МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ

(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Факультет «Радиоэлектроника летательных аппаратов»

Кафедра «Радиофизика, антенны и микроволновая техника»

**Реферат**

**«Туманные вычисления и Интернет вещей»**

по дисциплине: «Информационные технологии»

Выполнил студент группы М4В-301Б

Специальность: «Радиотехника»

Голованов Илья Сергеевич.

Оценка

Москва, 2020

Термин Fog Computing («туманные вычисления») был введен в оборот вице-президентом компании [Cisco](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Cisco_Systems" \o "Cisco Systems) Флавио Бономи (Flavio Bonomi) в 2011 году. Он предложил концепцию Fog Computing по аналогии с «облачными вычислениями» (Cloud Computing), как расширение «облака» до границ сети. Технологически, концепция Fog Computing тесно связана с распределёнными (облачными) дата-центрами, в которых серверы [дата-центров](https://www.tadviser.ru/index.php/%D0%A6%D0%9E%D0%94) могут располагаться во многих местоположениях, вплоть до границы сети. Дата-центры могут быть небольшими (контейнерного, модульного или мобильного исполнения), являясь фактически «выносами» крупных дата-центров. Таким образом, отличительная черта Fog Computing - приближенность к конечным пользователям и поддержка их мобильности.

Развитие [интернета вещей (IoT, Internet of Things)](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_Internet_of_Things_(IoT)) потребовало поддержки мобильности устройств IoT для различных местоположений с геолокацией и с небольшой задержкой на обработку данных. Поэтому была предложена новая платформа для удовлетворения таких требований, которая и получила название Fog computing – «туманные вычисления». Её основной особенностью является обработка данных в непосредственной близости от источников их получения, без необходимости их передачи в крупные [дата-центры](https://www.tadviser.ru/index.php/%D0%A6%D0%9E%D0%94) только для того, чтобы их там обработать и передать назад результаты.

Таким образом, становится ясным происхождение термина «туманные вычисления»: когда густое облако опускается до поверхности земли (на границу сети), мы видим туман.

Архитектура туманных вычислений приводит к минимизации накладных расходов на передачу данных, впоследствии чего улучшается производительность вычислений на облачных платформах и уменьшается потребность в обработке и хранении больших объёмов избыточных данных. В основе парадигмы туманных вычислений лежит факт постоянного увеличения необходимого устройствам Интернета вещей (англ. Internet of Things (IoT)) объёма информации, причем количество информации (по объёму, разнообразию и скорости) также растет из-за постоянно расширяющегося количества устройств.

Устройства IoT предоставляют богатую функциональность для конечных пользователей. Эти устройства нуждаются в вычислительных ресурсах для обработки полученных данных, а для обеспечения высокого уровня качества требуются быстрые процессы принятия решений. Этот факт может привести к проблемам масштабируемости и надежности при использовании стандартной архитектуры клиент-сервер, где данные считываются клиентом и обрабатываются сервером. Если сервер будет перегружен в традиционной архитектуре клиент-сервер, тогда устройства могут оказаться непригодными для использования. Парадигма туманных вычислений призвана обеспечить масштабируемое децентрализованное решение этой проблемы. Это достигается путем создания новой иерархически распределенной и локальной платформы между облачной системой и устройствами конечного пользователя. Платформа туманных вычислений способна фильтровать, агрегировать, обрабатывать, анализировать и передавать данные, что приводит к экономии времени и ресурсов связи.

Парадигму туманных вычислений можно рассматривать (в широком смысле) как инструмент для многих передовых технологий. Можно выделить основные функциональности, предоставляемые туманными системами:

быстрый анализ;

интероперабельность между устройствами;

увеличение или уменьшение времени отклика;

централизованное управление устройствами IoT или управление конкретной машиной;

низкое потребление пропускной способности;

эффективное энергопотребление;

абстракция устройства и многие другие.

Критические проблемы безопасности туманных систем

Туманные вычисления используются для повышения удобства использования облачной платформы и увеличения её потенциала. С появлением широкой применимости тумана и аналогичных технологий, таких как граничные вычисления (Edge computing), облачка (Cloudlets) и микроцентр данных (Micro-data center), увеличивается и количество атак, которые могут поставить под угрозу конфиденциальность, целостность и доступность информации, обрабатываемой в них.Эти проблемы напрямую влияют на распределенный, общий характер облачных вычислений. Являясь виртуализированной средой, такой же как облако, платформа тумана также может быть затронута теми же угрозами.

Cloud Security Alliance совместно с другими исследователями определили следующие критические проблемы безопасности, существующие в облачных и туманных инфраструктурах:

Целевая кибератака (англ. Advance Persistent Threats (APT)) — атака, целью которой является компрометация инфраструктуры компании, в результате которой похищаются данные и интеллектуальная собственность компании.

Проблема системы контроля и управления доступом (англ. Access Сontrol Issues (ACI)) — связана с атаками, приводящими к некорректному управлению доступом, позволяющими любому неавторизованному пользователю получать данные и привилегия для установки программного обеспечения на устройства и изменения их конфигураций.

Удержание аккаунта (англ. Account Hijacking (AH)) — атаки, целью которых является захват учётных записей пользователей для злонамеренной действий. Фишинг — это потенциальный метод захвата аккаунта.

Отказ в обслуживании (англ. Denial of Service (DoS)) — атаки, в результате которых подавляются конечные ресурсы системы, и законные пользователи не могут использовать её данные и приложения.

Нарушение конфиденциальности данных (англ. Data Breach (DB)) — связано с атаками, в результате которых злоумышленником освобождаются или похищаются конфиденциальные, защищенные данные пользователей.

Потеря данных (англ. Data Loss (DL)) — связана с атаками, в результате которых данные случайно (или злонамеренно) удаляются из системы. Потеря данных не обязательно может быть результатом атаки, а также может возникнуть из-за, например, стихийного бедствия.

Ошибки реализации API (англ. Insecure API (IA)) — многие поставщики облаков/тумана предоставляют интерфейсы прикладного программирования (API) для использования пользователями. Безопасность этих API-интерфейсов имеет решающее значение для безопасности любых реализованных приложений.

Уязвимости в системе и приложениях (англ. System and Application Vulnerabilities (SAV)) — это ошибки, связанные с неправильной конфигурацией программного обеспечения, с помощью которых злоумышленник может проникнуть в систему и её скомпрометировать.

Проблема внутреннего злоумышленника (англ. Malicious Insider (MI)) — в системе может существовать пользователь, который имеет авторизованный доступ к сети и системе, но решил действовать злонамеренно.

Проблема недостаточной должной добросовестности (англ. Insufficient Due Diligence (IDD)) — связана с ошибками, возникающими в результате спешки организации в принятии, разработке и внедрения функциональности в систему без достаточного тестирования.

Злоупотребление и недобросовестное использование (англ. Abuse and Nefarious Use (ANU)) — ситуация возникает, когда ресурсы предоставляются бесплатно, а злонамеренные пользователи используют указанные ресурсы для совершения злонамеренных действий.

Общие проблемы технологии (англ. Shared Technology Issues (STI)) — проблемы возникают из-за совместного использования инфраструктур, платформ или приложений. Например, базовые аппаратные компоненты не были разработаны для обеспечения сильных изолирующих свойств.

Смартфоны, умные часы и другие гаджеты тоже могут быть частью IoT. Но такие устройства, как правило, используют проприетарные протоколы связи от крупных разработчиков. Сгенерированные данные интернета вещей передаются на уровень тумана через протокол REST HTTP, который обеспечивает гибкость и функциональную совместимость при создании RESTful-сервисов. Это важно в свете необходимости обеспечения обратной совместимости с существующей вычислительной инфраструктурой, работающей на локальных компьютерах, серверах или кластере серверов. Локальные ресурсы, которые называют «узлами тумана», фильтруют полученные данные и обрабатывают их локально либо пересылают в облако для дальнейших вычислений.  
  
Облака поддерживают разные протоколы связи, среди которых чаще всего встречаются AMQP и REST HTTP. Так как HTTP общеизвестен и заточен под интернет, может возникнуть вопрос: «а не использовать ли его для работы с IoT и туманом?». Однако у данного протокола есть проблемы с производительностью. Об этом позже.  
  
В целом, существует 2 модели протоколов связи, подходящих под нужную нам систему. Это запрос-ответ и публикация-подписка. Первая модель известна шире, особенно в архитектуре сервер-клиент. Клиент запрашивает информацию с сервера, а тот получает запрос, обрабатывает его и возвращает ответное сообщение. По этой модели работают протоколы REST HTTP и CoAP.  
  
Вторая модель возникла из-за необходимости обеспечить асинхронную, распределённую, слабую связь между источниками, генерирующими данные, и получателями этих данных.  
  
  
  
Модель предполагает трёх участников: издатель (источник данных), брокер (диспетчер) и подписчик (получатель). Здесь клиент, выступающий в роли подписчика, не должен запрашивать информацию с сервера. Вместо отправки запросов он подписывается на определённые события в системе через брокера, ответственного за фильтрацию всех входящих сообщений и их маршрутизацию между издателями и подписчиками. А издатель, когда происходит событие, касающееся определённой темы, публикует его брокеру, который отправляет подписчику данные по запрошенной теме.  
  
По сути, эта архитектура основана на событиях. И такая модель взаимодействия интересна для приложений в IoT, облаке, тумане из-а её способности обеспечивать масштабируемость и упрощать взаимосвязь между различными устройствами, поддерживать динамическую связь «многие ко многим» и асинхронную связь. Среди наиболее известных стандартизированных протоколов обмена сообщениями, использующих модель «публикация-подписка», можно назвать MQTT, AMQP и DDS.  
  
Очевидно, что у модели «публикация-подписка» есть масса преимуществ:

* Издателям и подписчикам не нужно знать о существовании друг друга;
* Один подписчик может получить информацию от множества разных изданий, а один издатель может отправлять данные множеству разных подписчиков (принцип «многие ко многим»);
* Издатель и подписчик не обязаны быть активными одновременно для обмена данными, потому что брокер (работающий в качестве системы очередей) сможет хранить сообщение для клиентов, которые в данный момент не подключены к сети.

Однако и у модели «запрос-ответ» есть свои сильные стороны. В тех случаях, когда возможности серверной стороны для обработки запросов нескольких клиентов не являются проблемой, имеет смысл использовать уже проверенные надёжные решения.  
  
Также есть протоколы, которые поддерживают обе модели. Например, XMPP и HTTP 2.0, поддерживающие опцию «server push». IETF также выпустил CoAP. В попытке решить проблему обмена сообщениями было создано несколько других решений, таких как протокол WebSockets или использование протокола HTTP через QUIC (Quick UDP Internet Connections).  
  
В случае с WebSockets, хотя он и используется для передачи данных в режиме реального времени с сервера на веб-клиент и обеспечивает постоянные соединения с одновременной двунаправленной связью, он не предназначен для устройств с ограниченными вычислительными ресурсами. QUIC тоже заслуживает внимания, поскольку новый транспортный протокол даёт массу новых возможностей. Но так как QUIC ещё не стандартизирован, преждевременно прогнозировать его возможное применение и влияние на решения в сфере IoT. Так что WebSockets и QUIC мы оставляем в памяти с прицелом на будущее, но подробнее изучать пока не будем.

Время отклика

Одной из важнейших характеристик протоколов связи, особенно применительно к интернету вещей, является время отклика. Но среди существующих протоколов нет безусловного победителя, демонстрирующего минимальный уровень задержки при работе в разных условиях. Зато есть целая куча исследований и сравнений возможностей протоколов.

Например, результаты сравнения эффективности HTTP и MQTT при работе с IoT показали что время отклика для запросов у MQTT меньше, чем у HTTP. А при изучении времени приёма-передачи (RTT) MQTT и CoAP выяснилось, что средний RTT CoAP на 20% меньше, чем у MQTT.

Другой эксперимент с RTT у протоколов MQTT и CoAP проводился в двух сценариях: локальной сети и сети IoT. Оказалось, что средний RTT в 2-3 раза выше в сети IoT. MQTT с QoS0 показал более низкий результат в сравнении с CoAP, а MQTT с QoS1 продемонстрировал более высокий RTT благодаря ACK на прикладном и транспортном уровнях. Для разных уровней QoS задержки в сети без перегрузки у MQTT составили миллисекунды, а для CoAP — сотни микросекунд. Однако стоит помнить, что при работе в менее надёжных сетях MQTT, работающий поверх TCP, покажет совершенной другой результат.

Сравнение времени отклика у протоколов AMQP и MQTT путём увеличения полезной нагрузки показало, что при небольшой нагрузке уровень задержки почти одинаков. Но при передаче больших объёмов данных MQTT демонстрирует меньшее время отклика. Ещё в одном исследовании CoAP сравнили с HTTP в сценарии межмашинной связи с устройствами, развернутыми поверх транспортных средств и оснащенными датчиками газа, датчиками погоды, местоположением (GPS) и интерфейсом мобильной сети (GPRS). Время, необходимое для передачи сообщения CoAP через мобильную сеть, было почти в три раза короче, чем время, необходимое для использования сообщений HTTP.

Проводились исследования, в которых сравнивались не два, а три протокола. Например, сравнение производительности IoT-протоколов MQTT, DDS и CoAP в сценарии медицинского применения с использованием сетевого эмулятора. DDS превзошел MQTT с точки зрения испытанной задержки телеметрии в различных плохих условиях сети. CoAP на основе UDP работал хорошо для приложений, которым требовался быстрый отклик, однако из-за того, что он основан на UDP, произошла значительная непредсказуемая потеря пакетов.

Пропускная способность

Сравнение MQTT и CoAP с точки зрения эффективности использования пропускного канала проводилось как подсчёт общего количества данных, передаваемых за одно сообщение. CoAP показал меньшую пропускную способность, чем MQTT при передаче небольших сообщений. Но при сравнении эффективности протоколов с точки зрения соотношения количества полезных информационных байтов к общему количеству переданных байтов CoAP оказался эффективнее.

При анализе использования пропускного канала MQTT, DDS (с TCP в качестве транспортного протокола) и CoAP выяснилось, что CoAP, как правило, показывал сравнительно более низкое потребление полосы пропускания, которое не увеличивалось при увеличении потерь сетевых пакетов или увеличенной задержки сети, в отличие от MQTT и DDS, где в упомянутых сценариях наблюдался рост использования пропускной способности канала. В другом сценарии было задействовано большое количество устройств, передающих данные одновременно, что является типичным случаем в средах IoT. Результаты показали, что для более высокой загрузки лучше использовать CoAP.

При небольшой нагрузке CoAP использовал наименьшую пропускную способность, за ним следовали MQTT и REST HTTP. Однако, когда размер полезных нагрузок увеличился, наилучшие результаты были у REST HTTP.

Энергопотребление

Вопрос энергопотребления всегда имеет большое значение, а в системе IoT — особенно. Если сравнивать потребление электроэнергии у MQTT и HTTP, то HTTP «сжирает» намного больше. А CoAP более энергоэффективен по сравнению с MQTT, позволяя управлять питанием. При этом в простых сценариях MQTT больше подходит для обмена информацией в сетях интернета вещей, особенно если нет ограничений по мощности.

Другой эксперимент, в ходе которого сравнили возможности AMQP и MQTT на испытательном стенде мобильной или нестабильной беспроводной сети, показало, что AMQP предлагает больше возможностей в плане безопасности, тогда как MQTT является более энергоэффективным.

Безопасность

Безопасность — это ещё один важнейший вопрос, поднимаемый при изучении темы интернета вещей и туманных/облачных вычислений. Механизм безопасности обычно основан на TLS в HTTP, MQTT, AMQP и XMPP, на или DTLS в CoAP, а также поддерживающим оба варианта DDS.

TLS и DTLS начинаются с процесса установления связи между клиентской и серверной сторонами для обмена поддерживаемыми комплектами шифров и ключами. Обе стороны согласовывают комплекты, чтобы гарантировать, что дальнейшая связь происходит в безопасном канале. Разница между ними заключается в небольших модификациях, которые позволяют DTLS на основе UDP работать по ненадёжному соединению.

При тестовых атаках на несколько разных реализаций TLS и DTLS выяснилось, что TLS лучше справился с задачей. Атаки на DTLS были успешнее из-за его терпимости к ошибкам.

Впрочем, самая большая проблема этих протоколов заключается в том, что они изначально не были предназначены для использования в IoT и не предполагали работу в тумане или облаке. Через согласованный обмен (handshaking) они добавляют дополнительный трафик с каждым установлением соединения, что истощает вычислительные ресурсы. В среднем наблюдается увеличение на 6,5% для TLS и 11% для DTLS в служебной нагрузке по сравнению со связью без уровня безопасности. В богатых ресурсами средах, которые обычно расположены на облачном уровне, это не будет проблемой, но в связи между IoT и уровнем тумана это становится важным ограничением.

Что же выбрать? Однозначного ответа нет. MQTT и HTTP кажутся наиболее перспективными протоколами, так как считаются сравнительно более зрелыми и более стабильными решениями для IoT в сравнении с другими протоколами.

Fog Computing – новая ступень развития облачных вычислений, которая снижает задержки, возникающие при передаче данных в центральное облако и обеспечивает новые возможности создания интеллектуальных устройств интернета вещей.

Преимуществом туманных вычислений является снижение объема данных, передаваемых в облако, что уменьшает требования к пропускной способности сети, увеличивает скорость обработки данных и снижает

задержки в принятии решений. Туманные вычисления решают ряд самых распространенных проблем, среди которых:

высокая задержка в сети;

трудности, связанные с подвижностью оконечных точек;

потеря связи;

высокая стоимость полосы пропускания;

непредвиденные сетевые заторы;

большая географическая распределенность систем и клиентов.

Глобальный рынок Fog-систем оценивается в $18 млрд к 2022 году.

Самый большой потенциал развития технологии Fog computing имеют в следующих отраслях: энергетика, коммунальные службы, и транспорт, сельское хозяйство, торговля, а также здравоохранение и промышленное производство.

Энергетический сектор и коммунальные службы представляют собой наибольший рынок для систем Fog computing, с потенциалом роста до $3,84 млрд к 2022 году.

Сектор транспорта – второй по значимости потенциальный рынок для Fog computing с потенциалом роста до $3,29 млрд к 2022 году

Отрасль медицины представляет третий по величине рынок Fog computing, объём которого оценивается в $2,74 млрд к 2022 году.

Развитие в России

2016: Кремль поручил подготовить инфраструктуру туманных вычислений

1 июля 2016 года стало известно о том, что Кремль поручил Минкомсвязи, Минпромторгу, а также другим ведомствам подготовить инфраструктуру туманных вычислений.

По данным «Коммерсанта», администрация президента направила в Минкомсвязи, Минпромторг, «Ростелеком» и Агентство стратегических инициатив (АСИ) письмо с подписью президента Владимира Путина на тему развития туманных вычислений в России.

Другой источник в одном из профильных министерств в разговоре с газетой уточнил, что результаты выполнения поручения нужно представить в октябре 2016 года. Отмечается, что инициатива по работе в данной сфере исходит от «Ростелекома» и АСИ, чью идею поддержали в администрации президента.

«Коммерсантъ» сообщает, что Минпромторг обратился к нескольким российским технологическим компаниям с просьбой предоставить экспертизу проекта. В частности, соответствующую просьбу министерство направило компании «Т-Платформы», которая занимается разработкой вычислительной техники.