ВЫЗОВЫ И БУДУЩИЕ ТЕНДЕНЦИИ НАДЕЖНОГО ИНТЕРНЕТ ВЕЩЕЙ

Алевтина Александровна Мурадова
ТУИТ имени Мухаммада аль-Хорезми, PhD, доцент кафедры «Телекоммуникационный инжиниринг»
Email: a.muradova1982@inbox.ru

Аннотация: В статье представлены основные вызовы и будущие тенденции надежного Интернет вещей. Представлен обзор будущих приложений Интернета вещей и их основные коммуникационные требования, четыре основные области надежного Интернета вещей, включая показатели распределения ресурсов, управления задержками, безопасности и надежности. Выделены проблемы надежного Интернета вещей, связанные с методами машинного обучения, связью 6G и безопасностью на основе блокчейна.

Ключевые слова: Интернет вещей, распределение ресурсов, задержка, безопасность, метрики, безопасность IoT, IoT-продукты.

Abstract: The article presents the main challenges and future trends of a reliable Internet of Things. An overview of future IoT applications and their key communication requirements is presented, the four main areas of reliable IoT including resource allocation, latency management, security and reliability metrics. Challenges for a secure Internet of Things related to machine learning techniques, 6G communications, and blockchain-based security are highlighted.

Keywords: Internet of things, resource allocation, latency, security, metrics, IoT security, IoT products.

Annotatsiya: Maqolada ishonchli Internet ashyolarning asosiy muammolari va kelajakdagi tendentsiyalari keltirilgan. Kelajakdagi IoT ilovalari va ularning asosiy aloqa talablari haqida umumiy ma'lumot berilgan, ishonchli IoTning to'rtta asosiy yo'nalishi, jumladan, resurslarni taqsimlash, kechikishlarni boshqarish, xavfsizlik va ishonchlilik ko'rsatkichlari. Mashinani o'rganish texnikasi, 6G aloqasi va blokcheynga asoslangan xavfsizlik bilan bog'liq xavfsiz narsalar Interneti uchun muammolar ta'kidlangan.

Kalit so'zlar: Internet ashyolari, resurslarni taqsimlash, kechikish, xavfsizlik, ko'rsatkichlar, IoT xavfsizligi, IoT mahsulotlari.

ВВЕДЕНИЕ

Интернет вещей (IoT) является жизненно важным компонентом многих отраслей будущего. Благодаря интеллектуальной интеграции датчиков, беспроводной связи, вычислительных технологий и анализа данных Интернет вещей может повысить производительность и эффективность отраслей. Надежность передачи данных является ключом к реализации ряда приложений, предлагаемых Интернетом вещей. Интернет вещей позволяет использовать множество важных приложений, включая интеллектуальное управление дорожным движением, безопасное автономное вождение, экономию электроэнергии с помощью интеллектуальных сетей, удаленный мониторинг пациентов, мониторинг состояния машин, интеллектуальную промышленную автоматизацию и решения для безопасности умного дома. В эпоху Индустрии 4.0 и связи 6G приложения Интернета вещей произведут революцию в работе различных отраслей. Тремя основными компонентами Интернета вещей будут зондирование, связь и анализ данных [1,2].

ЛИТЕРАТУРА И МЕТОДОЛОГИЯ

Успешная работа приложений Интернета вещей зависит от надежной передачи данных между датчиками и серверами. Под надежностью

подразумевается надежная связь с высокой скоростью доставки пакетов, низкой задержкой и защитой от сетевых атак. Каждое приложение IoT может иметь разные требования к качеству обслуживания (QoS). Для реализации надежной и устойчивой сети Интернета вещей необходимо соблюдение требований QoS. Эффективная передача данных является ключевой задачей для обеспечения надежности приложений Интернета вещей. Это означает, что данные передаются с высокой скоростью, так что задержка находится в пределах требований QoS. Это возможно, когда оптимизированы такие ресурсы, как использование спектра, доступ к среде, мощность передачи, разгрузка вычислительных задач на туманные узлы и т.д. Более того, необходимы конфиденциальность и секретность общения, а также сохранение целостности данных.

Масштабный Интернет вещей и требования к приложениям

Масштаб массового Интернета вещей составит миллиарды машин, автомобилей и датчиков, подключенных к Интернету. Массовый Интернет вещей будет поддерживать множество новых приложений, таких как автономное вождение, игры на основе дополненной реальности, прогнозное обслуживание машин, автоматизированные хирургические системы и интеллектуальные сети. Что касается требований к связи, массовый Интернет вещей потребует сверхнадежности порядка 99,99999%. Это особенно необходимо для критически важных приложений, где на карту поставлена безопасность человека, таких как безопасное вождение и операции, связанные со здоровьем. Более того, эти массивные сети Интернета вещей могут позволить себе задержку менее 1 мс. Это необходимо для того, чтобы данные доставлялись вовремя, чтобы приложения могли принимать правильные решения [3,4].

Основные случаи использования Интернета вещей

Как показано на рисунке 1, четыре важных примера Интернета вещей включают Интернет транспортных средств (IoV), Интернет медицинских вещей

(IoMT), Промышленный Интернет вещей (IIoT) и Интернет интеллектуальных сетей (IoSG).

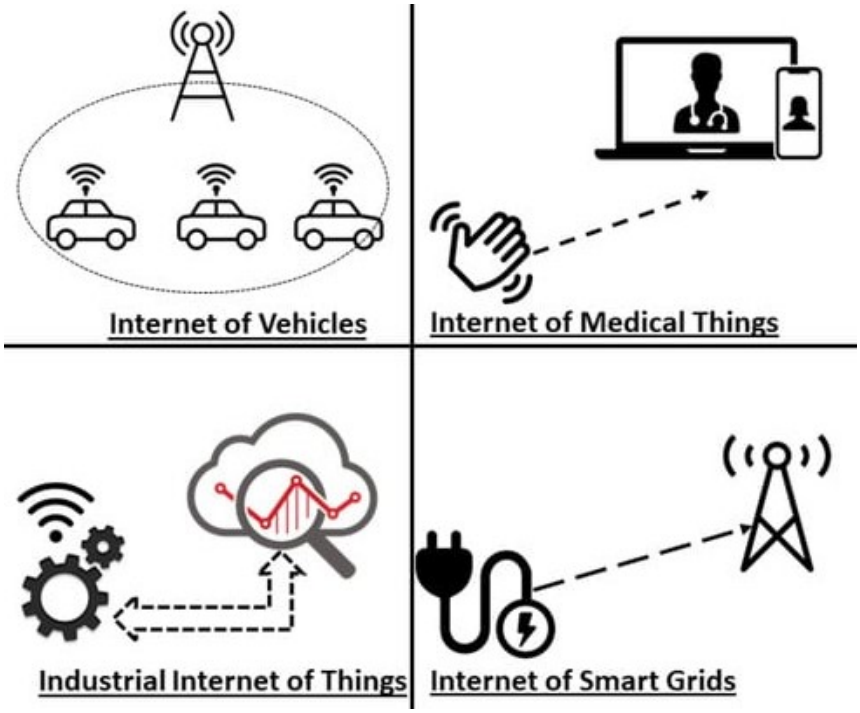

Рис.1. Проблемы надежной передачи данных в IoT

Интернет транспортных средств (IoV) является основным применением Интернета вещей в транспортной отрасли. В IoV используются транспортные средства, оснащенные беспроводными приемопередатчиками и инфраструктурными придорожными устройствами (RSU), расположенными в разных местах дороги. Эти приемопередатчики обеспечивают связь между транспортными средствами в пределах района, тем самым позволяя транспортным средствам иметь пространственную карту движения. Транспортные средства также могут обмениваться информацией о мобильности и дорожном движении с RSU, тем самым расширяя диапазон связи.

Интернет медицинских вещей (IoMT) является жизненно важным фактором для будущей индустрии здравоохранения. IoMT может предоставлять такие приложения, как удаленный мониторинг пациентов, автоматический мониторинг пациентов, находящихся в неотложной помощи, контроль цепочки медицинских поставок и отслеживание контактов в пандемических ситуациях.

Промышленный Интернет вещей (IIoT) - это новый вариант использования Интернета вещей. Подключив машины к Интернету, можно регулярно контролировать их состояние и планировать ремонт, тем самым сокращая простои. Более того, многие производственные процессы можно автоматизировать и разумно контролировать для повышения производительности. На основе полученных данных IIoT может обеспечить прогнозное обслуживание [5].

Интернет интеллектуальных сетей (IoSG) улучшает использование и распределение электроэнергии за счет подключения домашних устройств к сети. Интеллектуальные счетчики также могут быть размещены в домах, которые передают информацию об использовании электроэнергии в сеть. IoSG может сократить потребление электроэнергии, тем самым облегчая работу клиентов, а также уменьшая выбросы углекислого газа и сохраняя ресурсы электроэнергии.

Обзор надежной передачи данных в сети IoT

Представляем три основных компонента надежного распространения данных Интернета вещей. К ним относятся распределение ресурсов, управление задержкой и безопасность. Эффективное распределение ресурсов важно для надежного обмена данными между узлами и серверами Интернета вещей. Поскольку ресурс спектра ограничен из-за больших объемов данных, генерируемых узлами Интернета вещей, важно предложить методы интеллектуального использования спектра. Такие методы, как когнитивное управление спектром, можно использовать для совместного использования полос спектра несколькими узлами Интернета вещей [6].

Туманные вычисления - жизненно важная часть будущих сетей Интернета вещей. Туманные узлы, расположенные рядом с устройствами Интернета вещей, обеспечивают хранилище и вычислительную мощность сети Интернета вещей. Сети Интернета вещей могут размещать популярный и наиболее

полезный контент в кэш-хранилище этих туманных узлов. Следовательно, распределение кэш-памяти является важной задачей.

Управление задержкой - еще один важный элемент надежной передачи данных в IoT. Приложения Интернета вещей могут работать некорректно, если обмен данными не осуществляется с желаемой задержкой. Многие новые приложения, такие как автономное вождение и промышленная автоматизация, предъявляют строгие требования к задержке, и, следовательно, необходимо управление задержкой.

Точное прогнозирование трафика данных может поддерживать методы управления задержкой, поскольку знание предстоящего трафика на сервере IoT, а туманный узел позволяет лучше его обрабатывать. Следовательно, методы, основанные на искусственном интеллекте (ИИ), которые прогнозируют частоту и размер данных, могут быть очень полезными. Кроме того, другие сетевые технологии могут поддерживать сети IoT для быстрой передачи данных.

Безопасность является важным компонентом надежной передачи данных в IoT. В сети Интернета вещей может быть произведено несколько атак, которые могут поставить под угрозу конфиденциальность передаваемых данных. Более того, злонамеренные узлы могут вставлять в сеть поддельные и неверные данные, что может повлиять на принятие решений приложениями IoT. Для решения этой проблемы необходимы передовые криптографические методы, которые могут обеспечить безопасность передаваемых данных, сводя при этом необходимые накладные расходы к минимуму [7].

Блокчейн - это новая технология, которая может обеспечить надежную безопасность устройств Интернета вещей. Другие методы безопасности, такие как безопасность физического уровня, также могут повысить надежность сетей IoT. Эти методы могут работать в сочетании с криптографическими методами, обеспечивая надежное решение. Наконец, для обеспечения получения правильных данных также необходимы атаки на целостность данных и схемы обнаружения аномалий, на основании которых можно принимать решения.

К четырем ключевым аспектам надежной передачи данных в IoT относятся: методы распределения ресурсов, алгоритмы управления задержкой, решения по безопасности и показатели надежности для Интернета вещей на базе 6G.

Распределение ресурсов - важная область исследований приложений Интернета вещей. Поскольку устройства Интернета вещей ограничены в энергопотреблении, вычислениях и передаче, необходимы интеллектуальные и новые методы распределения ресурсов. Такие ресурсы, как спектр, мощность передачи узлов Интернета вещей, кэш-память туманных узлов с поддержкой Интернета вещей, вычислительная мощность узлов Интернета вещей и туманных узлов, а также скорость передачи данных, должны быть тщательно распределены. Задержка - важный показатель качества обслуживания для приложений Интернета вещей. Большинство приложений чувствительны к задержке и требуют более низкого значения задержки в пределах порогового значения, чтобы обеспечить надежную связь. Для уменьшения задержки Интернета вещей используются такие методы, как интеллектуальная повторная передача, распределение ресурсов, методы множественного доступа и физического уровня, прогнозирование трафика и сотрудничество с другими сетями. Безопасность - важное требование для надежной передачи данных в IoT. Для обеспечения надежности в IoT необходимы методы, обеспечивающие защиту от злоумышленников и их атак. Методы обеспечения безопасности включают методы криптографии, методы на основе блокчейна и методы обнаружения целостности данных.

Метрики надежности для Интернета вещей

Коэффициент доставки пакетов (PDR) - это широко используемый показатель надежности, который измеряет соотношение общего количества пакетов, полученных получателем, и общего количества пакетов, переданных передатчиком. Большинству приложений Интернета вещей требуется очень высокое значение PDR, поскольку оно гарантирует, что данные между узлами

будут передаваться без каких-либо ошибок. При связи 6G используется множество новых технологий и методов, которые повышают PDR до значения 99,9999999,99999%. Низкое значение PDR означает, что условия канала между передатчиком и приемником плохие из-за таких факторов, как многолучевое замирание. Вероятность сбоя является еще одним полезным показателем для распределения ресурсов, поскольку она указывает расстояние, на котором передатчик и приемник выходят за пределы зоны действия. В результате узел может выбрать оптимальную мощность передачи и схему модуляции на основе требований приложения IoT [8].

Еще одним важным показателем надежности для Интернета вещей является коэффициент занятости канала, который указывает на общую нагрузку данных в сети. Этот показатель может быть измерен радиостанцией IoT на основе процента времени, в течение которого радиостанция считает канал свободным.

Время между прибытием пакетов - это еще один показатель, который вычисляет разницу во времени между двумя последовательными пакетами в получателе. Переменное время между поступлением пакетов может привести к нежелательным задержкам при передаче результатов измерений датчиков на сервер, что снижает точность анализа данных приложения. Сквозная задержка пакета является важнейшим показателем, который предоставляет информацию о том, какая задержка требуется для передачи пакета.

Время проверки подписи - еще один важный показатель, который измеряет, сколько времени требуется для обработки сообщения с точки зрения безопасности получателя. Поскольку за короткое время получателю поступает много пакетов, им, возможно, придется стоять в очереди, прежде чем пройти процесс проверки подписи. Более длительное время проверки подписи означает, что общая сквозная задержка увеличивается.

Представлены будущие возможности и проблемы, связанные с созданием надежных приложений Интернета вещей. Обсуждены три важные

возможности, которые могут повысить надежность будущих приложений Интернета вещей. Эти возможности включают в себя методы машинного обучения, связь 6G и безопасность на основе блокчейна. Поскольку будущие приложения Интернета вещей будут генерировать большие объемы данных, необходимы интеллектуальные методы машинного обучения для анализа данных и получения полезной информации для повышения надежности Интернета вещей.

РЕЗУЛЬТАТЫ

Методы, основанные на регрессии, полезны для прогнозирования многих важных параметров Интернета вещей. Одним из применений регрессии является прогнозирование трафика данных и нагрузки в сети. Точно прогнозируя нагрузку трафика, можно реализовать оптимальное распределение ресурсов. Более того, прогнозирование трафика можно использовать для разработки эффективных методов контроля перегрузок. Еще одним применением прогнозирования трафика является оптимальная балансировка нагрузки для сетей IoT туманных вычислений. Используя прогнозируемую нагрузку (по количеству задач, полученных для вычисления) на разных узлах тумана, задачи можно справедливо распределить по узлам тумана.

Методы обучения с подкреплением также можно использовать в IoT для лучшего распределения ресурсов и балансировки нагрузки. Используя алгоритмы обучения с подкреплением, можно определить оптимальные действия, такие как выбор мощности передачи, размещение кэша в узлах тумана и коэффициенты разгрузки задач. Функция вознаграждения в этих алгоритмах может основываться на беспроводных помехах, суммарной скорости сети, времени разгрузки задач и времени доступа к кэшу.

Методы классификации, такие как k-ближайший сосед, деревья решений и т. д., могут использоваться для решения таких задач, как обнаружение аномалий для повышения безопасности. Вредоносные узлы могут осуществлять атаки на узлы Интернета вещей посредством передачи ложных данных или

подавления сигналов. Таким образом, крайне важно обнаруживать аномальный трафик для поддержания надежности сети IoT.

ОБСУЖДЕНИЕ

6G-коммуникации. Коммуникации 6G станут важной технологией для будущих приложений Интернета вещей. За счет улучшения связи с точки зрения достижимой скорости передачи данных, коэффициента доставки пакетов и задержки можно добиться надежного распространения данных между узлами Интернета вещей. 6G будет использовать терагерцевую связь, реконфигурируемые интеллектуальные поверхности (RIS) и массивные вычисления, чтобы значительно улучшить сквозную связь между различными узлами с поддержкой IoT.

Безопасность на основе блокчейна. Для приложений Интернета вещей необходимо разработать надежные механизмы безопасности. Некоторые приложения Интернета вещей имеют решающее значение, например мониторинг состояния здоровья, обмен данными о безопасности транспортных средств и т. д. Следовательно, атаки на эти приложения могут вызвать проблемы с безопасностью людей. Блокчейн - это эффективная технология, которая может обеспечить безопасную передачу данных благодаря механизму распределенного хранения записей и доказательства работы.

ЗАКЛЮЧЕНИЕ

В статье рассмотрена текущая работа и будущие возможности, связанные с надежной передачей данных в IoT. Представлены четыре ключевых компонента надежного обмена данными в контексте Интернета вещей, которые включают распределение ресурсов, управление задержками, показатели безопасности и надежности. Обсуждены методы и алгоритмы, которые были предложены для обеспечения надежности в IoT. Выделены основные проблемы, которые по-прежнему требуют внимания при внедрении надежных будущих сетей Интернета вещей.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Bhuiyan, M.N., Rahman, D.M., Billah, M. & Saha, D. (2021). Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities. *IEEE Internet Things J. 8*, pp.10474–10498.

2. L-Turjman, F.A., & Deebak, B.D. (2021). Seamless Authentication: For IoT-Big Data Technologies in Smart Industrial Application Systems. *IEEE Trans. Ind. Inform. 17*, pp. 2919–2927.

3. Bharadwaj, H.K., Agarwal, A., Chamola, V., Lakkaniga, N., Hassija, V., & Sikdar, B. (2021). A Review on the Role of Machine Learning in Enabling IoT Based Healthcare Applications. *IEEE Access. 9*, pp. 38859–38890.

4. Malik, U.M., Javed, M.A., Zeadally, S., & Islam, S.U. (2021). Energy efficient fog computing for 6G enabled massive IoT: Recent trends and future opportunities. *IEEE Internet Things J.*

5. Imran, K., Anjum, N., Mahfooz, S., Zubair, M., & Aman, M. (2021). Cluster-based group mobility support for smart IoT. *Comput. Mater. Contin*. *68*, pp. 2329–2347.

6. Shahid, H., Ashraf, H., Javed, H., Humayun, M., & AlZain, M.A. (2021). Energy optimised security against wormhole attack in IoT-based wireless sensor networks. *Comput. Mater. Contin*. *68*, pp. 1967–1981.

7. Butt, T.M., Riaz, R., Chakraborty, C., & Paul, A. (2021). Cogent and energy efficient authentication protocol for WSN in IoT. *Comput. Mater. Contin*. *68*, pp. 1877–1898.

8. Kanwal, S., Iqbal, Z., Irtaza, A., & Siddique, K. (2021). A genetic based leader election algorithm for IoT cloud data processing. *Comput. Mater. Contin. 68*, pp. 2469–2486.