УДК 681.31

Д. А. Еременко, А. В. Шоров
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Анализ сетевой безопасности эталонной архитектуры туманных вычислений

Приведены результаты анализа сетевой безопасности эталонной архитектуры туманных вычислений. Рассматриваемая архитектура представлена консорциумом OpenFog, в который входят такие ведущие компании, как Intel, Dell, Microsoft, Cisco и др. В архитектуре описаны типы связи Node-to-Node, Node-to-Cloud. В ходе анализа архитектуры были исследованы вопросы безопасности следующих типов связей: Node-to-Node, Node-to-Cloud и Node-to-Device. Для каждого типа связи были рассмотрены протоколы безопасности и выявлены возможные угрозы и уязвимости. Также приведены выводы о потенциальных методах защиты. Кроме того, в работе была рассмотрена предполагаемая модель угроз OpenFog Reference Architecture, описывающая типы угроз, уровни их реализации и аспекты безопасности.

Безопасность туманных вычислений, атаки на туманные вычисления, архитектура туманных вычислений, архитектура OpenFog RA, анализ сетевой безопасности туманных вычислений, связи в туманных вычислениях

Развитие концепции Internet of Things (IoT) послужило толчком для распространения различных типов устройств в компьютерных сетях по всему миру. Как правило, подобные устройства генерируют большое количество неоднородных, зашумленных данных. Информация, поступающая с подобных устройств, обычно обрабатывается центрами обработки данных (ЦОД), часто с использованием облачных технологий. Однако в последнее время получила развитие концепция так называемых туманных вычислений.

Туманные вычисления – это горизонтальная архитектура системного уровня, которая распределяет ресурсы и службы (такие как вычисления, хранение данных, управление и организация сети) между облачной вычислительной средой (ОВС) и конечным устройством/узлом. Данная архитектура основана на моделях IoT, 5G и ориентирована на задачи, требованиями к которым являются:

– ограниченные вычислительные ресурсы;
– высокая пропускная способность сети;
– сверхнизкая задержка прохождения сигнала;
– повышенные меры безопасности.

Этот подход расширяет традиционную модель облачных вычислений, позволяя выполнять обработку данных локально. Туманные вычисления сохраняют все преимущества облачных вычислений, таких как контейнеризация, виртуализация, оркестровка, управляемость и эффективность [1]. Туманная модель вычислений перемещает обработку данных и принятие решений из облака ближе к оконечным узлам, вплоть до датчиков и исполнительных механизмов IoT.

В данной статье описывается архитектура туманных вычислений, рассматриваются типы связей и проводится анализ их сетевой безопасности. Кроме того, предлагается интеграция инфраструктуры открытых ключей в туманные вычисления.

Эталонная архитектура OpenFog. На сегодняшний день разработкой концепции туманных вычислений занимаются множество ведущих IT-компаний, такие как Cisco Systems, Intel, Microsoft Corporation, Dell и др. В 2015 г. компаниями был создан консорциум OpenFog. Одна из главных задач этой организации – разработка системной архитектуры для туманных вычислений и прора-

ботка методов практического внедрения новой модели вычислений. В результате работы консорциум представил эталонную архитектуру туманных вычислений OpenFog Reference Aechitecture (OpenFog RA).

Эталонная архитектура OpenFog RA – это архитектура, затрагивающая средний и высокий уровень абстракции и разработанная для туманных узлов и сетей. Данная архитектура представлена на рис. 1.

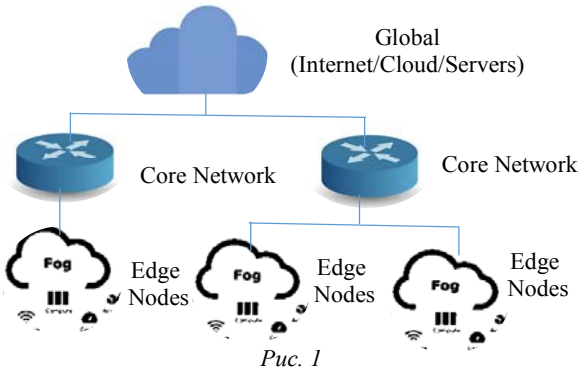

Рис. 1

OpenFog RA устанавливает набор основополагающих принципов, которые называются Pillars (столпы/колонны):

– безопасность;
– масштабируемость;
– открытость;
– автономия;
– RAS (надежность, доступность, удобство обслуживания);
– гибкость;
– иерархичность;
– программируемость.

Эталонная архитектура OpenFog RA представляет собой совокупность туманных узлов, включающих гибкую систему соединений и физически не привязанных к сети.

Архитектура туманных вычислений находит широкое применение в различных отраслях и рынках (среди них транспорт, сельское хозяйство, смарт-города, интеллектуальные здания, здравоохранение, гостиничный бизнес, энергетика и финансовые услуги). Она обеспечивает реализацию бизнес-проектов для приложений IoT, которые требуют принятий решений в реальном времени, низкую задержку, повышенную безопасность и ограниченный трафик сети.

Рассмотрим различные типы связей между узлами в туманных вычислениях. Можно выделить три типа связей [1]:

– Node-to-Cloud;
– Node-to-Node;
– Node-to-Device.

Соединение Node-to-Cloud сохраняет протоколы интернет-коммуникаций и API-интерфейсы, которые используются облачными серверами для взаимодействия с внешними устройствами (включая устройства IoT, персональные мобильные устройства, терминалы, автономные компьютеры и серверы). Почти все эти коммуникации в настоящее время осуществляются с помощью наборов протоколов, представленных в табл. 1.

Таблица 1

Приложения	Протокол	
	передачи данных	безопасности
Для предприятий	SOAP over HTTP	WSS
Мобильные и пользовательские	RESTful HTTP/COAP	TLS/DTLS

Как видно из табл. 1, протоколы относятся к прикладному уровню.

Соединение Node-to-Node. Распределенная туманная вычислительная платформа (ТВП) может состоять из иерархии туманных узлов, охватывающих несколько интернет-подсетей или административных доменов. Эти узлы ТВП должны взаимодействовать друг с другом, используя шаблон издатель-подписчик (на основе событий) и клиент-серверных сообщений, что позволит обеспечить прямое и своевременное взаимодействие. Для реализации этих парадигм обычно используются стеки протоколов, представленные в табл. 2.

Таблица 2

Приложения	Протокол	
	передачи данных	безопасности
Клиент-сервер	SOAP, RESTful HTTP/COAP	WSS, TLS/DTLS
Издатель-подписчик	MQTT, AMQP, RTPS	TLS/DTLS

Исходя из представленных данных, можно сделать вывод о том, что безопасность связи будет базироваться на безопасности протоколов TLS/DTLS и WSS.

Соединение Nod-to-Device. Данная связь описывает соединение между узлом и конечными устройствами. Эти устройства могут быть связаны с узлом с помощью различных коммуникационных протоколов (через различные коммуникационные среды). С использованием стека протоколов (TCP/UDP/IP) были предприняты усилия по конвергенции протоколов между беспроводными сетями, проводными сетями и промышленной автоматизацией.

Также существуют устройства, не адаптированные к интернет-протоколам со строго ограниченными ресурсами. Таким устройствам доступно только ограниченное множество криптографических функций (симметричные шифры, которые используют установленные вручную ключи). Эти устройства должны быть установлены в физически защищенных средах и подключены через аппаратные соединения к одному или нескольким узлам тумана, которые могут обеспечить большинство служб безопасности.

В табл. 3 представлены протоколы взаимодействия для связи Node-to-Device.

Таблица 3

Уровень	Протоколы
PHY & MAC Layer	WLAN: 802.11, WPAN: 802.15, PLC: PRIME, Automation: CIP
Wireless Protocol Stacks	Wi-Fi, Bluetooth, ZigBee
Adaptation Layer	WLAN/WPAN: 6LowPAN, PLC: PRIME IPv6 SSCS, Automation: Ethernet/IP
Transport/Network Layers	UDP over IPv6, TCP over IPv6, IPv6 Stack
Application Layer (Publish-Subscribe Messaging)	CoAP, MQTT, AMQP, RTPS
Routing	RPL, PCEP, LISP (Cisco)
Security	802.1AR – Secure Device Identity 802.1AE – Media Access Control (MAC) Security 802.1X – Port-Based (Authenticated) Media Access Control IPsec AH & ESP, Tunnel/Transport Modes (D)TLS – (Datagram) Transport Layer Security

Из табл. 3 следует, что самым распространенным протоколом беспроводной связи является протокол Wi-Fi. Поэтому при анализе данного типа связи этот протокол будет рассматриваться как протокол передачи данных.

Безопасность туманных вычислений. Безопасность – важнейший аспект туманных вычислений. Для обеспечения базовой функциональной совместимости должны существовать общие положения, которые будут учитывать региональные и государственные требования по безопасности. На их основе будет базироваться безопасность туманных вычислений.

Одним из основополагающих принципов безопасности OpenFog RA является криптография. Для того чтобы гарантировать на базовом уровне совместимость компонентов туманных вычислений, OpenFog RA адаптирует спецификацию FIPS 140-2 [2], которая содержит требования к безопасности для криптографических модулей. В ней определен список криптографических функций, а также алгоритмы их применения. Ответственность за сертификацию криптографических модулей ляжет на поставщиков и изготовителей.

Криптографический модуль OpenFog должен поддерживать минимальный набор следующих функций:

– симметричное шифрование: AES (128-bit), Triple-DES;

– асимметричное шифрование: DH, RSA, DSA;

– шифрование на эллиптических кривых: ECDH, ECDSA, ECQV;

– криптографические хэш-функции: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256;

– генератор случайных чисел;

– аутентификация сообщений: CCM, GCM, GMAC6, CMAC, HMAC.

Для защиты соединений в эталонной архитектуре OpenFog выделен отдельный уровень – защита соединений. На данном уровне реализуются коммуникационные службы безопасности, описанные в рекомендациях X.800 [3] для всех физических/виртуальных каналов связи среди всех объектов в иерархии Device-Fog-Cloud Computing:

• Конфиденциальность:

– сетевого соединения;

– сетевых пакетов;

– сетевого трафика.

• Целостность:

– сетевого соединения с восстановлением;

– сетевых пакетов (с возможностью обнаружения).

• Аутентификация:

– сетевого пакета (подтверждение правильности источника);

– сетевого соединения.

• Неотказуемость:

– источника;

– получателя.

Для реализации данных служб безопасности используются механизмы безопасности, представленные в табл. 4.

В данной таблице используется два вида обозначений: «+» – механизм используется для реа-

Таблица 4

Служба безопасности	Механизм защиты					
	Шифрование	ЭЦП	Контроль целостности данных	Дополнение трафика (padding)	Контроль маршрутизации	Нотаризация
Конфиденциальность сетевого соединения	+	–	–	–	+	–
Конфиденциальность сетевых пакетов	+	–	–	–	+	–
Конфиденциальность сетевого трафика	+	–	–	+	–	–
Целостность сетевого соединения с восстановлением	+	–	+	–	–	–
Целостность сетевых пакетов	+	+	+	–	–	–
Аутентификация сетевого пакета	+	–	–	–	–	–
Аутентификация сетевого соединения	+	–	–	–	–	–
Неотказуемость источника	–	+	+	–	–	+
Неотказуемость получателя	–	+	+	–	–	+

Таблица 5

Угроза	Аспект безопасности			
	Конфиденциальность	Целостность	Доступность	Аутентификация
Инсайдеры	Утечка данных	Изменение данных	Предоставление недоступных ресурсов	Подмена данных
Атаки на аппаратном уровне	Трояны, атака по сторонним каналам	Трояны	Радиопомехи, исчерпание полосы пропускания	Трояны
Атаки на программное обеспечение	Вредоносное программное обеспечение	Вредоносное программное обеспечение	DoS/DDoS, истощение ресурсов	Вредоносное программное обеспечение, социальная инженерия
Сетевые атаки	Прослушивание, анализ сетевого трафика	Пересылка сообщений	DoS/DDoS, Subnet Flooding	Spoofing, Man-in-Middle Attacks

лизации данной функции безопасности; «–» – механизм не предназначен для реализации данной функции безопасности.

Таким образом, при реализации требований механизмов безопасности X.800 будет обеспечена конфиденциальность, целостность, аутентификация и неотказуемость передачи сообщений.

Анализ безопасности. В эталонной архитектуре OpenFog RA приводится предполагаемая модель угроз. Она описывает типы угроз, уровни их реализации и аспекты безопасности, к которым относятся угрозы [1]. Модель угроз представлена в табл. 5.

Туманные вычисления представляют собой распределенную сеть, поэтому стоит уделить особое внимание сетевой безопасности. В [4] и [5] отмечается уязвимость туманных вычислений к атаке «человек посередине» (Man-in-Middle Attacks, MITM). Также в статьях заостряется внимание на том, что данная атака может быть проведена практически незаметно для потенциальной жертвы. Обе статьи вышли до опубликования эталонной архитектуры туманных вычислений, и в них не учитывается то, что в Open Fog RA приняты рекомендации X.800, которые устанавливают требования к строгой аутентификации соединения (сетевым пакетам), а также к шифрованию каналов связи. С учетом принятых требований и рекомендаций OpenFog RA проведение описанной в статьях атаки маловероятно.

Рассмотрим каждый тип связи эталонной архитектуры с точки зрения сетевой безопасности.

Node-to-Cloud и *Node-to-Node*. В обоих типах связи используется протокол безопасности TLS/DTLS, обеспечивающий конфиденциальность, аутентификацию и целостность соединения. На данный момент существует три типа атаки на TLS/DTLS: Bar Mitzvah [6], Logjam [7] и подмена клиентского SSL-сертификата. Рассмотрим каждый в отдельности.

Атака *Bar Mitzvah* направлена на взлом алгоритма симметричного шифрования RC4, который поддерживается протоколом TLS/DTLS. Для согласования параметров соединения в протоколе TLS/DTLS клиент и сервер обмениваются сообщениями ClientHello и ServerHello. Если в процессе согласования в качестве алгоритма симметричного шифрования будет выбран алгоритм RC4, то данные, которые будут зашифрованы этим алгоритмом, могут быть расшифрованы. Для того чтобы избежать атаки данного типа, достаточно исключить возможность выбора алгоритма RC4 на этапе согласования параметров соединения.

Атака *Logjam* производится на сессионные ключи, которые устанавливаются во время обмена по протоколу Диффи–Хеллмана с целью понижения их криптостойкости до 512-битных. Это возможно, если сервер поддерживает 512-битные ключи в протоколе Диффи–Хеллмана, используя специальный режим EXPORT_DHE. Чтобы защититься от данной атаки, так же, как и в предыдущем случае, достаточно корректно настроить сервер и отключить режим EXPORT_DHE.

Атака *подмены клиентского SSL-сертификата (MITM)*. Для осуществления атаки злоумышленнику необходимо каким-либо образом убедить жертву установить специально изготовленный клиентский SSL-сертификат, ключ от которого известен атакующему. В дальнейшем при согласовании сессионного ключа по алгоритму Диффи–Хеллмана, зная секретный ключ клиента, злоумышленник сможет вычислить сессионный ключ и нарушить конфиденциальность соединения. От данной атаки можно защититься, если использовать двухстороннюю аутентификацию.

Node-to-Device. Так как туманные вычисления мобильны, основной канал связи в большинстве случаев будет установлен с помощью соединения Wi-Fi. Злоумышленник может прослушивать канал связи, но нарушение конфиденциальности или целостности данных будет затруднено (если будут реализованы необходимые процедуры по защите соединения Wi-Fi и использованы протоколы TLS/IPsec). Однако данный вид соединения будет подвержен атакам на физическом уровне, таким как исчерпание полосы пропускания и постановка радиопомех, и ограничен дальностью связи Wi-Fi. При необходимости злоумышленник сможет забить радиочастотный канал связи и отключить пользователей от туманного узла. Если отказаться от Wi-Fi и перейти на технологии мобильной передачи данных 4G и потенциально 5G (в которых применяются технологии CDMA и ее развитие OFDMA), то это позволит противостоять атакам такого рода.

Для защиты первых двух типов соединений (Node-to-Cloud и Node-to-Node с использованием протоколов безопасности TLS/DTLS) достаточно корректной настройки сервера (настроить двухстороннюю аутентификацию и отключить возможность выбора шифрования симметричным алгоритмом RC4 и режима EXPORT_DHE).

Узким местом на данный момент в сетевой безопасности туманных вычислений является беспроводная передача данных с использованием Wi-Fi (Node-to-Device), из-за высокого риска появления угроз доступности сетевых узлов. Одним из возможных путей решения данной проблемы является переход на передачу данных с помощью мобильных сетей 4G (или 5G в будущем), в которых применяются технологии CDMA и ее развитие OFDMA.

В данной статье была рассмотрена эталонная архитектура туманных вычислений, которую представил консорциум OpenFog.

Далее были рассмотрены существующие связи в архитектуре туманных вычислений: Node-to-Cloud, Node-to-Node и Node-to-Device.

На основании анализа безопасности каждого вида связи были сделаны выводы об их уязвимостях и потенциальных методах защиты. Связи типа Node-to-Cloud и Node-to-Node могут быть уязвимы к атакам *Bar Mitzvah, Logjam* и *подмене клиентского SSL-сертификата.* Связь Node-to-Device будет наиболее уязвима к атакам на физическом уровне.

Важно отметить, что для использования протокола TLS/DTLS (соединения Node-to-Cloud и Node-to-Node) требуется разработка и внедрение в туманные вычисления инфраструктуры открытых ключей (PKI), поскольку PKI является необходимой составляющей протокола TLS/DTLS. К сожалению, в представленной архитектуре этот вопрос не освещается, но можно предположить, что центры сертификации будут реализованы в ЦОДах, как наиболее доверенных элементах системы, а каждый туманный узел будет иметь подписанный сертификат из ОВС, с помощью которого можно будет реализовать аутентификацию. Кроме того, потребуется реализовать кроссертификацию между ОВС, чтобы туманные узлы, которые имеют сертификаты из разных ЦОДов, смогли построить цепочку доверия.

Дальнейшая работа будет посвящена моделированию связей между конченными устройствами с использованием протокола ZeegBee и Wi-Fi для исследования сетевой безопасности связи Node-to-Device.

СПИСОК ЛИТЕРАТУРЫ

1. OpenFog Consortium Architecture Working Group. OpenFog Reference Architecture for Fog Computing. 2017. URL: https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf.

2. National Institute of Standards and Technology. FIPS PUB 140-2: Security Requirements for Cryptographic Modules. 2007. URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

3. International telecommunication union. Security architecture for open systems interconnection for ccitt applications. Recommendation X.800. Geneva, 1991. URL: https://www.itu.int/rec/T-REC-X.800-199103-I/en.

4. Dhande N. S. Fog computing: review of privacy and security issues // Intern. J. of Engineering Research and General Science. 2015. Vol. 3, № 2. P. 864–868.

5. Stojmenovic I., Wen S. The fog computing paradigm: Scenarios and security issues // Computer Science and Information Systems (FedCSIS), 2014 Federated Conf. on. IEEE, 2014. C. 8. URL: https://annals-csis.org/Volume_2/pliks/503.pdf.

6. Sarkar P. G., Fitzgerald S. Attacks on ssl a comprehensive study of beast, crime, time, breach, lucky 13 & rc4 biases. San Francisco: iSEC Partners, 2013.

7. Adrian D. Imperfect forward secrecy: How Diffie-Hellman fails in practice // Proc. of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015. C. 5–17. URL: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf.

D. A. Eremenko, A. V. Shorov
Saint Petersburg Electrotechnical University «LETI»

SECURITY ANALYSIS OF THE OPENFOG REFERENCE ARCHITECTURE

Fog computing is a system-level architecture that distributes resources and services along a cloud-to-thing continuum. Today the fog computing is actively developing.

In this paper, we present the security analysis of the fog computing architecture that is developed by OpenFog Consortium. During the analysis, we studied the following communication types: Node-to-Node, Node-to-Cloud, and Node-to-Device. For each communication types, we reviewed the security protocols, and identified the potential threats and vulnerabilities. In addition, the Open Fog Reference Architecture threat model that describes the types of threats, their implementation levels, and security aspects to which threats relate was examined.

Fog computing security, attacks on fog computing, fog computing architecture, OpenFog RA, network security analysis of fog computations, fog computations communications