pISSN 2073-2872
eISSN 2311-875X

АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ LTE-A ОТ НАПРАВЛЕННОГО ВОЗДЕЙСТВИЯ DoS-АТАК

Никита Вячеславович КОРМИЛЬЦЕВ [a,•], Александр Дмитриевич УВАРОВ [b], Ильдар Ильнатович ХАМАТНУРОВ [c], Марина Владимировна ТУМБИНСКАЯ [d]

[a] студент Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ, Казань, Российская Федерация
kormiltcev@hotmail.com
https://orcid.org/0000-0002-2289-5672
SPIN-код: 1580-1482

[b] студент Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ, Казань, Российская Федерация
obg-96@mail.ru
https://orcid.org/0000-0003-0337-2689
SPIN-код: 7184-4498

[c] студент Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ, Казань, Российская Федерация
ildarka96@mail.ru
https://orcid.org/0000-0002-4853-6774
SPIN-код: 2986-2610

[d] кандидат технических наук, доцент, Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация
tumbinskaya@inbox.ru
ORCID: отсутствует
SPIN-код: 4414-9302

[•] Ответственный автор

История статьи:
Получена 30.11.2018
Получена в доработанном виде 20.12.2018
Одобрена 11.01.2019
Доступна онлайн 15.02.2019

УДК 004.056
JEL: C63, M15

Ключевые слова:
LTE-A, информационная безопасность, обновление зоны отслеживания, DoS-атака

Аннотация

Предмет. LTE Advanced – стандарт мобильной связи, переживший целый ряд этапов развития, предусматривающий расширение полосы частот, агрегацию спектра и имеющий расширенные возможности многоантенной передачи данных MIMO с поддержкой ретрансляции сигнала.

Цели. Поиск и анализ уязвимостей в системе безопасности LTE Advanced, которая является современной коммуникационной системой, однако привлекает внимание злоумышленников, применяющих, в частности, такой вид телекоммуникационного воздействия, как DoS-атаки.

Методология. В работе рассматривается спецификация доступа Network Attached Storage в Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) с приведением описания двух выявленных уязвимостей протокола к DoS-атаке, построенной на процедуре обновления зон отслеживания (TAU).

Результаты. Проведен анализ некоторых уязвимостей в процедурах E-UTRAN и TAU. Выявлена причина отказа в обслуживании сигнализации «TRACKINGAREAUPDATEREJECT».

Выводы. Несмотря на то что LTE-A предоставляет некоторые механизмы для повышения безопасности мобильной системы связи, на практике нами была выявлена незащищенная передача сообщений для запуска DoS-атак и доказано существование дефектов в системе безопасности системы. Для их устранения предложено использовать таймер восстановления системы, отсоединяющий мобильные станции от сети с сообщением отклонения TAU в течение длительного периода заданного времени, после чего мобильные станции имеют возможность снова подключиться к сети, не беспокоя при этом остальных пользователей.

Для цитирования: Кормильцев Н.В., Уваров А.Д., Хаматнуров И.И., Тумбинская М.В. Анализ защищенности системы безопасности LTE-A от направленного воздействия DoS-атак // Национальные интересы: приоритеты и безопасность. – 2019. – Т. 15, № 2. – С. 376 – 392.
https://doi.org/10.24891/ni.15.2.376

Введение

В связи с растущим спросом на высокоскоростную передачу данных и отказоустойчивость сетей сотовой связи консорциум 3GPP приступил к улучшению стандарта Long Term Evolution (LTE), создав его новую версию – LTE-A [1]. Данный стандарт является отличным дополнением к сети радиодоступа (RAN), а также к сотовой базовой сети, движущейся в направлении всей системы IP-протоколирования. При помощи LTE-A передача голосовых и пакетных данных происходит не только между пользователями, но и между машинами – при помощи технологии Internet of Things (IoT)[1]. По данным журнала Gartner, к 2020 г. на IoT будет создано более 26 млрд устройств. Именно поэтому любое влияние на систему безопасности LTE-A может привести к серьезным последствиям, затрагивающим большое количество устройств [2–10]. Согласно уже проведенным исследованиям, мобильные телефоны продолжают оставаться уязвимыми для многих видов атак. В частности, было выявлено, что в сети 2G имеется ряд серьезных уязвимостей – таких как отсутствие взаимной аутентификации, которая позволяет атаковать пользователей, используя поддельные базовые станции и слабый алгоритм шифрования [11–14].

Несмотря на то что алгоритмы шифрования и аутентификации в протоколе LTE-A были существенно улучшены, данный протокол остается уязвимым для злоумышленников. По нашему мнению, у этого протокола также существует несколько потенциальных угроз безопасности. В частности, это фемтосоты, которые быстро становятся популярным и недорогим решением для расширения охвата мобильных систем, но их незаконное развертывание может серьезно повлиять на мобильные устройства, находящиеся в пределах их зоны покрытия.

В этой работе мы сфокусируемся на атаке мобильного устройства. Кроме того, посредством тщательного анализа спецификаций протокола сетевого доступа LTE-A[2], будут продемонстрированы две новые DoS-атаки на пользовательское оборудование (UE) [15]. Смоделированная нами атака будет основана на воздушном интерфейсе: сначала мы проанализируем безопасность процедуры обновления зоны отслеживания (TAU), затем, построив сценарии атаки, с помощью симулятора eNodeB и фактического UE получим соответствующие результаты атаки. Настоящая статья построена следующим образом: в ее начале мы рассмотрим сетевую архитектуру LTE-A, далее проведем анализ безопасности процедур TAU и возможности DoS-атаки на UE, после чего будет проведена практическая проверка, а в заключение будут представлены результаты и выводы.

Теоретические данные

Сетевая архитектура LTE-A. Как показано на *рис. 1*, сеть LTE-A состоит из Evolved Packet Core (EPC) и E-UTRAN [16]. EPC представляет собой сеть общего IP-интерфейса и включает в себя как объект управления мобильностью (MME), так и обслуживающий шлюз (SGW). E-UTRAN же состоит из сети базовых станций Evolved Universal Terrestrial Radio Access Network с сокращенным названием eNodeB (eNB), которые имеют прямую связь с UE. Стоит отметить, что сеть доступа для подключения

[1] *Зайцева И.Н., Гришаев В.Н.* Вопросы обеспечения безопасности в сети LTE при воздействии преднамеренных помех // Центральный научный вестник. 2017. № 17. С. 9–10; *Зубик С.А.* Анализ построения сети LTE // Точная наука. 2016. № 1. С. 8–10; *Жиба Г.В., Писаренко В.П., Захаров И.С., Шевцов А.Н.* Анализ помехоустойчивости каналов связи LTE и WIMAX // Транспорт Азиатско-Тихоокеанского региона. 2017. № 3. С. 17–21.

[2] *Константинов А.С., Дингес С.И.* Анализ программно-аппаратных средств тестирования абонентского радиооборудования сети LTE // Фундаментальные проблемы радиоэлектронного приборостроения. 2015. № 5. С. 22–24.

использует интерфейс S1, а eNodeB – интерфейс X2.

На *рис. 2* показан стек протоколов управления. В E-UTRAN канальный и физический уровни обеспечивают функцию передачи данных сообщений протокола радиоресурса (RRC) посредством сигналов NAS. В данной статье мы рассмотрим NAS и RRC, а также сигналы плоскости управления.

Связанные технические термины. В основном мы будем анализировать безопасность процедур TAU, а следующие приведенные термины будут использоваться на протяжении всего исследования.

Область отслеживания (TA) определяется как область, в которой пользователь может свободно перемещаться без обновления MME, ее основная функция заключается в управлении и представлении местоположений UE [17]. *Список зон отслеживания* (TAL) представляет собой схему, где UE получает список TA из ячейки и сохраняет его до тех пор, пока он не переместится в другую соту, не входящую в этот список. TAI – это идентификатор, который построен из кода мобильного телефона (MCC), кода мобильной сети (MNC) и кода зоны отслеживания (TAC). *Обновление зоны отслеживания* (TAU) информирует EPC о появлении в зоне доступности мобильного телефона. EPC способен управлять TA, в которых зарегистрированные UE находятся в состоянии ожидания и соединения [18].

Анализ уязвимости TAU

Согласно 3GPP TS 24.301, автономное обновление зоны отслеживания происходит, когда UE выполняет такие действия, как вхождение в новую зону TA, истечение срока действия периодического таймера обновления TA, переход в состояние UTRAN PMM-Connected или GPRS READY, при котором происходит повторный выбор EUTRAN и т.д. (*рис. 3*). Наиболее простой и распространенной атакой на LTE-A является DoS-атака с использованием симулятора eNodeB, которая и будет подробно изучена в данной статье.

Для начала необходимо рассмотреть процедуры обновления зон отслеживания. После присоединения к EPC UE переходит в состояние ожидания, в это время происходит процесс инициализации TAU и завершение соединения RCC. В этот самый момент и может происходить DoS-атака, которая состоит из шести последовательных шагов.

1. UE вводит новую TA, которая не входит в список TAI, завершая процедуру RRC и начиная процедуру TAU.

2. UE инициирует процедуру TAU, отправив сообщение запроса TAU вместе с параметрами RRC, указывающими выбранную сеть и старую глобально уникальную идентификацию MME (GUMMEI) в eNodeB.

3. eNodeB получает адрес MME из параметров RRC, также содержащих старый GUMMEI, идентификатор выбранной сети и RAT. Если данный MME не связан с eNodeB или GUMMEI недоступен, а UE указывает, что процедура TAU была вызвана перебалансировкой нагрузки, eNodeB начинает производить выбор нового MME.

4. Новая MME инициализирует тип старого узла, используя временную идентификацию UE (GUTI), полученную от самого UE, и отправляет сообщение с запросом контекста на старый MME для извлечения информации пользователя.

5. Если данный контекстный запрос отправляется на старую MME, то старая MME отвечает сообщением об ответе.

6. Если проверка целостности сообщения запроса TAU (в шаге 2) была нарушена, то аутентификация является обязательной.

После этого необходимо провести анализ уязвимостей и построение возможных сценариев атак. Благодаря использованию взаимной аутентификации на шаге 6 UE имеет возможность распознать поддельную базовую

станцию, поэтому единственной возможной атакой остается выдача сообщений об анормальном сигнале перед этапом аутентификации.

Сценарий предложенной атаки построен на первом условии запуска TAU, то есть поддельная базовая станция не находится в списке TAI UE, что позволяет начать процедуру TAU после того, как UE войдет в диапазон влияния поддельной eNodeB. В данном случае поддельная базовая станция может намеренно управлять сообщением отклонения TAU.

Содержимое сообщения TAU Reject показано на *рис. 4*, а детали основания EMM представлены в *табл. 1*. В EMM может быть задана такая причина отклонения, как № 8 (00001000); это означает, что услуги EPS (*Evolved Packet System*) и услуги non-EPS недоступны из-за отсутствия шифрования в передаче сообщений, после чего UE сразу обновит статус EU3 на «Недоступный роуминг». На этом этапе UE больше не будет пытаться получить доступ к нормальной сети LTE, 3G, GSM и продолжит оставаться в состоянии EMM-DEREGISTERED, то есть под длительным воздействием DoS-атаки.

Более того, в EMM также может быть задана причина отклонения № 7 (00000111) (услуги EPS не разрешены) – как показано в *табл. 1*, тогда UE сменит сеть 4G на уязвимую 2G.

Проверка и результаты исследования

В этом разделе будут приведены полученные результаты смоделированной атаки с использованием ПО Testing and Test Control Notation version 3 (TTCN-3) и программного кода для реализации указанного процесса. Согласно 3GPP TS 27.007 и проведенному анализу, необходимо использовать следующий алгоритм для проверки (*рис. 5*).

При завершении подготовки теста для проверки DoS-атак сначала необходимо создать компонент параллельного тестирования EUTRA_PTC и определиться с основной частью тестовой атаки. Затем необходимо вызвать функцию f_MTC_ConnectPTCs_LTEA_IRAT () для создания тестового компонента NASEMU_PTC, после чего соединить карту интерфейсов в каждом тестовом компоненте и реализовать связь между модулями MTC и PTC. Далее необходимо запустить тестовый компонент NASEMU_PTC для выполнения процедур DoS-атаки и вызвать функцию f_MTC_MainLoop (). Наконец, EUTRA_PTC завершает поведение тестовой DoS-атаки.

Далее описана авторская аппаратная и программная среда для тестирования и проверки. На *рис. 6* и *7* показана среда аппаратного соединения, управление которой осуществляется компьютерной системой (SP8380), производящей к тому же управление работой оборудования, самодиагностику системы, выполнение тестовых наборов TTCN-3. Заметим, что SP8300C – это многомодовый симулятор системы, каждый из SP8300C может поддерживать одну или две ячейки LTE/GSM.

Конфигурация IP-адресов аппаратных средств, а также основной список программного обеспечения системы приведены в *табл. 2* и *3*.

TS Manager, Log Tracer и UE Controller работают на главном сервере SP8380 с программным обеспечением SP8300C. Исполняемые файлы тестового набора третьего уровня TTCN-3 интегрированы в программное обеспечение диспетчера TS. TS Manager обладает удобным интерфейсом для управления выполнением тестов, а также выводом журналов в режиме реального времени в виде простых и понятных результатов. Интерфейс диспетчера TS содержит панель меню, панель быстрого доступа, набор тестов и окно плана тестирования, окно тестового окна, окно вывода, окно MSC, окно информации сигнализации.

После запуска диспетчера TS и подключения инструментов и конфигурации тестовых наборов мы можем использовать набор тестовых примеров TS Manager.

На *рис. 8* показан интерфейс DoS-атаки в сети 4G. MSC представлен в виде диаграммы последовательности сообщений, описанных формальным языком, используемым для описания порядка, в котором происходит взаимодействие между объектами и средой. В данном случае причина отказа осуществляется в «TRACKINGAREAUPDATEREJECT» сигнализации в значении 0000-0111B, как указано в *табл. 1*. Следует иметь в виду, что UE удаляется из сети 4G после атаки и может получить доступ только к сетям 3G или GSM. Кроме того, мобильный телефон будет оставаться в этом состоянии до перезапуска или даже придется повторно подключить SIM-карту для восстановления после атаки.

На *рис. 9* приведен результат выполнения тестовой DoS-атаки, отклоняющей всю стандартную сеть. Видно, что причина отказа от соты, содержащегося в сигнале «TRACKINGAREAUPDATEREJECT», составляет 00001000B, как упоминалось ранее. Сравнение эффекта атаки на UE показано на *рис. 10*. Видно, что UE исключается из сети стандартов со всех стандартов после атаки, включая сеть 4G, 3G и GSM. Как и в предыдущем случае, мобильный телефон будет оставаться в этом состоянии до перезапуска или даже будет необходимо повторно подключить SIM-карту для восстановления после атаки.

После проведенной проверки ясно, что фактические результаты системы и теоретический анализ являются последовательными. Что касается антиаварийных схем, то пользователи могут перезагрузить или повторно подключить SIM-карту для восстановления системы после атаки. По нашему мнению, относительно простым решением для предотвращения данной проблемы в будущем может стать использование таймера для восстановления системы после DoS-атак. В этом случае отсоединение UE от сети в течение длительного времени из-за сообщения отклонения TAU будет происходить до тех пор, пока заданное таймером время не истечет, после чего UE может снова подключиться к сети, не беспокоя об этом пользователей.

Таблица 1
Элемент эксплуатации EMM

Table 1
The component for running the Enterprise Mobility Management (EMM)

Наименование элемента	Содержание элемента
0 0 0 0 0 0 1 0	IMSI не известен в информационном элементе HSS
0 0 0 0 0 0 1 1	Незаконное UE
0 0 0 0 0 1 0 1	IMEI не принимается
0 0 0 0 0 1 1 0	Незаконный ME
0 0 0 0 0 1 1 1	Услуги EPS не разрешены
0 0 0 0 1 0 0 0	Услуги EPS и услуги, не связанные с EPS
0 0 0 0 1 0 0 1	UE не может идентифицироваться в сети

Источник: авторская разработка

Source: Authoring

Таблица 2
Стационарное оборудование

Table 2
Fixed equipment

Аппаратные средства	**IP-адрес**
SP8300C-1	10.0.0.1
SP8300C-2	10.0.0.2
SP8380 server	10.0.0.3

Источник: авторская разработка

Source: Authoring

Таблица 3
Список программного обеспечения системы

Table 3
The system software list

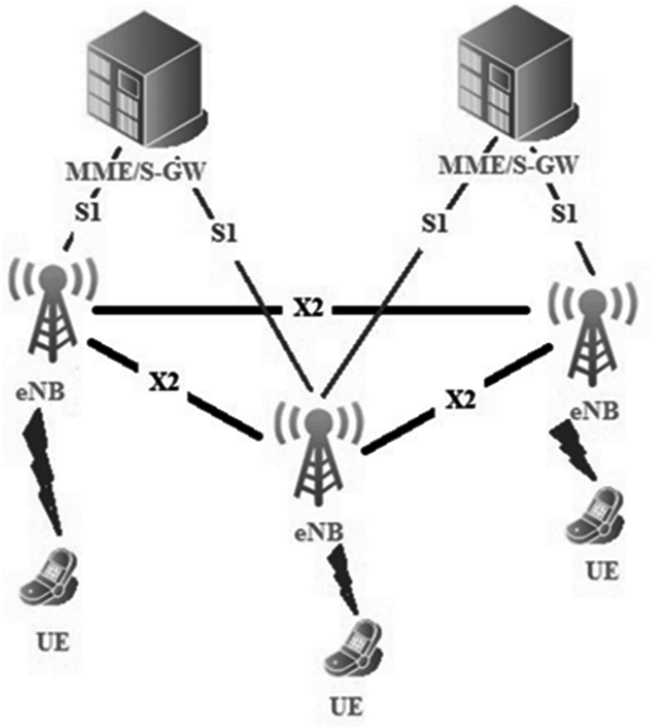
Программное обеспечение	**Описание**
TS Manager	Интерфейс взаимодействия, используемый для управления исследуемой системой и выполнения тестовых примеров
Test Case Software	ПО для выполнения сценариев возможных DoS-атак
UE Controller	Имитация мобильной станции
SP8300C	Имитация сот сотовой связи стандарта LTE/GSM
Log Tracer	ПО для ведения и хранение журнала событий в режиме реального времени

Источник: авторская разработка

Source: Authoring

Рисунок 1
Сетевая архитектура LTE-A

Figure 1
Network architecture of LTE Advanced

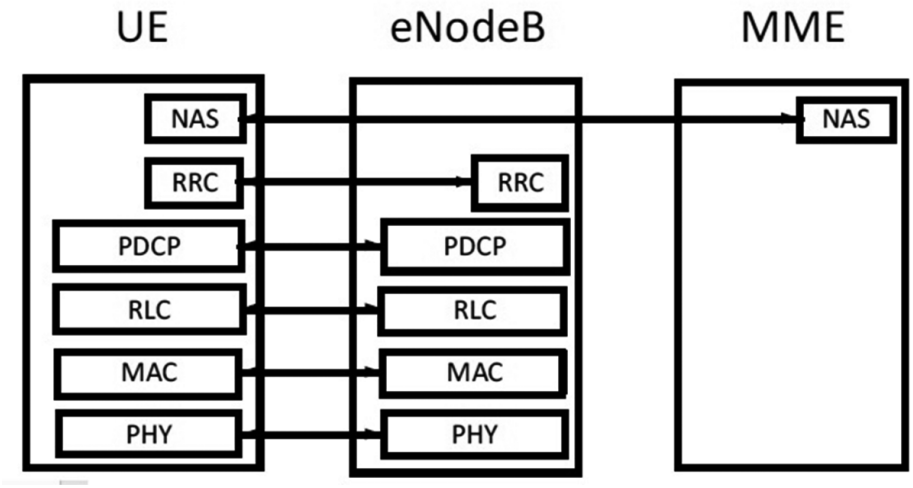


Источник: авторская разработка

Source: Authoring

Рисунок 2
Протоколы контроля целостности и управления

Figure 2
Integrity control and management protocols

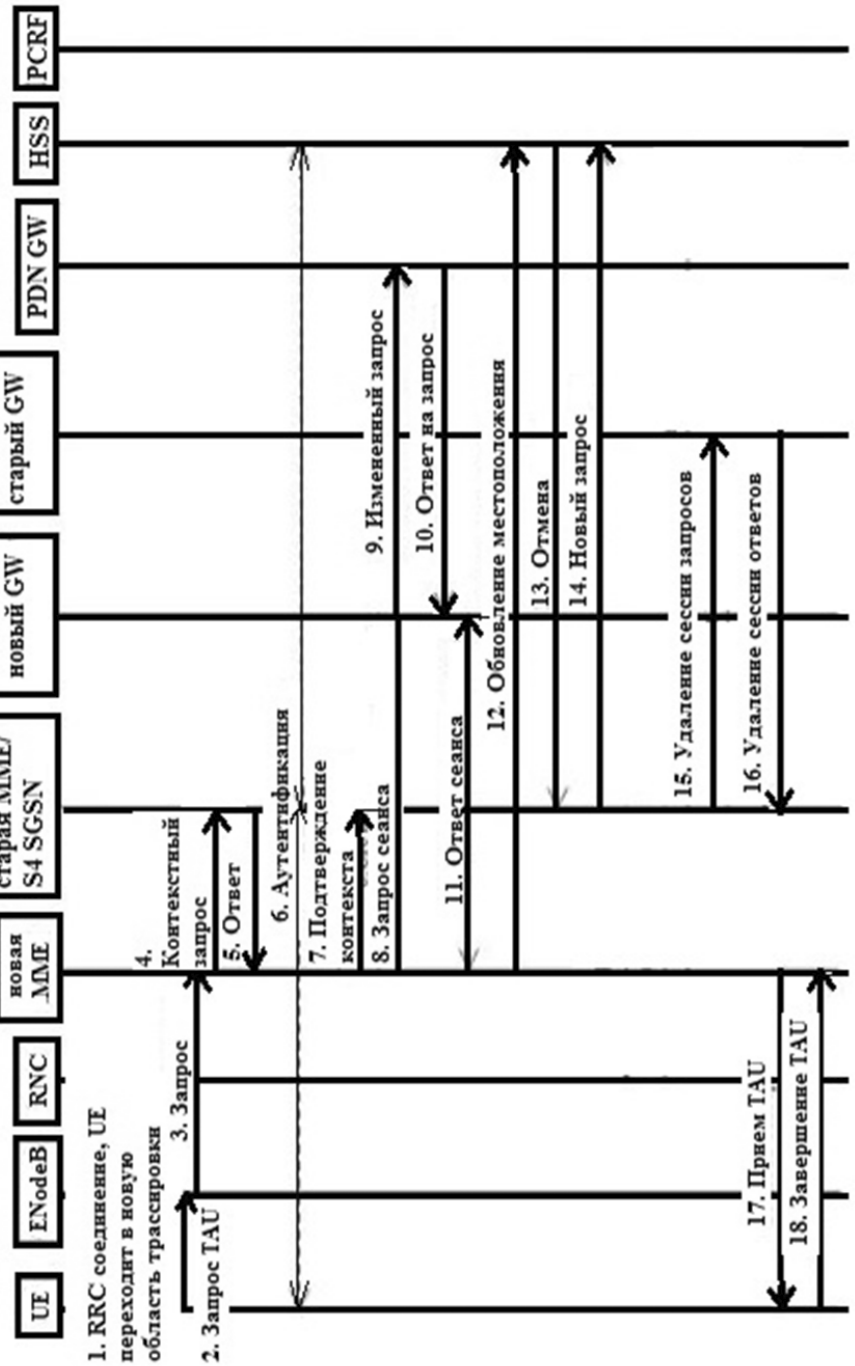


Источник: авторская разработка

Source: Authoring

Рисунок 3
Процедуры TAU

Figure 3
Tracking Area Update procedures



Источник: авторская разработка

Source: Authoring

Рисунок 4
Содержание сообщений

Figure 4
The content of messages

Информационный элемент
Протокольный дискриминатор
Тип заголовка безопасности
Отклонение зоны отслеживания
Идентификатор сообщения
EMM
Значение T3346
Расширенная EMM

Источник: авторская разработка

Source: Authoring

Рисунок 5
Алгоритм процесса атаки

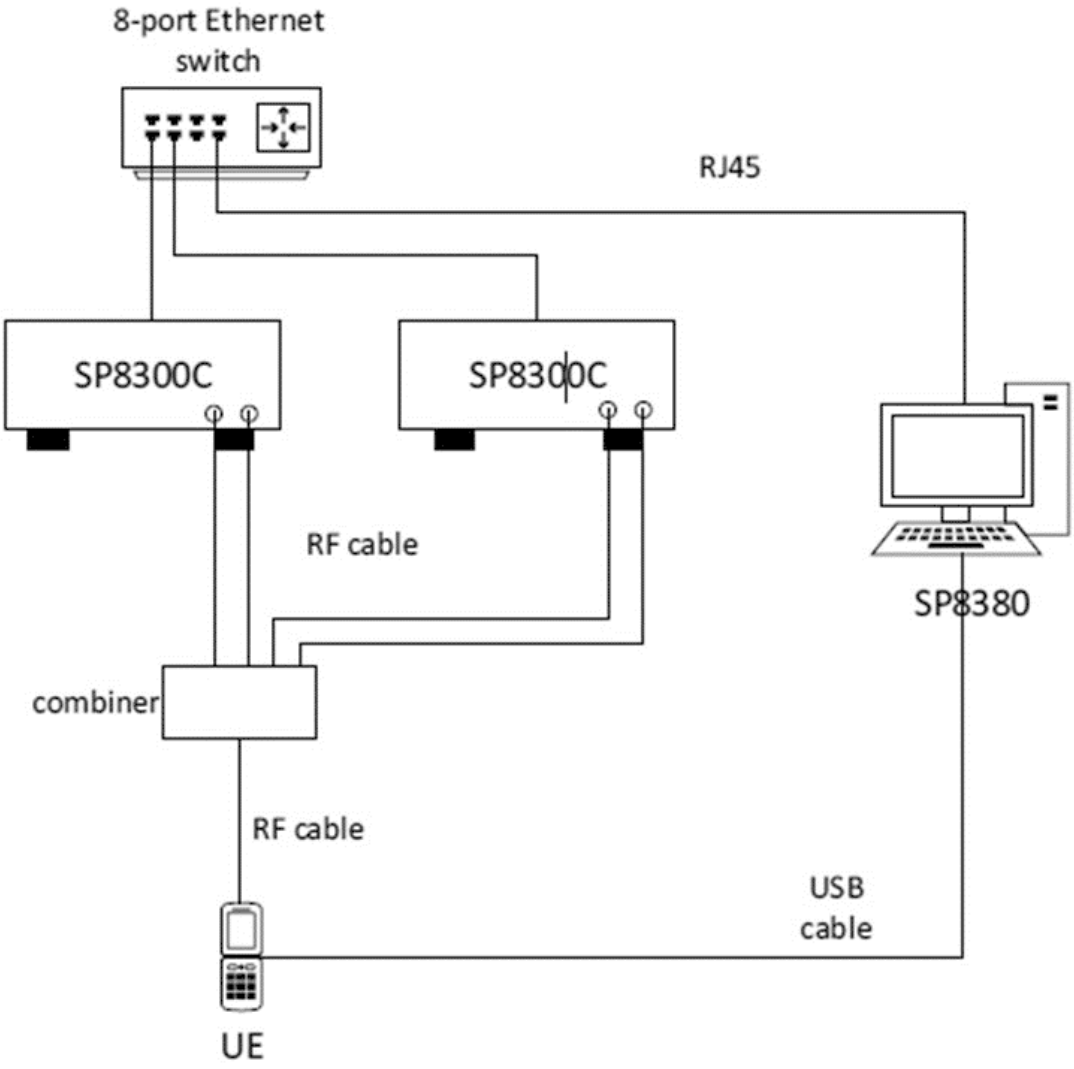
Figure 5
The attack algorithm

Источник: авторская разработка

Source: Authoring

Рисунок 6
Схема подключения оборудования

Figure 6
Equipment connection layout

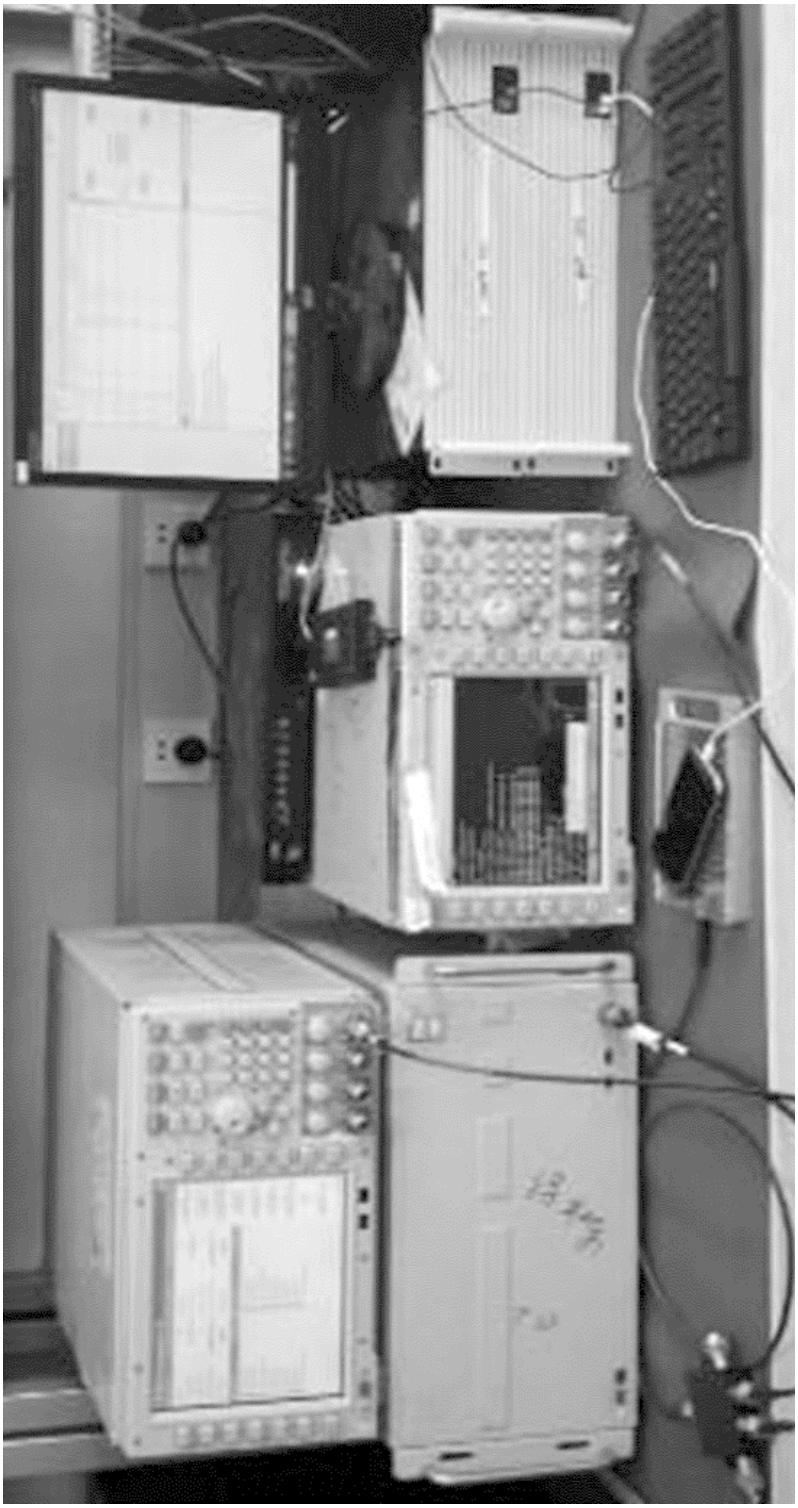


Источник: авторская разработка

Source: Authoring

Рисунок 7
Тестовая среда

Figure 7
The test environment



Источник: авторская разработка

Source: Authoring

Рисунок 8
Выходной сигнал 4G

Figure 8
4G output signal

Источник: авторская разработка

Source: Authoring

Рисунок 9
Результат отключения всех случаев

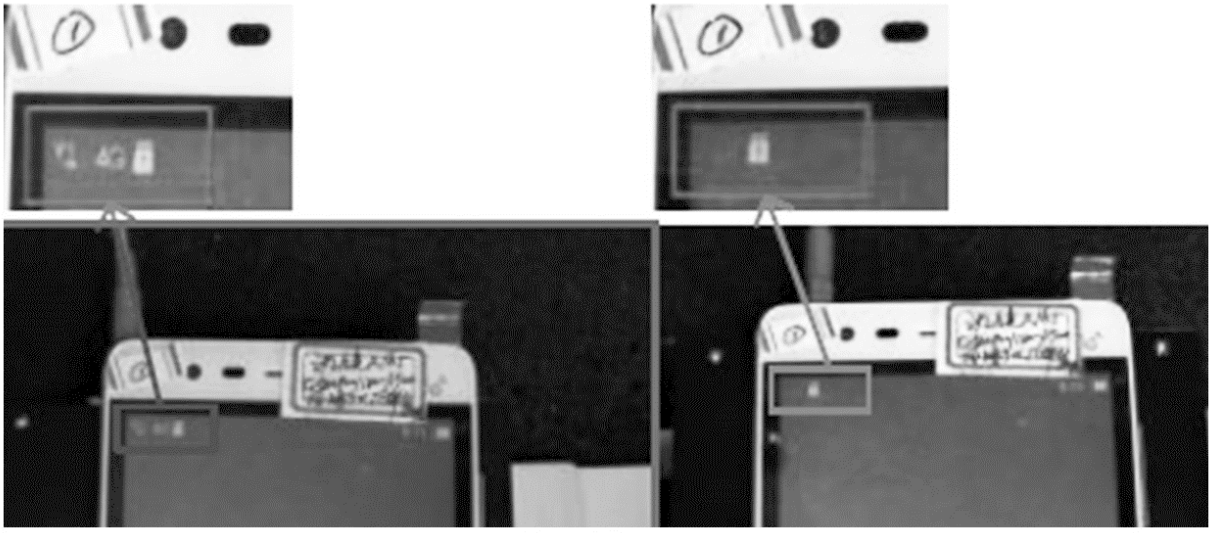
Figure 9
The outcome of disconnection in all cases

Источник: авторская разработка

Source: Authoring

Рисунок 10
UE отключен от всех сетей

Figure 10
UE disconnected from all networks



Источник: авторская разработка

Source: Authoring

Список литературы

1. *Комысов П.В., Надымов А.В.* Исследование интерференции в гетерогенных сетях стандарта LTE-A // Известия ЮФУ. Технические науки. 2018. № 1. С. 220–227.

2. *Дроздова В.Г., Завьялова Д.В.* Анализ и оптимизация ключевых показателей эффективности хэндоверов в мобильных сетях LTE // Вестник кибернетики. 2017. № 4. С. 146–153.

3. *Абдыраева Н.Р.* Особенности беспроводной широкополосной связи LTE с использованием фрактальной антенны на основе кривой Коха // Бюллетень науки и практики. 2018. № 3. С. 164–169.

4. *Тихнонов В., Нестеренко С., Бабич Ю. и др.* Разработка архитектуры интегрированной сети мобильного доступа 5G на основе адаптации технологии LTE // Восточно-европейский журнал передовых технологий. 2017. Т. 5. № 2. С. 42–49. URL: https://doi.org/10.15587/1729-4061.2017.111900

5. *Корионов И.П., Орлов В.Г.* Пользовательские аспекты безопасности в сетях LTE // Телекоммуникации и информационные технологии. 2017. № 2. С. 16–21.

6. *Наумов В.А., Мокров Е.В., Самуйлов К.Е.* Анализ временных характеристик процесса передачи данных подвижным пользователям в соте сети LTE // Информатика и ее применения. 2017. № 4. С. 79–84.

7. *Ермаков С.А., Коленбет Н.С., Юрасов В.Г., Батаронов И.Л.* Архитектура системы безопасности в сотовых сетях стандарта LTE // Информация и безопасность. 2014. № 4. С. 626–629.

8. *Гудкова И.А., Маркова Е.В.* Модель управления доступом к радиоресурсам с индивидуальными потоками на скорость передачи данных в сети LTE // T-COMM: Телекоммуникации и транспорт. 2014. № 8. С. 28–31. URL: https://cyberleninka.ru/article/v/model-upravleniya-dostupom-k-radioresursam-s-individualnymi-potolkami-na-skorost-peredachi-dannyh-v-seti-lte

9. *Мазхар Д., Филин М.* Оптимизация сети на основе LTE Advanced и частотного замещения // Наука и бизнес: пути развития. 2015. № 6. С. 128–130.

10. *Константинов А.С., Пестряков А.В.* Анализ фундаментальных ограничений максимальной скорости передачи информации в сети LTE-Advanced // T-COMM: Телекоммуникации и транспорт. 2017. № 12. С. 60–63.

11. *Листопад М.Е., Коротченко С.Е.* Совершенствование методики оценки системы информационной безопасности в России // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. № 6. С. 1162–1175. URL: https://doi.org/10.24891/ni.13.6.1162

12. *Терентьев А.М.* Выбор адекватных средств информационной защиты персонального компьютера в России // Национальные интересы: приоритеты и безопасность. 2012. № 33. С. 37–42. URL: https://cyberleninka.ru/article/v/vybor-adekvatnyh-sredstv-informatsionnoy-zaschity-personalnogo-kompyutera-v-rossii

13. *Ревенков П.В., Бердюгин А.А.* Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. 2016. Т. 12. № 11. С. 158–169. URL: https://cyberleninka.ru/article/v/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga

14. *Бармина С.С., Таджибаева Ф.М., Тумбинская М.В.* Корреляционный анализ и прогнозирование SYN-флуд атак // Прикладная информатика. 2018. № 4. С. 93–102.

15. *Петренко А.А., Петренко С.А.* Способ повышения устойчивости LTE-сети в условиях деструктивных кибератак // Вопросы кибербезопасности. 2015. № 2. С. 36–42.

16. *Асирян В.М., Шишкин М.О., Степанов М.С.* Оценка соты сети LTE при обслуживании эластичного трафика // Телекоммуникации и информационные технологии. 2018. № 1. С. 76–82.

17. *Тумбинская М.В., Сафиуллина А.М.* Информационная система принятия решений при выявлении компетенций управленческого персонала предприятий различных форм собственности // Менеджмент в России и за рубежом. 2013. № 6. С. 105–109.

18. *Тумбинская М.В.* Обеспечение защиты от нежелательной информации в социальных сетях // Вестник Мордовского университета. 2017. № 2. С. 264–288.

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-2872
eISSN 2311-875X

Threats and Security

ANALYSIS OF THE PROTECTION OF THE LTE-A SECURITY SYSTEM FROM THE TARGETED EXPOSURE OF DoS-ATTACK

Nikita V. KORMIL'TSEV [a,•], Aleksandr D. UVAROV [b], Il'dar I. KHAMATNUROV [c], Marina V. TUMBINSKAYA [d]

[a] Kazan National Technical Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI), Kazan, Republic of Tatarstan, Russian Federation
kormiltcev@hotmail.com
https://orcid.org/0000-0002-2289-5672

[b] Kazan National Technical Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI), Kazan, Republic of Tatarstan, Russian Federation
obg-96@mail.ru
https://orcid.org/0000-0003-0337-2689

[c] Kazan National Technical Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI), Kazan, Republic of Tatarstan, Russian Federation
Ildarka96@mail.ru
https://orcid.org/0000-0002-4853-6774

[d] Kazan National Technical Research Technical University named after A.N. Tupolev – KAI (KNRTU-KAI), Kazan, Republic of Tatarstan, Russian Federation
tumbinskaya@inbox.ru
ORCID: not available

[•] Corresponding author

Article history:
Received 30 November 2018
Received in revised form
20 December 2018
Accepted 11 January 2018
Available online
15 February 2019

JEL classification: C63, M15

Keywords: LTE-A, information security, tracking area update, DoS

Abstract

Subject The article analyzes to what extent the LTE Advanced networks are protected from the DoS attacks.

Objectives The research attempts to detect and analyze vulnerable loops in the LTE security system, which is a modern means of communication. However, it is often exposed to some malpractices, such as DoS attacks.

Methods The research discusses the specifics of Network Attached Storage access to Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). We also describe two instances of the protocol being exposed to DoS attack through the Tracking Area Update procedure (TAU).

Results We conducted an analysis of some exposures as part of E-UTRAN and TAU procedures and figured out what disrupted the service of TRACKINGAREAUPDATEREJECT warning system.

Conclusions and Relevance Although LTE-A standard provides for some mechanisms to enhance the security of mobile communication, we actually detected an unprotected transfer of messages to launch DoS attacks. We also proved deficiencies in the network security system. The drawbacks can be eliminated with the system recovery timer, which disconnects mobile stations from the networks and notifies TAU procedure is denied throughout a protracted period of time. Afterwards mobile stations regain access to the network without disturbing other users.

Please cite this article as: Kormil'tsev N.V., Uvarov A.D., Khamatnurov I.I., Tumbinskaya M.V. Analysis of the Protection of the LTE-A Security System from the Targeted Exposure of DoS-attack. *National Interests: Priorities and Security*, 2019, vol. 15, iss. 2, pp. 376–392.
https://doi.org/10.24891/ni.15.2.376

References

1. Komysov P.V., Nadymov A.V. [Investigation of interference in the heterogeneous networks of the LTE-A standard]. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences*, 2018, no. 1, pp. 220–227. (In Russ.)

2. Drozdova V.G., Zav'yalova D.V. [Analysis and optimization of handover key performance indicators in LTE mobile networks]. *Vestnik kibernetiki = Proceedings in Cybernetics*, 2017, no. 4, pp. 146–153. (In Russ.)

3. Abdyraeva N.R. [Feature of wireless communication LTE using a fractal antenna based on Koch curve]. *Byulleten' nauki i praktiki = Bulletin of Practice and Sciences*, 2018, no. 3, pp. 164–169. (In Russ.)

4. Tikhnonov V., Nesterenko S., Babich Yu. et al. [Developing the architecture of integrated 5G mobile network based on the adaptation of LTE technology]. *Vostochno-evropeiskii zhurnal peredovykh tekhnologii = Eastern European Journal of Enterprise Technologies*, 2017, vol. 5, no. 2, pp. 42–49. (In Russ.) URL: https://doi.org/10.15587/1729-4061.2017.111900

5. Korionov I.P., Orlov V.G. [User-related aspects of security in LTE networks]. *Telekommunikatsii i informatsionnye tekhnologii = Telecommunications and Information Technologies*, 2017, no. 2, pp. 16–21. (In Russ.)

6. Naumov V.A., Mokrov E.V., Samuilov K.E. [Performance measures analysis of data transfer process to mobile users in LTE cell]. *Informatika i ee primeneniya = Informatics and Applications*, 2017, no. 4, pp. 79–84. (In Russ.)

7. Ermakov S.A., Kolenbet N.S., Yurasov V.G., Bataronov I.L. [Architecture of the security system in the cellular networks of the LTE standard]. *Informatsiya i bezopasnost'= Information and Security,* 2014, no. 4, pp. 626–629. (In Russ.)

8. Gudkova I.A., Markova E.V. [On radio admission control scheme model for non-real-time services with maximum bit rate in LTE network]. *T-COMM: Telekommunikatsii i transport = T-COMM: Telecommunications and Transport*, 2014, no. 8, pp. 28–31.
URL: https://cyberleninka.ru/article/v/model-upravleniya-dostupom-k-radioresursam-s-individualnymi-potolkami-na-skorost-peredachi-dannyh-v-seti-lte (In Russ.)

9. Mazhar J., Filin M. [Optimization of network load based on LTE Advanced and frequency substitution]. *Nauka i biznes: puti razvitiya = Science and Business: Ways of Development*, 2015, no. 6, pp. 128–130. (In Russ.)

10. Konstantinov A.S., Pestryakov A.V. [Analysis of the fundamental limitations of the maximum data rate in the LTE-Advanced network]. *T-COMM: Telekommunikatsii i transport = T-COMM: Telecommunications and Transport*, 2017, no. 12, pp. 60–63. (In Russ.)

11. Listopad M.E., Korotchenko S.E. [Improving the method for evaluation of the information security system in Russia]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2017, vol. 13, no. 6, pp. 1162–1175. (In Russ.)
URL: https://doi.org/10.24891/ni.13.6.1162

12. Terent'ev A.M. [Choice of adequate information security software PC in Russia]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2012, no. 33, pp. 37–42. URL: https://cyberleninka.ru/article/v/vybor-adekvatnyh-sredstv-informatsionnoy-zaschity-personalnogo-kompyutera-v-rossii (In Russ.)

13. Revenkov P.V., Berdyugin A.A. [Cybersecurity in the Internet of Things and electronic banking]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2016, vol. 12, no. 11, pp. 158–169. URL: https://cyberleninka.ru/article/v/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga (In Russ.)

14. Barmina S.S., Tadzhibaeva F.M., Tumbinskaya M.V. [Correlation analysis and forecasting of SYN-flood attacks]. *Prikladnaya informatika = Applied Informatics*, 2018, no. 4, pp. 93–102. (In Russ.)

15. Petrenko A.A., Petrenko S.A. [Method for increasing the LTE-network stability in a destructive cyber attacks]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2015, no. 2, pp. 36–42. URL: https://cyberleninka.ru/article/v/sposob-povysheniya-ustoychivosti-lte-seti-v-usloviyah-destruktivnyh-kiberatak (In Russ.)

16. Asiryan V.M., Shishkin M.O., Stepanov M.S. [Evaluation of the LTE network cell when serving elastic traffic]. *Telekommunikatsii i informatsionnye tekhnologii = Telecommunications and Information Technologies,* 2018, no. 1, pp. 76–82. (In Russ.)

17. Tumbinskaya M.V., Safiullina A.M. [Decision-making information system in identifying the competences of management personnel of enterprises with different ownership forms]. *Menedzhment v Rossii i za rubezhom = Management in Russia and Abroad*, 2013, no. 6, pp. 105–109. (In Russ.)

18. Tumbinskaya M.V. [Providing protection from targeted information in social networks]. *Vestnik Mordovskogo universiteta = Bulletin of Mordovian University*, 2017, no. 2, pp. 264–288. (In Russ.)

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.