетей и управления ими, а также для передачи данных по этим сетям. Сети строятся как «стек» технологий. Интернет вещей представляет собой гибридную сеть из Интернета и сетей с ограниченными ресурсами, поэтому целесообразно изучить варианты использования стандартизованных для Интернета механизмов безопасности в IoT. Используя стандартизированные механизмы, связь в IoT может быть защищена на разных уровнях: на канальном уровне с безопасностью 802.15.4 Института инженеров по электротехнике и радиоэлектронике (IEEE), на сетевом уровне с безопасностью IP (IPsec) и на транспортном уровне с безопасностью транспортного уровня дейтаграмм (DTLS) [3-5].

В первом разделе представлены существующие технологии и протоколы безопасности интернета вещей. Во втором разделе обзора обсуждается технологии и протоколы используемые в IoT. В следующем разделе дается краткий обзор протоколов и механизмы безопасности в IoT. В последнем разделе обсуждаются проблемы безопасности и решения, показано сравнение протоколов, которые ранее обсуждались в предыдущих разделах.

II. Технологии и протоколы Интернета вещей

Интернет вещей (IoT) первоначально использовал существующую Интернет-инфраструктуру и существующие технологии. До разработки технологий IoT для поддержки приложений IoT были применены компьютеры и сетевые технологии с основными изменениями. Например, IPv4, который использовался в беспроводных сенсорных сетях (WSN), широко использовался в начале IoT для подключения узлов к Интернету с использованием одного IP-адреса, что требует дополнительных усилий для настройки. Однако многие проблемы возникли в результате использования технологий, которые не были разработаны с учетом IoT (например, отсутствие автоматической настройки в IPv4). В связи с этим возникла необходимость в разработке новых технологий для преодоления различных проблем, таких как эффективная маршрутизация, масштабируемость и мобильность, чтобы сделать разработку приложений IoT более простой и эффективной. Эти усовершенствования в технологиях IoT привели к широкому развертыванию приложений IoT в реальном мире во многих областях, таких как здравоохранение, промышленность и интеллектуальные здания [2]. На Рисунке 2 показана сеть IoT с ограниченными ресурсами, подключенная к IPv6 через беспроводную персональную сеть с низким энергопотреблением (6LoWPAN). Он также описывает типичный стек IoT с различными протоколами и технологиями безопасности на разных уровнях устройства IoT.

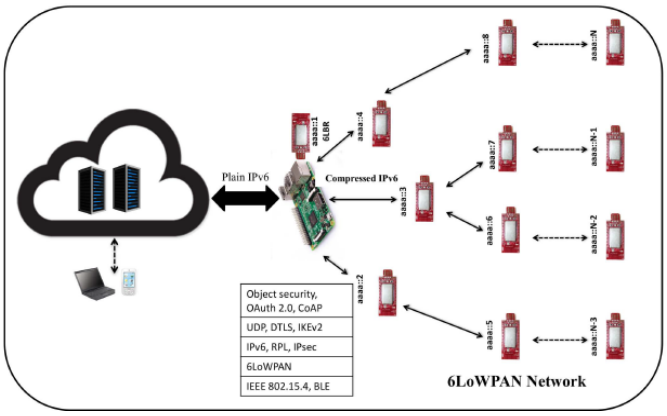

Рис. 2. Пример сети IoT с ограниченными ресурсами с разными протоколами безопасности и технологиями на разных уровнях.

На прикладном уровне OAuth 2.0 настраивается для устройств IoT с целью внедрения в IoT механизмов контроля детального доступа; безопасность объекта стандартизируется для защиты отдельных элементов данных; и протокол ограниченного применения (CoAP) утвердил себя в качестве нового веб-стандарта для IoT, который может нести сообщения безопасности объекта и сообщения OAuth. На транспортном уровне протокол UDP предпочтителен для устройств IoT, а протокол защиты транспортного уровня дейтаграмм (DTLS) связан с CoAP. В качестве альтернативы можно использовать протокол Internet Key Exchange версии 2 (IKEv2) для динамического установления и управления связями безопасности и связанными материалами ключа, когда предпочтительным является принятие IPsec (или сетевой безопасности). Кроме того, IPv6 отображает потенциально неограниченное адресное пространство и является сетевым протоколом и протоколом адресации для IoT, в то время как протокол маршрутизации IPv6 для сетей с низким энергопотреблением и с потерями (RPL) является стандартизированным решением для маршрутизации пакетов в условиях ограниченного, низкого мощности и сети с потерями [3]. Кроме того, 6LoWPAN был стандартизирован, чтобы обеспечить механизмы сжатия/распаковки и фрагментации/повторной сборки,

и, таким образом, чтобы более крупные пакеты помещались в кадры IEEE 802.15.4 (или аналогичные). Наконец, существует ряд возможностей на канальном и физическом уровне. Поскольку в IEEE 802.15.4, а также в Bluetooth Low Energy (BLE) имеется большой потенциал, безопасность в их присутствии также обсуждается.

Вышеописанный стек протокола IoT основан только на открытых технологиях. Они соответствуют доступности информации и ресурсов протокола, таких как технические спецификации, реализации и исходный код. Также некоторые протоколы безопасности открыты, хорошо изучены и могут быть улучшены исследователями безопасности, в то время как в других случаях организации, стоящие за ними, могут неохотно сотрудничать с сообществом специалистов по безопасности. Физический уровень и уровень канала передачи данных определены стандартом IEEE 802.15.4 [4]. Адаптивный уровень, называемый 6LoWPAN, появляется между уровнем канала передачи данных и сетевым уровнем, чтобы гарантировать взаимодействие с сетями, не относящимися к IoT, с использованием IPv6. На уровне приложений могут использоваться различные протоколы, такие как протокол ограниченного приложения (CoAP) или транспорт телеметрии очереди сообщений (MQTT). В зависимости от развернутого протокола IoT транспортный уровень определяется протоколом пользовательских дейтаграмм (UDP) или TCP соответственно.

III. Характеристика протоколов и механизмов безопасности в IoT

На Рисунке 2 в предыдущем разделе представлен стек, основанный на нескольких протоколах IoT, каждый из которых определяет определенный уровень стека. Каждый уровень независим и предоставляет свои собственные механизмы безопасности. Далее рассматриваем каждый протокол и механизм безопасности по отдельности.

Подпись и шифрование объектов CBOR. Краткое представление двоичных объектов (CBOR) – это формат сериализации двоичных данных, основанный на JSON. Он позволяет передавать объекты данных, которые содержат пары имя-значение, как и JSON, но в более сжатой форме. Это увеличивает скорость обработки и передачи. Он определен в IETF RFC 8949. Поскольку ожидается, что многие IoT-устройства будут ограничены в ресурсах, необходимо уменьшать объем информации, которая должна храниться, передаваться и обрабатываться. Это означает, что не только простой контент уровня приложения, но также зашифрованный контент, цифровые подписи и даже криптографические ключи должны быть представлены и закодированы компактным и эффективным способом. С этой целью CBOR подписывает и шифрует объекты (COSE) с целью создания криптографических форматов на основе краткого представления двоичных объектов (CBOR) [5]. Для устройств с ограниченными ресурсами COSE имеет огромный потенциал для создания облегченных представлений на основе CBOR криптографических ключей, шифрования, хэшей сообщений и цифровых подписей. Синтаксис кодированного сообщения CBOR подробно описывает базовую структуру COSE и общие заголовки COSE [6]. Кроме того, он разрабатывает объекты COSE с помощью специальных материалов криптографических ключей, а также с помощью криптоалгоритмов для шифрования/аутентификации данных и для вычисления кодов аутентификации сообщений (MAC). В [7], [8] предложено кодирование параметров, ключей и результатов RSA и других алгоритмов в качестве сообщений COSE.

CoAP. Протокол ограниченного приложения (CoAP) – это специализированный протокол Интернет-приложений для ограниченных устройств, как определено в RFC 7252. Он позволяет этим ограниченным устройствам связываться с более широким Интернетом с использованием аналогичных протоколов. Он основан на взаимодействии между запросами и ответами между конечными точками и может легко интегрироваться с широко распространенным протоколом передачи гипертекста (HTTP) для интеграции с классической сетью [9], [10]. Хотя протокол CoAP был разработан для ограниченных устройств и сетей, он не предоставляет себе никаких конкретных примитивов для безопасной связи [11]. Поэтому сообщения CoAP могут быть защищены следующими двумя путями:

1. Защита объектов для ограниченных сред RESTful (OSCORE).
2. Защита с помощью реального безопасного протокола связи DTLS.

DTLS. В случае защиты сообщения CoAP с помощью реальных безопасных протоколов связи спецификация CoAP рекомендует принять протокол DTLS [12]. В частности, Shelby et al. (2014) определяют привязку CoAP к DTLS в виде набора дельт для простого незащищенного CoAP. Если сообщение CoAP защищено с использованием DTLS, рассматривается схема URL coaps: //, а не схема coap: // для незащищенной связи. На практике DTLS позволяет двум устройствам аутентифицироваться друг с другом и обмениваться защищенными сообщениями CoAP. Engineering Инженерная рабочая группа по Интернету (IETF) выпустила профиль для безопасности транспортного уровня (TLS) и DTLS 1.2. Этот профиль обеспечивает безопасность связи для устройств с ограниченными ресурсами, используемых для сбора данных с помощью датчиков или для управления исполнительными механизмами в приложениях для промышленных систем управления, домашней автоматизации, интеллектуальных городов и других сетей [13]. DTLS отображает ряд различий по сравнению с TLS, что позволяет обеспечить безопасный обмен сообщениями поверх UDP и других ненадежных транспортных протоколов дейтаграмм.

OSCORE. Безопасность объектов для сред с ограничениями RESTful (OSCORE) – метод защиты на

уровне приложений протокола ограниченного приложения (CoAP) с использованием подписи и шифрования объектов CBOR (COSE). OSCORE обеспечивает сквозную защиту между конечными точками, обменивающимися данными с использованием CoAP или HTTP с отображением CoAP. OSCORE разработан для узлов и сетей с ограничениями, поддерживающих ряд прокси-операций, включая трансляцию между различными транспортными протоколами. В [14] описывается соответствующее предложение под названием «Защита объектов для ограниченных сред RESTful» (OSCORE). OSCORE – это протокол безопасности, основанный на объектах данных, позволяющий обмениваться сообщениями CoAP, которые защищены сквозной защитой через промежуточные узлы. OSCORE использует объекты COSE [6] для обеспечения целостности, сквозного шифрования и защиты воспроизведения сообщений CoAP. Использование OSCORE сигнализируется, в первую очередь, путем включения недавно определенной опции Object Security CoAP в защищенные сообщения CoAP. OSCORE может фактически комбинироваться и использоваться вместе с DTLS. На практике OSCORE предполагает, что контекст безопасности был предварительно установлен и согласован между клиентом CoAP и сервером CoAP, которые рассматриваются как конечные точки защищенной связи. Рабочая группа IETF по ограниченным средам RESTful (CoRE) провела основную работу по стандартизации этого протокола. Чтобы сделать протокол пригодным для приложений IoT и M2M, были добавлены различные новые функции. Ядро протокола указано в RFC 7252.

Сжатая IPsec. Стандарт 6LoWPAN [15] определяет, каким образом дейтаграммы IPv6 с большим весом могут передаваться по сетям с низким энергопотреблением и с потерями на основе IEEE 802.15.4 [16]. Для этого в 6LoWPAN представлен ряд схем сжатия заголовков, которые способны значительно уменьшить размер заголовков UDP, дейтаграмм IP и расширений IP. В настоящее время IP-безопасность (IPsec) [17] является стандартным решением безопасности для IPv6. В частности, хосты IPv6 в Интернете должны реализовать его и иметь возможность обрабатывать и обрабатывать пакеты, защищенные IPsec. В частности, транспортный режим IPsec обеспечивает защищенную сквозную связь между двумя узлами в Интернете. Следовательно, целесообразно адаптировать 6LoWPAN для обеспечения связи IPsec между объектами с поддержкой IPv6 (например, сенсорными узлами) в сетях 6LoWPAN и общими узлами IPv6 в Интернете. Представлено множество различных предложений для сжатия заголовков пакетов IPsec. Большинство схем сжатия применимы к общим интернет-хостам и конкретно не рассматривают сети 6LOWPAN, состоящие из устройств с ограниченными ресурсами. В [18] предлагают IPsec со сжатием 6LoW PAN, который в первую очередь предназначен для ограниченных в ресурсах устройств loT и сети.

IEEE 802.15.4. Стандарт IEEE 802.15.4 предоставляет спецификации для физического уровня и уровня управления доступом к среде (MAC), предназначенные для беспроводных низкоскоростных персональных сетей. Кроме того, уровень MAC IEEE 802.15.4 напрямую обеспечивает ряд служб безопасности, то есть аутентификацию данных, конфиденциальность данных и защиту от повторного воспроизведения для каждого пакета [16]. В частности, этот стандарт относится к криптографическому набору, основанному на 128-битной криптографии с симметричным ключом Advanced Encryption Standard (AES) [19]. Стандарт IEEE 802.15.4 не описывает, как устанавливать и распространять материал ключа в сети или как обращаться к аутентификации устройства. Вместо этого предполагается, что обе такие службы безопасности предоставляются и применяются высшими уровнями. Как следствие, стандарт предполагает, что заданная пара узлов отправителя и получателя успешно согласовала одни и те же параметры безопасности и общий общий материал ключа, прежде чем они смогут начать безопасную связь. Физический уровень определяет характеристики радиосвязи. Этот уровень позволяет протоколу работать в трех возможных частотных диапазонах: 2,4 ГГц (с 16 каналами), 915 МГц (с 10 каналами) и 868 МГц (с 1 каналом). Пропускная способность может достигать 250 Кбит/с при дальности связи 10 м. Более того, Физический уровень предлагает предотвращение столкновений и другие функции, обеспечивая пригодность в реальном времени.

Bluetooth Low Energy. Хотя, с одной стороны, IEEE 802.15.4 в настоящее время является стандартом, охватывающим физический и канальный уровни для сетей 6LoWPAN, другие новые технологии также развиваются. Например, BLE, практически продаваемый как Bluetooth Smart, относится к числу энергоэффективных коммуникационных технологий, доступных в настоящее время, и представляет собой привлекательную альтернативу. В частности, BLE зарекомендовал себя как легкая альтернатива для устройств с ограниченными ресурсами по сравнению с классическим Bluetooth. Стандарт Bluetooth 4.0 теперь также включает в себя спецификации BLE, которые включают режим широковещательной связи в дополнение к мощным соединениям между устройствами Bluetooth. Bluetooth 4.2 был опубликован в декабре 2014 года и предоставляет ряд новых функций, которые делают BLE перспективной и ценной технологией для IoT [20].

OAuth 2.0. OAuth – открытый протокол авторизации, который позволяет предоставить третьей стороне ограниченный доступ к защищённым ресурсам пользователя без необходимости передавать ей (третьей стороне) логин и пароль. Среда авторизации OAuth 2.0 зарекомендовала себя как один из наиболее широко принятых стандартов для управления процессами аутентификации [21]. Фактически, это позволяет решать

все типичные проблемы основанных на совместном использовании учетных данных, благодаря введению уровня авторизации и отделению роли клиента от роли владельца ресурса. В принципе, структура авторизации OAuth 2.0 позволяет клиентскому объекту (то есть хосту, процессу, пользователю) запрашивать и получать конкретный, регулируемый и ограниченный доступ к ресурсу, доступному на сервере ресурсов (RS), путем принудительного применения разрешение владельца соответствующего ресурса.

MQTT. MQTT – это открытый стандартный протокол, изначально созданный IBM. Этот протокол основан на модели публикации-подписки, разработанной для классических коммуникаций, а также облегченных коммуникаций M2M [22]. В отличие от CoAP, MQTT построен на TCP, поэтому безопасность протокола зависит от традиционного протокола безопасности уровня защищенных сокетов/транспортного уровня (SSL/TLS). MQTT обладает некоторыми интересными характеристиками, которые делают его совместимым с сетями с ограничениями. Это обеспечивает небольшую нагрузку на транспорт и ограничивает обмен протоколами для уменьшения сетевого трафика в среде с низкой пропускной способностью. Использование TCP с MQTT обеспечивает решение для уменьшения предсказуемых потерь соединения в ненадежной сети.

IV. Анализ проблем безопасности и пути их решения

В этом разделе рассмотрим наиболее важных практических аспектов, касающихся безопасности в IoT. Хотя обеспечить надежную безопасность в Интернете уже сложно, на самом деле в IoT это гораздо сложнее, поскольку «вещи» будут поддерживать версию 6 Интернет-протокола (IPv6), будут глобально доступными и чрезвычайно разнородными (включая сенсорные устройства, смартфоны, стандартные компьютеры и даже облачные среды) и обычно развертываются в физически незащищенных, необслуживаемых средах. Более того, большинство из них не предоставляют никакого обычного пользовательского интерфейса, такого как дисплей или клавиатура. В то же время ограниченные среды IoT наследуют ограничения, типичные для традиционных беспроводных сенсорных сетей (WSN), например, ограниченные вычислительные и энергетические ресурсы, топологии с множеством соединений и беспроводные линии с потерями. Для решения этих проблем разрабатываются и стандартизируются различные протоколы для устройств и сетей IoT. Краткое описание представленных протоколов приведено в Таблице 1 [2].

Таблица 1. Обзор протоколов и механизмов

Протокол	Уровень стека	Цель	Причины для принятия
Подпись и шифрование объектов CBOR	Приложение	Сериализация структур данных	Эффективное кодирование сообщения, защищенные на прикладном уровне
OSCORE	Приложение	Безопасная сквозная связь между клиентом и сервером CoAP	Требуется при наличии посредников, которые могут законно проверять и избирательно изменять сообщения CoAP
DTLS	Транспорт	Безопасный обмен данными между клиентом и сервером DTLS	Необходим для полной защиты сообщений CoAP
Сжатая сеть IPsec	Сеть	Защищенная транзитная связь между двумя узлами IPsec	Требуется для полной защиты транспортных пакетов. Сжатие 6LoWPAN, чтобы справиться с ограничением нижних уровней
IEEE 802.15.4 службы безопасности	Физический	Защищенная транзитная связь между двумя узлами 802.15.4	Требуется для полной защиты сетевых пакетов и особенно контроля трафика
Bluetooth Low Energy	Физический	Безопасный обмен данными между двумя узлами Bluetooth	Уровень безопасности равен стандартному Bluetooth. Возможные белые списки частных адресов на уровне ссылок
OAuth 2.0	Приложение	Выдача и применение авторизаций для доступа к ресурсам на удаленном сервере	Основанный на Сервере авторизации, он полностью разделяет клиентов и владельцев ресурсов

Каждый уровень стэка безопасности интернета вещей независим и предоставляет свои собственные механизмы безопасности. Безопасность в IEEE 802.15.4 предлагает шифрование данных с использованием режима работы блочного шифрования AES-CCM*. Этот протокол является разновидностью алгоритма AES-CCM; он предоставляет те же функции и добавляет возможность использования только возможностей шифрования. Размер ключа фиксирован до 128 бит, как и размер блока открытого текста. Безопасность на сетевом уровне. Сетевой уровень полагается на IPv6, поэтому авторы рассматривают IP-безопасность (IPSec) только как механизм безопасности для обеспечения взаимодействия с Интернетом. В [18] и [23] представлены подходы IPSec и обмена ключами, чтобы сделать их подходящими для сред с ограничениями. Безопасность, обеспечиваемая транспортным уровнем, зависит от протокола, используемого на прикладном уровне. Если используется CoAP, то транспортный протокол – UDP, а обеспечиваемый механизм безопасности – DTLS; если MQTT развернут, то TCP

используется в качестве транспортного протокола, а соответствующий механизм безопасности – SSL/TLS.

V. Заключение

Каждый уровень стэка безопасности интернета вещей независим и предоставляет свои собственные механизмы безопасности. Безопасность в IEEE 802.15.4 предлагает шифрование данных с использованием режима работы блочного шифрования AES-CCM*. Этот протокол является разновидностью алгоритма AES-CCM; он предоставляет те же функции и добавляет возможность использования только возможностей шифрования. Размер ключа фиксирован до 128 бит, как и размер блока открытого текста. Безопасность на сетевом уровне. Сетевой уровень полагается на IPv6, поэтому авторы рассматривают IP-безопасность (IPSec) только как механизм безопасности для обеспечения взаимодействия с Интернетом. Безопасность, обеспечиваемая транспортным уровнем, зависит от протокола, используемого на прикладном уровне. Если используется CoAP, то транспортный протокол – UDP, а обеспечиваемый механизм безопасности – DTLS; если MQTT развернут, то TCP используется в качестве транспортного протокола, а соответствующий механизм безопасности – SSL/TLS.

Интернет вещей (IoT) является одной из самых горячих тенденций в исследованиях в любой области, поскольку IoT – это взаимодействие между несколькими устройствами, вещами и объектами. В таком взаимодействии безопасность и защита конфиденциальности являются ключевыми проблемами при передаче таких конфиденциальных данных по сети IoT для обработки и хранения в облаке. В данной работе представлены существующие технологии и протоколы безопасности интернета вещей, обсуждались технологии и протоколы используемые в IoT и дан краткий обзор протоколов и механизмы безопасности в IoT. В будущей работе авторы стремятся построить модель безопасности взаимосвязанных вычислительных устройств на основе облегченной и безопасной схемы аутентификации для Интернета вещей. Данная работа облегчит правильно ориентироваться в стэке протоколов безопасности интернета вещей.

Библиография

[1] Kolias C., Kambourakis G., Stavrou A., Voas J. DDoS in the IoT: Mirai and other Botnets // Computer. – 2017. – No. 507. – P. 80-84.

[2] Hassan Q.F. Internet of things A to Z: Technologies and applications. – New York: John Wiley & Sons, Inc, 2018.

[3] Winter T., Thubert P., Brandt A., Hui J.W., Kelsey R., Levis P., Pister K., Struik R., Vasseur J.P., Alexander R.K. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. – Fremont: Internet Engineering Task Force, 2012.

[4] 802.15.4-2015 – IEEE Standard for Low-Rate Wireless Networks. [Electronic source]. – Access mode: https://ieeexplore.ieee.org/document/7460875 (date of access: 25/12/2020).

[5] Bormann C., Hoffman P. Concise Binary Object Representation (CBOR), RFC 7049. – Fremont: Internet Engineering Task Force, 2013.

[6] Schaad J. CBOR Object Signing and Encryption (COSE), RFC8152. – Fremont: Internet Engineering Task Force, 2017.

[7] Jones M.B. Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages, RFC8230. – Fremont: Internet Engineering Task Force, 2017.

[8] Schaad J. CBOR encoded message syntax: Additional algorithms. – Fremont: Internet Engineering Task Force, 2016.

[9] Fielding R.T., Reschke J. Hypertext Transfer Protocol (HTTP/1.1): Message syntax and routing. RFC 7230. – Fremont: Internet Engineering Task Force, 2014.

[10] Fielding R.T., Reschke J. Hypertext Transfer Protocol (HTTP/1.1): Semantics and content. RFC 7231. – Fremont: Internet Engineering Task Force, 2014.

[11] Shelby Z., Hartke K., Bormann C. Constrained Application Protocol (CoAP). RFC 7252. – Fremont: Internet Engineering Task Force, 2014.

[12] Rescorla E., Modadugu N. Datagram Transport Layer Security version 1.2. RFC 6347. – Fremont: Internet Engineering Task Force, 2012.

[13] Tschofenig H., Fossati T. Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things. RFC 7925. – Fremont: Internet Engineering Task Force, 2016.

[14] Selander G., Mattson J., Palombini F., Seitz L. Object Security for Constrained RESTful Environments (OSCORE), draft-ietf-core-object-security09 (work in progress). – Fremont: Internet Engineering Task Force, 2018.

[15] Hui J.W., Thubert P. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282. – Fremont: Internet Engineering Task Force, 2011.

[16] IEEE 802.15.4-2011 – IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). [Electronic source]. – Access mode: https://standards.ieee.org/standard/802_15_4-2011.html (date of access: 25/12/2020).

[17] Kent S., Seo K. Security architecture for the internet protocol. RFC 4301. – Fremont: Internet Engineering Task Force, 2005.

[18] Raza S., Duquennoy S., Voigt T., Roedig U. Demo abstract: securing communication in 6LoWPAN with compressed IPsec // The 7th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS'11). – Piscataway: Institute of Electrical and Electronics Engineers Inc, 2011.

[19] Advanced Encryption Standard (AES). [Electronic source]. – Access mode: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (date of access: 25/12/2020).

[20] Bluetooth Special Interest Group. Bluetooth Specification – Version 4.2. 2014. https://www.bluetooth.com/specifications/specs/ (date of access: 25/12/2020).

[21] Hardt D. The OAuth 2.0 Authorization Framework. RFC 6749. – Fremont: Internet Engineering Task Force, 2012.

[22] Banks A., Gupta R. MQTT version 3.1.1, OASIS Standard. [Electronic source]. – Access mode: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqttv3.1.1.html (date of access: 25/12/2020).

[23] Raza S., Voigt T., Jutvik V. Lightweight ikev2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 Security. [Electronic source]. – Access mode: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.2588&rep=rep1&type=pdf (date of access: 25/12/2020).

Жанар Сабыртаевна КАЖЕНОВА,
Докторант кафедры вычислительной техники и программного обеспечения Казахского агротехнического университета имени Сакена Сейфуллина, 010011, пр. Женис, 62, Нур-Султан, Республика Казахстан.
E-mail: kazhenova7138-1@murdoch.in

Жанат Елубаевна КЕНЖЕБАЕВА,
кандидат технических наук, исполняющий обязанности ассоциированного профессора кафедры вычислительной техники и программного обеспечения Казахского агротехнического университета имени Сакена Сейфуллина, 010011, пр. Женис, 62, Нур-Султан, Республика Казахстан.
E-mail: kenzhebayeva@lund-univer.eu

Security in IoT Protocols and Technologies: An Overview

Zhanar S. Kazhenova, Zhanat Ye. Kenzhebayeva

***Abstract*—The IoT opens up a vast area for creative applications that will change the world and human lives. Small, sensitive devices connected to the Internet will enable all-encompassing computing. This study describes widely accepted technologies and standards for IoT networks, and provides an overview of the most well-known security protocols and technologies currently available for adoption in the IoT, at different levels of a typical communication stack. The first section introduces existing IoT security technologies and protocols. The second section of the overview discusses the technologies and protocols used in the IoT. The next section provides a brief overview of the protocols and security mechanisms in the IoT. The last section discusses security issues and solutions, and shows a comparison of the protocols that were previously discussed in the previous sections. In future work, the authors seek to build a security model for interconnected computing devices based on a lightweight and secure authentication scheme for the Internet of Things. This study will simplify the correct navigation of the IoT security protocol stack.**

Keywords: **internet of things, devices, data transfer, stack, private information.**

REFERENCES

[1] Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. (2017). DDoS in the IoT: Mirai and other Botnets. *Computer*, 50(7), 80-84.

[2] Hassan, Q.F. (2018). *Internet of things A to Z: Technologies and applications*. New York: John Wiley & Sons, Inc.

[3] Winter, T., Thubert, P., Brandt, A., Hui, J.W., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J.P., Alexander, R.K. (2012). *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550*. Fremont: Internet Engineering Task Force.

[4] 802.15.4-2015 – IEEE Standard for Low-Rate Wireless Networks. (2016). https://ieeexplore.ieee.org/document/7460875.

[5] Bormann, C., Hoffman, P. (2013). *Concise Binary Object Representation (CBOR), RFC 7049*. Fremont: Internet Engineering Task Force.

[6] Schaad, J. (2017). *CBOR Object Signing and Encryption (COSE), RFC8152*. Fremont: Internet Engineering Task Force.

[7] Jones, M.B. (2017). *Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages, RFC8230*. Fremont: Internet Engineering Task Force.

[8] Schaad, J. (2016). *CBOR encoded message syntax: Additional algorithms*. Fremont: Internet Engineering Task Force.

[9] Fielding, R.T., Reschke, J. (2014). *Hypertext Transfer Protocol (HTTP/1.1): Message syntax and routing. RFC 7230.* Fremont: Internet Engineering Task Force.

[10] Fielding, R.T., Reschke, J. (2014). *Hypertext Transfer Protocol (HTTP/1.1): Semantics and content. RFC 7231*. Fremont: Internet Engineering Task Force.

[11] Shelby, Z., Hartke, K., Bormann, C. (2014). *Constrained Application Protocol (CoAP). RFC 7252*. Fremont: Internet Engineering Task Force.

[12] Rescorla, E., Modadugu, N. (2012). *Datagram Transport Layer Security version 1.2. RFC 6347*. Fremont: Internet Engineering Task Force.

[13] Tschofenig, H., Fossati, T. (2016). *Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things. RFC 7925*. Fremont: Internet Engineering Task Force.

[14] Selander, G., Mattson, J., Palombini, F., Seitz, L. (2018). *Object Security for Constrained RESTful Environments (OSCORE), draft-ietf-core-object-security09 (work in progress).* Fremont: Internet Engineering Task Force.

[15] Hui, J.W., Thubert, P. (2011). *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282*. Fremont: Internet Engineering Task Force.

[16] IEEE 802.15.4-2011 – IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). (2011). https://standards.ieee.org/standard/802_15_4-2011.html.

[17] Kent, S., Seo, K. (2005). *Security architecture for the internet protocol. RFC 4301*. Fremont: Internet Engineering Task Force.

[18] Raza, S., Duquennoy, S., Voigt, T., Roedig, U. (2011). Demo abstract: securing communication in 6LoWPAN with compressed IPsec. In: *The 7th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS'11)*. Piscataway: Institute of Electrical and Electronics Engineers Inc.

[19] Advanced Encryption Standard (AES). (2001). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[20] Bluetooth Special Interest Group. Bluetooth Specification – Version 4.2. (2014). https://www.bluetooth.com/specifications/specs/.

[21] Hardt, D. (2012). *The OAuth 2.0 Authorization Framework. RFC 6749*. Fremont: Internet Engineering Task Force.

[22] Banks, A., Gupta, R. MQTT version 3.1.1, OASIS Standard. (2014). http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqttv3.1.1.html.

[23] Raza, S., Voigt, T., Jutvik, V. (2012). *Lightweight ikev2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 Security*. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.2588&rep=rep1&type=pdf.

Zhanar S. KAZHENOVA,
Doctoral Student at the Department of Computing and Software, Saken Seifullin Kazakh Agrotechnical University, 010011, 62 Zhenis Ave., Nur-Sultan, Republic of Kazakhstan.
E-mail: kazhenova7138-1@murdoch.in

Zhanat Ye. KENZHEBAYEVA,
PhD in Technical Sciences, Acting Associate Professor at the Department of Computing and Software, Saken Seifullin Kazakh Agrotechnical University, 010011, 62 Zhenis Ave., Nur-Sultan, Republic of Kazakhstan.
E-mail: kenzhebayeva@lund-univer.eu