БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ В СЕТЯХ 4G/LTE

Белянков Д. А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В. Ю. – д. т. н., доцент

В работе рассмотрена беспроводная технология 4G/LTE и проблемы, связанные с обеспечением ее безопасности и конфиденциальности.

За последние несколько десятилетий мобильные системы стали незаменимыми для выполнения пользователями своих повседневных задач. Это привело к быстрому развитию беспроводных технологий таких как 2G, 3G, 4G и 5G для мобильных сетей. Беспроводная технология 4G была изобретена для улучшения качества широкополосной связи и обеспечения возможности использования мультимедийных программ.

Существуют множество технологических достижений, которые обеспечивают беспроводные сети 4G/LTE по сравнению с более ранними технологиями. Во-первых, мобильные системы 4G/LTE отлично работают, используя модель TCP/IP. Это фактически снижает финансовые и вычислительные затраты, когда портативные устройства могут подключаться к интернету с использованием интернет-протокола (IP) без каких-либо ограничений для ранее закрытых сотовых конфигураций. Тем не менее, благодаря широкому разнообразию протоколов связи, включенных в модель TCP/IP, беспроводные сети 4G/LTE сталкиваются с множеством проблем безопасности и конфиденциальности.

Ключевые проблемы для обеспечения безопасности беспроводных сетей 4G/LTE можно обобщить в трех аспектах. Во-первых, мобильные устройства могут выходить в Интернет из любого места и поэтому уязвимы для взлома различными продвинутыми постоянными угрозами (APT). Во-вторых, хотя мобильные системы на базе IP регулярно обновляются с помощью криптографических механизмов и механизмов безопасности, это влияет на их производительность и пропускную способность обработки трафика, что требует безопасных и обновленных стандартов и архитектур беспроводной связи. И третье, хотя производители выпускают новые поколения технологий 4G/LTE, они не регулярно разрабатывают новые стандарты для смягчения уязвимостей и сдерживания роста кибер-угроз.

Международный союз электросвязи (ITU) объявил Международный стандарт усовершенствованной подвижной электросвязи (IMT-Advanced) для беспроводных сетей 4G. Беспроводная технология 4G включает следующие критерии: высокая скорость передачи данных, которая составляет 100 Мбит/с для мобильных устройств и 1 Гбит/с для компьютерных устройств, высокое качество обслуживания (QoS) и высокая скорость работы сети и ее покрытие.

Архитектура LTE включает в себя модули, необходимые для установки сетевых протоколов между базовыми станциями и мобильными системами. Архитектура включает в себя три модуля: пользовательское оборудование (UE), универсальная наземная сеть радиодоступа (E-UTRAN) и улучшенное пакетное ядро (EPC). Оборудование пользователя, например, ноутбуки или смартфоны, могут подключаться к беспроводной сети через развитый узел NodeB (eNodeB), используя базовые станции E-UTRAN. ENodeB использует некоторые сетевые протоколы доступа для обмена сообщениями с UE. E-UTRAN связывается с EPC, который является инфраструктурой на основе IP, в то время как EPC связывается с поставщиком проводной IP-сети.

Контроль безопасности 4G/LTE. Уровни абстракции вставляются в архитектуру 4G/LTE в виде уникальных идентификаторов (ID) для смартфонов (т. е. UE). Временный уникальный идентификатор используется на SIM-карте для предотвращения кражи идентификаторов злоумышленниками. Другим методом улучшения безопасности 4G является добавление защищенного выделения между UE и MME. Хотя для беспроводной технологии 4G/LTE используется несколько элементов управления безопасностью, ее дизайн, основанный на архитектуре с открытым IP-адресом, и изощренность хакеров APT затрудняют безопасность и конфиденциальность систем 4G/LTE.

Для обеспечения безопасности мобильных устройств, использующих беспроводные технологии 4G/LTE, должна быть обеспечена защита соединений между UE и MME, а также между элементами проводных сетей и мобильными станциями. Удовлетворения этих требований безопасности 4G/LTE можно добиться путем добавления расширенной иерархии ключей, длительной аутентификации и согласования ключей и дополнительной безопасности взаимодействия для сетевых элементов. Требования подразделяются на ключевые блоки и сквозную безопасность LTE.

Ключевые блоки включают в себя следующие элементы [1]:

- Ключ безопасности и иерархии. LTE имеет пять ключевых стратегий, используемых для соединений EPS и E-UTRAN. Ключи объявляются следующим образом: ключи шифрования и целостности KANS используются для защиты трафика без доступа (NAS) между UE и MME, шифрование KUP используется для шифрования трафика между UE и eNodeB и ключи шифрования и целостности KPRC используются для защиты управления радиоресурсами (RRC) между UE и eNodeB.

- Ключевой менеджмент. Управление ключами LTE включает в себя три функции: создание, распространение и генерация ключей. Важно, чтобы беспроводная технология 4G/LTE имела механизмы управления ключами, которые предотвращают кражу ключей, поскольку мобильные устройства с инфраструктурой на основе IP могут часто получать доступ к различным беспроводным сетям.

- Аутентификация, шифрование и защита целостности. LTE зависит от использования регулярного обновления процесса аутентификации путем обмена порядковыми номерами в сообщениях механизмов шифрования. Протокол IPsec и туннели также используются для обеспечения конфиденциальности данных пользователей при передаче трафика между узлами LTE.

- Уникальные идентификаторы пользователей. LTE имеет несколько механизмов идентификаторов пользователей, которые мешают злоумышленникам изучать идентификационные данные мобильных пользователей. Механизмы идентификаторов содержат следующее: международный идентификатор мобильного оборудования (IMEI), который является постоянным уникальным идентификатором для каждой мобильной станции, M-TMSI, который является временным идентификатором, который определяет UE внутри MME, и временный идентификатор сотовой радиосети (C-RNTI), который является уникальным и временным идентификатором UE.

Комплексная безопасность LTE включает в себя следующие элементы [2]:

- Соглашение об аутентификации и ключе (AKA). Основой безопасности LTE является аутентификация UE и беспроводных сетей. Это может быть достигнуто с использованием AKA процесса, который утверждает, что обслуживающая сеть аутентифицирует личность пользователя, а UE сертифицирует сетевую подпись. AKA создает ключи шифрования и целостности, применяемые для создания различных сеансовых ключей.

- Конфиденциальность и целостность сигнализации. Безопасность плоскостей управления сетевым доступом достигается, когда сигнализация уровня RCC и NAS зашифрована и защищена целостность. Защита шифрования и целостности сигнализации LTE RRC выполняется на уровне протокола конвергенции пакетных данных (PDCP), тогда как уровень NAS обеспечивает защиту путем шифрования сигнализации уровня NAS. Эта защита не может быть уникальным образом выполнена для каждого соединения UE, но она выполняется через доверенные соединения между AGW и eNodeB.

- Конфиденциальность плоскости пользователя. LTE имеет функцию безопасности для плоскости пользователя посредством шифрования данных / голоса между UE и eNodeB. Шифрование выполняется на уровне IP с использованием основанных на IPsec туннелей между AGW и eNodeB, но из-за соображений производительности и эффективности защита от проникновения на уровне пользователя не обеспечивается.

Кроме всего прочего беспроводная технология 4G/LTE сталкивается с различными типами кибератак, которые могут повлиять на целостность, конфиденциальность, доступность и аутентификацию: атаки против конфиденциальности данных мобильных пользователей пытаются раскрыть конфиденциальные данные / мультимедиа пользователей; атаки против целостности пытаются изменить обмен данными между точками доступа 4G и мобильными пользователями. Механизмы аутентификации и сохранения конфиденциальности с хэш-функциями широко используются для защиты беспроводных сетей 4G от атак целостности; атаки против аутентификации пытаются нарушить процесс аутентификации клиент-сервер и/или сервер-клиент; атаки на доступность пытаются сделать недоступными такие службы, как служба маршрутизации данных. Для защиты от этих атак обычно используются брандмауэры и системы обнаружения вторжений.

Несмотря на большое количество научно-технических исследований и разработок, которые были проведены для обеспечения безопасности беспроводных сетей 4G / LTE, существует несколько проблем, которые должны быть в центре внимания исследователей, а именно: разработка гибкой и масштабируемой архитектуры 4G/LTE, которая может решать проблемы безопасности, так как существует множество устройств и систем, которые обычно связаны с сетями 4G, что приводит к уязвимостям и лазейкам в сетях; обнаружение DoS-атак, которые пытаются нарушить беспроводные сети 4G, поскольку хакеры часто создают новые сложные варианты против eNodeB, UE и прерывистых служб приема; отслеживание местоположения означает отслеживание присутствия UE в определенной ячейке; существуют технические пробелы в вопросах масштабируемости сети, безопасности и конфиденциальности с помощью SDN.

Список использованных источников:0

1 Mohapatra SK, Swain BR, Das P Comprehensive survey of possible security issues on 4G networks. I0nt J Netw Secur Appl.2015. – 62.

2. Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Jan-icke H Security for 4G and 5G cellular net-works: a survey of existing authentication and privacy-preserving schemes. J Netw Comput Appl. 2017. – 55–82.