



5G и INDUSTRY 4.0

Н.А. Захаров (НПП «Дозор» ОАО «Концерн КЭМЗ»)

Рассмотрены особенности сетевой технологии 5G, актуальные для промышленности. Отдельное внимание уделено реализации связи в миллиметровом диапазоне. Показана возможность совместного использования сетевой инфраструктуры за счет применения сетевой нарезки, виртуализации сетевых функций, программной конфигурации сетей.

Ключевые слова: 5G, IoT, Industry 4.0, сетевая нарезка, виртуализация сетевых функций, программно-конфигурируемая сеть, миллиметровый диапазон.

Введение

В ближайшем будущем число новых приложений Internet of Things (IoT) и запросов потребителей значительно возрастет. Соответственно, увеличится объем генерируемых данных и число используемых сервисов. Это создаст сложную ситуацию, поскольку приложениям потребуется более быстрая, «интеллектуальная», простая, надежная и масштабируемая структура, чем раньше. Фактически текущая архитектура IoT не будет достаточно надежной и доступной для приложений IoT следующего поколения. Следовательно, станет невозможным поддерживать устройства IoT из-за чрезвычайно большого числа устройств и сетевых служб. Технологии, которые были использованы для разработки сегодняшних архитектур, не обеспечат плавного перехода к увеличивающемуся числу абонентов и сервисов [1]. Решению указанных проблем будет способствовать ожидаемое внедрение нового поколения сотовой связи — 5G. Оно характеризуется высокой скоростью обмена данными (от 1 Гбит/с), малыми задержками, большим числом активных соединений. Технология 5G в первую очередь интересна тем, что она обеспечит инфраструктуру для IoT применительно к концепции Industry 4.0.

Особенности реализации сети

В контексте 5G речь идет о нескольких прорывных технологиях, реализация которых еще несколько лет назад казалась фантастикой [2]. На физическом уровне получаем следующее:

- работа в миллиметровом диапазоне длин волн (30...300 ГГц);
- применение пространственного разделения каналов и пространственной модуляции (приемные и передающие устройства обладают узкими диаграммами направленности, используются многоканальные антенные системы);
- применение новых сигнально-кодовых конструкций с соответствующим усложнением алгоритмов обработки сигналов в абонентских устройствах;

- существенно более плотное расположение базовых станций, то есть переход от макросот к микро- и пикосотам;

- использование действительно полнодуплексного режима (вместо временного и частотного дуплексирования, как в современных системах), то есть базовая станция должна в одной частотной полосе принимать и передавать информацию от множества устройств.

Принципиально важным является переход к новой архитектуре построения сети. Сегодняшние сети являются сотово-центрическими (основным элементом сети является базовая станция, где сосредоточены функции управления доступом). В сети 5G происходит переход к концепции устройство-центрической сети. Часть функций сетевого управления (вход в сеть, установление соединения и т.п.) возлагается на абонентские устройства, а не на сеть. В сетях предыдущих поколений абонентские устройства связывались исключительно с базовыми станциями, в сети 5G реализована непосредственная связь устройств между собой. Эта связь, что принципиально важно, осуществляется в рамках глобально связанной сети. Таким образом, мы получаем мобильные динамически формирующиеся и реконфигурируемые mesh-сети.

Сети становятся гетерогенными. Часть функций управления сетью децентрализуется, часть переносится в облако. Сети 5G будут использовать в своей работе как сантиметровый диапазон (ниже 6 ГГц), так и миллиметровый (28...95 ГГц). В сантиметровом диапазоне наблюдаем дальнейшее развитие сети 4G, в то время как в миллиметровом проявляется инновационный подход к построению беспроводных сетей. Высокая несущая частота позволяет обеспечить скорость обмена от 1 Гбит/с. Для связи в миллиметровом диапазоне требуются направленные антенны. Их применение дает значительный энергетический выигрыш по сравнению с сетями предыдущих поколений. Следствием направленности антенных систем является повышение эффективности использования частотного ресурса за счет пространственной селективности — соседние

устройства могут, не мешая друг другу, работать на одной частоте. Следует также отметить высокое затухание электромагнитных волн диапазона 60 ГГц в воздухе, что снижает помехи от соседних устройств. Малая длина волны влечет за собой малые размеры антенны, что позволяет встраивать антенные решетки в электронные компоненты абонентских устройств. Интеграция антенного устройства в изделие, выполненное по технологии низкотемпературной керамики (LTCC — low temperature cofired ceramic), рассмотрена в [3].

Концепция сетевой нарезки

Обычно для удовлетворения противоречивых требований к производительности, задержке, безопасности, надежности и гибкости создаются отдельные сегменты коммуникационной инфраструктуры. Это влечет за собой высокую стоимость и большое время развертывания. Поэтому желательно организовать совместное использование несколькими арендаторами одной физической сети [4]. Для разделения единой общей инфраструктуры на несколько логически независимых сетей используется сетевая нарезка (network slicing). Концепция сетевой нарезки является ключевой для раскрытия потенциала сетей 5G. Для реализации сетевой нарезки, используются технологии виртуализации сетевых функций (NFV Network Function Virtualization) и программно-конфигурируемой сети (SDN Software-Defined Networking).

Для задач сетевой нарезки в архитектурах 5G выделяют три основных категории: широкополосную передачу данных, интенсивный обмен данными между машинами, коммуникации с малой задержкой. Для критической инфраструктуры Industry 4.0 актуальны две последние позиции.

Предлагаемый в [4] подход к сетевой нарезке использует NFV и SDN, чтобы обеспечить функциональность и производительность 5G. В традиционных коммуникационных инфраструктурах такие функции, как баланс нагрузки, брандмауэр и обнаружение вторжения реализуются в заказных аппаратных устройствах. В противоположность этому NFV переносит данную функциональность в виртуальные сетевые функции, исполняемые на коммерческих коробочных серверных платформах, например, в облаках. Таким образом, серийно выпускаемые компьютерные компоненты хранения и коммутации могут быть использованы для гибкого развертывания, масштабирования и распространения сетевых служб, как это требуется для коммуникаций 5G. С концепцией NFV тесно связана технология SDN. Обычно децентрализованные устройства, такие как маршрутизаторы, осуществляют коммутацию пакетов, а также управление сетью. В SDN выделенные устройства передающего уровня (Data Plane), например, коммутаторы без функций маршрутизатора, осуществляют физическую пересылку данных. Маршрутизация сосредоточена на управляющем уровне (Control Plane) посредством так называемого SDN-контроллера. Формирование

управляющих воздействий основывается на глобальном, а не локальном состоянии сети, передающий и управляющий уровни могут обновляться независимо. Таким образом повышаются производительность и эффективность, сеть может быть гибко сконфигурирована централизованным образом, что удовлетворяет требованиям критической инфраструктуры. SDN и NFV являются взаимодополняющими подходами, поскольку контроллер может динамически направлять потоки данных между VNF, являясь сам VNF.

Industry 4.0 стремится встряхнуть нынешний производственный ландшафт за счет использования «интеллектуального» промышленного оборудования с расширенными возможностями. Современная тенденция сервитизации производства, то есть перехода от продажи товара к поставке комплекса товара и услуг его поддержки обещает новые дополнительные услуги для промышленных операторов и клиентов. С другой стороны, промышленные сети столкнутся с процессом трансформации, чтобы поддержать гибкость, ожидаемую от производственных процессов следующего поколения, и обеспечить возможность межзаводской кооперации. Сети 5G будут играть ключевую роль в реализации возможностей Industry 4.0, расширяя парадигму сетевой нарезки для поддержки требований использования в гетерогенных доменах в промышленности. Для соединения различных промышленных объектов можно создавать по требованию экземпляры срезов логических ресурсов, что обеспечит необходимые возможности сквозного подключения. Применительно к робототехнике перспективно перемещать сложные вычислительные задачи с физических устройств на облачную платформу. Данный подход значительно увеличивает потенциал роботов, обеспечивая при этом возможности реконфигурации по требованию.

С учетом развертывания большого числа программных сервисов в нескольких облачных и туманных центрах обработки данных сложность системы управления может заметно возрасти. Тогда централизованная система оркестровки может оказаться неспособной координировать виртуальные производственные функции и своевременно принимать соответствующие решения. Процессы управления могут быть делегированы в пределах определенного среза, а соответствующие контроллеры могут быть реализованы в виде экземпляров виртуальных функций в туманной архитектуре. Конфиденциальные данные с производства могут контролироваться и анализироваться в пределах предприятия, передача их внешним абонентам возможна только после соответствующей обработки. Далее рассмотрим участников построения сети и сетевого обмена и варианты их изоляции для защиты чувствительных данных

Доверие и изоляция в сетях 5G

В предоставлении, эксплуатации и использовании мобильной сети 5G участвуют следующие заинтересованные стороны [5].

— Поставщики оборудования и программного обеспечения предоставляют оборудование и программное обеспечение, необходимое для реализации и эксплуатации сети.

— Поставщик инфраструктуры (Infrastructure Provider InP) владеет и управляет (полностью или частично) сетевой инфраструктурой и предлагает инфраструктуру как услугу (Infrastructure as a Service — IaaS). Для этого InP закупает аппаратное и программное обеспечение у соответствующих поставщиков.

— Поставщик услуг мобильной связи использует услугу IaaS, предоставляемую InP, для предоставления услуг мобильной связи абонентам и услуг виртуальной сети арендаторам (то есть предоставляет клиентам сетевые срезы).

— Оператор мобильной связи сочетает роли InP и поставщика услуг мобильной связи.

— Арендатор — пользователь виртуальной сети, то есть организация, арендующая виртуальную сеть у оператора. Типичным арендатором является предприятие. Пользователей услуг мобильной связи обычно называют подписчиками. Этот термин часто ассоциируется с человеком и плохо подходит для описания связи в Industry 4.0. Поэтому будем считать пользователями мобильной связи мобильные устройства. Арендатор сетевого среза определяет, какие мобильные устройства могут его использовать. Назовем набор этих устройств мобильными устройствами арендатора.

— Оператор сети передачи данных это организация, управляющая сетью передачи данных, то есть сетью, доступной через мобильную сеть. Примерами сетей передачи данных являются корпоративные сети, на которых размещены корпоративные приложения или сети предприятий Industry 4.0.

Перечисленные выше заинтересованные стороны не могут полностью самоизолироваться друг от друга, в ряде случаев они вынуждены доверять друг другу. Поставщики инфраструктуры и операторы мобильной связи, покупающие и устанавливающие оборудование, должны доверять своим поставщикам технических и программных средств. Причина заключается в том, что уязвимости в аппаратной и программной части трудно обнаружить даже при тщательном тестировании приобретаемых технических и программных средств. Провайдер облачной инфраструктуры обычно может иметь доступ к обрабатываемым в ней данным, принадлежащим как оператору мобильной связи, так и арендаторам. Оператор и арендаторы также должны доверять друг другу.

Изоляция посредством непосредственной передачи данных

Пользователи мобильных сетей, которые не хотят полагаться на безопасность, обеспечиваемую сетью, могут использовать технологию непосредственной передачи данных over-the-top (OTT). Типичным примером такой связи является использование протокола HTTPS для доступа, например,

к portalу Internet-банкинга. Аналогично, арендатор среза при подключении мобильных устройств к сети передачи данных может применять защиту OTT между мобильными устройствами и объектом в сети, например, шлюзом VPN. Взаимная аутентификация и настройка безопасного туннеля между мобильным устройством и сетью данных осуществляются за счет использования стандартных протоколов, таких как TLS или IKEv2. Для устранения двойного шифрования можно отказаться от шифрования радиосигнала.

Аутентификация может быть выполнена в пользовательской плоскости, что означает, что подключение к пользовательской плоскости должно быть установлено в то время, когда арендатор еще не знает, является ли мобильное устройство одним из его мобильных устройств или нет. Обеспечение безопасности в OTT требует, чтобы арендатор управлял собственной базой данных мобильных устройств и предоставлял учетные данные для мобильных устройств. Поэтому мобильному устройству в этом сценарии требуется два набора учетных данных: один для подключения к мобильной сети, а другой для доступа к сети данных.

Технология OTT не способствует изоляции ресурсов, но она может обеспечить конфиденциальность и целостность трафика клиента даже от мобильного оператора. Тем не менее, оператор по-прежнему может получать много метаданных о трафике, например, какие абоненты получают доступ к сети данных, их местоположение, когда они обращаются к сети, их время и объемы связи, отношения связи и т.д. Поэтому для высокочувствительных служб необходимо применять более жесткие меры.

Поскольку при использовании инфраструктуры оператора полная изоляция от него невозможна, арендаторы, стремящиеся максимизировать свою конфиденциальность, должны управлять своей собственной инфраструктурой, где это возможно. Для этого возможны следующие технические решения.

Частная сеть 5G

Предприятие использует собственные базовые станции на своей территории, а трафик обрабатывается локальной сетью радиодоступа 5G и базовой сетью и передается в сеть данных предприятия, в которой размещаются серверы приложений Industry 4.0. Сетью и мобильными устройствами управляет исключительно предприятие. Работая в такой частной сети, предприятие может достичь хорошей изоляции. Это не идеальное решение, поскольку радиоканал, даже когда он используется в помещении, доступен для перехвата и анализа внешним злоумышленником. Отметим, что предприятие все равно должно доверять другим сторонам, например поставщику сетевого оборудования и программного обеспечения, а также обслуживающему персоналу, который настраивает и поддерживает частную сеть (если эти задачи не выполняются собственным персоналом предприятия).

Люди, которые проводят долгое время в Сети, могут ощущать разрыв с ней почти так же сильно, как отключение одного из органов чувств.

Мерси Шелли

Локальная частная сеть 5G и роуминг в общедоступной сети

В приведенном выше примере многие мобильные устройства арендатора могут никогда не покидать наиболее чувствительную область, то есть территорию предприятия, но могут быть и другие устройства, которым требуется подключения и за пределами ограниченного покрытия частной сети. Для них можно использовать сеть мобильного оператора. Для внешнего покрытия между предприятием и оператором может быть установлено соглашение о роуминге, которое позволяет мобильным устройствам предприятия использовать общедоступную сеть. Когда одно из мобильных устройств предприятия подключается к общедоступной сети, оно предоставляет информацию, которая указывает, что мобильное устройство принадлежит предприятию. Публичная сеть затем аутентифицирует мобильное устройство на основе информации, которую она извлекает из частной сети предприятия, и в случае успеха разрешает мобильному устройству использовать публичную сеть. Трафик может быть впоследствии защищен ключом, полученным во время аутентификации, но этот ключ используется совместно мобильным устройством и общедоступной сетью, и не может изолировать трафик от мобильного оператора. Для обеспечения защиты трафика от оператора при работе с частной сетью необходимо применять защиту OTT, как описано выше.

Частная сеть 5G с использованием срезов внешней сети

Вместо роуминга предприятие может арендовать срез в публичной сети, который включает только

нижний слой стека радиодоступа и подключается к частной сети, которая обеспечивает более высокие уровни радиодоступа и функции базовой сети.

Заключение

Internet of Things является одним из ключевых компонентов Industry 4.0. Внедрение технологии 5G позволит снять существующие ограничения на число абонентов, объем передаваемых данных и скорость обмена. Механизм сетевой нарезки обеспечивает совместное использование инфраструктуры многими участниками, каждому из которых выделяется собственная виртуальная сеть. Для достижения большей изоляции критических процессов могут применяться различные сочетания частных и общедоступных сетей 5G.

Список литературы

1. H. Rahimi, A. Zibaeenejad and A.A. Safavi, "A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2018, pp. 81-88. doi: 10.1109/IEMCON.2018.8614777.
2. Шахнович И. Системы беспроводной связи 5G: телекоммуникационная парадигма, которая изменит мир. Краткие тезисы // Электроника: наука, технология, бизнес. 2015. № 7. стр. 48 -55.
3. F. Foglia Manzillo et al. "A Multilayer LTCC Solution for Integrating 5G Access Point Antenna Modules," in IEEE Transactions on Microwave Theory and Techniques, vol. 64, no. 7, pp. 2272-2283, July 2016. doi: 10.1109/TMTT.2016.2574313.
4. F. Kurtz, C. Bektas, N. Dorsch and C. Wietfeld. "Network Slicing for Critical Communications in Shared 5G Infrastructures - An Empirical Evaluation," 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, 2018, pp. 393-399. doi: 10.1109/NETSOFT.2018.8460110.
5. P. Schneider, C. Mannweiler and S. Kerboeuf. "Providing strong 5G mobile network slice isolation for highly sensitive third-party services," 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, 2018, pp. 1-6. doi: 10.1109/WCNC.2018.8377166.

Захаров Николай Анатольевич – канд. техн. наук, руководитель, Научно-производственное подразделение «Дозор» ОАО «Концерн КЭМЗ». Контактный телефон (495) 640-09-47. E-mail nazakharov@npp-dozor.ru

Численное моделирование для предотвращения деформации изделия при 3D-печати металлом

Специалисты компании "КАДФЕМ Си-Ай-Эс" представили на конференции «3D Концентрат» (г. Воронеж) результаты численно-экспериментального исследования деформированного состояния деталей, напечатанных методом SLM из жаропрочного сплава на никелевой основе.

Численное моделирование процесса 3D-печати помогает решить ряд вопросов на этапе подготовки производства, например, определить температурные напряжения в изделии и места потенциального трещинообразования или выявить деформированное состояние изделия после печати и провести коррекцию геометрии, чтобы обеспечить точность формы. В основе этой технологии лежит метод конечных элементов и его реализация в виде связанного решения тепловой и механической задачи.

Одной из отраслей, в которой применение технологии может быть особенно актуально – авиационное и космическое двигателестроение. Это связано с тем, что, во-первых, использование 3D-печати позволяет снизить массу двигательной установки и, следовательно, повысить эксплуатационные характеристики аппарата. Во-вторых, аддитивные технологии могут

сократить затраты на производство, например, за счет уменьшения сроков изготовления опытных образцов и времени простоя конструкторского подразделения. Кроме того, в этих отраслях промышленности значительную часть изделий составляют тонкостенные детали сложной формы, особенно подверженные короблению в процессе селективного лазерного сплавления.

На конференции были продемонстрированы результаты численного моделирования процесса 3D-печати с использованием сырья отечественного производства, а также приведено сравнение отклонения формы образцов из этого материала, напечатанных методом SLM, от размеров, полученных в результате численного моделирования. Для определения фактической формы образцов использовалось 3D-сканирование. Результаты исследования показали, что численное моделирование с использованием ANSYS Additive позволяет прогнозировать искажение формы деталей не только качественно, но и количественно. Технология также позволяет скорректировать исходную геометрическую модель изделия, чтобы минимизировать его коробление после печати.

<https://www.cadfem-cis.ru>