УДК 004.7

Т.В. Лавровская

Харьковский национальный университет радиоэлектроники, Харьков

АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ В LTE-СИСТЕМАХ

В статье представлены основные этапы развития и модернизации беспроводных сетей стандарта LTE. Рассмотрены основные характеристики радиоинтерфейса, с указанием технологий, применяемых для увеличения пропускной способности системы и повышения скорости передачи данных. Поскольку главной задачей технологии LTE является обеспечение требуемого уровня защиты информации, передаваемой по беспроводному каналу, поэтому особое внимание в работе уделено анализу существующих методов обеспечения безопасности в сетях 4G.

Ключевые слова: *LTE-система, базовая станция, OFDM, пропускная способность системы, помехозащищенность, технология MIMO.*

Введение

Постановка проблемы. Прогресс в технике и микроэлектронике привел к бурному развитию беспроводных цифровых коммуникаций.

Беспроводные сети передачи данных обеспечивают гибкость архитектуры, возможность динамического изменения топологии, высокую скорость передачи данных, быстроту проектирования и развертывания. Эти преимущества делают их важнейшим направлением развития цифровых коммуникаций. Особое внимание следует уделить вопросам обеспечения требуемого уровня защищенности систем мобильной связи, так как для перехвата сигнала в радиоканале злоумышленнику достаточно иметь комплект оборудования, аналогичный комплекту абонента сети.

Цель статьи: провести анализ существующих методов обеспечения безопасности в сетях 4G.

Изложение основного материала

Особенности радио интерфейса технологии LTE. Технология LTE применятся в диапазоне частот от 2,5 до 2,7 ГГц с шириной полосы пропускания от 1,4 до 20 МГц, что позволит объединить операторов связи, обладающих различными полосами пропускания. Скорость передачи данных для соединения Downlink (от базовой станции к абоненту) достигнет придела до 326,4 Мбит/с, а для Uplink (от абонента к базовой станции) до 172,8 Мбит/с.

Радиус действия базовой станции (БС) LTE составляет 5 км, но при необходимости может достигать 30 км, а случае возникновения необходимости, и до 100 км, при достаточном поднятии антенны [1].

При этом оборудование LTE позволит одновременно поддерживать не менее 200 активных соединений на каждую 5-МГц ячейку. А также появится возможность поддержки соединений для абонентов, движущихся со скоростью до 350км/ч.

Время отклика между оборудованием пользователя и БС сокращенно до 10 мс, а время перехода из неактивного состояния в активное доведено до 100 мс.

Звонок или сеанс передачи данных, инициированный в зоне покрытия LTE, технически может быть передан без разрыва в сеть 3G.

LTE базируется на трех основных технологиях: мультиплексирование посредством ортогональных несущих OFDM, многоантенные системы MIMO и эволюционная системная архитектура сети[2].

Принципы построения радиоинтерфейса по технологии LTE. В LTE-системах используют адаптивные антенные решётки со слабо коррелированными антенными элементами, именуемыми технологией MIMO. Данная технология повышает помехозащищенность, уменьшает вероятность битовой ошибки BER, увеличивает пропускную способность системы, а также дальность передачи информации, за счет расширения полосы частот или увеличения излучаемой мощности.

В LTE схема канального кодирования, предшествующего обработке MIMO, параллельная. При параллельной схеме входные данные демультиплексируются на два потока, каждый из которых в отдельности подвергается помехоустойчивому кодированию. Закодированные потоки подаются в схему MIMO. На приемной стороне осуществляются обратные операции, после снятия помехоустойчивого кода в обеих ветвях декодированные данные подаются обратно в приемник – обработчик MIMO. Этот алгоритм называется алгоритмом последовательного исключения демодулированнных компонент SIC (Successive Interference Cancellation) [3].

Для синхронизации в технологии MIMO с OFDM используют метод пилотных сигналов (поднесущих).

Для борьбы с затуханием в канале и для повышения скорости передачи данных при малой BER используется мультиплексирование с ортогональным частотным разделением каналов OFDM. Этот метод позволяет бороться с частотно-селективными замираниями и с межсимвольной интерференцией за счет выделения абонентам частотно-временных

ресурсных блоков. Для обеспечения передачи информации большому количеству пользователей в диапазоне одного радиоспектра для нисходящего канала используют технологию OFDMA на основе технологии OFDM. Под OFDMA понимается множественный доступ с ортогональным частотным разделением, при котором приписываются наборы поднесущих отдельным пользователям, тем самым позволяя одновременную низкоскоростную передачу данных для нескольких абонентов. OFDMA-символ включает собственно зону передачи данных и предшествующий ему защитный интервал. Сам символ – это совокупность модулированных ортогональных несущих [4].

Для восходящего канала в LTE используется технология SC-FDMA (Single-Carrier Frequency-Division Multiple Access), в которой поднесущие модулируются одновременно и одинаково, но модуляционные символы короче. То есть символы передаются последовательно. Такое решение обеспечивает меньшее отношение максимального и среднего уровней мощности, в результате чего повышается энергоэффективность абонентских устройств и упрощается их конструкция [5].

Каждая поднесущая модулируется квадратурной фазовой модуляцией QPSK иди одним из видов квадратурной амплитудной модуляцией 16QAM и 64QAM. Четыре фазовых состояния QPSK позволяют одним символом передавать два бита, 16QAM четыре бита, а 64QAM – шесть бит в одном символе [6].

Для защиты от ошибок, которые могут быть вызваны замиранием сигнала, шумами и помехами, применяются методы повторной передачи искаженных или утраченных частей данных. Для этого в технологии LTE реализована динамическая эффективная двухуровневая система повторной передачи, реализующая протокол HARQ (Hybrid Automatic Repeat Query), который дополнен высоконадежным протоколом селективного повтора ARQ.

Протокол HARQ предоставляет приемному устройству избыточную информацию, дающую ему возможность исправлять определенную часть ошибок. Повторные передачи по протоколу HARQ создают дополнительную информационную избыточность, нужную в том случае, если для устранения ошибок первой передачи оказалось недостаточно. Повторная передача пакетов осуществляется посредством протокола ARQ. Данное решение обеспечивает малую задержку передачи пакетов.

Кроме того, каждая БС в технологии LTE контролирует уровень помех от соседних сот. Периодически между БС происходит обмен индикаторами перегрузки OI (Overload Indicator), который указывает, в каком ресурсном блоке уровень помех превышает пороговое значение. Индикатор OI формируется по результатам измерения БС уровней помех и фонового шума для каждого частотного блока в соте [3].

Защита данных в системах LTE. В системах LTE используются механизмы безопасности для сетей 3G, которые позволяют обеспечить аутентификацию абонентов, конфиденциальность пользовательских данных, а также конфиденциальность данных при их передаче по протоколам U-Plane (пользовательские данные) и C-Plane (управляющие), а также комплексную защиту протокола C-Plane при его совместном использовании с другими международными стандартами обмена. Для аутентификации применятся процедура аутентификации и согласования ключей AKA (Authentication and Key Agreement). БС осуществляют хранение ключа шифрования только на период сеанса связи с мобильным терминалом. Алгоритмы шифрования и обеспечения комплексной безопасности основываются на технологии Snow 3G и стандарте AES. Планируется использовать еще два дополнительных алгоритма, на случай если один из алгоритмов будет взломан, оставшиеся должны обеспечить безопасность сети LTE. В настоящее время для проверки целостности данных и шифрования алгоритмы, используемые в LTE, имеют 128-битные ключи. Но существует возможность использования 256-битных ключей. В качестве алгоритмов шифрования используются следующие:

- 128-EEA1 основанный на алгоритме Snow 3G. В точности повторяет алгоритм UEA2, специфицированный для сетей UMTS;
- 128-EEA2 основанный на алгоритме AES.

Для проверки целостности данных, спецификации предлагают следующие алгоритмы:

- 128-EIA1 основанный на алгоритме Snow 3G. В точности повторяет алгоритм UIA2, специфицированный для сетей UMTS;
- 128-EIA2 основанный на алгоритме AES.

Для закрытия данных в сетях LTE используется потоковое шифрование методом наложения на открытую информацию псевдослучайной последовательности с помощью оператора «исключающее или».

Так же, как и в сетях третьего поколения, приложение USIM и Центр аутентификации (AuC) осуществляет предварительное распределение ключей (ключа K). Когда механизм AKA инициализируется для осуществления двусторонней аутентификации пользователя и сети, генерируются ключ шифрования CK и ключ общей защиты, которые затем передаются из программного обеспечения USIM в Мобильное оборудование (ME) и из Центра аутентификации в Центр регистрации (HSS).

Мобильное оборудование и Центр регистрации, используя ключевую пару (CK;IK) и ID используемой сети, вырабатывает ключ KASME. Устанавливая зависимость ключа от ID сети, Центр регистрации гарантирует возможность использования ключа только в рамках этой сети. Далее KASME передается из Центра регистрации в устройство мобильного управления (MME) текущей сети, где используется в качестве базовой информации ключевой иерархии.

На основании KASME вырабатывается ключ KNASenc, необходимый для шифрования данных протокола NAS между мобильным устройством и устройством мобильного управления (MME), и ключ KNASint, необходимый для защиты целостности. Когда мобильное устройство подключается к сети, MME генерирует ключ KeNB и передает его базовым станциям. В свою очередь, из ключа KeNB вырабатывается ключ KUPenc, используемый для шифрования пользовательских данных протокола U-Plane, ключ KRRCenc для протокола RRC (Radio Resource Control – протокол взаимодействия между Мобильными устройствами и базовыми станциями) и ключ KRRClint, предназначенный для защиты целостности [7].

Чтобы свести к минимуму подверженность атакам, БС должна обеспечивать безопасную среду, которая гарантирует выполнение операций, шифрования и расшифрования пользовательских данных, хранения ключей. Поэтому меры противодействия разработаны специально для минимизации вреда, наносимого в случае кражи ключевой информации из БС:

- проверка целостности устройства;
- взаимная аутентификация БС оператора (выдача сертификатов);
- безопасные обновления;
- механизм контроля доступа;
- синхронизация времени;
- фильтрация трафика [8].

Поскольку в случае проведения успешной атаки на БС злоумышленник получит контроль над ресурсами БС и доступ ко всем конфиденциальным данным.

Взаимодействие БС и опорной сети основывается на протоколах IPsec и IKE. Сильные криптографические методы обеспечивают защиту типа точка-точка для соединения между опорной сетью и пользовательским устройством.

В LTE сохраняются и методы аутентификации пользователей по привязке к карте USIM, как в традиционной мобильной связи: пользователь может заблокировать доступ к телефону по PIN-коду.

Выводы

В работе проанализированы современные методы и средства обеспечения требуемого уровня защиты данных при передаче по беспроводному каналу.

Дальнейшим шагом для улучшения защищенности LTE - систем является расчет оптимального изменения вносимых сопротивлений в зависимости от шага (d) при различных топологиях антенных решеток MIMO.

Список литературы

1. Гордиенко С.Б. Технология LTE - возможность создания широко-полосных высокоскоростных сетей мобильной связи / С.Б. Гордиенко, С.С. Гордиенко, В.В. Олейник // Зв'язок. – 2010. – №3. – С. 22-24.

2. Тихвинский В.О. Сети мобильной связи LTE: технологии и архитектура / В.О. Тихвинский, С.В. Терентьев. – М.: Эко-Трендз, 2010. – 284 с.

3. Варукина Л.А. Радиодоступ LTE: еще один аргумент в пользу революции / Л.А. Варукина // Вестник связи. – 2010. – № 2. – С. 34-37.

4. Технология OFDM [Электронный ресурс]. – Режим доступа к ресурсу: www/ URL: http://bwa.lgp.kz/ofdm.php – 13.04.14 г. – Загл. с экрана.

5. Основные характеристики LTE [Электронный ресурс] – Режим доступа к ресурсу: www/ URL: http://habrahabr.ru/post/114401 – 09.05.14 – Загл. с экрана.

6. Гепко И.А. Современные беспроводные сети: состояние и перспективы развития: учебник для студентов вузов [Текст] / И.А. Гепко, В.Ф. Олейник, Ю.Д. Чайка, А.В. Бондаренко. – К.: «Экмо», 2009 – 672 с.

7. Особенности обеспечения ИБ в сетях LTE [Электронный ресурс]. – Режим доступа к ресурсу: www/ URL:http://www.rusnauka.com/12_KPSN_2014/Informatica/4_166376.doc.htm - 04.05.14 – Загл. с экрана

8. Защита данных в LTE – системах [Электронный ресурс]. – Режим доступа к ресурсу: www/ URL:http://ru.wikipedia.org/wiki/Архитектура_системы_безопасности_в_сетях_LTE - 05.05.14 – Загл. с экрана

Поступила в редколлегию 15.05.2014

Рецензент: д-р техн. наук, проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ В LTE-СИСТЕМАХ

Т.В. Лавровська

У статті представлені основні етапи розвитку і модернізації безпровідних мереж стандарту LTE. Розглянуті основні характеристики радіоінтерфейсу, з вказівкою технологій, вживаних для збільшення пропускної спроможності системи і підвищення швидкості передачі даних. Оскільки головним завданням технології LTE є забезпечення необхідного рівня захисту інформації, передаваної по безпровідному каналу, тому особлива увага в роботі приділена аналізу існуючих методів забезпечення безпеки в мережах 4G.

Ключові слова: *LTE-система, базова станція, OFDM, пропускна спроможність системи, перешкодозахист, технологія MIMO.*

AN ANALYSIS OF METHODS OF INCREASE OF PROTECTED IS IN LTE-SYSTEMS

T.V. Lavrovskaya

The basic stages of development and modernization of off-wire networks of standard of LTE are presented in the article. Basic descriptions of radiointerface are considered, with pointing of technologies, applied for the increase of carrying capacity of the system and rev-up communication of data. As a main task of technology of LTE is providing of the required level of priv, transferrable on an off-wire channel, therefore the special attention is in-process spared the analysis of existent methods of providing of safety in the networks of 4G.

Keywords: *LTE-system, base station, OFDM, carrying capacity of the system, interference immunity, technology of MIMO.*