Прячущийся на виду сигнал: Атака на заслонение физического сигнала в LTE

Ходжун Ян, Сангвук Бэ, Минчеол Сон, Хонгиль Ким, Сонг Мин Ким и Йонгдэ Ким,
KAIST

https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

Эта статья включена в сборник трудов 28-го симпозиума по безопасности USENIX.

14-16 августа 2019 года - Санта-Клара, Калифорния, США

Открытый доступ к материалам 28-го симпозиума по безопасности USENIX спонсируется USENIX.

Прятки в обычном сигнале: Атака на заслонение физического сигнала в LTE

Ходжун Ян, Сангвук Бэ, Минчоль Сон, Хонгиль Ким, Сон Мин Ким и Йонгдэ Ким
Корейский передовой науки и технологий (KAIST)
{omnibusor, hoops, mcson, hongilk, songmin, yongdaek}@kaist.ac.kr

Аннотация

Связь Long-Term Evolution (LTE) основана на открытой среде, поэтому легитимный сигнал потенциально может быть подделан вредоносным сигналом. Хотя большинство сигнальных сообщений LTE защищены от модификации с помощью криптографических примитивов, широковещательные сообщения в LTE никогда не были защищены от нарушения целостности. В этой статье мы впервые представляем атаку с внедрением сигнала, которая использует фундаментальные недостатки широковещательных сообщений в LTE и модифицирует передаваемый сигнал в эфире. Эта атака, получившая название "затенение сигнала" (`SigOver`), имеет семь преимуществ и отличий по сравнению с существующими атаками с использованием поддельной базовой станции. Например, при разнице в мощности с легитимным сигналом в 3 дБ атака `SigOver` продемонстрировала 98 % успеха по сравнению с 80 % успеха атак с использованием поддельной базовой станции, даже при разнице в мощности в 35 дБ. Учитывая, что атака `SigOver` является новой примитивной атакой, она дает пять новых сценариев атак и их последствий. Наконец, обсуждение двух потенциальных контрмер оставляет практичный и надежный механизм защиты в качестве будущей работы.

1 Введение

Технология Long-Term Evolution (LTE) использует широковещательные сигналы для передачи важной информации от сотовой сети к пользовательским устройствам. Как минимум, информация, передаваемая базовой станцией LTE, которая называется развитым узлом (eNB), включает в себя информацию о синхронизации и конфигурации радиоисточника, необходимые для доступа пользовательского оборудования (UE) к сотовой сети. На основе полученных широковещательных сигналов UE регистрируется в сети, выполняя процедуру аутентификации и согласования ключей (AKA). После регистрации UE отслеживает широковещательные сигналы для достижения различных целей. Например, когда UE не имеет соединения с eNB из-за своей неактивности, ему необходимо регулярно прослушивать пейджинговые сообщения, чтобы проверить переданные ему сообщения. Даже когда UE имеет активное соединение с eNB, UE продолжает прослушивать широковещательные сигналы, чтобы определить потенциальные возможности. существенные изменения в общесистемных радиоконфигурациях, которые необходимо обновить, и определить поступление сообщений, предназначенных для нескольких UE.

Несмотря на различные практические применения, широковещательная сиг- нала не защищена ничем. В LTE связь между UE и сетью защищена только после успешной аутентификации и процедур квитирования безопасности, а именно процедур режима безопасности Non-Access Stratum (NAS) и Access Stratum (AS) для защиты *одноадресных* сообщений. Незащищенные широковещательные сигналы могут быть неизбежны в определенной степени в беспроводной связи; однако они подвергают систему и UE различным уязвимостям, которые могут быть использованы.

В предыдущих работах [21, 26, 36, 39, 40] сообщалось о нескольких атаках, использующих *незащищенные* широковещательные сигналы. Как правило, в таких атаках используется поддельная базовая станция (FBS), которая привлекает UE к подключению к себе, передавая сигнал сильнее, чем сигналы легитимных базовых станций. Атаки в основном используют пейджинговые сообщения, что приводит к нежелательным последствиям для UE, например, выходу из строя и разряду батареи. Примечательно, что такие атаки на основе FBS обладают заметными характеристиками (например, высокой мощностью сигнала) и/или результатами (например, отказ в обслуживании), которые позволяют UE-жертвам идентифицировать присутствие FBS (подробнее см. раздел 3.5).

В этой статье мы предлагаем новый подход, называемый атакой `SigOver`, который внедряет манипулированный широковещательный сигнал в UE без использования FBS. Атака `SigOver` записывает часть легитимного сигнала с помощью манипулируемого сигнала атаки. Атака `SigOver` основана на том, что UE декодирует более сильный сигнал при одновременном приеме нескольких перекрывающихся сигналов, что называется "*эффектом накидки*" [51]. Основным техническим компонентом атаки является синхронизация синхронизации атакующего сигнала с целевым легитимным сигналом таким образом, чтобы UE декодировало только атакующий сигнал (см. раздел 3). Эта атака является одновременно скрытной и далеко идущей. Незаметной она является потому, что сигнал атаки, передаваемый на значительно низком уровне мощности, перекрывает только целевой сигнал, в то время как другие сигналы/сообщения между UE-жертвой и сетью остаются нетронутыми. Это далеко...

достигается благодаря тому, что сигнал атаки может одновременно воздействовать на большое количество близлежащих UE с малым количеством сигналов и низкими вычислительными затратами. Отметим, что атака SigOver не требует активной связи с UE, и она не передает сообщения между UE и eNB.

Атака SigOver - это первая практическая реализация *атаки заслонения сигнала на широковещательные сигналы LTE* с использованием недорогой платформы Software Defined Radio (SDR) и библиотеки LTE с открытым исходным кодом [43]. Атака SigOver была реализована на практике благодаря решению следующей проблемы: *синхронизация по времени и частоте*. Чтобы затмить легитимный сигнал с помощью вредоносного сигнала, атака SigOver должна быть жестко синхронизирована по времени с физическим каналом нисходящего канала eNB, к которому прислушивается UE-жертва. Для достижения временной синхронизации мы используем сигналы синхронизации eNB, которые передаются периодически с фиксированным временным интервалом. Для точной частотной синхронизации мы используем генератор, настроенный на Глобальную систему позиционирования (GPS).

Реалистичность атаки SigOver была проверена путем ее тестирования на 10 смартфонах (перечисленных в разделе 5), подключенных к действующей сети[1]. Для экспериментов мы ввели пять новых сценариев атаки, которые включали сигнальный шторм, отказ в обслуживании (DoS) против UE, падение сети и отслеживание местоположения UE (раздел 5). Результаты экспериментов показали, что атака SigOver затеняет целевой сигнал и заставляет устройство-жертву декодировать его с 98 %-ной вероятностью успеха и разницей в мощности всего в 3 дБ по сравнению с легитимным сигналом. С другой стороны, атаки, использующие FBS, имеют только 80 % успеха даже при разнице в мощности 35 дБ. Это означает, что атака SigOver значительно эффективнее, чем атаки с использованием FBS.

Наконец, в разделе 6 обсуждаются две потенциальные меры противодействия атаке SigOver: (1) решение на основе цифровой подписи и (2) обнаружение на основе оценки канала. Более того, практическое и надежное решение против атаки SigOver оставлено в качестве будущей работы.

Наш вклад в это дело сводится к следующему:

- **Первая атака на затенение сигнала в LTE:** Насколько нам известно, атака SigOver - это первая реализация атаки с затенением сигнала на широковещательные сигналы LTE.
- **Реализация и оценка:** Мы демонстрируем практичность и скрытность атаки SigOver с помощью интенсивных экспериментов в реальных условиях с высоким процентом успешных атак.
- **Новые сценарии атак и их последствия:** Мы представляем новые сценарии атак и подробно анализируем их последствия на основе проведенных экспериментов.
- **Меры противодействия:** Мы исследуем стратегии предотвращения и обнаружения атак SigOver, например, цифровая подпись на широковещательных сигналах для предотвращения и использование изменяющейся природы физического сигнала для обнаружения.

[1] Все эксперименты проводились с разрешения операторов.

2 Фон

В этом разделе мы приводим краткое описание архитектуры сети LTE и основных процедур установления радиосоединения, управления мобильностью и обеспечения безопасности между устройством и сетью LTE. (Аббревиатуры, используемые в данной статье, приведены в таблице в Приложении B).

2.1 Архитектура сети LTE

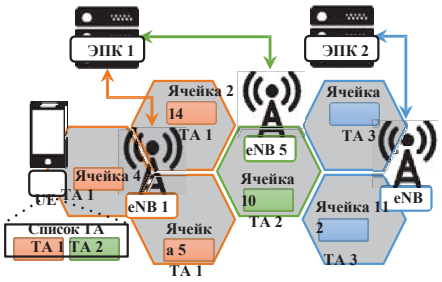


Рисунок 1: Архитектура сети LTE

Сеть LTE состоит из компонентов UE, eNB и Evolved Packet Core (EPC), как показано на рисунке 1.

UE - это конечное устройство, которое предоставляет различные услуги LTE (т. е. услуги передачи голоса и данных) пользователю, подписавшемуся на них. Оно включает в себя смарт-карту, называемую универсальным модулем идентификации абонента (USIM), которая хранит постоянный идентификатор (Inter- national Mobile Subscriber Identity, IMSI) или временный идентификатор (Globally Unique Temporary Identity, GUTI) для идентификации пользователя, а также криптографический ключ для шифрования и защиты целостности.

eNB - это базовая станция LTE, которая обеспечивает беспроводное соединение для UE, чтобы они могли получать услуги, включенные в сеть LTE. Одна eNB охватывает несколько участков (в LTE они сотами), которые идентифицируются идентификатором соты физического уровня (PCI).

Сеть EPC отвечает за такие функции управления, как аутентификация, управление мобильностью и сеансами связи, а также за услуги пользовательской плоскости. Для управления мобильностью субъект управления мобильностью (MME) в сети EPC управляет набором областей отслеживания (TA), каждая из которых содержит несколько eNB.

2.2 Первоначальный доступ к физическому уровню LTE

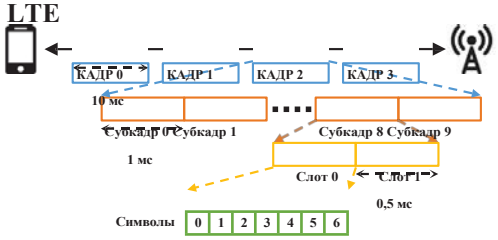


Рисунок 2: Рамочная структура LTE типа 1 [2]

Кадр LTE. UE и eNB взаимодействуют друг с другом на основе структуры радиокадра, как показано на рисунке 2[2].

[2] В этом проекте использовался режим LTE-Frequency Division Duplex (FDD). исследование, используемое большинством операторов в мире [18].

Каждый кадр имеет длительность 10 мс и состоит из 10 подкадров, каждый из которых имеет длительность 1 мс. Один подкадр далее делится на два слота равной длительности, и каждый слот состоит из семи символов ортогонального частотного мультиплексирования (OFDM).

Планирование нисходящего канала. В LTE радиоресурсы выделяются в виде блока физических ресурсов (PRB) [2], который содержит 12 поднесущих (каждая с полосой пропускания 15 КГц) и занимает один слот во времени (0,5 мс). Количество доступных PRB в частотной полосе определяется пропускной способностью системы. В зависимости от размера данных, eNB распределяет PRB в течение субкадра (1 мс), который является наименьшим временным интервалом планирования.

Оценка канала. Когда сигнал проходит по каналу без проводов, он искажается под воздействием нескольких факторов, например, затухания, фазового сдвига и шума. Чтобы учесть эти факторы, беспроводные устройства оценивают канал с помощью следующего уравнения: $Y(k) = H(k)X(k)$, где $Y(k)$, $H(k)$ и $X(k)$ представляют собой сигнал, принятый UE, коэффициент канала и сигнал, переданный eNB, соответственно. В LTE UE выполняет оценку канала на основе референс-сигнала (RS), передаваемого eNB. UE вычисляет $H(k)$ из $H(k) = \frac{Y(k)}{X(k)}$, поскольку ему уже известны значения $X(k)$ и $Y(k)$ PC. Чтобы минимизировать влияние шума при оценке каналов, $H(k)$ RS усредняется с помощью окна усреднения.

Поиск соты. Когда UE включается, ему необходимо найти подходящую соту для установления . Для этого он сначала пытается измерить индикатор силы принимаемого сигнала (RSSI) для частотных каналов-кандидатов. UE выбирает канал с наивысшим RSSI, основываясь на результатах измерения. После этого UE получает синхронизацию времени на основе субкадров и PCI соты, прослушивая первичный сигнал синхронизации (PSS) и вторичный сигнал синхронизации (SSS). Затем UE декодирует главный информационный блок (MIB) для получения системного номера кадра (SFN) и других физических каналов.

Сбор системной информации. После завершения процедуры поиска ячеек UE декодирует канал индикации физического управления (PCFICH) и канал управления физическим спуском (PDCCH) для декодирования данных нисходящего канала. UE знает количество символов OFDM, используемых для передачи PDCCH в каждом субкадре через PCFICH. Затем UE декодирует PDCCH, который содержит информацию о блоках повторного источника данных и схеме демодуляции, требуемой UE. После декодирования этих двух каналов UE декодирует другую системную информацию, передаваемую через физический общий канал нисходящего канала (PDSCH). Существует 22 блока системной информации (SIB), каждый из которых содержит различную системную информацию, связанную с сотой [3]. Среди них SIB1 и SIB2 необходимы UE для подключения к соте. Доступность других SIB указывается в SIB1.

Случайный доступ. UE выполняет процедуру случайного доступа к каналу (RACH) для установления радиосоединения с eNB. Для этого UE случайным образом выбирает последовательность преамбул случайного доступа (RA) и передает ее на eNB. Если та же последовательность преамбул не передается одновременно от другого UE, UE успешно завершает процедуру RA.

2.3 Управление мобильностью

Управление радиоресурсами (RRC). После выполнения всех вышеперечисленных шагов UE выполняет процедуру установления соединения с eNB (так называемая процедура установления соединения RRC). По завершении процедуры UE переходит в состояние *RRC Connected*, в котором он может взаимодействовать с eNB. При отсутствии входящих и исходящих данных в течение определенного периода времени радиосоединение между UE и eNB разрывается, и UE переходит в состояние *RRC Idle*, чтобы сократить расход батареи.

Non-Access Stratum (NAS). NAS - это протокол сетевого уровня между UE и MME для управления мобильностью и сеансами. Чтобы зарегистрироваться в сети LTE, UE выполняет процедуру ATTACH. После того как UE успешно зарегистрировано в сети LTE, MME узнает TA, к которому принадлежит UE, и предоставляет UE список идентификаторов TA (TAI). Этот список TAI используется UE для сообщения MME о своем местоположении.

Поведение в состоянии простоя. В состоянии *простоя RRC* UE периодически просыпается для чтения пейджинговых сообщений и SIB 1. Когда на UE поступает входящее сообщение, MME, отслеживающий UE, посылает пейджинговое сообщение всем eNB во всех TA, назначенных UE, и эти eNB передают пейджинговое сообщение, чтобы проинформировать UE о прибывшем сообщении. Пейджинговое сообщение содержит временный или постоянный идентификатор UE. Если UE получает пейджинговое сообщение, оно отправляет в сеть LTE запрос соединения RRC и сообщение запроса услуги. Пейджинговые сообщения также используются для уведомления о смене формации системы или для оповещения о чрезвычайных ситуациях, таких как система предупреждения о землетрясениях и цунами (ETWS) и система оповещения о мобильной связи (CMAS). UE также считывает SIB1 для идентификации текущего TA. Если UE входит в новый TA, которого нет в списке TAI, UE отправляет MME запрос на обновление зоны отслеживания (TAU), чтобы сообщить о своем местоположении. Кроме того, UE периодически измеряет мощность и качество обслуживающей соты и соседних сот, рассчитывая мощность принимаемого опорного сигнала (RSRP) и качество принимаемого опорного сигнала (RSRQ). Если RSRP соседней соты превышает RSRP обслуживающей соты на определенный порог, UE выбирает новую соту и переходит на нее (т. е. повторный выбор соты).

2.4 Создание контекста безопасности

Когда UE устанавливает беспроводное соединение с eNB, оно регистрируется в сети LTE для достижения полного соединения с сетью (такое поведение называется ATTACH), предоставляя свой постоянный идентификатор IMSI. Затем MME и UE взаимно аутентифицируют друг друга и выполняют ключ

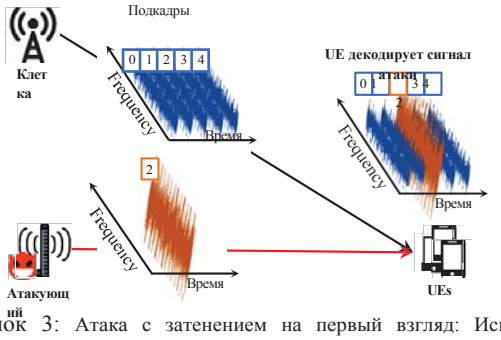


Рисунок 3: Атака с затенением на первый взгляд: Используя фиксированные тайминги передачи субкадров LTE, злоумышленник вводит поддельный субкадр (коричневый), который точно *заслоняет* легитимный субкадр (синий) без ошибок.

процедура согласования для создания *контекста безопасности* (т. е. контекста безопасности NAS) для шифрования и защиты целостности. После процедуры аутентификации и согласования ключей (AKA) большинство сообщений между UE и MME шифруются и защищают целостность с помощью криптографических примитивов. С другой , все начальные процедуры, предшествующие созданию контекста безопасности в процедуре AKA, не шифруются и не защищают целостность. К таким незащищенным сообщениям относятся pag- ing, SIBs и несколько начальных сообщений сетевого уровня, указанных в стандарте LTE [5].

3 Затмевающие широковещательные сообщения LTE

В этом разделе мы представим модель атаки, а затем опишем атаку `SigOver`. Атака `SigOver` демонстрируется на примере широко используемого сегодня SDR (Uni- versal Software Radio Peripheral (USRP) [16]). Наконец, мы сравниваем атаку `SigOver` с типичными атаками FBS, чтобы показать эффективность первой.

3.1 Модель атаки

Мы предполагаем активного противника с минимальными привилегиями. Предлагаемая модель атаки может быть описана следующим образом: (i) Противник не знает LTE-ключ UE-жертвы. (ii) Противник может подслушивать широковещательные сообщения нисходящего канала, передаваемые из легитимной соты LTE на UE жертвы. Однако, поскольку ключ жертвы недоступен, зашифрованные сообщения не могут быть расшифрованы. Отметим, что (ii) тривиально достижимо, поскольку сообщения передаются через открытую среду. При вышеуказанных предположениях мы покажем, что активный противник может внедрить вредоносные сообщения в UE(ы) жертвы, перезаписав легитимные сообщения. Это достигается путем тщательной подготовки сообщения, которое перекрывает легитимное сообщение по времени и частоте. В разделе 3.5 мы обсуждаем фундаментальные различия между предложенной моделью атаки и типичными FBS-атаками [21, 22, 36, 37, 39].

3.2 Обзор атак `SigOver`

В этом разделе кратко описана конструкция атаки `SigOver`. Как обсуждалось в разделе 2, нисходящий канал LTE планируется с гранулярностью субкадров длительностью 1 мс. Каждый подкадр кодируется базовой станцией отдельно и, соответственно, декодируется UE. При такой структуре кадров на рисунке 3 концептуально показана атака `SigOver`, когда злоумышленник вводит поддельный подкадр (коричневый цвет), который точно *заслоняет* легитимный подкадр (синий цвет). Поскольку субкадры декодируются независимо друг от друга, легитимные (не затененные) субкадры, как правило, не затрагиваются. В то же время инжектированный субфрейм создается таким образом, что UE, получившие и декодировавшие субфрейм, ведут себя на основе включенной в него информации, что обычно приводит к аномальному или злонамеренному поведению - поведению, спровоцированному злоумышленником. Уязвимость, присущая широковещательным сообщениям LTE, позволяет злоумышленникам осуществлять различные типы атак, используя сообщения, выглядящие законно (т. е. коварно).

В принципе, атака `SigOver` использует эффект захвата [51], при котором более сильный сигнал декодируется при столкновении в эфире нескольких одновременных беспроводных сигналов (т. е. легитимных и поддельных субфреймов). Это справедливо для сигналов с небольшой разницей в мощности в 3 дБ [29]. Двумя техническими проблемами для запуска атаки `SigOver` являются (i) тщательная разработка затеняющего сообщения для декодирования UE-жертвами (раздел 3.3) и (ii) жесткие требования к времени и частоте передачи для точного затенения (раздел 3.4).

3.3 Создание вредоносного подкадра

Здесь мы проиллюстрируем, как создать подкадр, который может быть декодирован на UE-жертве для успешной атаки.

Подбор конфигурации связи. Для атаки `SigOver` злоумышленник должен сначала определить физическую конфигурацию легитимной соты, на которой находятся UE-жертвы, чтобы определить структуру атакующего подкадра. Необходимая информация о физической конфигурации для построения действительного подкадра включает PCI, пропускную способность канала, конфигурацию PHICH и схему передачи (или количество антенных портов); все эти данные доступны атакующему, как только он размещается в той же легитимной соте. В частности, PCI вычисляется из PSS/SSS, а остальная информация получается из MIB. Кроме того, атакующий должен синхронизироваться с SFN легитимной ячейки, который также доступен в MIB, чтобы определить время введения подкадра атаки.

Структурирование и введение подкадров. В LTE, когда UE читает широковещательное сообщение, оно декодирует следующую информацию из субкадра: i) индикатор формата управления (CFI), который содержит структуру канала управления, ii) информацию управления нисходящим каналом (DCI), которая содержит выделенные ресурсы (т. е. блоки ресурсов) для сообщения, и iii) блоки ресурсов (RB), которые содержат само сообщение. CFI и DCI представляют собой

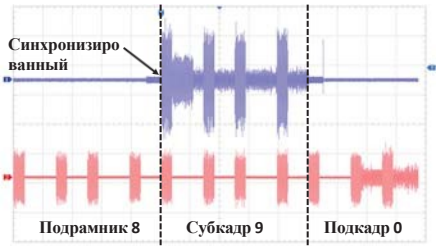


Рисунок 4: Снимок осциллографа, показывающий точную временную синхронизацию.
различие между легитимным (красным) и поддельным сигналом (синим).

передаются по PCFICH и PDCCH соответственно; а сообщение передается по PDSCH. Таким образом, для инъекции подкадра злоумышленнику необходимо создать подкадр, содержащий PCFICH, PDSCH и PDSCH. Однако инжектированный подкадр, содержащий эти значения, может быть некорректно закодирован на UE из-за ошибки оценки канала. Обратите внимание, что UE оценивает канал по RS, передаваемому легитимным eNB, но результат оценки может быть неадекватным для правильного декодирования инжектированного подкадра. Чтобы решить эту проблему, RS включается в подкадр для атаки `SigOver`, что значительно повышает устойчивость атаки `SigOver`.

Последняя техническая проблема, связанная с декодированием искусственного субкадра, касается оценки и выравнивания беспроводного канала для восстановления после искажения сигнала из-за канала. При атаке `SigOver` канал оценивается либо преимущественно (даже исключительно, в зависимости от случая пейджинга) по созданному подкадру (*RRC Idle*), либо по последовательным подкадрам (*RRC Connected*) вместе с несколькими легитимными подкадрами. В первом случае для атаки достаточно одной инъекции (т. е. декодирования поддельного субкадра). Во втором случае для эффективного отражения беспроводного канала между злоумышленником и UE-жертвой необходимы многократные инъекции. Согласно нашим измерениям (раздел 4), в которых вводился один подкадр для каждого SFN, атака `SigOver` достигает более 98 % успеха менее чем за секунду, сохраняя надежную связь для легитимных подкадров. В Приложении A мы приводим эмпирические результаты, показывающие, что легитимная связь минимально страдает от атаки `SigOver` при использовании нескольких сервисов, включая веб-браузинг и потоковую передачу.

3.4 Точное затенение

Перезатенение требует, чтобы подстроенный подкадр точно перекрывал легитимный сигнал как во временной, так и в частотной областях. В этом подразделе рассматривается, как это достигается.

Временная синхронизация. Чтобы точно заслонить легитимные субкадры, злоумышленнику необходимо знать тайминг субкадра (чтобы определить, когда начинается субкадр) и SFN (чтобы определить, когда вводить субкадр относительно номера кадра) от легитимной ячейки. Злоумышленник получает тайминг подкадра из сигналов синхронизации (т. е. PSS/SSS), а SFN - из MIB легитимной ячейки. Атакующий

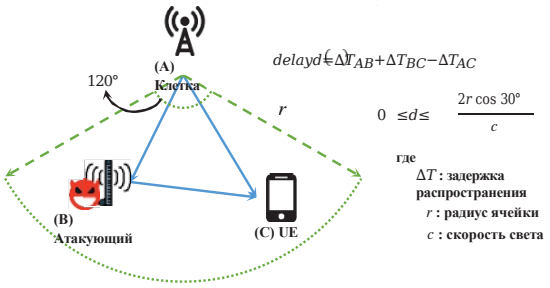


Рисунок 5: Задержка распространения в трехсекторной конфигурации соты в зависимости от местоположения UE жертвы и атакующего. Предполагается, что атакующий и жертвенный UE находятся в зоне действия соты (форма зеленого сектора).

непрерывно получает тайминг подкадра и обновленный SFN, поскольку эти значения меняются со временем в зависимости от состояния канала. Зная тайминг подкадра и SFN, атака `SigOver` точно синхронизирует время передачи подстроенного подкадра с временем передачи целевого широковещательного сообщения (см. Рисунок 4).

Однако, как показано на рисунке 5, созданный подкадр, переданный с полученным временем подкадра, все равно может прибыть на UE с небольшим смещением времени (относительно легитимного подкадра) из-за задержки распространения. Хотя задержка
(d) неизбежна (поскольку задержка распространения неизмерима для злоумышленника), ее влияние минимально. Это объясняется тем, что процессор базовой полосы в UE спроектирован таким образом, чтобы компенсировать задержку, связанную с мобильностью и влиянием окружающей среды [48]. Поскольку максимальная компенсируемая задержка зависит от базового процессора UE, мы проводим следующие эксперименты для измерения задержки. Мы предположили типичную трехсекторную конфигурацию соты, где угол передачи соты составляет 120° [10]. Задержка (d) максимальна, когда атакующий и жертвенный UE расположены на обоих концах дуги. Это означает d = 8,*66* мкс при типичном радиусе соты около 1,5 км в городских условиях. Мы измерили допустимое смещение на двух устройствах с разными базовыми частотами (Qualcomm и Exynos), и оно оказалось больше, чем максимальная задержка (т. е. 8,66 *мкс*) (подробные результаты экспериментов приведены в разделе 4).

Синхронизация частоты. Рабочая частота радиоустройства определяется генератором, который неизбежно испытывает специфическое для устройства смещение, случайным образом накладываемое при изготовлении и возникающее в процессе эксплуатации под воздействием окружающей среды (например, температуры). Такое несовершенство генератора отражается на радиосигнале в виде смещения несущей частоты. В LTE существует ряд легкодоступных методов [27, 50] для компенсации смещения до определенного уровня (например, до± 7,5 КГц для компенсации на основе PSS в LTE с шагом поднесущей 15 КГц [38]). Поэтому для надежной реализации атаки `SigOver` набор смещений должен постоянно поддерживаться ниже этого уровня в UE.

Стандарт LTE определяет минимальную частотную точ-.

Таблица 1: Сравнение SigOver, FBS и MitM-атак

	Скрытность	Энергоэффективность	Устойчивое развитие
FBS	Низкий	Низкий	Низкий
MitM	Ограниченный*	Низкий	Ограниченный*
SigOver	Высокий	Высокий	Высокий

* "Ограниченный" означает, что атака работает в ограниченной среде.

рация базовой станции± 50 ppb [1] для макробазовых станций. Чтобы удовлетворить это требование, eNB оснащаются высокоточными генераторами и дополнительными технологиями, такими как протокол точного времени и GPS. В отличие от этого, SigOver атака проводилась на типичном недорогом SDR с неаккуратным осциллятором (± 2500 ppb для USRP X310 [16]). Для уменьшения смещения частоты до необходимого уровня был использован GPS-дисциплинированный генератор (GPSDO), а именно кристаллический генератор с печным управлением (OCXO). GPSDO обеспечивает достаточную точность± 25 ppb [14, 32] и отличается высокой стабильностью (± 1 ppb при блокировке GPS). Это указывает на смещение частоты до± 270 Гц (на частоте 3,6 ГГц со смещением 75 ppb), в пределах частотного диапазона LTE FDD 460 МГц-3,6 ГГц [6]. Наш эксперимент подтверждает, что все 10 устройств (перечисленных в разделе 5) могут компенсировать такое небольшое смещение частоты, чтобы обеспечить надежную атаку SigOver.

3.5 Сравнение SigOver, FBS и MitM-атак

Хотя атаки FBS и "человек посередине" (MitM) могут быть использованы для манипулирования широковещательными сообщениями в LTE, в литературе встречается только первая. В этом разделе мы подробно анализируем атаки FBS и MitM в сравнении с атакой SigOver с точки зрения скрытности, энергоэффективности и устойчивости (см. табл. 1).

3.5.1 Атаки с использованием FBS

Атака FBS - одна из наиболее распространенных атак на сотовые сети [21, 22, 26, 36, 39, 40]. При FBS-атаке злоумышленник (т. е. FBS) привлекает UE-жертвы в свой лагерь, передавая более сильный сигнал, чем легитимные соты. Затем злоумышленник передает незащищенные, но выглядящие легитимно сообщения на UE-жертву. Атака FBS имеет следующие ограничения по сравнению с атакой SigOver.

Энергоэффективность. В общем случае UE выбирает соту, передающую сигнал с наибольшей мощностью. Однако до сих пор не изучено, насколько более сильный сигнал должна передавать FBS по сравнению с легитимной базовой станцией, чтобы привлечь близлежащие UE-жертвы. Это важный вопрос, на который необходимо ответить злоумышленнику, поскольку более высокая мощность увеличивает вероятность привлечения UE с большим риском быть обнаруженным с помощью измерителей мощности (например, RSRP, RSRQ). Согласно экспериментальным измерениям, атака FBS достигает 100% успеха при 40 дБ, в то время как атака SigOver была 98% успешной при 3 дБ (см. табл. 2). В частности, достижения сопоставимой успешности атаки FBS требуется потребление энергии в 5000 раз больше, чем для атаки SigOver.

(a) (b) Ат

Рисунок 6: Сигнальные сообщения во время атак FBS и SigOver

Скрытность. В общем случае FBS настраивается на маскировку под легитимную базовую станцию, как это было представлено в предыдущих исследованиях [21, 22, 39, 40]. Например, FBS передает те же сообщения MIB и SIB1/2, что и легитимная ячейка, и может использовать те же PCI, чтобы сделать себя неотличимым от легитимных. Тем не менее, FBS неизбежно несет в себе несколько уникальных и четких сигнатур для де- тектирования [25, 30, 33, 49, 53]. Во-первых, как уже говорилось, при атаке FBS используется× 10 000 более мощная энергия (см.× 2 для SigOver at- tack), чем у легитимной ячейки, что является явным признаком FBS. Во-вторых, когда FBS привлекает UE-жертву, находящийся на законной соте, жертва должна пройти процесс повторного выбора соты, в ходе которого UE-жертва считывает MIB и SIB1/2 сообщения от FBS (рис. 6a). В-третьих, работа FBS может сильно отличаться от работы легитимной станции из-за ее ограниченных физических возможностей по сравнению с реальной базовой станцией[3]. К таким эксплуатационным характеристикам относятся относительно низкая скорость передачи пейджинга, а также другие радиочастотные свойства, такие как большое смещение частоты из-за низкой стоимости оборудования. Наконец, FBS не может установить безопасное соединение с UE или передавать защищенные сообщения NAS между UE и сетью (т. е. MME), что приводит к отказу в обслуживании UE. Таким образом, существует высокая вероятность того, что UE сможет обнаружить FBS. С другой стороны, механизм атаки SigOver заключается в точном заслонении определенного широковещательного сообщения без вмешательства в синхронизацию между UE-жертвой и текущей ячейкой. Поэтому, как показано на рисунке 6b, UE не выполняет повторный выбор соты или перенастройку каких-либо параметров, специфичных для соты. UE, подвергшийся атаке SigOver, поддерживает безопасные сигнальные соединения с легитимными eNB и MME.

Устойчивость. Если UE-жертва заходит на FBS, он не может получать услуги через FBS. Это может быть использовано UE в качестве потенциального механизма обнаружения FBS, как упоминалось выше. Чтобы избежать такого обнаружения, FBS может использовать следующую стратегию: она инжектирует вредоносное сообщение в UE и разрывает соединение (например, вызывая отказ радиосвязи или инициируя повторный выбор соты на UE), чтобы UE-жертва вернулся в легитимную соту. Однако в этом сценарии вводимое

[3] Атака, спонсируемая государством и обладающая неограниченными ресурсами и возможностями, не рассматривалась.

Сообщение должно быть выбрано таким образом, чтобы атака продолжалась даже при смене соты (например, `TAU Reject` [39]) или оказывала немедленное воздействие на UE (например, аварийное предупреждение [21]). Таким образом, использование широковещательных сообщений (например, сообщений SIB), которые обновляются при смене обслуживающей соты, не является подходящим вектором атаки. Это делает атаку FBS либо ограниченной в плане масштаба атаки (поскольку количество сообщений, которые можно использовать, очень ограничено), либо менее устойчивой по продолжительности.

3.5.2 MitM-атаки

Недавно был обнаружен новый тип FBS-атаки, получивший название aL- TEr [37]. Это MitM-атака, использующая FBS с возможностями eNB и UE. Компонент eNB в составе FBS выдает себя за легитимную eNB, ретранслируя сообщения от eNB к UE-жертве. Кроме того, компонент UE в составе FBS выдает себя за UE-жертву, передавая сообщения от UE к eNB. Находясь между UE-жертвой и eNB, MitM-атака манипулирует сообщениями пользовательской плоскости, поскольку в LTE сообщения не защищены от нарушения целостности. Атака MitM наследует два вышеупомянутых ограничения атаки FBS, а именно высокое энергопотребление и низкую скрытность, поскольку атакующий MitM должен привлекать UE-жертвы одним и тем же способом. Между тем, в принципе, атака MitM не влияет на соединение между UE-жертвой и eNB, что делает атаку устойчивой. Однако мы заметили, реализовать MitM-атаку нетривиально по разным причинам. Во-первых, чтобы поддерживать связь с UE-жертвой, MitM-злоумышленник должен передавать все сообщения, передаваемые по восходящей и нисходящей линии связи между UE-жертвой и eNB. Для этого злоумышленник должен знать настройки радиоресурса UE, установленные eNB, и соответствующим образом настроить радиоресурс для UE. В противном случае радиосвязь между UE и eNB может стать неустойчивой или оборваться. Однако, поскольку сообщение, содержащее настройку радиоресурса (т. е. `RRC reconfiguration`), зашифровано, злоумышленник не может правильно настроить радиоресурс UE. Отметим, что `реконфигурация RRC` содержит большое количество конфигураций PHY, MAC, RLC и PDCP для UE.

Чтобы решить эту проблему, атака aLTEr использовала эвристическую конфигурацию радиостанции при следующих условиях:
(i) UE-жертва получает услугу, используя *радиоконфигурацию по умолчанию*, и (ii) радиоконфигурация оператора по умолчанию является стабильной. То есть для каждой радиоконфигурации изменяется лишь несколько параметров (например, конфигурация запроса планирования (SR) и индикатора качества канала (CQI)), а остальные остаются неизменными. Таким образом, злоумышленнику нужно угадать только конфигурации CQI и SR. Однако в реальном мире eNB часто меняет радиоконфигурацию UE в зависимости от используемой UE услуги и/или текущего состояния канала (например, инициирование агрегации несущих, запуск услуги голосового/видеовызова, приоритет услуги или изменение качества канала из-за мобильности). Мы заметили, что когда UE смотрит видео на YouTube в течение 2 минут при плохом канале.

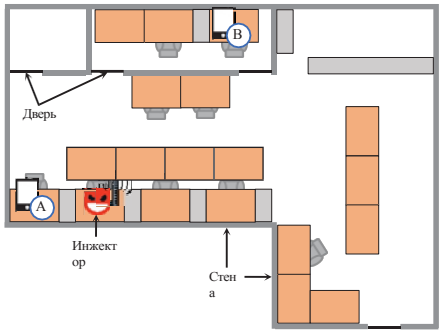


Рисунок 7: Эксперименты проводятся в двух местах расположения UE, A и B: A находится на расстоянии 2 м от злоумышленника с прямой видимостью. B находится на расстоянии 10 м от злоумышленника, отделенного него стеной (т. е. без прямой видимости). Мы называем первое и второе местоположение LOS и NLOS соответственно.

В этом случае он получил от eNB 9 сообщений о реконфигурации `RRC`, причем длина каждого сообщения варьировалась от 18 байт до 109 байт. Отметим, что, поскольку злоумышленник может знать только длину сообщения и последовательность его доставки, он может неправильно угадать конфигурацию. Мы также заметили, что 8 из 9 сообщений имеют различные конфигурации CQI, которые также необходимо угадать.

Эти ограничения применимы ко всем MitM-атакам, даже если злоумышленник пытается манипулировать широковещательным сообщением. Однако атака `SigOver` не страдает от таких ограничений, поскольку она использует только постоянную радиоконфигурацию, полученную из MIB легитимной ячейки (см. раздел 3.3).

4 Эксперимент в реальном мире

В этом разделе мы проведем атаку `SigOver` в естественных условиях и проанализируем ее надежность.

4.1 Экспериментальная установка

Мы реализуем атаку `SigOver` на основе *pdsch_enodeb*, которая содержит базовую функцию передачи как srsLTE [43]. Мы добавляем встроенную функцию приема для синхронизации времени с легитимной ячейкой. Субкадры были созданы с помощью библиотеки srsLTE. Кроме того, использовался USRP X310 [16], оснащенный дочерней платой UBX [15] и GPSDO [14], который был подключен к компьютеру Intel Core i5-3570 с Ubuntu 14.04. Чтобы затмить сигнал от легитимного eNB, USRP при необходимости дополнялся усилителем ZVE-2W-272 [28]. Жертвами UE являются коммерческие смартфоны, которые работают в легитимной соте LTE с полосой пропускания 20 МГц. Кроме того, для анализа переданных и принятых сообщений на UE использовались средства диагностического (например, SCAT и XCAL [8, 42]). На рисунке 7 показаны два места в университетском офисе, где были проведены две серии экспериментов: (LOS) UE жертвы и злоумышленника находились в одной комнате, разделенные расстоянием в 2 м. (NLOS) UE жертвы и атакующий находились в разных комнатах, разделенных

стена и расстояние 10 м. Эти два окружения использовались для экспериментов на протяжении всего исследования.

Детали реализации. Злоумышленник получает информацию о целевой доброкачественной ячейке (PCI, MIB) с помощью *pdsch_ue* или диагностических инструментов [8, 42]. Она получает временную синхронизацию с целевой сотой (имитируя процедуру, когда доброкачественное UE садится на соту, получая PSS/SSS и MIB). После того как она получает время прибытия и информацию SFN о кадре LTE, переданном доброкачественной сотой, она передает злонамеренное сообщение в целевую SFN. После этого она непрерывно получает PSS/SSS (каждые 5 мс) и MIB (каждые 10 мс), передаваемые добросовестной ячейкой, и обновляет информацию о синхронизации. Самопомехи могут вызвать проблемы с синхронизацией, поскольку Rx и Tx находятся на одной частоте. Однако, точному затенению, `SigOver` at- tack может минимизировать влияние на легитимные PSS/SSS и MIB (не было случая потери синхронизации из-за самопомех).

В качестве незначительной проблемы USRP X310 генерировал непреднамеренно высокий пиковый сигнал в начале и в конце сигнала при выполнении серийной передачи, что характерно для атаки `SigOver`. Это связано с изменением состояния фронтальных компонентов SDR. Когда передачи не было, он находился в состоянии бездействия. Когда передача происходила, переход в состояние передачи вызывал нежелательный шум. Мы решаем эту проблему простым добавлением нуля к переднему и заднему концам сигнала, чтобы отделить нежелательный шум от исходного сигнала, и компенсацией задержки, вызванной добавлением нуля при передаче.

Этические соображения. В качестве атакующего устройства мы используем направленную вниз куполообразную антенну, чтобы минимизировать помехи, идущие вверх. Кроме того, мы проводим эксперименты на первом уровне подвала, который является самым нижним этажом здания. Во время экспериментов доступ на цокольный этаж был закрыт, чтобы обычные пользователи не могли получить несанкционированный сигнал. Результаты экспериментов по воздействию модифицированного сигнала показали, что пользователи, находящиеся как наверху, так и снаружи здания, нормально общаются с легитимной базовой станцией, не подвергаясь воздействию сигнала. Атака сигнального шторма, описанная в разделе 5.1.1, была проведена в экранированной тестовой сети оператора, так как атака может вызвать DoS в рабочей сети.

4.2 Практичность

В этом разделе мы оцениваем практичность и устойчивость атаки `SigOver` в условиях LOS/NLOS. Мы используем смартфон LG G7 ThinQ с SnapDragon845, который является новейшим LTE-чипсетом Qualcomm. Мы вводим пейджинговое сообщение с S-TMSI[4], намеренно установленным как недопустимое значение `0xAAAAAAAA`, чтобы отличить введенный подкадр от легитимных подкадров.

[4] S-TMSI - это сокращенная форма GUTI.

Таблица 2: Успешность атак `SigOver` и FBS *

Относительная мощность (дБ)	1	3	5	7	9
`SigOver`	38%	98%	100%	100%	98%
Относительная мощность (дБ)	25	30	35	40	45
Атака FBS	0%	0%	80%	100%	100%

* FBS устанавливает ту же полосу частот, PCI, MIB и SIB1, что и легитимная ячейка. Если UE-жертва садился на FBS в течение 10 с после его срабатывания, атака считалась успешной. Эксперимент с FBS проводился 10 раз для каждого уровня мощности. Эксперимент `SigOver` проводился со 100 пейджинговыми сообщениями для каждого уровня мощности.

Таблица 3: Успешность атаки `SigOver` в различных условиях.

	LOS	NLOS
RRC Подключено	97%	98%
RRC Idle	100%	98%

Энергозатраты. Атака `SigOver` использует эффект захвата, когда вводится более сильный сигнал, чтобы затмить легитимный сигнал, который находится на более низком уровне мощности. Более того, мы подаем 100 пейджинговых сообщений на UE-жертву в состоянии *RRC Idle* и измеряем успешность атаки в зависимости от относительной мощности между поданным и легитимным сигналами в среде LOS. В таблице 2 показано, что атака `SigOver` достигает успеха в 98% при 3 дБ.

Стойкость атаки. В таблице 3 приведены показатели успешности атаки `SigOver` для различных комбинаций экспериментальных настроек (LOS/NLOS) и состояний RRC (Idle/Connected). Каждое измерение представляло собой среднее значение 120 инжектированных пейджинговых сообщений. В состоянии *RRC Idle* мы вводим пейджинговое сообщение точный момент пейджинга (например, субкадр 9) и пейджинговый кадр (например, SFN%256 = 144) для UE-жертвы. Как обсуждалось в разделе 3.3, в состоянии *простоя RRC* оценка канала выполняется только по инжектированному сигналу, в то время как в состоянии *соединения RRC* рассматривается среднее значение канала, оцененного по набору инжектированных и легитимных сигналов. Другими словами, в состоянии *RRC Idle* инжектированные сигналы декодируются индивидуально, без влияния легитимных сигналов; таким образом, успешные атаки (т. е. правильное декодирование) могут быть достигнуты с помощью одной инжекции. Однако в состоянии *RRC Connected* для преодоления влияния легитимных сигналов требуется повторная инъекция. Для этого мы вводим пейджинговое сообщение в точный момент/кадр пейджинга для UE-жертвы. Одновременно мы также вводим подкадр с RS в каждом SFN, чтобы отразить канал вводимого сигнала и обеспечить успешную атаку. Как показано в табл. 3, коэффициент успешности атаки `SigOver` превысил 97 % в различных состояниях RRC, а также при настройках LOS и NLOS, что подтверждает устойчивость атаки `SigOver` по отношению к режимам работы и факторам окружающей среды (например, многоканальность). Наконец, во время экспериментов UE-жертва не сообщал о сбоях в радиоканале и не инициировал восстановление радиосоединения (т. е. запрос `RRC Reestablishment`). Это означает, что атака `SigOver` не наносит ущерба UE-жертве и его сервисам. Более того, мы убедились, что атака `SigOver` сохраняет 100-процентный коэффициент успешности для более чем 100 сообщений SIB 1 и SIB 2 в состоянии *простоя RRC* и при установке LOS.

Таблица 4: Допустимое время работы двух смартфонов.

Время (*мкс*)	LG G7 (Qualcomm)	Galaxy S9 (Exynos)
Мин.	-2.93	-2.60
Макс.	9.77	8.46
Максимальный допуск*	12.7	11.06

* Обратите внимание, что атака SigOver успешна, если *d*< Макс. допуск, независимо от радиуса ячейки; где *d* определено в разделе 3.4.

Охват атаки. Как описано в разделе 3.4, подстроенный субкадр может поступить на UE-жертву с небольшим временным смещением из-за задержки распространения инжектированного сигнала от at-таккера до UE-жертвы. Декодирование поддельного субкадра
требует, чтобы смещение было ограничено в пределах допустимого диапазона чипсета LTE UE. Таким образом, наибольшее допустимое смещение определяет максимальную задержку распространения; или, эквивалентно, максимальное расстояние между злоумышленником и UE (т. е. зону покрытия атаки). Охват атаки был оценен экспериментально, при этом задержка распространения между злоумышленником и UE эмулировалась путем сдвига по времени таймингов передачи подстроенных субкадров. Мы постепенно изменяли сдвиг в единицах 10 сэмплов (=0,33 мкс при 30,72 М/с) до тех пор, пока поддельные субкадры не были декодированы, что указывает на максимальную допустимую задержку. В таблице 4 представлены результаты измерений задержки, полученные на двух смартфонах с разными базовыми частотами - LG G7 (Qualcomm) и Galaxy S9 (Exynos). Смещение допуска постоянно превышало 8,66 *мкс* во всех случаях. С учетом зависимости между допуском и расстоянием, рассмотренной в разделе 3.4, результаты показывают, что атака SigOver может охватывать всю городскую соту (типичный радиус 1,5 км) в любое время, независимо от взаимного расположения UE и атакующего.

5 Сценарии атак и их последствия

В этом разделе представлены несколько сценариев атак с использованием SigOver, а также их практические последствия. Атака SigOver может быть использована для эксплуатации двух широковещательных сообщений: SIB и пейджинга. Все атаки были проведены в системе LOS, представленной в разделе 4, за исключением атаки сигнального шторма. Для проверки предложенных атак на различных типах чипсетов базовой полосы использовались десять смартфонов с поддержкой LTE: один Intel (iPhone XS), шесть Qualcomm (Galaxy S4/S8/S9, LG G2/G6/G7) и три Exynos (Galaxy S6/S8/S9), оснащенных чипсетами.

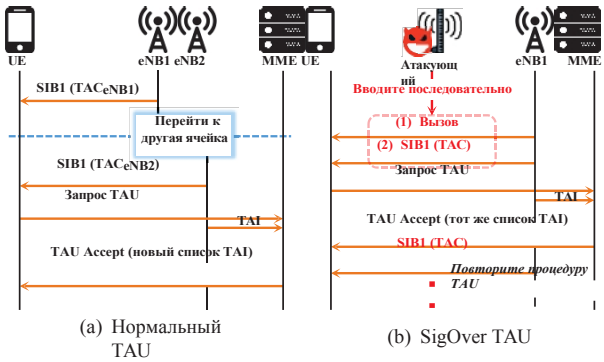
5.1 Атаки, использующие SIB

В этом разделе мы рассмотрим два типа атак с использованием SIB-инъекций, а именно сигнальный шторм и выборочный DoS.

5.1.1 Сигнальный шторм

Механизм атаки. Когда UE переходит в новую соту, UE извлекает код зоны отслеживания (TAC[5]), содержащийся в SIB1, из новой соты и проверяет его с помощью списка TAI в

[5] TAC - это сокращенная форма TAI.



(a) Нормальный TAU (b) SigOver TAU

Рисунок 8: Нормальный и атакующий случай для процедур TAU

UE. Если TAC не включен в список TAC на UE, UE инициирует процедуру TAU, чтобы уведомить сеть LTE об обновленном TAC. Атака SigOver приводит к сигнальному шторму путем многократного запуска недействительных TAU. На рис. 8 показан процесс атаки в сравнении с нормальной (т. е. без атаки) операцией. Сначала злоумышленник затеняет пейджинговое сообщение с полем system_Info_Modification, установленным как true, тем самым заставляя UE прочитать SIB1. Затем SIB1 затеняется с помощью поддельного TAC, что приводит к TAU. Следует отметить, что сообщения запроса TAU направляются на легитимный eNB, поскольку атака SigOver сохраняет радиосвязь между жертвой и легитимным eNB. Повторение этой процедуры приводит к сигнальному шторму в сети LTE. Напротив, при нормальных условиях TAU выполняется только один раз, каждый раз, когда UE переходит на другой TA, не включенный в список TAI.

Проверка. Данная атака была проверена на тестовой LTE-сети оператора с девятью LTE-устройствами[6], зарегистрированными в тестовой сети. На каждом устройстве были запущены инструменты диагностического мониторинга (например, SCAT, XCAL [8, 42]) для анализа сигнальных сообщений со стороны UE на протяжении всей атаки. Рисунок 9 показывает, что одно UE выполняет в среднем семь процедур TAU в секунду, что маловероятно в обычных условиях без атаки. Более того, сигнальные сообщения со стороны UE были проанализированы, чтобы лучше понять поведение сети в условиях атаки. Когда UE-жертва выполняет TAU с поддельным TAC (независимо от достоверности значения TAC), сеть возвращает тот же список TAC, который был предоставлен ранее при легитимной регистрации. Это происходит потому, что обслуживающая ячейка не изменилась. То есть список TAC по-прежнему не включает поддельный TAC жертвы UE. Следовательно, UE-жертва повторно выполняет TAU после получения сообщения SIB1 от злоумышленника. По данным Nokia [31], в часы пиковой нагрузки UE генерирует около 45 запросов на обслуживание[7]. Однако сигнальный шторм, вызванный атакой SigOver, приводит к более значительному сетевому трафику, например, атакующий способен вызвать в среднем 25 200 TAU на UE за один раз.

[6] iPhone был исключен, поскольку наш инструмент мониторинга не поддерживает это

[7] UE отправляет запрос на обслуживание во время инициации соединения с сетью LTE.

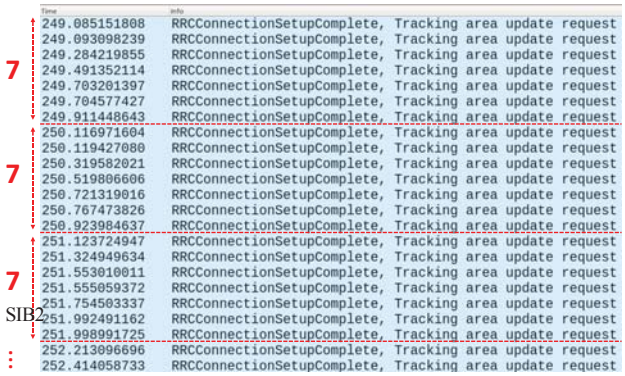


Рисунок 9: Снимок Wireshark сообщений `TAU Request`, сгенерированных в результате подмены SIB1.

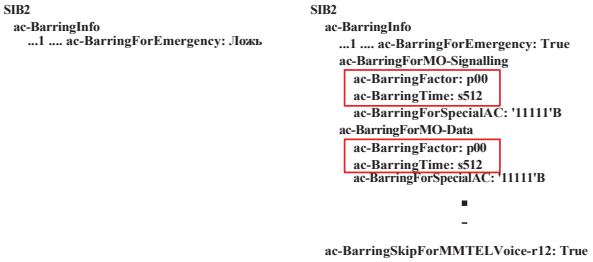
час. Учитывая, что количество сигнальных сообщений, генерируемых через TAU и сервисный запрос, одинаково, злоумышленник может генерировать больше трафика, чем в час пик, в 560 раз. Это наглядно демонстрирует значительное влияние атаки "сигнальный шторм", которая создает большую нагрузку на сеть и приводит к сильному разряду батареи UE.

Усиленное влияние чипсета Qualcomm. Устойчивая атака "сигнальный шторм" требует от злоумышленника постоянного ввода сообщений SIB1. Однако смартфоны, базовым блоком Qualcomm (например, Galaxy S4/S8/S9, LG G2/G6/G7), давали сбои, генерируя TAU неограниченное количество раз после однократной инъекции SIB1. В частности, UE продолжал выполнять процедуру TAU даже после того, как злоумышленник прекратил инъекцию SIB1[8]. Неисправное UE демонстрирует пользователю нормальное поведение, что говорит о том, что услуга передачи данных/вызова может использоваться без помех для пользователя. Хотя неисправность можно устранить, переведя UE в авиарежим, пользователь вряд ли сделает это, не заметив никаких проблем. Это говорит о том, атака устойчива, даже если приложить малозатратные усилия для усиления ее воздействия.

Невозможность использования FBS или неавторизованных UE. Атака сигнального шторма кажется достижимой с помощью FBS. Однако внедрение вредоносного SIB1 (содержащего поддельный TAC) через FBS не приводит к атаке сигнального шторма. Это объясняется тем, что при использовании FBS запрос `TAU` от UE-жертвы направляется в FBS, а не в легитимную сеть LTE. Другими словами, сигналы не достигают сети LTE; таким образом, атака сигнального шторма по своей сути недостижима для FBS. Более того, использование нескольких неавторизованных UE может спровоцировать сигнальный шторм в сети. Однако этот подход ограничен в отношении масштабируемости, поскольку для того, чтобы вызвать тот же эффект, что и при атаке `SigOver`, требуется несколько радиоустройств и SIM-карт для каждого устройства. На сайте

[8]Основной причиной этой неисправности является логика реализации чипсета Qualcomm LTE, которая не считывает SIB1 после завершения работы.

TAU. В результате они не смогли распознать легитимный SIB1, содержащий правильный TAC, и TAU выполнялся до повторного считывания легитимного SIB1.



(a) Оригинальный (b) Вредоносный SIB2

Рисунок 10: Функция управления доступом в сообщении SIB2

С другой стороны, атака `SigOver` использует одно радиоустройство, охватывающее всю соту, и заставляет нескольких аутентичных пользователей, находящихся в соте, инициировать процедуру TAU.

5.1.2 Избирательный DoS с помощью запрета доступа

Механизм атаки. Сотовая сеть контролирует количество UE, которые могут получить доступ к сети. Эта функция для управления объемом трафика и поддержания стабильности сети в определенных условиях, например, при стихийном бедствии. Контроль осуществляется с помощью параметра *BarringFactor* в SIB2, который используется атакой `SigOver` для блокировки UE-жертвы. Установив значение *BarringFactor* равным 0 (через затенение), злоумышленник может ограничить весь трафик данных и сигнализацию от UE (т. е. мобильное происхождение)[9], что приводит к DoS.

На рис. 10 представлена конфигурация вредоносного SIB2 в подстроенном субкадре в сравнении с оригинальным SIB2 в легитимном субкадре. Чтобы максимизировать воздействие атаки, `SigOver` устанавливает *BarringTime* на 512 с, что является максимальным значением в соответствии со стандартом. Обратите внимание, что *время Bar- ringTime* может быть обновлено, если злоумышленник повторит атаку в течение оставшегося *времени BarringTime*; таким образом, может быть достигнут постоянный DoS. Чтобы должным образом внедрить модифицированный субкадр (аналогично сигнальному шторму), злоумышленник сначала затеняет пейджинговое сообщение с помощью `system_Info_Modification`. После этого она подслушивает легитимный SIB1, чтобы извлечь SFN, из которого злоумышленник может получить расписание следующего SIB2 для затенения. Потенциальным расширением этой атаки является сервис-специфический DoS *для выборочного* блокирования только целевых сервисов (например, голосовых вызовов, видеоконференций и SMS). Для этого используется новая функция запрета конкретных услуг, представленная в спецификациях 3GPP [7].

Проверка. Эта атака была проверена на 10 различных моделях смартфонов. После успешной атаки `SigOver` (т. е. получения инжектированного пейджинга и SIB2) все сервисы передачи данных, включая просмотр веб-страниц и потоковое видео, были заблокированы на всех 10 устройствах. Анализ журналов устройств показал, что все устройства не смогли инициировать ни одного соединения, когда приложения делали несколько запросов на соединение. Это подтверждает целесообразность блокировки с помощью `SigOver`. Более того, DoS, специфичный для конкретного сервиса, был подтвержден с помощью

[9] Злоумышленник также может заблокировать мобильный конечный трафик, канал пейджинга на UE-жертве.

Samsung Galaxy S9 на базе чипсета Exynos. **Сравнение с FBS.** FBS также может внедрить вредоносный SIB2. Однако атака действует только при включенном FBS и немедленно прекращается при его выключении. Это происходит потому, что UE-жертва подключается к легитимной соте вскоре после отключения от FBS. Во время подключения к легитимной соте пострадавшее UE считывает легитимный SIB2, который восстанавливает услуги UE. И наоборот, услуги UE-жертвы остаются заблокированными после прекращения атаки `SigOver`, поскольку при этом не происходит повторного выбора соты. Кроме того, FBS не может достичь DoS с выбором услуг, поскольку не может предоставлять услуги LTE.

5.2 Атаки, использующие подкачку

В этом разделе мы представим три атаки с помощью `SigOver` на пейджинговое сообщение: DoS-атака, падение сети и отслеживание местоположения.

5.2.1 DoS-атака путем затенения пейджинга с помощью IMSI

Механизм атаки. Когда GUTI UE недоступен, сеть посылает пейджинговое сообщение с IMSI в качестве идентификатора UE. Как определено в стандартах 3GPP, после получения сообщения, содержащего IMSI, UE завершает все сеансы обслуживания и инициирует процедуру регистрации, используя IMSI в качестве идентификатора [5]. Это означает, что DoS-атака может быть реализована путем инъекции пейджингового сообщения с IMSI[10]. Точнее, злоумышленник вводит пейджинговое сообщение, содержащее IMSI UE-жертвы, в пейджинговом ок-казионе/кадре UE-жертвы. Эта атака отрывает UE от услуг сотовой сети, которые включают голосовые вызовы и услуги передачи данных, что свидетельствует о DoS на UE. Поскольку процедура регистрации (которая следует за прекращением предоставления услуг) автоматически восстанавливает услуги, атака поддерживается путем повторной отправки пейджингового сообщения.

Проверка. Эта атака была проверена на 10 различных моделях смартфонов в двух различных состояниях работы (*RRC Idle* и *RRC Connected*). В частности, в состоянии *RRC Idle* мы убедились, что UE успешно получили затененное пейджинговое сообщение. Более того, внутренние журналы UE подтвердили ожидаемое воздействие атаки, т. е. отсоединение от сети с последующей процедурой регистрации, что привело к DoS.

Для следующего эксперимента мы запустили атаку на UE в состоянии *RRC Connected*. Обратите внимание, что атака `SigOver` позволяет злоумышленнику передать поддельное сообщение UE по существующему радиосоединению между UE и eNB. Сначала мы совершили голосовой вызов на UE-жертве, чтобы UE войти в состояние *RRC Connected*. Затем мы передали UE сообщение с IMSI. Интересно отметить, что не все UE обрабатывают пейджинговые сообщения в состоянии *RRC Connected*. В частности, Samsung Galaxy S8/S9, LG G6/G7 (Qualcomm), Samsung Galaxy S8/S9 (Exynos) и Apple iPhone XS (Intel) правильно обработали пейджинговый месседж с IMSI, после чего вызов был немедленно прерван (завершение обслуживания). Между тем Samsung Galaxy S6 (Exynos), а также Galaxy S4, LG G2 (Qualcomm) не ответили на атаку в состоянии *RRC Connected*.

Несоответствия между устройствами обусловлены неоднозначностью стандартов 3GPP. Механизм, используемый для обработки пейджинга в состоянии *RRC Connected*, определен нечетко, без конкретных указаний на пейджинг с IMSI, например, только формирование пейджинга с уведомлением о системной информации или CMAS/ETWS [3]. В итоге, путем инъекции пейджингового сообщения с IMSI, атака `SigOver` может реализовать DoS на UE-жертве в состояниях *RRC Idle* и *RRC Connected*, в зависимости от устройства.

Сравнение с FBS. Этот сценарий атаки был подробно рассмотрен в предыдущих работах [21, 35] с использованием FBS. Хотя воздействие и векторы атаки эквивалентны, применимость существующих атак ограничена по сравнению с атакой `SigOver`. Это связано с тем, что атака `SigOver` позволяет злоумышленнику доставить пейджинговое сообщение на UE, имеющее активное радиосоединение с сетью, в то время как другие работы применимы только к UE, не использующим никаких услуг, что указывает на более широкую применимость атаки `SigOver`.

5.2.2 Атака на понижение рейтинга сети с помощью CS Paging

Механизм атаки. При этой атаке злоумышленник вводит пейджинговое сообщение с уведомлением о коммутации каналов (CS) (с S-TMSI UE-жертвы), чтобы намеренно понизить рейтинг UE-жертвы до сети 3G. После получения пейджингового сообщения CS UE инициирует процесс переключения на обратный канал и переходит в сеть 3G. Таким образом, атака `SigOver` позволяет злоумышленнику заставить UE перейти на более медленное соединение.

Проверка. Мы экспериментально подтвердили, что UE жертвы в состоянии *RRC Idle* немедленно переключался на сеть 3G при получении CS-пейджинга злоумышленника, после чего вскоре возвращался обратно в сеть LTE из-за отсутствия актуального сервиса в сети 3G. Атака была эффективна для современных смартфонов, например Samsung Galaxy S8/S9, LG G6/G7 (Qualcomm) и Samsung Galaxy S8/S9 (Exynos), поскольку они могли отвечать на сообщение CS-пейджинга как в состоянии *RRC Idle*, так и в *состоянии RRC Connected*. Однако, как и в случае с пейджинговой атакой с IMSI, некоторые смартфоны не отвечали на пейджинг CS в состоянии *RRC Connected* и, следовательно, были защищены от атаки. Интересно, что когда Samsung Galaxy S8 (Qualcomm) в результате атаки перешел в сеть 3G, LTE-соединение так и не было восстановлено при использовании услуги передачи данных.

Сравнение с существующими атаками. Tu *et al*. продемонстрировали атаку снижения пропускной способности на UE-жертву, вызвав пейджинг CS, что похоже на нашу атаку [47]. Однако в этом исследовании сеть была вынуждена отправлять пейджинговое сообщение от имени атакующего, устанавливая

[10] Приобретение IMSI подробно рассматривается в предыдущих работах [11, 44].

вызов с UE в сети 3G. Следует отметить, что при атаке SigOver пейджинговое сообщение передается непосредственно злоумышленником. Эта атака по своей сути раскрывает номер телефона злоумышленника, что делает атаку легко обнаруживаемой оператором. В отличие от этого, атака SigOver беззвучно передает пейджинговое сообщение CS на UE-жертву. Кроме того, в существующих работах не удается перевести UE-жертву в состояние *RRC Connected* в сети 3G, поскольку сеть не отправляет пейджинговое сообщение на UE-жертву в состоянии *RRC Connected*; в то время как атака SigOver может доставить пейджинговое сообщение.

5.2.3 Крупномасштабное отслеживание UE

Механизм атаки. Как объясняется в разделе 2, после завершения процедуры RA UE пытается установить RRC-соединение, отправляя в соту запрос на соединение (содержащий идентификатор UE). Если UE обладает ранее назначенным временным идентификатором (т.е. S-TMSI), то этот идентификатор также включается в запрос на соединение. В противном случае выбирается случайное значение. После получения запроса UE сота отвечает установкой соединения, содержащей идентификатор UE (S-TMSI или случайное значение). Проверяя эту идентификацию, каждое UE может определить, была ли процедура RA успешной. Если процедура не удалась, UE повторяет процедуру RA. Вышеупомянутая процедура, используемая для разрешения конфликтов соединений, называется *разрешением противоречий*. В этой атаке злоумышленник использует технику разрешения конфликтов для выполнения грубого отслеживания местоположения жертвы. Сначала злоумышленник, зная S-TMSI UE жертвы, отправляет пейджинговое сообщение с S-TMSI[11]. Затем злоумышленник подслушивает сообщения установки соединения, передаваемые из легитимной соты[12]. При получении сообщения установки соединения, содержащего S-TMSI UE-жертвы, злоумышленник подтверждает, что UE-жертва находится в зоне действия соты, прослушивая нисходящие сообщения.

Проверка. Мы проверили эту атаку, используя все модели смартфонов, представленные в данной работе. Мы подтвердили, что злоумышленник определить присутствие UE-жертвы путем инъекции одного пейджингового сообщения и подслушивания сообщения о настройке соединения, отправленного на UE-жертву.

Сравнение с FBS. FBS может достичь тех же результатов, отслеживая IMSI в сообщении Identity Response. Однако FBS требует активного соединения с жертвой для передачи сообщения. Таким образом, атака ограничена FBS в отношении скрытности и энергоэффективности. В предыдущем исследовании сообщалось, что сопоставление RNTI-TMSI может применяться для пассивного мониторинга TMSI жертвы [37]; однако атака SigOver обеспечивает активный метод, с помощью которого можно определить местонахождение жертвы.

[11]Из-за недостатка места подробное обсуждение того, как злоумышленник получает S-TMSI целевого UE, было опущено. Однако этот вопрос был подробно рассмотрен в предыдущих работах [19, 22, 23, 37].

[12]Поскольку процедура соединения RRC не зашифрована, злоумышленник может
подслушивать любые сообщения нисходящей линии связи во время процедуры соединения UE.

6 Защита от атаки SigOver

В этом разделе мы представим два варианта стратегии защиты от атаки SigOver. Мы начинаем с обоснования целесообразности фундаментального решения в качестве превентивной меры, при которой все широковещательные сигналы подписываются цифровой подписью использованием инфраструктуры открытых ключей (PKI). Затем мы обсуждаем краткосрочное решение для обнаружения атаки SigOver, которое использует изменение природы физического сигнала во время обработки заслоняющего сигнала.

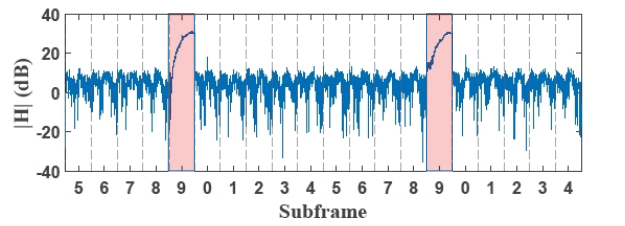
6.1 Цифровая подпись широковещательных сообщений

Поскольку атака SigOver использует отсутствие защиты целостности в широковещательных сообщениях, одним из естественных способов защиты от атаки SigOver является использование защиты целостности в сообщениях с помощью схемы цифровой подписи. Для этого каждая базовая станция иметь сертификат, выданный ее оператором, а UE должен быть снабжен корневым сертификатом (например, самоподписанным оператором) для проверки сертификата базовой станции. Однако такая естественная защита имеет, по крайней мере, несколько проблем, связанных с развертыванием и техническими аспектами.

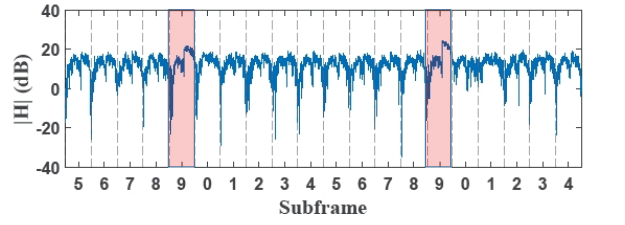
Проблемы развертывания: В 5G 3GPP ввел шифрование IMSI с открытым ключом при первоначальной регистрации, чтобы обеспечить защиту конфиденциальности постоянного идентификатора. Для этого каждому UE предоставляется открытый ключ его домашнего оператора, поэтому предполагается, что механизм предоставления открытого ключа для UE уже существует. Этот механизм предоставления может также использоваться для предоставления открытого ключа (или сертификата подписи) для проверки сертификата базовой станции. Однако в сценариях роуминга UE необходимо получить открытый ключ оператора посещаемой сети, которому доверяет домашний оператор. Это, по сути, требует PKI для глобальных сетей сотовой связи, охватывающих весь мир, и нетривиальных отношений доверия между несколькими операторами в разных юрисдикциях. Кроме того, еще одним очевидным бременем является управление списками отзыва сертификатов.

Технические проблемы: Подписание каждого отдельного широковещательного сообщения может привести к значительным вычислительным затратам на базовой станции, учитывая низкую периодичность основных широковещательных сообщений, таких как MIB (40 мс) и SIB1/2 (80 мс). Кроме того, увеличение размера сообщения в связи с передачей подписи и сертификата (например, при использовании нового SIB) приведет к увеличению энергопотребления базовой станции. Аналогично, с точки зрения UE, проверка сертификата и подписи потребует дополнительного потребления энергии, что приведет к более быстрому разряду батареи. Такое энергопотребление может быть нежелательным для маломощных устройств Интернета вещей, которые должны жить много лет без замены батарей.

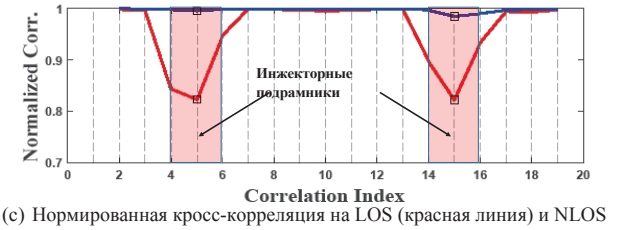
Схема подписи на основе идентификатора (IBS) [9, 41] может рассматриваться как экономически эффективная альтернатива, поскольку она имеет существенно низкие затраты на управление ключами и исключает затраты на передачу и проверку сертификатов. Однако IBS требует от UE синхронизации с открытыми параметрами KMS [17]. Это проблематично для UE, которые не имеют



(a) Настройка LOS



(b) Настройка NLOS



(c) Нормированная кросс-корреляция на LOS (красная линия) и NLOS (синяя линия)

Рисунок 11: Колебания величины оценки канала после атаки `SigOver`: Внезапные изменения величины могут быть использованы для метрики обнаружения.

подписки, так как они могут не получить публичные параметры из сети. Обратите внимание, что устройства без подписки также должны получать сообщения ETWS или CMAS, если у них есть возможности сотовой связи.

6.2 Использование разнообразия каналов

Согласно теории связи, беспроводной канал значительно изменяется при смещении всего на четверть длины волны, что составляет 3,57 см для 2,1 ГГц LTE [46]. Это называется разнообразием каналов, и оно очень применимо к атакующему и жертве UE, которые, как ожидается, будут находиться в разных местах - т. е. беспроводной канал между атакующим и UE, скорее всего, будет отличаться от канала между eNB и UE. Поэтому подача атакующего сигнала, который отражает канал между атакующим и UE, естественным образом заставляет информацию о канале, восстановленную на UE, отклоняться от того, когда присутствуют только легитимные субкадры (без атаки). Другими словами, обнаружение такого отклонения в канале может служить в качестве техники защиты.

Беспроводной канал можно условно представить в виде H [46] в комплексном представлении. Величина $H||$ однозначно определяет различные беспроводные каналы в зависимости от того, насколько эффективно мощность сигнала. Следовательно, резкое изменение $H||$ является эффективной метрикой для обнаружения атаки `SigOver`.

На рисунке 11a представлены $H||$ инжектированного (субкадр 9) и легитимного сигналов, измеренных во время эксперимента в условиях LOS, когда злоумышленник находится на расстоянии 2 м от UE жертвы. Это наглядно демонстрирует сильные колебания $H||$ во время атаки, что свидетельствует о легкости обнаружения.

Несмотря на эффективность, надежность использования канала проблематична. В частности, общее применение методики к различным сценариям не является тривиальным различных факторов, потенциально влияющих на H. На рис. 11b показан пример отказа обнаружения в установке NLOS, когда мощность инжектированного сигнала была низкой. То есть влияние атакующего сигнала на H постепенно ослабевает по мере уменьшения энергии, вплоть до того, что его трудно обнаружить. Рисунок 11c наглядно демонстрирует эту проблему, где падение корреляции было нечетким в установке NLOS, в отличие от установки LOS (сильный инжекционный сигнал). Таким образом, использование канала является потенциальным решением, но мы оставляем разработку надежных методов в качестве будущей работы.

6.3 Обсуждение потенциальных решений

Оба подхода, рассмотренные в предыдущих разделах, имеют проблемы, которые необходимо решить, и/или ограничения. Однако отметим, что продемонстрированные в разделе 5 эксплойты - это лишь несколько примеров, а не исчерпывающий список. Последствия атаки `SigOver` будут более масштабными и разрушительными, если сотовая сеть будет использоваться в критически важных областях, например, в автомобильных сетях и промышленных системах. Поэтому, в принципе, необходимо внутренние уязвимости сотовой системы в области широковещания. В то же время рекомендуется, чтобы критически важные службы имели собственную защиту безопасности, а не полагались на защиту других уровней протокола. Например, проблему ETWS или CMAS лучше решать на уровне приложений[13], а не на основе защиты SIB, поскольку SIB является лишь транспортным механизмом для этих критических прикладных сообщений.

7 Связанные работы

В этом разделе мы описываем предыдущие работы, использующие концепцию затенения сигнала. Затем мы представляем сигнальный шторм, а также атаки, использующие защиту от нецелостности.

Затенение сигнала в беспроводном канале. Атаки на затенение сигнала, использующие открытую среду и эффект захвата, широко применяются в проводных системах, таких как GPS [20, 45] и низкоскоростные беспроводные персональные сети (LR-WPAN) [52]. Пёппер *и др.* представили атаку с подменой символов в канале с аддитивным белым гауссовским шумом (AWGN) [34], с тонким затенением сигнала на уровне символов. Однако для этого требуется точная информация о времени, амплитуде и фазе, что труднодостижимо в реальных условиях.

[13] 3GPP уже провела исследование аспектов безопасности системы общественного оповещения (PWS) [4].

мир. Аналогично данному исследованию, Вильгельм и др. продемонстрировали возможность затенения сигнала и его влияние на IEEE
802.15.4 [52]. По сравнению с этим, атака SigOver является первым комплексным исследованием, в котором реализовано затенение сигнала в LTE, а также подтверждена его осуществимость. Более того, мы новые сценарии атак с использованием атаки SigOver.

Манипулирование сообщениями в LTE. LTEInspector [21] обнаружил атаку на перехват пейджингового канала и атаку с подстановкой пейджинговых сообщений, что похоже на данное исследование. Однако данное исследование имеет два ключевых отличия: 1) определение атаки вклинивания и 2) метод ее реализации. Во-первых, при атаке SigOver жертва беззвучно инжектирует вредоносные сообщения, одновременно заставляя жертву продолжать синхронизироваться с легитимным eNB. В результате во время атаки SigOver ответное сообщение по восходящей линии связи жертвы естественным образом отправляется на легитимный eNB. Однако в LTEInspector UE-жертва передал свое ответное сообщение по восходящей линии связи вредоносному eNB после получения манипулированного сообщения, что является универсальным ответным действием для атаки с FBS. Таким образом, она более похожа на существующие атаки с использованием FBS. Во-вторых, атака SigOver перезаписывает целевой сигнал вредоносными сигналами, не требуя соединения с вредоносной базовой станцией. Для этого мы исследуем различные требования к атаке SigOver, как описано в разделе 3. Несмотря на другие требования, LTEInspector рассматривал только цикл пейджинга и его время, которые являются частью требований синхронизации по времени.

Атаки, использующие защиту от нецелостности. Был проведен обширный повторный поиск по манипулированию сообщениями с отсутствующей/слабой защитой целостности [21, 22, 26, 36, 39, 40]. Как обсуждалось в разделе 3.5, такие атаки в основном используют FBS. Хотя они используют широковещательные сообщения в LTE, эти атаки имеют ограниченные последствия. Это связано с тем, что их логика работы неизбежно приводит к ограничениям в отношении скрытности, энергоэффективности и устойчивости атак.

8 Заключительные замечания и дальнейшая работа

Затенение сигнала - интуитивно понятный метод манипулирования широковещательными сообщениями LTE без защиты целостности, который не рассматривался в предыдущих исследованиях. В этой статье мы представляем атаку SigOver, которая является первой реализацией атаки на затенение сигнала в сети LTE. Мы реализуем атаку SigOver с помощью недорогого SDR и библиотеки LTE с открытым исходным кодом, решая при этом проблемы, связанные с удовлетворением строгих требований к передаче и созданием вредоносного кадра. Осуществимость и эффективность атаки SigOver была продемонстрирована на примере пяти новых атак, а также был обширный анализ относительных преимуществ атаки SigOver перед атаками FBS и MitM. Ключевыми особенностями атаки SigOver являются скрытность, энергоэффективность и устойчивость, которые не были достигнуты одновременно предыдущими атаками. Оценка показала, что атака SigOver достигает 98 % успеха при низких стоимость электроэнергии.

Наконец, были предложены два потенциальных подхода к защите от атаки SigOver, которые используют цифровую подпись и разнообразие каналов. Как известно, оба подхода имеют свои проблемы и ограничения, которые необходимо решить, однако они могут быть использованы в качестве основы разработки надежного и прочного решения.

Сотовая индустрия стремительно переходит к сети 5G - системам сотовой связи, оснащенным передовыми радиотехнологиями и улучшенными средствами безопасности. Однако фундаментальные вопросы безопасности вещания, рассмотренные в данной статье, не нашли своего . Учитывая значительные изменения, внесенные в новое радио 5G (NR), оценка 5G NR против атаки SigOver остается в будущем. Поскольку данная статья привлекает внимание к безопасности широковещательных сообщений, мы считаем, что стандартный орган 3GPP и сообщество сотовых сетей должны серьезно подойти к разработке широковещательных сообщений.

Благодарности

Мы искренне благодарим доктора Су Бум Ли за его подробные и ценные комментарии к ранней версии проекта. Кроме того, мы хотели бы поблагодарить анонимных рецензентов за их внимательные комментарии. Работа выполнена при поддержке гранта Института планирования и оценки информационно-коммуникационных технологий (IITP), финансируемого правительством Кореи (MSIT) (2018-0-00831, A Study on Physical Layer Security for Het- erogeneous Wireless Network).

Ссылки

[1] 3GPP. ETSI TS 36.104. Базовая станция (БС), радиопередача и прием, 2017 г.

[2] 3GPP. ETSI TS 36.211. Физические каналы и модуляция, 2011 г.

[3] 3GPP. ETSI TS 36.331. Спецификация протокола RRC, 2017.

[4] 3GPP. TR 33.969. Исследование аспектов безопасности системы общественного оповещения (PWS), 2014 г.

[5] 3GPP. TS 24.301. Протокол Non-Access-Stratum (NAS) для Evolved Packet System (EPS); этап 3, 2017.

[6] 3GPP. TS 36.101. Передача и прием радиосигналов пользовательским оборудованием (UE), 2017.

[7] 3GPP. TS 36.331. Evolved Universal Terrestrial Ra- dio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification, 2017.

[8] ACCUVER. XCAL. http://accuver.com/acv_products/xcal/.

[9] Дэн Боне и Мэтт Франклин. Шифрование на основе идентификации с использованием пары Вейля. На *ежегодной международной конференции по криптологии*, стр. 213-229. Springer, 2001.

[10] Бруно Клеркс и Клод Оестгес. *Беспроводные сети MIMO: каналы, методы и стандарты для многоантенных, многопользовательских и многосотовых систем*. Academic Press, 2013.

[11] Адриан Дабровски, Никола Пьянта, Томас Клепп, Мартин Мулаццани и Эдгар Вайпль. IMSI - поймай меня, если сможешь: Ловцы IMSI-ловушек. В *материалах 30-й ежегодной конференции по приложениям компьютерной безопасности*, стр. 246-255. ACM, 2014.

[12] Себастьян Эггер, Тобиас Хоссфельд, Раймунд Шац и Маркус Фидлер. Время ожидания в качестве опыта для веб-сервисов. *Четвертый международный семинар по качеству мультимедийного опыта (QoMEX), 2012*, стр. 86-96. IEEE, 2012.

[13] Хуанита Эллис, Чарльз Пёрселл и Джой Рахман. *Конвергенция сетей передачи голоса, видео и данных: архитектура и дизайн, от VoIP до беспроводной связи*. Elsevier, 2003.

[14] Ettus. GPSDO OCXO. https://www.ettus.com/product/details/GPSDO-MINI.

[15] Ettus. Плата UBX 160 МГц. https://www.ettus.com/product/details/UBX160.

[16] Эттус. Спецификация USRP X300/X310. https://www.ettus.com/content/files/X300_X310_Spec_Sheet.pdf.

[17] Майкл Гровс. Elliptic Curve-Based Certificate- less Signatures for Identity-Based Encryption (ECCSI). *RFC6507*, 2012.

[18] GSA. Эволюция от LTE к 5G: состояние глобального рынка. Aug. 2018.

[19] Бьонгдо Хонг, Сангвук Бэ и Йонгдэ Ким. GUTI Reallocation Demystified: Отслеживание местоположения сотового телефона с изменением временного идентификатора. В *материалах Симпозиума по безопасности сетей и распределенных систем (NDSS)*, 2018.

[20] Тодд Е Хамфрис, Брент М Ледвина, Марк Л Псиаки, Брэди В О'Хэнлон и Пол М Кинтнер. Оценка угрозы спуфинга: Разработка портативного гражданского спуфера GPS. *Труды конференции лаборатории радионавигации*, 2008.

[21] Саид Рафиул Хуссейн, Омар Чоудхури, Шагуфта Мехназ и Элиза Бертино. LTEInspector: Системно-атический подход к адверсарному тестированию 4G LTE. В *материалах конференции по безопасности сетей и распределенных систем (NDSS)*, 2018.

[22] Хонгиль Ким, Джихо Ли, Юнкю Ли и Йонгдэ Ким. Прикосновение к неприкасаемым: Динамический анализ безопасности плоскости управления LTE. На *симпозиуме IEEE по безопасности и конфиденциальности (SP)*. IEEE, 2019.

[23] Денис Фу Куне, Джон Кельндорфер, Николас Хоппер и Йонгдэ Ким. Утечки данных о местоположении в воздушном интерфейсе GSM. *Труды симпозиума по безопасности сетей и распределенных систем (NDSS)*, 2012.

[24] Юнес Лабьяд, Мохаммед Моугит, Абдеррахим Марзук и Абделькрим Хакик. Влияние использования G. 729 на производительность передачи голоса по LTE. *Interna- tional Journal of Innovative Research in Computer and Communication Engineering*, 2(10), 2014.

[25] Чжэньхуа Ли, Вэйвэй Ван, Кристо Уилсон, Цзянь Чэнь, Чэнь Цянь, Тэхо Чжун, Лань Чжан, Кебин Лю, Си-Аньян Ли и Юньхао Лю. FBS-Radar: Обнаружение фальшивых базовых станций в масштабах дикой природы. In *NDSS*, 2017.

[26] Хуан Линь. LTE REDIRECTION: принуждение целевого сотового телефона LTE в небезопасную сеть. *Конференция по безопасности Hack In The Box (HITBSecConf)*, 2016.

[27] Константинос Манолакис, Давид Мануэль Гутьеррес Эстевез, Фолькер Юнгникель, Вэнь Сюй и Кристиан Дрюс. Закрытая концепция синхронизации и поиска ячеек в системах 3GPP LTE. *Конференция 2009 IEEE Wireless Commu- nications and Networking Conference*, страницы 1-6, апрель 2009.

[28] мини-схема. ZVE-2W-272. https://www.minicircuits.com/WebStore/dashboard.html?model=ZVE-2W-272%2B.

[29] Йохан Моберг, Маттиас Лёфгрен и Роберт С Карлссон. Пропускная способность канала случайного доступа WCDMA. На *саммите IST по мобильной связи*, 2000.

[30] Питер Ней, Ян Смит, Габриэль Кадамуро и Тадайоши Коно. SeaGlass: обеспечение защиты от IMSI-ловушек в масштабах города. *Proceedings on Privacy Enhancing Technolo- gies*, 2017(3):39-56, 2017.

[31] Дэвид Новосвиат. Управление сигнальным трафиком основной сети LTE. https://www.nokia.com/blog/managing-lte-core-network-signaling-traffic/.

[32] OPENBTS. Ettus Research USRP. http://openbts.org/w/index.php?title=Ettus_Research_USRP.

[33] Парк Шинджо, Альтаф Шайк, Равишанкар Боргаонкар, Ан-Дрю Мартин и Жан-Пьер Сейферт. White-Stingray: Оценка приложений для обнаружения IMSI-ловушек. На *семинаре USENIX по наступательным технологиям (WOOT). USENIX Association*, 2017.

[34] Кристина Пёппер, Нильс Оле Типпенхауэр, Борис Данев и Срджан Капкун. Исследование манипуляций с сигналами и сообщениями в беспроводном канале. В *материалах Европейского симпозиума по исследованиям в области компьютерной безопасности (ESORICS)*, 2011.

[35] Мухаммад Таки Раза, Фатима Мухаммад Анвар и Сонгву Лу. Выявление слабых мест в безопасности LTE на межпротокольном уровне и в . *In- ternational Conference on Security and Privacy in Com- munication Systems*, pages 312-338. Springer, 2017.

[36] Дэвид Руппрехт, Кай Янсен и Кристина Пёппер. Испытание функций безопасности LTE: A Frame- work to Evaluate Implementation Correctness. На *10-м семинаре USENIX по наступательным технологиям (WOOT)*, 2016.

[37] Дэвид Руппрехт, Катарина Колс, Торстен Хольц и Кристина Пёппер. Взлом LTE на втором уровне. На *симпозиуме IEEE по безопасности и конфиденциальности (SP)*. IEEE, 2019.

[38] Стефания Сезия, Мэтью Бейкер и Иссам Туфик. *LTE - долгосрочная эволюция UMTS: от теории к практике*. John Wiley & Sons, 2011.

[39] Альтаф Шаик, Равишанкар Боргаонкар, Н Асокан, Валт-Тери Ниеми и Жан-Пьер Сейферт. Практические атаки на конфиденциальность и доступность в системах мобильной связи 4G/LTE. *Труды симпозиума по безопасности сетей и распределенных систем (NDSS)*, 2016.

[40] Альтаф Шайк, Равишанкар Боргаонкар, Шинджо Парк и Жан-Пьер Сейферт. О влиянии неавторизованных базовых станций в самоорганизующихся сетях 4G/LTE. In *WISEC*, pages 75-86, 2018.

[41] Ади Шамир. Криптосистемы на основе идентификации и схемы подписи. На *семинаре по теории и применению криптографических методов*, страницы 47-53. Springer, 1984.

[42] Инструмент для сбора и анализа сигналов (SCAT). `https://github.com/fgsect/scat`.

[43] srsLTE. https://github.com/srsLTE/srsLTE.

[44] Дэхён Штробель. Ловец IMSI. *Кафедра безопасности коммуникаций, Рурский университет Бохума*, 14, 2007.

[45] Нильс Оле Типпенхауэр, Кристина Пёппер, Каспер Бонне Расмуссен и Срджан Капкун. О требованиях успешным атакам на спуфинг GPS. В *материалах 18-й конференции ACM по безопасности компьютеров и коммуникаций*, с. 75-86. ACM, 2011.

[46] Дэвид Тсе и Прамод Вишванатх. *Основы беспроводной связи*. Cambridge university press, 2005.

[47] Гуань-Хуа Ту, Чи-Ю Ли, Чуньи Пэн и Сонгву Лу. Как технология голосовых вызовов создает угрозы безопасности в сетях 4g lte. *Конференция IEEE по коммуникациям и сетевой безопасности (CNS), 2015*, с. 442-450. IEEE, 2015.

[48] Ян-Яап Ван де Бик, Магнус Санделл и Пер Ола Борхессон. ML-оценка временного и частотного смещения в OFDM-системах. *IEEE transactions on signal processing*, 45(7):1800-1805, 1997.

[49] Тхань Ван До, Хай Тхань Нгуен, Николов Момчил и др. Обнаружение IMSI-ловушек с помощью мягких вычислений. *Международная конференция по мягким вычислениям в науке о данных*, стр. 129-140. Springer, 2015.

[50] Ци Ванг, Кристиан Мельфурер, Кристиан Мельфурер и Маркус Рупп. Синхронизация несущей частоты в нисходящем канале 3GPP LTE. На *21-м ежегодном международном симпозиуме IEEE по персональной, внутренней и мобильной радиосвязи*, стр. 939-944, сентябрь 2010 г.

[51] Камин Уайтхаус, Алек Ву, Фред Цзян, Джозеф По-ластр и Дэвид Каллер. Использование эффекта захвата для обнаружения и восстановления столкновений. На конференции *Embedded Net- worked Sensors, 2005. EmNetS-II. The Second IEEE Workshop on*, pages 45-52. IEEE, 2005.

[52] Маттиас Вильгельм, Йенс Б. Шмитт и Винсент Лендерс. Практические атаки на манипулирование сообщениями в беспроводных сетях IEEE 802.15. 4. *Труды MMB & DFT*, 2012.

[53] Чжоу Жуань, Сяоюй Цзи, Таймин Чжан, Чжучуань Чжан, Вэньюань Сюй, Чжэньхуа Ли и Юньхао Лю. Fbsleuth: Криминалистика поддельных базовых станций с помощью радиочастотной печати пальцев. В *материалах Азиатской конференции по компьютерной и коммуникационной безопасности 2018 года*, стр. 261-272. ACM, 2018.

Приложение

A Влияние на качество услуг

Мы измеряем влияние качества услуг при атаке `SigOver`, когда вредоносные пейджинговые сообщения передаются в каждом субкадре 9. Это означает, что легитимные субкадры в субкадре 9 затеняются и теряются, а не затененные легитимные субкадры также могут быть затронуты поддельными субкадрами. В частности, RS недобросовестных субкадров нарушает оценку канала, усредненную среди недобросовестных и не затененных легитимных субкадров (в состоянии *RRC Connected*), что может нарушить эквализацию и привести к ошибкам. Несмотря на эти факторы, влияние атаки `SigOver` оказалось минимальным, что было продемонстрировано в данном разделе на ряде распространенных, но разных сервисов: голосовые вызовы, веб-серфинг, загрузка FTP и прямая трансляция. Отметим, что измерения проводились при надежной атаке `SigOver` (коэффициент успешности >97%) для UE в состоянии *RRC Connected*.

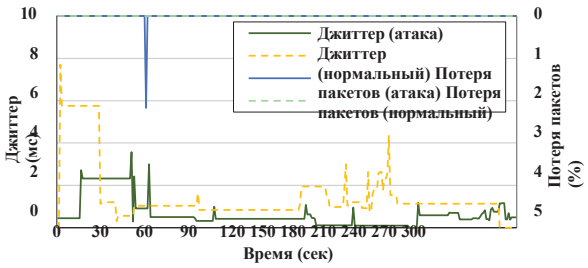


Рисунок 12: Джиттер вызова и потеря пакетов

Голосовой вызов. UE, работающие в сети LTE, используют в качестве сервиса голосовые вызовы по LTE (VoLTE). Мы оцениваем влияние атаки `SigOver` на ключевые факторы, касающиеся производительности VoLTE [13], или, эквивалентно, качества звонков, например, скорость передачи данных, джиттер и потери пакетов. Для сравнения эти показатели были измерены до и после атаки. Скорость передачи данных после атаки оставалась стабильной и для краткости не приводится. На рисунке 12 показаны джиттер и потеря пакетов. Джиттер постоянно составлял менее 10 мс, а потеря пакетов в основном нулю. Более того, оба показателя достаточны для поддержки высокого качества услуг связи [24]. Таким образом, атака `SigOver` остается незаметной, не снижая качества работы пользователей.

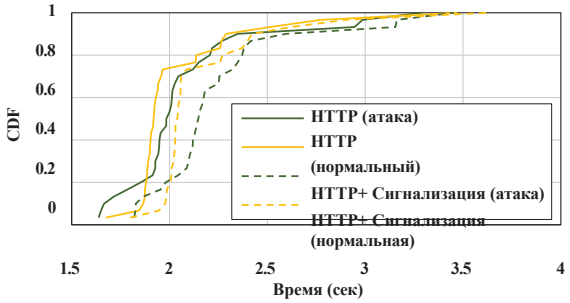


Рисунок 13: Время загрузки веб-страницы

Веб-браузинг. Мы распространили измерения на веб-браузинг, который является одним из наиболее часто используемых сервисов. В частности, время, необходимое для загрузки нескольких одинаковых веб-страниц с атакой и без нее. На рисунке 13 представлены результаты, где "HTTP" представляет собой общую продолжительность обмена данными HTTP для загрузки страницы. 'Signaling' - время, необходимое для установления соединения RRC. При атаке `SigOver` время от установления RRC-соединения до загрузки веб-страницы задерживается в среднем всего на 80 мс по сравнению со случаем без атаки. Предыдущие исследования [12] показали, что влияние такой задержки на качество обслуживания пренебрежимо мало.

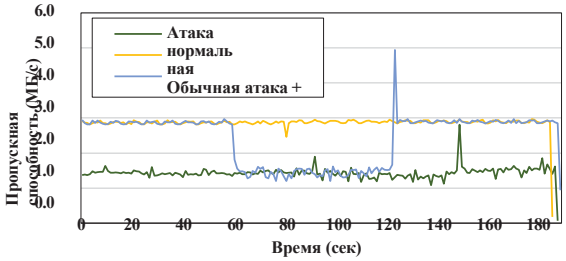


Рисунок 14: Пропускная способность FTP

Загрузка с FTP. На рисунке 14 показано, что производительность FTP значительно отличается при использовании `SigOver` at- tack. Это объясняется динамически управляемой модуляцией для преодоления битовых ошибок при передаче данных. Атака `SigOver` приводит к битовым ошибкам, которые вынуждают UE использовать надежную модуляцию QPSK, которая имеет ограниченную пропускную способность. В то же время без этой атаки битовая ошибка остается низкой. В этом случае UE использует 64QAM, который менее устойчив, но поддерживает более высокую пропускную способность, чем QPSK. Тем не менее, это влияние менее вероятно для пользователей, а FTP редко используется на смартфонах.

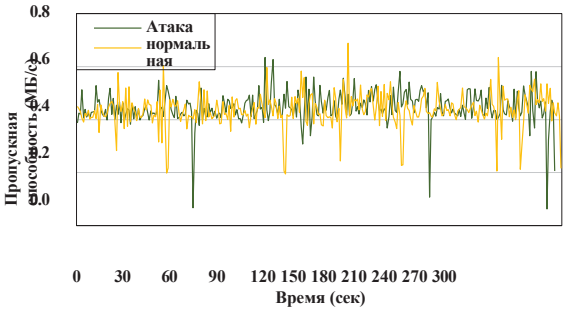


Рисунок 15: Пропускная способность YouTube Live: Среднее значение составило 0,445 и 0,436 МБ/с для атаки и нормального случая, соответственно.

Прямая трансляция. На рисунке 15 показана пропускная способность прямой трансляции YouTube с разрешением 1080p. В целом, при атаке `SigOver` на 5-минутный не возникло ни буферизации, ни прерывания. Результат прямой трансляции отличается от результата загрузки с FTP, так как пропускная способность потоковой передачи была не такой высокой, как у FTP.

B АКРОНИМЫ

3GPP Проект партнерства третьего поколения **AKA** Аутентификация и ключевое соглашение **AS** Страта доступа
CFI Индикатор формата управления
CMAS Коммерческая мобильная система оповещения
CQI Индикатор качества канала
CS Переключение цепи
DCI Информация управления нисходящей линии связи
eNB Эволюционировавший узел B
EPC Эволюционное пакетное ядро
ETWS Система предупреждения о землетрясениях и цунами
FBS Поддельная базовая станция
FDD Дуплекс с частотным разделением
GPSDO Дисциплинированный осциллятор GPS
GUTI Глобально уникальный временный идентификатор **IMSI** Международный идентификатор мобильного абонента **LOS** Линия видимости
LTE Долгосрочная эволюция
MIB Главный информационный блок **MME** Mobility Management Entity
NAS Страта без доступа
NLOS Нелинейная видимость
OFDM Ортогональное мультиплексирование с частотным разделением
PCFICH Индикатор формата физического управления CHannel
PCI Физический уровень Идентификация ячейки
PDCCH Физический канал управления нисходящим каналом **PDSCH** Физический общий канал нисходящего канала **PHICH** Физический канал индикации гибридного ответа **PRB** Блок физического ресурса
PSS Первичный сигнал синхронизации
RA Случайный доступ
RACH Канал случайного доступа
РБ Блок ресурсов
RRC Управление радиоресурсами
RS Контрольный сигнал
RSRP Приемная мощность эталонного сигнала **RSRQ** Качество приема эталонного сигнала **SAE** Эволюция системной архитектуры
SDR Программно-определяемое радио
SFN Номер системного кадра
SIB Системный информационный блок
SSS Сигнал вторичной синхронизации
S-TMSI Временный идентификатор мобильного абонента SAE
TA Зона отслеживания
TAI Идентичность TA
TAU Обновление зоны отслеживания
UE Пользовательское оборудование