АНАЛИЗ ОСНОВНЫХ УЯЗВИМОСТЕЙ СЕТЕЙ СТАНДАРТА LTE

© 2016 г. В.М. АНТОНОВА, Н.Е. БОГОМОЛОВА

Московский технический университет связи и информатики,
Московский государственный технический университет им. Н.Э. Баумана

В настоящее время большое количество систем безопасности, такие как охранные системы, контроль физического доступа, мониторинг датчиков, а также системы телеметрии, используют сеть LTE для передачи данных. В статье приведен анализ ключевых видов атак на элементы сети LTE, реализуемые без применения взлома криптосистем и протоколов безопасности. А также сделаны предположения по контролю трафика в таких сетях.

Сеть LTE состоит из двух важнейших компонентов: сети радиодоступа E-UTRAN и базовой сети EPC (рис. 1).

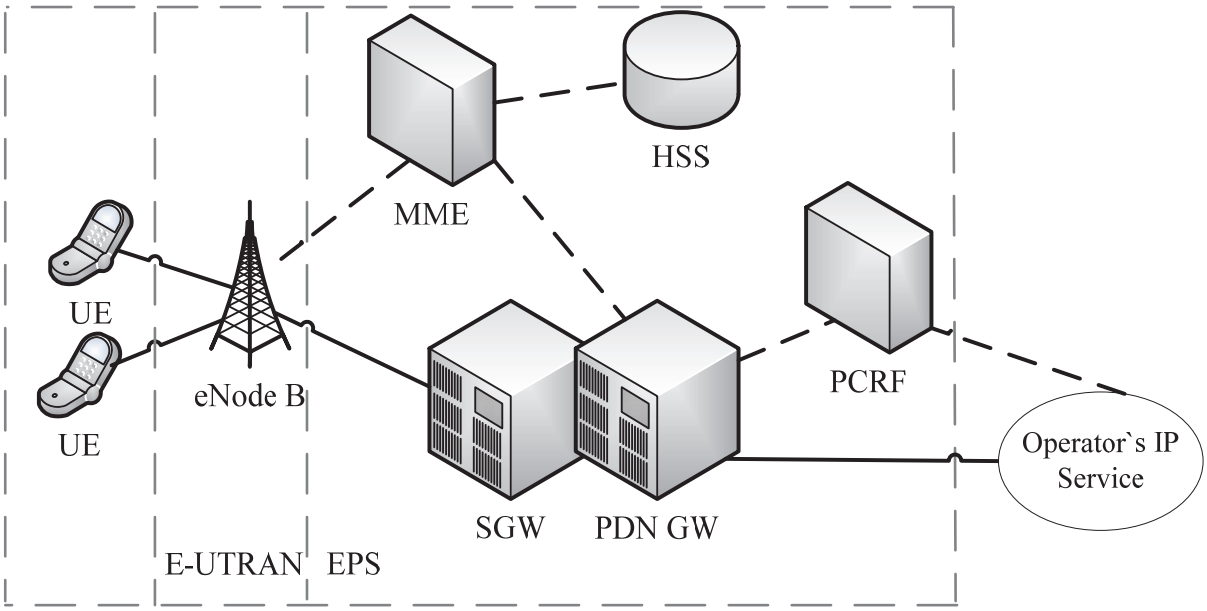

Рис. 1. Архитектура сети LTE.

Взаимодействие сети LTE с сетями 3GPP (UMTS/GSM/HSPA+) осуществляется как при обеспечении роуминга, так и хендовера. Взаимодействие сети LTE с другими 3GPP сетями, для оказания традиционных услуг телефонии, осуществляется с помощью как традиционной технологии коммутации каналов (TDM), так и технологии коммутации пакетов на базе сервисной подсистемы IMS.

Взаимодействие сети LTE с сетями не-3GPP разделяется на взаимодействие с сетями с гарантированной безопасностью – «надежными» и взаимодействие с сетями, безопасность которых не гарантирована – «ненадежными». В качестве «надежных» сетей могут выступать присоединенные сети других стандартов, в качестве «ненадежных» - общедоступные IP-сети Интернета. Взаимодействие сети LTE с

«надежными» сетями стандартов не-3GPP осуществляется посредством шлюза PDN GW, взаимодействие с «ненадежными» сетями – посредством шлюза ePDG.

Усложнение характера трафика, в частности снижение речевой нагрузки по сравнению с объемом мультимедийных сообщений при организации различных видов мобильного доступа приводит к тому, что требуемое качество обслуживания, в том числе безопасность, может быть обеспечено только при использовании эффективных методов повышения пропускной способности, так как именно при беспроводном доступе могут возникать резкие перекосы нагрузки из-за стохастического перемещения абонентов по зонам мобильной сети. Так как все протоколы и схемы взаимодействия являются открытыми, а передача данных осуществляется на базе протокола IP это может вызвать проблемы с безопасностью информации.

Характерной особенностью проблемы защиты информации является необходимость полного описания множества угроз информационной безопасности. Каждый неучтенный дестабилизирующий фактор может существенно снизить эффективность защиты. Тем не менее, проблема описания полного множества угроз в настоящее время не формализована в полной степени. Обусловлено это тем, что передающаяся по сети LTE информация подвергается воздействию большого числа угроз.

Проблемы обеспечения безопасности в сетях LTE решаются сразу на нескольких уровнях сети: на радио интерфейсе, на внутренней сети оператора, а также на стыках взаимодействия различных операторов.

В пассивном варианте злоумышленник прослушивает канал связи между мобильным устройством и базовой станцией; а в активном варианте - в дополнение к прослушиванию, злоумышленник оказывает воздействие на уже циркулирующий трафик.

Поскольку шифрование пользовательских данных транслируемых через эфир прекращается на уровне соты сети LTE, аппаратное вмешательство в устройство позволяет раскрыть конфиденциальную информацию ничего не подозревающего пользователя.

Кроме того, атаки типа подмена доверенного объекта, атаки на сетевые службы с использованием Интернет протоколов, атаки-сообщения о ложном местоположении или атаки несанкционированной переконфигурации радиоаппаратуры усложняют для оператора сети LTE процесс управления интерференцией и средствами контроля питания, что неблагоприятно сказывается на качестве обслуживания.

На основании работ по контролю за трафиком [1, 3], проводимых ранее, авторами была разработана модель, позволяющая менять верхнюю скорость трафика, который не чувствителен к задержкам - эластичного, то есть трафика, который получается от передачи файлов по сети или межмашинного обмена данными. Свойством эластичного трафика является то, что он изменяет свою скорость согласно пропускной способности сети, что дает возможность существенно повысить эффективность использования ресурса передачи информации.

Повсеместное увеличение пользователей с интеллектуальными модемами создает большое рост эластичного трафика на сетях [2]. Контроль эластичного вида трафика, за чет введения порога на максимально допустимый объем трафика, позволит снизить угрозы безопасности на сети LTE. Для этого с помощью имитационного моделирования при фиксированных параметрах: пропускной способности соты, интенсивности поступления заявок на передачу файлов и средней величине файла, величина загрузки единицы ресурса соты уменьшалась до момента пока выполнялись нормы качества обслуживания эластичного трафика. В модели так же был учтен трафик, происходящий от разговорных соединений, который чувствителен к задержкам и имеет постоянную скорость передачи по сети. На рис. 2 представлен график, который показывает результат оценки максимально допустимого объема трафика, который может быть передан в соте при фиксированной пропускной способности соты с заданной величиной максимальных потерь. Как видно из графика, с уменьшением загрузки единицы ресурса потери заявок падают. Для значений коэффициента загрузки единицы ресурса менее 0,95 потери заявок на передачу

данных и потери заявок на передачу сервисов реального времени становятся менее 0,55.

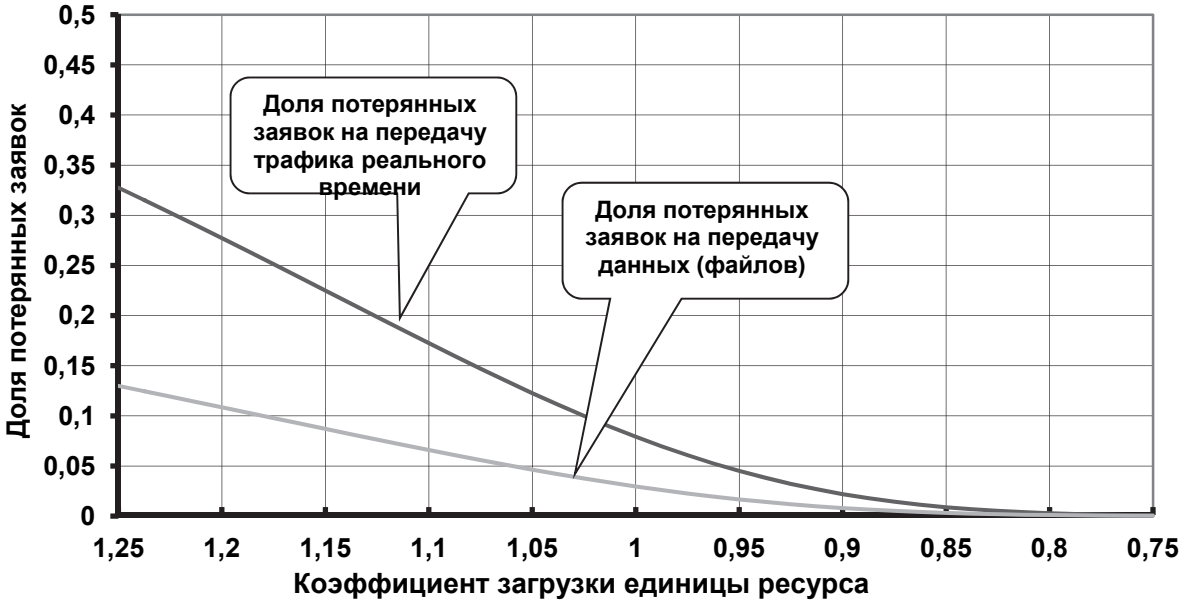

Рис. 2. Результат максимально допустимого объема трафика.

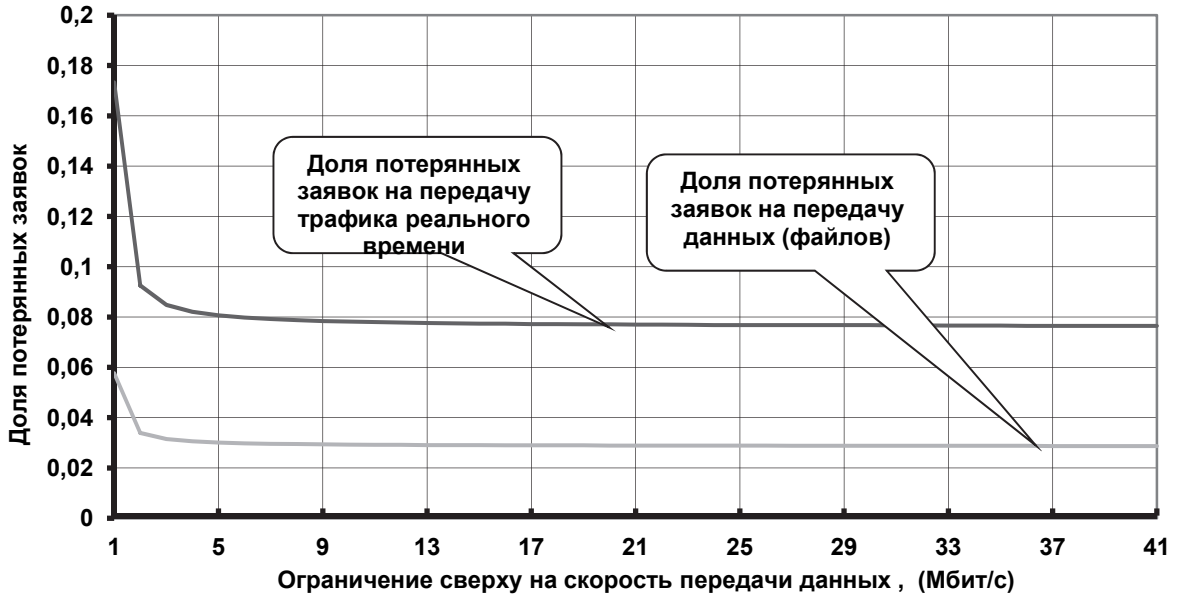

Рис. 3. Зависимость потерь заявок от увеличения максимальной доступности ресурса для передачи эластичного трафика.

Увеличивая максимальную скорость для передачи эластичного трафика, оператор ускорят ускоряет передачу файлов по сети, используя пропускную способность соты, не задействованную на обслуживание трафика реального времени.

Сформулированное предположение можно проиллюстрировать численным примером, задав следующие параметры: пропускная способность соты = 100 Мбит/с, скорость трафика реального времени = 3 Мбит/с, минимальная скорость передачи эластичного вида трафика = 1 Мбит/с, средняя длина файла = 16 Мбит, количество заявок от трафика реального времени в 100 раз меньше чем на передачу эластичного.

Если увеличивать максимальную скорость передачи эластичного файла, при фиксированных остальных значениях, то характеристики пропускной способности соты

улучшаются за счет ускорения передачи файлов, как показано на рис. 3. В моделировании максимальная скорость для передачи эластичного трафика увеличивалась до 40 Мбит/с. Как видно, с ростом скорости эластичного трафика потери падают. При чем, не только для заявок на передачу файлов, но и для трафика реального времени. Это происходит из-за ускоренного освобождения ресурса сети. Как показывает моделирование, максимальный эффект достигается при скорости = 10 Мбит/с, дальнейшее ее увеличение существенно не сказывается на значениях характеристик потерь.

Такие методы контроля эластичного трафика предполагается использовать в дальнейшем для моделей контроля целостности и доступности.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 16-29-09497 офи-м).

СПИСОК ЛИТЕРАТУРЫ

1. *Степанов С.Н*. Теория телетрафика: концепции, модели, приложения. – М.: Горячая линия – Телеком, 2015. – 868 с.
2. *Антонова В.М., Цирик И.А*. Управление доступом новых требований на фрагменте сети LTE. / Материалы научно-технической конференции Фундаментальные проблемы радиоэлектронного приборостроения «INTERMATIC-2015», 145-147 с.
3. *Антонова В.М*. Оценка канального ресурса для разноскоростных соединений на фрагменте сети LTE, Журнал «Естественные и технические науки», 2014, № 10, с. 356-358.