УДК 621.391

АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ В СЕТЯХ СВЯЗИ ЧЕТВЕРТОГО ПОКОЛЕНИЯ (LTE)

М.В. Ульянов, Д.О. Ульянова, студенты гр. ИТм-191, I курс.
Научный руководитель: С. А. Асанов, ст. преподаватель.
Кузбасский государственный технический университет имени Т.Ф. Горбачева, г. Кемерово

Представлены цели и задачи создания стандарта LTE. Проведен анализ основных качественных и количественных показателей сетей нового поколения и дан ответ на важный вопрос не превратятся ли мобильные сети в Интернет с присущими ему опасностями и проблемами.

Развитие информационных технологий создает фундамент современной экономики государства и благосостояния ее людей. Без высокоскоростного мобильного интернета, доступного прямо здесь и сейчас, представить современную жизнь достаточно сложно. Видео-хостинги, потоковые сервисы воспроизведения музыки, общение по Skype или другому популярному мессенджеру с функцией видео звонков – всё это требует качественного высокоскоростного соединения. Поэтому целями создания стандарта LTE являются: увеличение возможностей высокоскоростных систем мобильной связи; уменьшение стоимости передачи данных; возможность предоставления широкого спектра услуг по приемлемой для конечных потребителей стоимости.

Однако улучшение качественных и количественных показателей сетей нового поколения выдвигает и новые требования, связанные с повышением безопасности передаваемой информации. Поскольку технология 4G полностью основана на протоколе IP, не превратятся ли мобильные сети в Интернет с присущими ему опасностями и проблемами информационной безопасности? Мобильная связь четвертого поколения предусматривает использование целого спектра технологий, которые раньше развивались параллельно. Опора на множество различных технологий затрудняет поиск уязвимостей в LTE, что хорошо с точки зрения безопасности: взлом радиоканала для одних методов может сработать, а для других нет. В сетях 4G весь трафик проходит через единую архитектуру по протоколу IP. Поэтому в компании Cisco считают, что все угрозы безопасности передаваемой информации связаны именно с протоколом IP. Базовые станции в LTE стали более интеллектуальными и самостоятельными они получили возможность маршрутизировать трафик, что позволило организовывать соединения между абонентами напрямую, минуя ядро сети. В результате у злоумышленников появилась возможность атаковать сами базовые станции, которые работают только по протоколу IP, поэтому облегчается несанкционированный доступ к сети и, следовательно, могут быть использованы классические атаки на канальном уровне, широковещательные штормы и другие варианты нападений. Чтобы свести к минимуму

подверженность атакам конфиденциальную информацию, базовая станция должна обеспечить выполнение таких важных операций как кодирование и расшифровку пользователей данных, а также хранение ключей. Для минимизации вреда наносимого в случае кражи информации о ключах из базовых станций разработаны специальные меры противодействия: проверка целостности устройства; взаимная аутентификация базовой станции оператора (выдача сертификатов); безопасные обновления; механизм контроля доступа; синхронизация времени и фильтрация трафика.

В настоящее время вредоносное программное обеспечение на компьютерах стало широко распространённым явлением, становится все больше вредоносного ПО для мобильных устройств, особенно на платформе Android (https://securelist.ru/mobile-malware-evolution-2019/95602/), следовательно, внедрение высокоскоростного стандарта LTE приносит в мобильные средства связи все те угрозы, которые мы сейчас наблюдаем в ситуации с обычными компьютерами. Первая очевидная угроза атаки: DoS на сеть (Denial of Service). Емкость радиоканала в LTE предполагается большая, но все, же она имеет конечное значение. Сетевые ресурсы базовой станции делятся между абонентами, и хотя есть ограничения для монополизации полосы отдельным пользователем, тем не менее, атака на отказ в обслуживании сети вполне возможна.

Другая угроза: вирусные атаки. Хотя таким атакам подвержены устройства, а не сеть, технология LTE увеличивает скорость распространения вредоносных программ, поскольку сам этот стандарт является высокоскоростным.

Третья опасность: атаки на дополнительные сервисы, которые также могут быть уязвимы для самых разнообразных атак как из Интернета, так и из мобильной сети. Вполне возможно, что, атаковав один из сервисов, злоумышленники смогут внедрить в клиентские устройства опасные программы.

Нельзя забывать и об ограничениях LTE. Например, увеличение скорости подключения оборачивается обычно уменьшением радиуса действия базовой станции, в среднем для 4G он составляет около 5 км, и зависит от используемого частотного диапазона. Поэтому базовых станций в сети становится больше, и они располагаются ближе друг к другу. В результате триангуляционный метод определения местоположения абонента по сигналам базовых станций работает точнее. С одной стороны, это можно использовать, например, для контроля за перемещением грузов и многого другого. Но с другой стороны, сервисы геопозиционирования (Locationbased service, LBS) можно использовать и для слежки за абонентом, что создает опасность новых угроз конфиденциальности персональных данных.

Еще одна особенность LTE в том, что эта технология ориентирована на подключение интеллектуальных пользовательских устройств: компьютеров с LTE-модемами, планшетов или смартфонов. С их распространением число потенциально опасных сервисов будет только возрастать. Взлом такого сервиса позволит злоумышленникам получить доступ к ценной информации

провайдера и построить новые схемы преступлений и незаконного получения денег.

Есть также проблемы и с самим стандартом. Очень остро стоит задача взаимодействия с недоверенными (не LTE) сетями. Если трафик между пользовательским оборудованием и базовой станцией шифруется (это требование стандарта) и угроза нарушения конфиденциальности становится неактуальной, то взаимодействие базовой станции с радиоконтроллером других сетей, не предъявляющих требований к шифрованию данных (например, 3G) по умолчанию никак не защищено, а следовательно, это брешь для возможных атак со стороны злоумышленников.

Другой проблемой является отсутствие обязательной аутентификации между ядром сети и базовой станцией. Эту опцию оператор связи для снижения своих издержек по развертыванию сети LTE может и не задействовать вовсе.

И все же разработчики мобильной технологии LTE позаботились о ее защите несколько больше, чем разработчики Интернета. Поэтому мобильная сеть является более надежной и безопасной, чем всемирная сеть так как, в основном, защита возложена на более интеллектуальные базовые станции. Все функции защиты в LTE объединены стандартом и подразумевают защиту на нескольких уровнях: на уровне доступа к сети; на уровнях сетевого и пользовательского доменов; на уровне приложений; на уровне отображения и конфигураций. Каждый из этих уровней предполагает аутентификацию и авторизацию всех устройств, чего нет в Интернет. Кроме того, технология LTE предусматривает использование не только адреса, но и системы распространения ключей шифрования для всех устройств, подключенных к сети с возможностью перехода со 128 на 256 битные ключи и введения новых алгоритмов, сохраняя обратную совместимость. Таким образом, даже если один из алгоритмов будет взломан, оставшиеся обеспечат безопасность сети LTE.

Также в сетях LTE сохраняются и методы аутентификации пользователей по привязке к SIM карте, как в традиционной мобильной связи. Само по себе это не препятствует проведению атак на сеть, но создает условия неотвратимого расследования инцидентов безопасности.

Исходя из изложенного, можно сделать вывод о том, что механизмы безопасности в сетях LTE разработаны с учётом имеющегося опыта по противодействию вредоносным воздействиям на сети IP, закреплены стандартом, обязательным к применению, поддерживают механизмы расширения и усиления защиты в будущем. Таким образом, сеть LTE является сетью с приемлемым уровнем безопасности и значительно более высоким, чем Интернет.

Список литературы:

1. Аналитический обзор защиты данных в сетях LTE По материалам NTT DO C O MO Technical Journal Vol. 11 No. 3 http://advancedmonitoring.ru/article/detailphp 7ELEMENTJD-56
2. LTE and the Evolution to 4G Wireless Design and Measurement C hallenges. Bonus Material: Security in the LTE-SAE Network, Agilent technologies 2010 p.