до миллиметрового диапазона. Во многих из этих неоднородных сетей применяются такие технологии, как динамическое перераспределение спектра (DSS) с использованием сети 4G, а также спутниковая связь и Wi-Fi, благодаря чему создаётся экономичная и надёжная система повсеместного беспроводного доступа. Общие платформы и законченные пользовательские решения позволяют разработчикам и операторам этих неоднородных сетей получать данные о состоянии сети на основании обширного множества параметров с использованием большого количества взаимосвязанных систем.

Корпоративная культура, поощряющая свободу мысли, создаёт хорошие условия для полезного применения этих данных с целью внедрения инноваций и повышения качества обслуживания клиентов любого 5G-сервиса. Кроме того, такая культура создаёт фундамент для новых технологий и приложений, способствующих повышению качества жизни.

3. Для выстраивания успешных партнёрских отношений необходима прозрачность

Третий фактор успеха основан на представлении о прозрачности как о ключевом компоненте, необходимом для выстраивания успешных партнёрских отношений между компаниями, правительственными структурами, научными учреждениями, организациями по стандартам и консорциумами. Прозрачность информации о функционировании продукта, коммерческих соглашениях и обязательствах – основной фактор успешного партнёрства и взаимной уверенности, приводящий к росту объёма инвестиций.

Одним из способов обеспечения прозрачности для сетей, устройств и сервисов 5G является использование методов тестирования, позволяющих проводить точные измерения и гарантировать достоверность ожидаемых результатов. Применяя инструменты для снижения неопределённости, заинтересованные лица (в том числе разработчики продуктов и мобильные операторы) могут создавать надёжные решения, соответствующие ожиданиям клиентов. Инструменты тестирования, позволяющие оценить функциональность любой разработки в рамках совместного проекта или коммерческого соглашения, формируют надёжный фундамент для достижения прозрачности в масштабах всей отрасли.

Двигатель инноваций для всего человечества

Эти три фактора успеха – доверие, прозрачность и свобода мысли – способствуют переходу к мобильной связи нового поколения, 6G, в рамках которой будет реализована технология повсеместного беспроводного сетевого доступа, которая прослужит человечеству не один десяток лет. Наше будущее сформируют инновации, основанные на коллективной разработке новых технологий и сценариев эксплуатации для многих отраслей, которые всё чаще взаимодействуют между собой. Эти факторы успеха способствуют реализации широкого спектра возможностей для наших клиентов и отрасли в целом, а также стимулируют развитие здравоохранения, логистики и транспортной инфраструктуры.

Компания Keysight обладает необходимым опытом для создания, развития и коммерциализации взаимосвязанных прорывных технологий в различных отраслях. Таким образом, Keysight выступает в роли катализатора для новых идей и проектов, которые помогут сделать жизнь каждого из нас более здоровой, насыщенной и наполненной возможностями.

Обеспечение безопасности в мире 5G

Сатиш Дханасекаран (Keysight Technologies)

В статье рассказывается о том, какие потребуется предпринять меры для обеспечения высокого качества работы сетей связи нового поколения и как эти сети изменят облик телекоммуникационных систем.

Переход к технологиям 5G станет революцией в области мобильной связи. 5G-устройства должны обеспечить увеличение скорости и снижение задержки передачи данных, повсеместную доступность сети и невиданный ранее уровень надёжности. Это приведёт к появлению новых услуг и сценариев использования, далеко выходящих за рамки обычной связи между абонентами. Быстрое развёртывание 5G-сетей создаёт огромный потенциал для объединения экономики на всех уровнях. Однако при этом вскрываются и потенциальные уязвимости, которые должны быть устранены.

Переход к виртуализированным сетям с центральной ролью программного обеспечения меняет облик телекоммуникационных систем

Повышение эффективности и рентабельности 5G-сетей достигается благодаря технологиям виртуализации, в которых центральную роль играет программное обеспечение. При этом происходит переход от специального оборудования к программным компонентам, работающим на основе готовых коммерческих аппаратных продуктов (COTS). Рост доли программного обеспечения в 5G-системах продолжает стимулировать интенсивное развитие данного сегмента. К сожалению, эти технологические инновации также приводят к росту числа потенциальных атак на системы. Хотя базовые функции сетей 5G реализуются

на основе новых и разнообразных версий системной архитектуры, на смену специализированным интерфейсам приходят хорошо известные технологии, такие как HTTP и обработка запросов на основе передачи состояния представления (REST API). Всё это увеличивает число уязвимостей и вероятность кибератак.

Виртуализация сетевых функций (NFV) приведёт к значительному повышению уровня масштабируемости по сравнению с традиционными решениями на основе платформ. Технология NFV основана на использовании комплекта программных средств и инфраструктуры, в которой реализуются функции сети. Несмотря на то что виртуализация очень полезна в плане масштабируемости и эффективности использования аппаратных ресурсов, переход на программные платформы, состоящие из множества компонентов от разных поставщиков (зачастую с открытыми кодами), повышает риск уязвимости для всей системы. Кроме того, в случае сегментирования («нарезки») 5G-сети, при котором широко используются технологии виртуализации, огромную важность приобретает изоляция сегментов и предотвращение утечек данных между ними.

Ещё одно важное следствие внедрения сетей 5G – повсеместное распространение сетевых устройств, которые станут неотъемлемой частью повседневной жизни. Сети 5G предусматривают новые сценарии использования, для которых потребуются новые стандарты качества обслуживания в соответствии с изменившимися требованиями к надёжности, пропускной способности и времени задержки для важнейших компонентов инфраструктуры и систем, работающих в масштабе реального времени. Хотя уже существуют (или разрабатываются) стандарты обеспечения и оценки безопасности сети в различных отраслях (автотранспорте, медицине, инженерных сетях и т.д.), общий уровень стандартизации устройств Интернета вещей остаётся неудовлетворительным. Слабая защищённость многочисленных сетевых устройств может легко привести к перебоям в предоставлении основных и второстепенных услуг 5G-операторов.

5G-сети организованы невероятно сложным образом, а развёртывание элементов инфраструктуры на пределе технологических возможностей делает обеспечение их безопасности ещё более сложной задачей. Столкнувшись со сложностями, операторы могут привлекать сторонних лиц для конфигурирования и управления сетями, предоставляя права администратора потенциальным злоумышленникам. Неудачная конфигурация системы может поставить сеть под угрозу независимо от наличия и использования функций безопасности, определяемых стандартом.

Заявленный уровень качества услуг в сетях 5G потребует принятия мер по обеспечению безопасности

Мировая технологическая экосистема добилась значительного прогресса в плане обеспечения надёжности инфраструктуры. Правительственные организации внимательно анализируют риски безопасности, связанные с сетями и системами 5G. Группа по обеспечению безопасности сетевых инфраструктур (NIS) Европейского союза провела оценку рисков, связанных с кибербезопасностью 5G-сетей. Вскоре после этого картину угроз для систем 5G проанализировало Европейское агентство кибербезопасности (ENISA). Аналогичные исследования и мероприятия проводятся и в других регионах. В то же время операторы мобильной связи разработали схему обеспечения безопасности сетевого оборудования (NESAS), в создании которой приняли участие компания 3GPP и Ассоциация GSMA. Эта схема призвана повысить уровень безопасности в мобильной отрасли. Схема NESAS основана на комплексном подходе к оценке жизненного цикла разработки продуктов, а также на сценариях испытаний безопасности, определяемых стандартом 3GPP SA3 для сетевого оборудования.

Тем не менее увеличение риска атак требует усиленного внимания к безопасности, особенно по сравнению с предыдущими поколениями систем мобильной связи.

Сегодня пользователям отрасли доступен целый ряд инструментов обеспечения безопасности, в том числе анализ оконечных точек, тест на проникновение в систему, сканирование уязвимостей, нечёткое тестирование (фаззинг), а также решения для идентификации и управления доступом. Все эти инструменты могут использоваться совместно в целях проверки всех аспектов инфраструктуры связи.

На протяжении последних 15 лет компания Keysight проводит исследования в области безопасности на базе собственного Центра прикладных исследований угроз безопасности (ATI). Деятельность ATI в сочетании с портфелем комплексных инструментов для разработки и тестирования коммуникационных систем обеспечивает уникальное положение компании Keysight на рынке решений для обеспечения безопасности систем 5G.

Комплексное испытание безопасности станет первоочередной задачей

Хотя внедрение стандартов 5G, несомненно, приведёт к повышению уровня безопасности по сравнению с сетями предыдущих поколений, всё же будет оставаться ряд областей, в которых потребуется дальнейшая работа по обеспечению безопасности сетей 5G. Сложность 5G-сетей требует внимательного подхода к конфигурированию систем и управлению аспектами безопасности, а также ужесточения требований к безопасности для сторонних администраторов, что в конечном счёте означает внедрение строгого контроля по всей цепочке поставок.

Увеличение доли программных компонентов в сетях 5G и бурное развитие Интернета вещей станут факторами развития средств обеспечения безопасности. Это должно стать главной задачей предприятий отрасли по мере дальнейшего развития 5G-инфраструктуры. В различных сегментах отрасли уже доступны новые стандарты безопасности и рекомендованные практики для всех этапов разработки программного обеспечения – от проектирования архитектуры до написания программного кода, тестирования и выпуска. Расширение списка уязвимостей и угроз означает, что компании должны уделять повышенное внимание разработке и обновлению средств проверки безопасности. Это требует применения автоматизированных инструментов, подлежащих своевременному обновлению в соответствии с последними выявленными угрозами.