МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ

Региональный семинар МСЗ

«ТЕНДЕНЦИИ РАЗВИТИЯ КОНВЕРГЕНТНЫХ СЕТЕЙ: РЕШЕНИЯ МСТ-NGN, 4G и 5G»

Тезисы докладов

17-11 ноября 2118 года

Кип

В сборнике опубликованы тезисы докладов участников Регионального семинара МСЭ для стран СНГ и Грузии «Тенденции развития конвергентных сетей: решения пост-NGN, 4G и 5G», который проходил на базе Государственного университета телекоммуникаций в период с 17 по 18 ноября 2016 года в г. Киев, улица Соломенская, 7.

В материалах Регионального семинара МСЭ освещаются актуальные вопросы развития сетей пост - NGN; услуги и качество обслуживания в сетях; планирование и оптимизация сетей мобильной связи; безопасность в сетях мобильной связи; нормативно-правовые и экономические аспекты внедрения технологий 4G и 5G.

Наконечный В.С.,
д.т.н., *СНтСу директор*
Учебно-научного института защиты информации,
Государственный университет телекоммуникаций,
г. *Киев, Украина*
Мордвинцев Н.В*.у*
к.т.н*.9* ***доцент,*** *доцент кафедры*
информационной безопасности факультет №4
Харьковский университет внутренних дел,
г. *Харьков, Украина*

ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ В СЕТЯХ ПОСТ - NGN

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?

Развитее IT создает фундамент современной экономики государства и благосостояния ее людей. Без высокоскоростного мобильного интернета, доступного прямо здесь и сейчас, уже нельзя. Видеохостинги, потоковые сервисы воспроизведения музыки, общение по Skype или другому популярному мессенджеру с функцией видеозвонков - 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 недорогих услуг.

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?

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.

Безопасность в сетях мобильной связи

В настоящее время вирусы на компьютерах стали делом обычным, троянцев для Android становится все больше, следовательно, внедрение высокоскоростного стандарта LTE может принести 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 ограничения. 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 забьюать 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 (Location-based service, LBS) можно использовать и для слежки за абонентом, что создает опасность новых угроз.

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 сети 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 Интернете. Кроме того, технология LTE предусматривает использование не только IP-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.

Помимо алгоритмов шифрования и обеспечения комплексной безопасности в сетях 4G используются дополнительные алгоритмы. Таким образом, даже если один из алгоритмов будет взломан, оставшиеся обеспечат безопасность сети LTE. В сетях LTE сохраняются и методы аутентификации пользователей по привязке к SIM карте, как в традиционной мобильной связи. Пользователь может заблокировать доступ к телефону по PIN-коду.

Таким образом, специалисты по безопасности совместно с разработчиками LTE постоянно отслеживают появление новых угроз безопасности и предпринимают все необходимые шаги для обеспечения целостности и конфиденциальности передаваемых данных.

Учитывая огромную экономическую и политическую важность введения в Украине технологий 4G Президент Порошенко подписал указ о начале работы по их внедрению в нашей стране.

Литература

1. *Аналитический обзор защиты данных в сетях LTE По материалам NTT DOCOMO Technical Journal Vol. 11 No. 3*
http://advancedmonitoring. ru/article/detailphp 7ELEMENTJD-56

2. LTE and the Evolution to 4G Wireless Design and Measurement Challenges. Bonus Material: Security in the LTE-SAE Network, Agilent technologies 2010 p. 7