КЛАССИФИКАЦИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ ДЛЯ IoT

Сеидуллаев Мадияр Камалович
Ассистент
Ташкентский университет информационных технологий
имени Мухаммада ал-Хоразми

Муродов Маъмуржон Маърупович
Ташкентский университет информационных технологий
имени Мухаммада ал-Хоразми

Аннотация: *С появлением умных домов, умных городов и всего умного Интернет вещей (IoT) стал областью невероятного влияния, потенциала и роста, и Cisco Inc. прогнозирует к 2020 году иметь 50 миллиардов подключенных устройств, большинство этих IoT-устройств легко взломать и скомпрометировать. Как правило, эти IoT-устройства ограничены в вычислительных ресурсах, хранилищах и пропускной способности сети, поэтому они более уязвимы для атак, чем другие конечные устройства, такие как смартфоны, планшеты или компьютеры.*

В этой статье мы представляем и рассматриваем основные проблемы безопасности для IoT. Мы рассматриваем и классифицируем популярные проблемы безопасности в отношении многоуровневой архитектуры IoT, а также протоколов, используемых для работы в сети, связи и управления..

Ключевые слова: *Безопасность, IoT, протоколы IoT, сетевая безопасность***.**

Введение

С быстрым ростом интеллектуальных устройств и высокоскоростных сетей Интернет вещей (IoT) получил широкое признание и популярность в качестве основного стандарта для сетей с низким энергопотреблением и потерями (LLN), имеющих ограниченные ресурсы. Он представляет собой сеть, в которой «вещи» или встроенные устройства с датчиками связаны между собой через частную или общедоступную сеть [1,2]. Устройствами в IoT можно управлять удаленно для выполнения желаемой функциональности. Затем обмен информацией между устройствами происходит через сеть, в которой используются стандартные протоколы связи. Интеллектуальные подключенные устройства или «вещи»

варьируются от простых носимых аксессуаров до больших машин, каждая из которых содержит сенсорные чипы. Например, смарт-обувь Lenovo содержит чипы, обеспечивающие поддержку отслеживания и анализа данных о фитнесе [3]. Точно так же электрические приборы, включая стиральные машины и холодильники, могут управляться удаленно через IoT. Камеры безопасности, установленные для наблюдения за местом, можно контролировать удаленно в любой точке мира.

Помимо личного использования, IoT также служит потребностям сообщества. Различные интеллектуальные устройства, которые выполняют различные функции, такие как мониторинг операций в больницах, определение погодных условий, обеспечение отслеживания и связи в автомобилях, а также идентификация животных с помощью биочипов, уже служат конкретным потребностям сообщества [4]. Данные, собранные с помощью этих устройств, могут обрабатываться в режиме реального времени для повышения эффективности всей системы.

Будущее значение IoT очевидно благодаря его применению в повседневной жизни. Он продолжает быстро расти из-за развития аппаратных методов, таких как улучшение пропускной способности за счет включения сетей на основе когнитивного радио для решения проблемы недостаточного использования частотного спектра [5,6]. В литературе беспроводные сенсорные сети (WSN) и межмашинное взаимодействие (M2M) или киберфизические системы (CPS) теперь превратились в неотъемлемые компоненты более широкого термина IoT. Следовательно, проблемы безопасности, связанные с WSN, M2M или CPS, продолжают возникать в контексте IoT, где протокол IP является основным стандартом для подключения. Поэтому вся архитектура развертывания должна быть защищена от атак, которые могут помешать услугам, предоставляемым IoT, а также могут создать угрозу конфиденциальности, целостности или конфиденциальности данных. Поскольку парадигма IoT представляет собой набор взаимосвязанных сетей и разнородных устройств, она наследует традиционные проблемы безопасности, связанные с компьютерными сетями. Ограниченные ресурсы создают дополнительные проблемы для безопасности IoT, поскольку небольшие устройства или вещи, содержащие датчики, имеют ограниченную мощность и память. Следовательно, решения по обеспечению безопасности должны быть адаптированы к ограниченным архитектурам.

Архитектура IoT и проблемы безопасности

Типичное развертывание IoT содержит разнородные устройства со встроенными датчиками, соединенными через сеть, как показано на рис. 1.

Устройства в IoT однозначно идентифицируются и в основном характеризуются низким энергопотреблением, небольшим объемом памяти и ограниченными вычислительными возможностями. Шлюзы развертываются для подключения устройств IoT к внешнему миру для удаленного предоставления данных и услуг пользователям IoT.

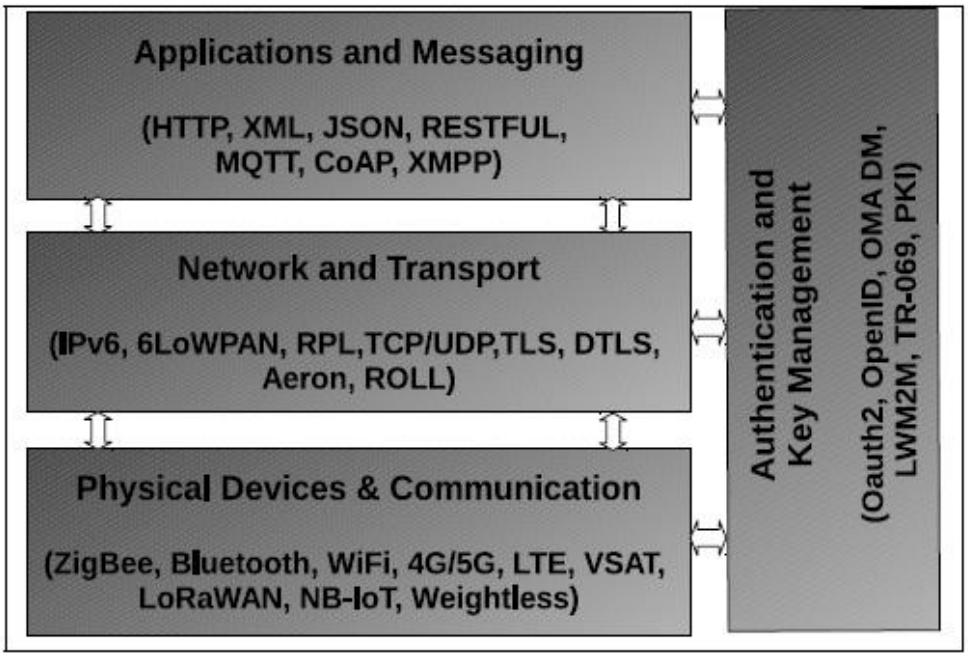

Рис. 1. Общие стандарты и протоколы IoT.

Протоколы и стандарты IoT

На рис. 1 показана многоуровневая архитектура с общими протоколами IoT, используемыми для приложений и обмена сообщениями, маршрутизации/переадресации, физических устройств, а также для управления ключами и аутентификации. Он включает в себя стандарты и протоколы для обычно используемых низкоскоростных беспроводных персональных сетей (LR-WPAN) [7] и недавно разработанные протоколы для протоколов на основе маломощных глобальных сетей (LPWAN).

Для LR-WPAN стандарт IEEE 802.15.4 описывает два низкоуровневых уровня: физический уровень и уровень управления доступом к среде (MAC). Спецификация физического уровня относится к связи по беспроводным каналам, имеющим различные полосы частот и скорости передачи данных. Спецификация уровня MAC связана с механизмами доступа к каналу, а также с синхронизацией. Из-за небольшого размера максимальной единицы передачи (MTU), используемой в стандарте IEEE 802.15.4, уровень адаптации IPv6 по беспроводной персональной сети с низким энергопотреблением (6LoWPAN) встроен над уровнем канала, чтобы обогатить сенсорный узел IP. на основе

коммуникативных возможностей. Каждое устройство в IoT уникально идентифицируется сетевым адресом IPv6. Протокол маршрутизации для сетей с низким энергопотреблением и потерями (RPL) [8] используется для поддержки сред 6LoWPAN. Стандарт RPL поддерживает двухточечный трафик, а также связь между несколькими точками и одной точкой.

Из-за ограниченной полезной нагрузки дизайн приложения в IoT включает протокол пользовательских дейтаграмм (UDP) [9] для связи, поскольку он считается более эффективным и менее сложным, чем TCP. Кроме того, сжатие заголовка UDP может быть выполнено для лучшего использования ограниченного пространства полезной нагрузки [10]. Для управляющих сообщений, таких как указание недостижимого пункта назначения и обнаружение соседей, 6LoWPAN использует протокол управления сообщениями в Интернете (ICMP) [11]. Протокол ограниченных приложений (CoAP) [12] предоставляет модель, основанную на запросе и ответе, для сетей с низким энергопотреблением и потерями, существующих в средах с ограничениями. Протокол CoAP поддерживает асинхронную передачу сообщений, а также обеспечивает сопоставление HTTP для доступа к ресурсам IoT через HTTP.

LPWAN обеспечивает дальнюю связь «вещей» в IoT. В отличие от беспроводной глобальной сети, которая требует большей мощности для работы с высокой скоростью передачи данных, она поддерживает связь с низким энергопотреблением и низкой скоростью передачи данных. LPWAN использует протокол LoRaWAN для связи между шлюзами и конечными устройствами, поддерживая различные скорости передачи данных в сети устройств с батарейным питанием. Точно так же узкополосный IoT (NB-IoT) представляет собой протокол 3GPP для связи в сетях LPWAN для обеспечения покрытия внутри помещений при использовании спектра LTE. Протокол Weightless использует три различных стандарта связи в LPWAN для поддержки однонаправленного, двунаправленного и маломощного режимов соответственно.

Требования безопасности для Интернета вещей

Для безопасного развертывания IoT необходимо учитывать различные механизмы и параметры, как описано ниже.

Конфиденциальность данных и целостность

Поскольку данные IoT проходят через несколько переходов в сети, для обеспечения конфиденциальности данных требуется надлежащий механизм шифрования. Из-за разнообразной интеграции сервисов, устройств и сети данные, хранящиеся на устройстве, уязвимы для нарушения

конфиденциальности из-за компрометации узлов, существующих в сети IoT. Устройства IoT, подверженные атакам, могут заставить злоумышленника повлиять на целостность данных, изменив сохраненные данные в злонамеренных целях.

Аутентификация, авторизация и идентификация

Для защиты связи в IoT требуется аутентификация между двумя сторонами, общающимися друг с другом. Для привилегированного доступа к службам устройства должны быть аутентифицированы. Разнообразие механизмов аутентификации для IoT существует в основном из-за разнообразных гетерогенных базовых архитектур и сред, которые поддерживают устройства IoT. Эти среды создают проблему для определения стандартного глобального протокола для аутентификации в IoT. Точно так же механизмы авторизации гарантируют, что доступ к системам или информации предоставляется авторизованным. Правильная реализация авторизации и аутентификации приводит к созданию надежной среды, которая обеспечивает безопасную среду для связи. Кроме того, учет использования ресурсов вместе с аудитом и отчетностью обеспечивает надежный механизм для обеспечения безопасности управления сетью.

Доступность услуг

Атаки на устройства IoT могут препятствовать предоставлению услуг посредством обычных атак типа «отказ в обслуживании». Различные стратегии, в том числе атаки воронки, глушение противников или атаки повторного воспроизведения, используют компоненты IoT на разных уровнях для ухудшения качества обслуживания (QoS), предоставляемого пользователям IoT.

Энергоэффективность

Устройства IoT обычно ограничены в ресурсах и характеризуются низким энергопотреблением и меньшим объемом памяти. Атаки на архитектуру IoT могут привести к увеличению энергопотребления за счет переполнения сети и исчерпания ресурсов IoT из-за избыточных или поддельных запросов на обслуживание.

Единичные точки отказа

Непрерывный рост разнородных сетей для инфраструктуры на основе IoT может выявить большое количество единых точек отказа, которые, в свою очередь, могут ухудшить качество услуг, предусмотренных IoT. Это требует разработки защищенной от несанкционированного доступа среды для большого количества IoT-устройств, а также предоставления альтернативных механизмов реализации отказоустойчивой сети.

Классификация проблем безопасности

Поскольку парадигма IoT охватывает широкий спектр устройств и оборудования, от небольших встроенных процессоров до крупных высокопроизводительных серверов, необходимо решать проблемы безопасности на разных уровнях.

Классификация проблем безопасности для IoT представлена на рис. 3 вместе со ссылками на публикации, относящиеся к каждой проблеме. Мы классифицируем угрозы безопасности в отношении архитектуры развертывания IoT, как описано ниже.

• Проблемы с безопасностью низкого уровня.
• Проблемы с безопасностью среднего уровня
• Проблемы безопасности высокого уровня.

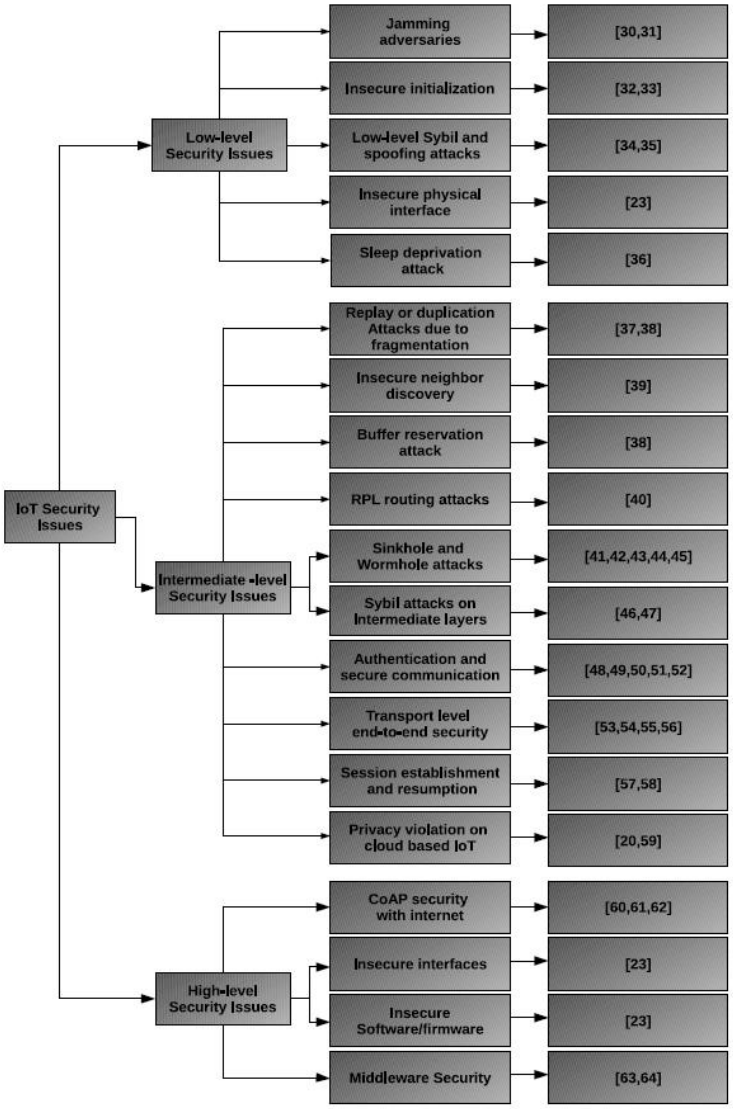

Рис. 3. Классификация вопросов безопасности и связанных с ними публикаций

Проблемы с безопасностью низкого уровня

Первый уровень безопасности связан с вопросами безопасности на физическом и канальном уровнях связи, а также на аппаратном уровне, как подробно описано ниже.

Глушение противников. Атаки глушения на беспроводные устройства в IoT нацелены на ухудшение сетей за счет излучения радиочастотных сигналов без следования определенному протоколу [13,14].

Радиопомехи серьезно влияют на работу сети и могут повлиять на отправку и получение данных законными узлами, что приводит к сбоям в работе или непредсказуемому поведению системы.

Небезопасная инициализация. Безопасный механизм инициализации и настройки IoT на физическом уровне обеспечивает надлежащее функционирование всей системы без нарушения конфиденциальности и нарушения работы сетевых сервисов [15,16]. Связь физического уровня также должна быть защищена, чтобы сделать ее недоступной для неавторизованных получателей.

Низкоуровневая Сибилла и спуфинговые атаки. Атаки Sybil в беспроводной сети вызываются вредоносными узлами Sybil, которые используют поддельные удостоверения для снижения функциональности IoT. На физическом уровне узел Sybil может использовать случайные поддельные значения MAC для маскировки под другое устройство с целью истощения сетевых ресурсов [17,18]. Следовательно, законным узлам может быть отказано в доступе к ресурсам.

Небезопасный физический интерфейс. Несколько физических факторов создают серьезные угрозы для надлежащего функционирования устройств в IoT. Плохая физическая безопасность, доступ к программному обеспечению через физические интерфейсы и инструменты для тестирования/отладки могут быть использованы для компрометации узлов в сети.

Приступ лишения сна. Устройства с ограниченным энергопотреблением в IoT уязвимы для атак «лишения сна», заставляя сенсорные узлы бодрствовать. Это приводит к разрядке батареи, когда в среде 6LoWPAN настроено выполнение большого количества задач.

Проблемы безопасности среднего уровня

Вопросы безопасности промежуточного уровня в основном связаны с управлением связью, маршрутизацией и сеансами на сетевом и транспортном уровнях IoT, как описано ниже.

Атаки воспроизведения или дублирования из-за фрагментации. Фрагментация пакетов IPv6 требуется для устройств, соответствующих

стандарту IEEE 802.15.4, для которого характерен небольшой размер кадра. Восстановление полей фрагментов пакетов на уровне 6LoW-PAN может привести к истощению ресурсов, переполнению буфера и перезагрузке устройств. Дубликаты фрагментов, отправленные вредоносными узлами, влияют на повторную сборку пакета, тем самым препятствуя обработке других легитимных пакетов.

Небезопасное обнаружение соседей. Архитектура развертывания IoT требует уникальной идентификации каждого устройства в сети. Передача сообщений для идентификации должна быть безопасной, чтобы гарантировать, что данные, передаваемые на устройство при сквозной связи, достигают указанного адресата. На этапе обнаружения соседей перед передачей данных выполняются различные шаги, включая обнаружение маршрутизатора и разрешение адреса. Использование пакетов обнаружения соседей без надлежащей проверки может иметь серьезные последствия наряду с отказом в обслуживании.

Атака с резервированием буфера. Поскольку принимающему узлу требуется резервировать буферное пространство для повторной сборки входящих пакетов, злоумышленник может использовать это, отправляя неполные пакеты. Эта атака приводит к отказу в обслуживании, поскольку другие пакеты фрагментов отбрасываются из-за того, что пространство занято неполными пакетами, отправленными злоумышленником.

Атака маршрутизации RPL. Протокол маршрутизации IPv6 для сетей с низким энергопотреблением и потерями (RPL) уязвим для нескольких атак, запускаемых через скомпрометированные узлы, существующие в сети. Атака может привести к истощению ресурсов и прослушиванию.

Атаки воронками и червоточинами. При атаках воронки атакующий узел отвечает на запросы маршрутизации, тем самым направляя пакеты через атакующий узел, который затем может быть использован для злонамеренных действий в сети. Атаки на сеть могут еще больше ухудшить работу 6LoWPAN из-за атак червоточины, при которых между двумя узлами создается туннель, так что пакеты, поступающие на узел, немедленно достигают другого узла. Эти атаки имеют серьезные последствия, включая прослушивание, нарушение конфиденциальности и отказ в обслуживании.

Сивилла атакует промежуточные слои. Подобно атакам Sybil на низкоуровневые уровни, узлы Sybil могут быть развернуты для снижения производительности сети и даже нарушения конфиденциальности данных. Связь узлов Sybil с использованием поддельных идентификаторов в сети может

привести к рассылке спама, распространению вредоносных программ или запуску фишинговых атак.

Аутентификация и безопасная связь. Устройства и пользователи в IoT должны быть аутентифицированы с помощью систем управления ключами. Любая лазейка в безопасности на сетевом уровне или большие накладные расходы на защиту связи могут подвергнуть сеть большому количеству уязвимостей. Например, из-за ограниченных ресурсов необходимо свести к минимуму накладные расходы на безопасность транспортного уровня дейтаграмм (DTLS), а криптографические механизмы, обеспечивающие безопасную передачу данных в IoT, должны учитывать эффективность, а также дефицит других ресурсов.

Сквозная безопасность на транспортном уровне. Сквозная безопасность на транспортном уровне направлена на обеспечение безопасного механизма, чтобы данные от узла-отправителя поступали к желаемому узлу-получателю надежным образом. Для этого требуются комплексные механизмы аутентификации, которые обеспечивают безопасную передачу сообщений в зашифрованном виде без нарушения конфиденциальности при работе с минимальными накладными расходами.

Установление и возобновление сеанса. Перехват сеанса на транспортном уровне с поддельными сообщениями может привести к отказу в обслуживании. Атакующий узел может выдать себя за узел-жертву, чтобы продолжить сеанс между двумя узлами. Узлы связи могут даже потребовать повторной передачи сообщений путем изменения порядковых номеров.

Нарушение конфиденциальности в облачном IoT Различные атаки, которые могут нарушить конфиденциальность личности и местоположения, могут быть запущены в облачном или устойчивом к задержкам сетевом IoT. Точно так же злонамеренный поставщик облачных услуг, на котором основано развертывание IoT, может получить доступ к конфиденциальной информации, передаваемой в желаемое место назначения.

Проблемы безопасности высокого уровня

Проблемы безопасности высокого уровня в основном связаны с приложениями, работающими в IoT, как описано ниже.

Безопасность CoAP с Интернетом. Уровень высокого уровня, содержащий прикладной уровень, также уязвим для атак. Протокол ограниченного приложения (CoAP), являющийся протоколом веб-передачи для ограниченного устройства, использует привязки DTLS с различными режимами безопасности для обеспечения сквозной безопасности. Сообщения CoAP следуют

определенному формату, определенному в RFC-7252, который необходимо зашифровать для безопасной связи. Точно так же поддержка многоадресной рассылки в CoAP требует адекватных механизмов управления ключами и аутентификации.

Небезопасные интерфейсы. Для доступа к услугам IoT интерфейсы, используемые через Интернет, мобильные устройства и облачные технологии, уязвимы для различных атак, которые могут серьезно повлиять на конфиденциальность данных.

Небезопасное программное обеспечение/прошивка. Различные уязвимости в IoT включают уязвимости, вызванные небезопасным программным обеспечением/прошивкой. Код с такими языками, как JSON, XML, SQLi и XSS, необходимо тщательно тестировать. Точно так же обновления программного обеспечения/прошивки должны выполняться безопасным образом.

Безопасность промежуточного программного обеспечения. Промежуточное ПО IoT, предназначенное для обеспечения связи между разнородными объектами парадигмы IoT, должно быть достаточно безопасным для предоставления услуг. Различные интерфейсы и среды, использующие промежуточное программное обеспечение, должны быть включены для обеспечения безопасной связи.

Заключение

Современные IoT-устройства небезопасны и неспособны защитить себя. Это связано в основном с ограниченными ресурсами в устройствах IoT, незрелыми стандартами и отсутствием безопасного проектирования, разработки и развертывания аппаратного и программного обеспечения. Усилия по определению надежного глобального механизма для защиты уровней IoT также затрудняются из-за разнообразия ресурсов в IoT. В этой статье мы рассматриваем и анализируем основные проблемы безопасности IoT. Мы классифицируем эти проблемы в зависимости от уровней высокого, среднего и низкого уровня IoT.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[2] D. Giusto, A. Iera, G. Morabito, L. Atzori, The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, Springer Publishing Company, Incorporated, 2014.

[3] B. Heater, Lenovo shows off a pair of intel-powered smart shoes, 2016. URL https://techcrunch.com/2016/06/09/lenovo-smart-shoes/.

[4] M. Rouse, I. Wigmore, Internet of things, 2016. URL http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT..

[5] A.A. Khan, M.H. Rehmani, A. Rachedi, Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions, IEEE Wirel. Commun. 24 (3) (2017) 17–25. http://dx.doi.org/10.1109/MWC.2017.1600404.

[6] F. Akhtar, M.H. Rehmani, M. Reisslein, White space: Definitional perspectives and their role in exploiting spectrum opportunities, Telecommun. Policy 40 (4) (2016) 319–331. http://dx.doi.org/10.1016/j.telpol.2016.01.003.

[7] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

[8] IEEE, IeEEE Standard for Local and metropolitan networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), 2012. URL https://standards.ieee.org/findstds/standard/802.15.4-2011.html.

[9] T. Winter, P. Thubert, A. Brandt, J.W. Hui, R. Kelsey, Rfc 6550 - rpl: ipv6 routing protocol for low-power and lossy networks, 2012. URL https://tools.ietf.org/html/rfc6550.

[10] J. Postel, User datagram protocol, 1980. URL https://tools.ietf.org/html/rfc768.

[11] J.W. Hui, P. Thubert, Compression format for IPv6 datagrams over IEEE 802.15.4-based networks, 2011. URL https://tools.ietf.org/html/rfc6282.

[12] A. Conta, S. Deering, M. Gupta, Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification, 2006. URL https://tools.ietf.org/html/rfc4443.M.A. Khan, K. Salah / Future Generation Computer Systems 82 (2018) 395–411 409

[13] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (CoAP), 2014. URL https://tools.ietf.org/html/rfc7252.

[14] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. http://dx.doi.org/10.1145/1062689.1062697.

[15] G. Noubir, G. Lin, Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30.

[16] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. for. Sec. 9 (10) (2014) 1617–1628. http://dx.doi.org/10.1109/TIFS.2014.2341453.

[17] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Process. Mag. 30 (5) (2013) 29–40.

[18] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3) (2009) 492–503.