DOI 10.37882/2223-2966.2023.08.30

РАЗЛИЧНЫЕ АСПЕКТЫ ОПТИМИЗАЦИИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ

Смольянников Илья Викторович
главный специалист — научный сотрудник,
ФГАНУ «Центр информационных технологий и систем органов исполнительной власти имени А.В. Старовойтова»
ilyasm211@gmail.com

Аннотация. Благодаря достижениям в современных технологиях Интернет стал использоваться для обмена данными между достаточно небольшими устройствами с ограниченными ресурсами. Их количество уже достигает миллиардов, что создает Интернет вещей в нынешнем его понимании, но отсюда и появляется проблема по оптимизации сетей из-за большого объема трафика, который генерируют эти устройства.
Цель статьи заключена в структуризации и описании проблем и вопросов по оптимизации сети Интернета вещей.
В статье приведены основные проблемы, которые необходимо решить при оптимизации сети передачи данных Интернета вещей, таких как, перегрузки, маршрутизация, энергосбережение, надежность, безопасность. Обсуждается оптимизация сети в Интернете вещей и классификация алгоритмов. На основе последних научных работ обсуждаются современные методы оптимизации сети. В заключении статьи приводится список будущих задач, которые необходимо решить для оптимизации сети Интернета вещей.

Ключевые слова: оптимизация сети; качество обслуживания; Интернет вещей; энергосбережение; надежность; безопасность.

VARIOUS ASPECTS OF OPTIMIZING THE INTERNET OF THINGS NETWORK

I. Smolyannikov

Summary. Thanks to advances in modern technology, the Internet has become used to exchange data between fairly small devices with limited resources. Their number already reaches billions, which creates the Internet of Things in its current sense, but from here comes the problem of optimizing networks due to the large amount of traffic that these devices generate.
The purpose of the article is to structure and describe the problems and issues of optimizing the Internet of Things network.
The article presents the main problems that need to be solved when optimizing the Internet of Things data transmission network, such as congestion, routing, energy saving, reliability, security. The optimization of the network in the Internet of things and the classification of algorithms are discussed. Modern methods of network optimization are discussed on the basis of recent scientific works. The article concludes with a list of future challenges that need to be addressed to optimize the IoT network.

Keywords: network optimization; quality of service; Internet of things; energy saving; reliability; safety.

Введение

С развитием коммуникационных линий, сетей передачи данных и распределенных вычислений в мире появилась новая ветвь сети, которая называется Интернет вещей. В связи с чем стало появляться все больше и больше устройств, которые одновременно подключены к сети интернет. Их количество уже исчисляется миллиардами. Каждое из таких устройств подключается в сети через свою собственную технологию, будь то сотовая связь или подключение типа машина-машина, используя различные варианты беспроводных технологий. Все это создает определенный набор характеристик, от которых зависит надежность связи в сети Интернета вещей. Сама сеть в себя включает совокупность используемой архитектуры, протоколов, различных предоставляемых услуг, компонентов безопасности. В настоящее время основная тенденция Интернета вещей рассматривается как Интернет будущего, в котором миллиарды взаимосвязанных вещей и устройств используют современные технологии, расширяя при этом возможности в оказании услуг [7].

В Интернете вещей трафик должен управляться децентрализовано относительно приложения, например, как система управления движением, где отдельные узлы обмениваются информацией о своем трафике, что помогает планировать трафик на основе скорости данных из каждого источника, чтобы избежать заторов трафика [1].

Одной из сфер применения устройств Интернета вещей является использование датчиков в системах жизнеобеспечения или предотвращения катастроф, например, при пожаре. В таких системах сеть должна быть наиболее надежной, чтобы обеспечить полноту всех передаваемых данных, но при этом не создавать повышенную нагрузку на другие компоненты. Поэтому там может применяться стратегия с несколькими маршрутизаторами, для обеспечения энергоэффективности, потому что некоторые узлы будут находиться в спящем режиме и наиболее ближайший узел будет брать на себя роль активного узла, для сбора информации и доставки данных каких-либо задержек и ущерба энергоэффективности [3].

Долговечность функционирования сеть может быть изменена путем выбора наиболее оптимального пути среди множества доступных, если использовать для этого модель линейного программирования. Вышеупомянутые факторы затрудняют эффективное использование и управление ресурсами спектра для приложений Интернета вещей, поскольку Интернет вещей рассматрива-

ется как часть будущего Интернета, охватывающего все виды доменов и промышленных приложений. Если эти сетевые проблемы не будут решены, то нехватка ресурсов станет препятствием для дальнейшего развития Интернета вещей. В отличие от этого, высокий приоритет следует уделять оптимизации использования сетевых ресурсов миллиардами новых беспроводных устройств, подключаемых к Интернету в будущем, чтобы способствовать эффективному использованию сети.

В статье будут рассмотрены несколько возможностей улучшения стабильности сетей Интернета вещей:

— различные типы алгоритмов с целью оптимизации сети в Интернета вещей.
— недавних исследовательские работы наряду с новыми подходами, опубликованными в области различных параметров сети, таких как маршрутизация сети, энергосбережение, контроль перегруженности, неоднородность, масштабируемость сети, надежность, качество обслуживания и безопасность сети.

Оптимизация сети и интернет вещей

Как правило, оптимизация сети определяется как технология, используемая для повышения производительности сети для любой среды. Это играет важную роль в Интернете вещей, поскольку с каждым днем в сеть поступает большое количество данных от различных устройств и приложений [10]. Оптимизация сети предлагает различные преимущества, такие как более быстрая скорость передачи данных, восстановление данных, устранение избыточных данных и увеличение времени отклика приложения и сети.

Проблема оптимизации сети в Интернете вещей привлекает все большее внимание, так как ожидается, что количество новых устройств с течением времени будет постоянно расти. Из чего можно сделать вывод, что необходимо найти максимально эффективное решение для оптимизации, чтобы уменьшить будущий всплеск объемов трафика, который так или иначе будет влиять на оказание других услуг, не связанных с Интернетом вещей. Ведь трафик, генерируемый устройствами Интернета вещей от устройства к устройству и всегда неоднороден. Кроме того, необходимо регулировать трафик Интернета вещей, чтобы контролировать работу устройств Интернета вещей и его сервисов. Приложение Интернета вещей генерирует меньше данных, однако интеграция устройств в приложение генерирует больший объем трафика из-за управляющих сообщений. Следовательно, этот трафик, не связанный с приложениями, создает значительную дополнительную нагрузку на сеть. Таким образом, чтобы преодолеть эту нагрузку, требуется эффективный механизм для адресации и оптимизации обмена сообщениями от устройств Интернета вещей.

Классификация алгоритмов

Обычно задача оптимизации состоит из входных факторов, выходных данных, ограничений и различных целевых функций. Задача оптимизации сети в IoT включает в себя множество компонентов, которые будут объединены с использованием различных комбинаций и методов, направленных на решение конкретной сетевой задачи. В целом, можно выделить два важных метода оптимизации:

— Применение известной системы оптимизации для решения проблемы (готового фреймворка).
— Разработка новой работы, основанной на эвристическом методе решения задачи.

Вышеописанные подходы совсем не взаимоисключают друг друга. Иногда целесообразнее их комбинировать, особенно если рассматриваемая проблема сложном сложная или, уже известные подходы не дают ощутимого результата. Эвристический подход состоит из алгоритма, который обеспечивает более быстрое аппроксимационное решение для более сложной задачи и жадного подхода, который обеспечивает оптимальное решение, путем принятия допущений. Оба этих подхода обеспечивают оптимальное решение сложных задач и оба обеспечивают производительность, близкую к оптимальной.

Все эти алгоритмы можно разбить на следующие виды:

— Алгоритмы, основанные на методе роя частиц (PSO) [8];
— Генетические алгоритмы (GA);
— Генетический алгоритм сортировки без доминирования II (NSGA-II);
— Алгоритмы, основанные на нечеткой логике;
— Стохастические алгоритмы;
— Эвристические алгоритмы;
— Эволюционные алгоритмы (EA);
— Меметические алгоритмы (MA).

В дополнение к вышеприведенным алгоритмам существует множество других, которые помогают оптимизировать сеть Интернета вещей. Рассмотрим несколько таких алгоритмов, описанных в научных статьях:

В одной из своих работ [5], авторы предложили Байесовский подход к сетевой модели для идентификации вторжений в сети Интернета вещей. Эта модель обладает большими возможностями динамической идентификации основных узлов для обеспечения лучшей функции безопасности, которая может быть достигнута с использованием исторических данных.

Авторы статьи «Исследование по применению иерархической кластеризованной системы на основе тех-

нологии маршрутизации с использованием алгоритмов искусственного интеллекта для обеспечения качества обслуживания маршрутизации на основе сервиса» [4] предложили алгоритм на основе искусственного интеллекта для формирования вычислительных кластеров, выбора оптимального маршрута и выполнения многолучевой маршрутизации для достижения лучшего качества обслуживания.

Современные решения оптимизации сетей

Для оптимальной работы сетей IoT было предложено множество схем оптимизации сети.

На сегодняшний день Интернет потребляет 5 % производимой энергии, с учетом этих прогнозов необходимо, чтобы устройства IoT были энергоэффективными для обеспечения надежной связи. Для решения этих проблем приведем некоторую информацию о масштабах и ограничениях различных работ, связанных с множеством параметров, такими как маршрутизация сетей, энергосбережение, перегруженность, неоднородность, масштабируемость, надежность, качество обслуживания (QoS) и безопасность.

Маршрутизация

Маршрутизация — это процесс выбора пути для отправки данных по одной или нескольким сетям. Эти данные генерируются M2M или машиной для связи с объектами. Эти генерируемые данные должны быть перенаправлены, чтобы выбрать кратчайший путь или оптимальный путь для достижения цели. Процесс хранения информации о маршрутах доставки данных подразделяется на три типа:

1. Реактивный: этот протокол создает маршруты только тогда, когда источник хочет отправить данные в пункт назначения, следовательно, он также известен как протокол маршрутизации по требованию.
2. Упреждающий: этот протокол поддерживает таблицу маршрутизации, которая периодически обновляется на основе свежего списка назначений, поэтому он известен как протокол, управляемый таблицей.
3. Гибридный — Этот протокол представляет собой комбинацию как реактивных, так и проактивных протоколов маршрутизации.

Для доставки данных от источника к месту назначения используются различные методы, в качестве примера можно рассмотреть облегченный алгоритм пересылки для упорядочивания многоадресной рассылки в сетях с низкой мощностью (LLN) для обнаружения сервиса в интеллектуальных объектах. Этот протокол использует метод локального заполнения для устройств с рабочим циклом, использующих сети низкой мощности с протоколом маршрутизации для таких сетей (RPL), что помогает устройствам с ограниченной памятью использовать многоадресную рассылку [11]. Этот метод позволяет избежать прямых зацикливаний с помощью фильтров Блума для идентификации повторяющихся пакетов и предотвращения зацикливаний.

В качестве другого примера можно привести улучшенную схему многолучевой маршрутизации для сетей без четкой структуры (AOMDV) [6]. Такая схема динамически выбирает стабильный маршрут в сети Интернет при помощи регулярного обновления таблиц, относящихся к Интернет соединению. Этот протокол требует два дополнительных пакета с информацией о маршруте, но при этом снижает задержку получения информации между конечными узлами, потерю пакетов и частоту обнаружения.

Энергосбережение

Для продления срока службы сети, в приложениях Интернета вещей важную роль играют методы и механизмы энергосбережения, и режим ожидания. Рассмотрим несколько коммуникационных стандартов, которые позволяют достигнуть эту цель:

1. IEEE 802.11ah — это протокол беспроводной сети, более предназначенный для экономии энергии чем стандарт IEEE 802.11. Работает в диапазоне в два аза больше, чем у предшественника, использую безлицензионный канал 900МГц. Для экономии энергии имеет две станции, а именно станции TIM и станции не-TIM. Станции TIM периодически получают информацию о буферизованном трафике для них от точки доступа в так называемом информационном элементе TIM, отсюда и название. Станции не-TIM используют новый механизм целевое время пробуждения (TWT), который позволяет снизить накладные расходы на связь. Целевое время пробуждения — это функция, позволяющая точке доступа определять конкретное время и набор временных интервалов для осуществления доступа к среде. Таким образом, целевое время пробуждения снижает энергопотребление сети, а рассмотренный стандарт использует небольшие сигналы вместо подтверждения, чтобы сохранить энергию.
2. ZigBee — это беспроводной протокол, определяемый уровнем 3 и выше стандарта IEEE 802.15.4. Существует два типа узлов в сети ZigBee: Полнофункциональное устройство (FFD), которое выступает в роли координатора, а также как общий узел, и другой — устройства с уменьшенной функциональностью (RFD), который действует только как общий узел. Существует технология синхронизированного перехода в спящий режим

(SST) для облегчения перехода в спящий режим всех узлов сети ZigBee, включая полнофункциональные устройства (FFD). Во многих приложениях маршрутизация требуется в течение очень ограниченного промежутка времени. Благодаря этому, SST позволяет множеству устройств переходить в спящий режим в периоды простоя сети, тем самым экономя энергию устройств. Кроме того, существует множество методов, которые позволяют узлам переходить в спящий режим, когда нет события для экономии энергии.

3. Bluetooth с низким энергопотреблением (BLE): BLE также известен как Bluetooth Smart, который работает в операционной системе почти всех мобильных телефонов, настольных компьютеров и ноутбуков. BLE требует в десять раз меньше мощности, чем у стандартного Bluetooth, потому что BLE использует архитектуру главный/подчиненный, в которой главный компонент определяет время бодрствования подчиненного, чтобы он мог войти в сон после того, как он отправил всю информацию главному узлу. Таким образом, это преимущество делает BLE идеальным для приложений Интернета вещей, так как это даже с очень маленькой батареей.
4. LoRaWAN — данный протокол предназначен для устройств, работающих от аккумулятора, что делает его идеальным для применения в приложениях Интернета вещей [2]. Он поддерживает двунаправленную связь, мобильность, безопасность и т.д., которые так требуются в Интернете вещей, но еще что более важно он является энергоэффективным протоколом. Протокол также поддерживает большое количество устройств, что решает проблему масштабируемости и упрощает получение энергии, необходимую для устройств Интернета вещей.

Благодаря всем вышеупомянутым стандартам связи BLE, ZigBee и IEEE 802.11ah широко используются в большинстве приложений Интернета вещей, а LoRaWAN является новым стандартом для связи в сетях Интернета вещей.

Контроль перегрузки

По оценкам технических экспертов к 2024 году может насчитываться около 30 миллиардов устройств, подключенных к Интернету. В результате огромного количества устройств может возникнуть риск перегрузки сети. Поэтому для решения этой проблемы требуется эффективный механизм контроля перегрузки. Перегруженность в Интернете вещей является результатом сочетания различных типов устройств и сервисов, которые постоянно передают свои данные в неоднородной форме.

Благодаря использованию встроенных технологий в Интернет вещей, это приводит к широкому внедрению устройств малого размера и с меньшим количеством памяти, например, датчики и исполнительные механизмы, в приложениях реального времени. С увеличением числа таких устройств объем производимых данных и потребность в сети также неограниченно растут. Из чего можно сделать вывод, что обработка данных от таких устройств и обеспечение эффективной сети для них является одной из самых сложных задач в Интернете вещей.

Надежность

Сетевые технологии, используемая в Интернете вещей по своей сути неуправляема в большинстве приложений, а надежность является наиболее важным параметром качества.

Параметры качества обслуживания (QoS) сети рассматриваются с различных точек зрения и размеров, таких как пропускная способность, задержка, скорость потери пакетов, избежание помех и дрожания [9]. Следовательно, QoS должен определяться по-разному для разных технологий. Очень трудно эффективно обеспечить качество обслуживания в беспроводных сетях из-за разрыва между сегментами управления и распределением ресурсов общих беспроводных устройств.

Также немаловажным фактором является и безопасность. Безопасность является жизненно важным требованием для защиты данных, передаваемых в сети, поэтому она является оптимальным требованием для обеспечения эффективного механизма защиты данных от различных видов нарушений.

Будущие задачи

Развитие Интернета вещей для поддержки коммуникационной инфраструктуры приводит к появлению новых сервисов для различных областей применения, например, домашняя сеть, умный город, бизнес, логистика, медицина и т.д. Но такая эволюция порождает новые проблемы и задачи для управления использования сети. Рассмотрим несколько из таких проблем и задач:

— Сетевая маршрутизация: проблемами будут являться — обеспечение эффективного механизма маршрутизации на канальном уровне, уменьшение накладных расходом на маршрутизацию, выбор наилучшего энергоэффективного алгоритма среди различных типов. Задача — выбрать идеальные энергоэффективные алгоритмы среди различных доступных типов, поскольку разные алгоритмы используют разные методы при выборе главной части кластера и технику при выборе маршрута

— Безопасность: проблемы — обеспечение безопасности данных от большего количества атак из-за разнообразия устройств, раскрытие сети из-за недостатка в технологиях и их реализации, атака на сети по второстепенным каналам. Задачи — попытка взлома системы путем обнаружения слабых мест в физической реализации криптографической системы с помощью электромагнитных утечек, информации о времени, потреблении энергии и многих других факторов приводит к проникновению злоумышленника в систему, поэтому задача разработчика заключается в реализации более надежного алгоритма криптографии. Уязвимость безопасности в сети возникает по двум основным причинам, таким как уязвимости в нерассмотренные угрозы во время всей настройки сети Интернета вещей и недостатки при внедрении и моделировании технологий и протоколов. Таким образом, задача состоит в том, чтобы обеспечить механизм безопасности в этой ситуации.

Интернет сильно изменил привычный образ жизни. Он перевел взаимодействие между людьми на новый уровень. Интернет вещей обладает потенциалом привнести новое измерение в этот процесс, позволяя осуществлять связь с различными устройствами. Но с его развитием увеличивается количество объектов, из которых он состоит, поэтому на передний план выходит больше проблем по оптимизации сети. В статье рассмотрены несколько аспектов, при помощи которых можно в той или иной степени проводить оптимизацию сети Интернета вещей. Рассмотрены основные параметры сети Интернета вещей, такие как маршрутизация, перегрузки, надежность, энергосбережение. В качестве примеров были приведены результаты последних исследовательских статей. В конечном итоге были определены будущие задачи и вопросы дальнейшей оптимизации сети Интернета вещей, что может помочь приступить к будущим работам по оптимизации.

ЛИТЕРАТУРА

1. Accettura N. et al. Decentralized traffic aware scheduling for multi-hop low power lossy networks in the internet of things // 2013 IEEE 14th International Symposium on «A World of Wireless, Mobile and Multimedia Networks»(WoWMoM). — IEEE, 2013. — С. 1–6.
2. Haxhibeqiri J. et al. A survey of LoRaWAN for IoT: From technology to application // Sensors. — 2018. — Т. 18. — №. 11. — С. 3995.
3. Liu Y. et al. FFSC: an energy efficiency communications approach for delay minimizing in internet of things // IEEE Access. — 2016. — Т. 4. — С. 3775–3793.
4. Long N.T., Thuy N.D., Hoang P.H. Research on applying hierachical clustered based routing technique using artificial intelligence algorithms for quality of service of service based routing // Internet Things Cloud Comput. — 2015. — Т. 3. — №. 6–1. — С. 1–8.
5. Sun F., Wu C., Sheng D. Bayesian Networks for Intrusion Dependency Analysis in Water Controlling Systems //Journal of Information Science & Engineering. — 2017. — Т. 33. — №. 4.
6. Zhou J. et al. Ad hoc on-demand multipath distance vector routing protocol based on node state // Communications and Network. — 2013. — Т. 5. — №. 03. — С. 408–413.
7. Бидельманова С.Р. ИНТЕРНЕТ ВЕЩЕЙ: ПЕРСПЕКТИВЫ СОЗДАНИЯ УМНОЙ СРЕДЫ В БЛИЖАЙШЕМ БУДУЩЕМ // Advances in Science and Technology. — 2018. — С. 77–82.
8. Казакова Е.М. Краткий обзор методов оптимизации на основе роя частиц //Вестник КРАУНЦ. Физико-математические науки. — 2022. — Т. 39. — № 2. — С. 150–174.
9. Лушпа И.В. Оценка надежности в концепции Интернета вещей //Новые информационные технологии в автоматизированных системах. — 2016. — № 19. — С. 216–218.
10. Цветков В.Я. Интернет вещей как глобальная инфраструктура для информационного общества // Современные технологии управления. — 2017. — № 6 (78). — С. 3.
11. ЭРИКСОН Г.М., БОРОСС К.А. ЭФФЕКТИВНЫЙ СЕТЕВОЙ УРОВЕНЬ ДЛЯ ПРОТОКОЛА IPv6. — 2019.

Журнал «Современная наука: актуальные проблемы теории и практики»