УДК 004.5
DOI 10.33764/2618-981X-2023-8-1-142-149

Д. Н. Титов[1], Е. В. Рыжкова[1]*

Угрозы безопасности Интернета вещей

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: alena.tarasova.2014@mail.ru

Аннотация. Парадигма Интернета вещей (IoT) относится к сети физических объектов или «вещей», встроенных в электронику, программное обеспечение, датчики и средства подключения, позволяющие объектам обмениваться данными с серверами, централизованными системами и другими подключенными устройствами на основе различных коммуникационных инфраструктур. Данные Интернета вещей, собранные с различных датчиков и узлов передаются в облако через Интернет. Устройства Интернета вещей используются потребителями, здравоохранением, а также предприятиями. Поскольку использование устройств Интернета вещей растет, появляются и его уязвимости. Анализ показывает, что массовое внедрение Интернета вещей с интеграцией новых технологий создает новые проблемы безопасности в парадигме Интернета вещей. В статье обсуждаются вызовы безопасности Интернета Вещей.

Ключевые слова: Интернет вещей (IoT), безопасность IoT, конфиденциальность данных IoT, машинное обучение

D. N. Titov[1], E. V. Ryzhkova[1]*

Internet of Things Security Threats

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: alena.tarasova.2014@mail.ru

Abstract. The Internet of Things (IoT) paradigm refers to a network of physical objects or "things" embedded in electronics, software, sensors, and connectivity that allow objects to communicate with servers, centralized systems, and other connected devices based on various communication infrastructures. IoT data collected from various sensors and nodes is transmitted to the cloud via the Internet. IoT devices are being used by consumers, healthcare as well as businesses. As the use of IoT devices grows, so do IoT vulnerabilities. The analysis shows that the massive introduction of the Internet of Things with the integration of new technologies creates new security issues in the IoT paradigm. The article discusses the security challenges of the Internet of Things.

Keywords: Internet of Things (IoT), IoT security, IoT data privacy, machine learning

Введение

Интернет соединяет нас с физическим миром через персональные мониторы состояния здоровья, бесконтактные сети, «умные дома», «умные автомобили» и сети автоматизации. Эти новые сети предоставляют огромные возможности, но также сопряжены с огромными рисками [1]. В ближайшее время сеть 5G станет базовой инфраструктурой для устройств Интернета вещей с огромной емкостью передаваемых данных и массовым подключением устройств, что обеспечит еще большее внедрение таких устройств в наше окружение. Однако из-за непрерыв-

ных и всепроникающих возможностей сбора данных и управления IoT вызывает на сегодняшний день опасения по поводу безопасности. Развертывание существующих решений безопасности для Интернета вещей непросто из-за неоднородности устройств, высокой динамичности и большого масштаба их применения.

Методы и материалы

Технология Интернета вещей (IoT) позволяет Интернету выходить в реальный мир физических объектов. Такие технологии, как RFID, беспроводная связь малой дальности, локализация в реальном времени и сенсорные сети, становятся все более распространенными. Мы переживаем смену парадигмы, при которой повседневные предметы становятся взаимосвязанными и умными [2]. Однако человеческое понимание и опыт использования взаимодействующих интеллектуальных вещей и интеллектуальных систем развивались не такими темпами, что создает проблемы с огромными техническими последствиями, последствиями для безопасности. Исследователи изучают эту технологию с трех основных точек зрения: научной теории, инженерного проектирования и пользовательского опыта. Исследования направлены на расширение прав и возможностей пользователей, предоставляя им знания, необходимые для понимания окружающей среды и управления ею. Будущее сосредоточено во внедрении искусственного интеллекта во всех областях интернета вещей, включая управление дорожным движением, энергетику, мониторинг, промышленное производство, строительство, сельское хозяйство, управление окружающей средой, умный дом, дистанционное медицинское обслуживание и т.д. Необходимо создать умное сетевое общество, в котором ресурсы должны эффективно использоваться с положительным воздействием на население. Все эти инновационные разработки Интернета вещей создают новые проблемы безопасности и открывают области исследований, требующие решения.

Подключенные устройства Интернета вещей являются движущей силой «умного» мира, где вещи играют жизненно важную роль в нашей повседневной жизни. Подключенные узлы в основном представляют собой метки RFID (радиочастотной идентификации) или беспроводные датчики. Хотя TCP/IP (Transport control protocol/Internet protocol) является основным протоколом, используемым для интернет-связи, устройствам Интернета вещей может потребоваться использовать протокол связи малой дальности для подключения к центральному узлу, откуда данные передаются на сервер или в облако [3]. Протоколы связи малой дальности включают near field communication (NFC), Bluetooth, IEEE 802.15.4, Wi-fi, ZigBee и т.п. В типичной архитектуре Интернета вещей существует три основных уровня: уровень восприятия, транспортный/сетевой уровень и прикладной уровень. Каждый из этих уровней имеет свои собственные проблемы безопасности, которые необходимо учитывать [4]. Уровень восприятия содержит физические устройства Интернета вещей, которые воспринимают различные параметры среды. Если злоумышленники получат контроль над этими устройствами, они смогут извлечь из них конфиденциальную информацию [5]. Транс-

портный/сетевой уровень основан на инфраструктуре Интернета, которая позволяет передавать данные между уровнем восприятия и прикладным уровнем. Прикладной уровень включает в себя хранение, анализ и представление данных конечному пользователю. Аппаратное и программное обеспечение на этих различных уровнях, в основном, управляются и поддерживаются разными организациями.

Существует много опубликованных работ по безопасности Интернета вещей, в которых рассмотрены документы, связанные с безопасностью устройств Интернета вещей, архитектурой Интернета вещей, протоколами для защищенных коммуникаций Интернета вещей и текущими тенденциями в области безопасности Интернета вещей. Как было указано ранее, физические узлы подключаются по протоколу связи на короткие расстояния, такому как Wi-Fi и так далее. Исследования показали, что эти технологии также уязвимы. Разработан и оценен алгоритм сквозной безопасности для Интернета вещей с использованием технологии IPSec, которая повышает безопасность. Авторы протестировали различные криптографические алгоритмы (AES, 3DES, SHA1, SHA2) на реальных беспроводных сенсорных узлах для достижения безопасности WSNS с использованием IPSec и VPv6 в отношении времени шифрования и энергопотребления. Наиболее защищенные сети Wi-Fi, защищенные с помощью Wi-Fi protected access (WPA/2), могут стать жертвой атаки с переустановкой ключа [6]. Все эти решения предназначены специально для коммуникационного уровня любых решений IoT, но не являются полным решением для обеспечения безопасности Интернета вещей.

Для разработки и внедрения комплексных решений безопасности для Интернета вещей важно идентифицировать угрозы и вызовы сетей, устройств и приложений Интернета вещей. Internet Engineering Task Force (IETF) выявила несколько угроз безопасности Интернета вещей [7]:

1) клонирование устройств Интернета вещей ненадежным производителем;

2) замена вещей вредоносными вещами более низкого качества;

3) атака «человек посередине» во время ввода в эксплуатацию и из-за отсутствия надлежащих механизмов аутентификации и авторизации;

4) замена злоумышленником встроенного программного обеспечения (ПО) вредоносным кодом;

5) угроза безопасности конфиденциальных данных;

6) атака типа «отказ в обслуживании»;

7) атака на маршрутизацию;

8) атака подслушивания в плохо сконфигурированной сети Интернета вещей;

9) извлечение параметров безопасности из физически незащищенных устройств Интернета вещей.

В исследованиях безопасности Интернета вещей необходимо рассмотреть следующие ключевые проблемы безопасности Интернета вещей [8].

Идентификация устройства. Уникальная идентификация устройств Интернета вещей имеет решающее значение. Серверы доменных имен (DNS) присваи-

вают имена подключенным устройствам Интернета вещей. Но DNS также уязвимы для различных атак, таких как атака «человек посередине», атака позиционирования кэша DNS и так далее. Злоумышленники могут повторно использовать украденные идентификационные данные устройства и выполнять различные виды вредоносных действий в сети.

Проблема с прошивкой устройств. Обновление прошивки и установка исправлений безопасности на устройства Интернета вещей могут оказаться непростыми. Каждый день в Интернете появляются новые уязвимости в системе безопасности. Пользователям устройств Интернета вещей может потребоваться отслеживать обновления, установленные на устройствах. Сегодня устройства Интернета вещей не поддерживают оперативное обновление. Пользователям может потребоваться размонтировать устройство для установки встроенного ПО или его обновлений. Внедрение новой системы управления устройствами уменьшило бы проблемы, связанные с обновлением встроенного ПО [9].

Аутентификация и авторизация. Сети Интернета вещей состоят из огромного количества устройств. Эти устройства должны иметь возможность гибко подключаться к сети в любое время. Поскольку устройства Интернета вещей производят или обрабатывают конфиденциальные данные, они должны аутентифицироваться для получения и передачи данных на шлюз. Уязвимости в системе безопасности увеличиваются при использовании паролей по умолчанию, установленных производителями без их изменения, а также при использовании слабых паролей на любом устройстве. Авторизация не менее важна, чем аутентификация. Устройства Интернета вещей должны иметь возможность читать и записывать в определенную область базы данных, чтоб не дать злоумышленнику возможность получить доступ на чтение и запись конфиденциальной области данных, если устройство скомпрометировано.

Реализация алгоритмов безопасности. Устройства Интернета вещей, в основном, – небольшие, с ограниченными мощностью, возможностями обработки информации и памятью. Реализация сложных криптографических алгоритмов в устройствах с ограниченными возможностями совершенно невозможна. Даже шифрование может быть затруднено из-за возможностей устройства. Эти устройства могут стать жертвой атак по побочным каналам. Злоумышленники могут применить обратный инжиниринг для восстановления обычных данных, передаваемых по сети. Внедрение облегченных алгоритмов шифрования на этих устройствах может снизить вероятность подслушивания.

Безопасность связи. Безопасная связь очень важна для передачи конфиденциальных данных Интернета вещей в режиме реального времени через Интернет. Как обсуждалось ранее, многие устройства Интернета вещей не шифруют данные перед передачей через Интернет. Безопасная частная сеть может уменьшить уязвимости, но, поскольку данные Интернета вещей необходимо отправлять и получать по большой сети, во многих случаях безопасная частная сеть не может быть подходящим решением. Упаковка данных Интернета вещей на промежуточном уровне также может уменьшить проблемы.

Безопасность приложений. Данные пользователей с узлов Интернета вещей хранятся в облаке, в Интернете или на мобильных устройствах. Даже безопасная связь не защитит пользовательские данные, если злоумышленник получит доступ к данным из Интернета, облака или мобильных устройств. Таким образом, безопасность данных Интернета вещей, хранящихся в облачном Интернете и на мобильных устройствах, также является сложной задачей.

Аварийное восстановление и управление инцидентами. Устройства Интернета вещей могут быть размещены где угодно. Сбой в узле Интернета вещей может привести к огромной проблеме. Надлежащий план аварийного восстановления и управление инцидентами в реальном времени очень ограничены для устройств Интернета вещей, где чувствительная информация обрабатывается датчиками Интернета вещей.

Обнаружение уязвимостей и управление ими. Обнаружение различных уязвимостей в системе безопасности узлов Интернета вещей и управление ими являются сложной задачей. Поскольку сети Интернета вещей состоят из множества устройств Интернета вещей, обнаружить затронутый узел не очень легко. Внедрение новых структур даст решение этой проблемы.

Доступность и сбои в обслуживании. Устройства Интернета вещей всегда должны быть доступны для мониторинга или сбора данных. Они могут быть скомпрометированы, физически повреждены или украдены, что приведет к прерыванию обслуживания. Высокая доступность устройств Интернета вещей очень важна для систем мониторинга в режиме реального времени.

Конфиденциальность и целостность данных. Только разрешенный пользователь должен иметь доступ к персональным данным пользователей. Перед получением доступа к данным кем-либо другим требуется надлежащее разрешение. Данные должны быть надежно удалены, когда в них больше не будет необходимости.

Человеческий фактор. Справиться с ленивыми пользователями устройств Интернета вещей непросто. Например, если пользователь автомобиля не заменит поврежденное устройство, это может представлять угрозу для его жизни или для кого-либо еще.

Результаты

Основываясь на проблемах безопасности Интернета вещей, рассмотренных выше, были определены следующие вопросы для дальнейших исследований:

– идентификатор конечного устройства Интернета вещей для надежной аутентификации и авторизации;

– доверие между различными компонентами в парадигме Интернета вещей;

– конфиденциальность пользовательских данных, генерируемых конечными устройствами Интернета вещей;

– сквозная защита данных Интернета вещей при достаточном обеспечении безопасности и стандартизации.

Обсуждение

Любое решение для обеспечения безопасности Интернета вещей должно учитывать три основных свойства информации: конфиденциальность, целостность и доступность. Конфиденциальность данных или информации означает, что доступ к данным ограничен для неуполномоченных лиц. Целостность гарантирует оригинальность данных, т.е. то, что данные не были изменены каким-либо неуполномоченным лицом. Доступность означает доступ к данным в любое время [10]. Защищенные системы Интернета вещей должны обеспечивать все эти качества информации, получаемой из всех интеллектуальных систем.

Для обеспечения безопасности в IoT очень важно иметь упрощенное общее представление любой системы Интернета вещей. Предлагаем общее шестиуровневое упрощенное представление парадигмы Интернета вещей и требований безопасности на каждом уровне в табл. 1.

Таблица 1

Многоуровневое представление Интернета вещей и его требований к безопасности

Имя слоя	Требование безопасности
Слой физических сенсорных объектов	Безопасность конечного устройства
Локальный уровень связи	Безопасность локальной связи
Слой объектов шлюза	Безопасность данных шлюза
Уровень интернет-коммуникации	Безопасность в Интернете
Уровень облачного хранения и анализа данных	Безопасность облачных данных
Прикладной уровень интернета вещей	Безопасность приложений

Любое типичное приложение Интернета вещей может быть заменено описанной выше многоуровневой моделью. Но IoT продвигается вперед с принятием решений в режиме реального времени, например, самоуправляемому автомобилю необходимо немедленно решить, следует ли ему остановиться или продолжать движение, когда он определит человека на пешеходном переходе в нескольких метрах от транспортного средства. В этой ситуации в игру вступает распределенный интеллект для Интернета вещей.

Защита устройств Интернета вещей на основе искусственного интеллекта и машинного обучения – это новая область исследований. Подход к обеспечению безопасности на основе искусственной нейронной сети был протестирован на испытательном стенде в лабораторной среде [11], данные были собраны из пограничной сети и проанализированы. также были обнаружены правильное значение датчика и неправильная задержка, неправильное значение датчика и правильная задержка, а также неправильная задержка и неправильное значение датчика. Важными являются дальнейшие исследования для улучшения этой концепции и тестирования разработанной системы в большой лабораторной среде. Для повышения безопасности устройств Интернета вещей в недавних исследованиях

также были предложены методы обнаружения вредоносных программ, контроля доступа, аутентификации и безопасной перегрузки с использованием машинного обучения.

Доверие между сущностями очень важно для обеспечения безопасности устройств Интернета вещей. Устройства IoT взаимодействуют с другими устройствами, развернутыми другим поставщиком, только доверенное устройство должно иметь возможность выполнять сопряжение и передавать данные другой стороне. Для достижения доверия очень важна уникальная идентификация устройств. В [12] авторы предложили структуру доверительного управления для Интернета вещей, а также ее модель, основанную на машинном обучении. Поскольку устройства Интернета вещей должны иметь возможность подключаться к сети и выходить из нее в любое время, важными являются дальнейшие исследования для достижения динамического доверия к сети Интернета вещей.

Чтобы поддерживать огромную пропускную способность и массовое подключение с гибкостью и интеллектом, базовая сеть 5G будет включать облачные вычисления с комбинацией SDN и NFV [12]. Концепция 5GEx позволит осуществлять многодоменную и мультитехнологичную связь между различными сетевыми объектами. По мнению многих исследователей, сеть 5G увеличит межмашинную связь (M2M), а также увеличит количество приложений, работающих с ней, что позволит человеку эффективно взаимодействовать с машинами. Безопасность 5G – это еще одна открытая область для исследований.

Заключение

Интернет вещей – это междисциплинарная область, где технологии взаимодействуют с людьми, повышая качество жизни за счет улучшения условий труда и повышения производительности. По мере увеличения числа устройств Интернета вещей многие новые области технологий интегрируются с IoT для управления, подключения и совместной работы с центральным сервером. Были обсуждены двенадцать проблем безопасности для функционирования Интернета вещей. Использование распределенного интеллекта позволит принимать решения по каждому устройству IoT и сократит ненужную передачу данных в сети. В статье была представлена упрощенная универсальная модель с шестью уровнями, которая может представлять систему безопасности любой системы Интернета вещей. Грамотная реализация распределенного интеллекта в этой многоуровневой модели обеспечит полную безопасность функционирования Интернета вещей. Применение машинного обучения в IoT растет во всех его секторах, включая безопасность Интернета вещей. Алгоритмы машинного обучения улучшают механизмы функционирования Интернета вещей, но они также создают проблемы его безопасности. Скомпрометированный узел Интернета вещей может быть обучен с использованием вводящих его в заблуждение данных, и он может вести себя неожиданно, что может быть очень вредным. Для защиты узлов Интернета вещей от несанкционированного доступа требуется надежная инфраструктура Интернета вещей. Огромное количество конфиденциальных данных, которое может быть получено из будущих систем Интернета вещей, может быть скомпрометиро-

вано. Для обеспечения безопасности, конфиденциальности и доверия к будущим сетям Интернета вещей и данным Интернета вещей должно быть расширено использование алгоритмов машинного обучения, распределенного интеллекта, виртуализации сетевых функций, программно-определяемой сети, блокчейн-технологий и беспроводной сети 5G. Использование этих новых технологий позволяет решить часть проблем с безопасностью, но и создает новые проблемы безопасности, требующие решения в ходе дальнейших исследований.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Суомалайнен А. Интернет вещей: видео, аудио, коммутация: ДМК Пресс, 2019. – 122 с.

2. Santucci, G. The internet of things: Between the revolution of the internet and the metamorphosis of objects. Vision and Challenges for Realising the Internet of Things, 2010. – P. 11–24.

3. Мачей К. Интернет вещей. Новая технологическая революция: Эксмо, 2017. – 330 с.

4. Sardeshmukh, H., & Ambawade, D. Internet of Things: Existing protocols and technological challenges in security. In Intelligent Computing and Control, 2017 International Conference on IEEE. – Pp. 1–7.

5. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications (2017). – 84. – Pp. 25–37.

6. Al-Gburi, A., Al-Hasnawi, A., & Lilien, L. Differentiating Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls. In Computer and Network Security Essentials. Springer, Cham. 2018. – Pp. 153–172.

7. Мешалкин В. П., Дли М. И., Пучков А. Ю., Лобанева Е. И. Предварительная оценка прагматической ценности информации в задаче классификации на основе глубоких нейронных сетей // Прикладная информатика. – 2021. – Т. 16. – № 3. – С. 9–20. DOI: 10.37791/2687-0649-2021-16-3-9-20.

8. Krishna, B. S., & Gnanasekaran, T. A systematic study of security issues in Internet-of-Things (IoT). In I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on 2017, February. – Pp. 107–111.

9. Ramadhan, A. A survey of security aspects for Internet of Things in healthcare. In Information Science and Applications (ICISA) 2016 (pp. 1237–1247). Springer, Singapore.

10. Varadarajan, P., & Crosby, G. Implementing IPsec in wireless sensor networks. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference (pp. 1–5). IEEE.

11. Sain, M., Kang, Y. J., & Lee, H. J. (2017, February). Survey on security in Internet of Things: State of the art and challenges. In Advanced Communication Technology (ICACT), 2017 19th International Conference (pp. 699–704). IEEE.

12. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal. – 4(5). – Pp. 1250–1258.