LTrack: Скрытое слежение за мобильными телефонами в LTE

Мартин Котуляк
ETH Zürich

Симон Эрни
ETH Zürich

Патрик Леу
ETH Zürich

Марк Рёшлин
ETH Zürich

Срджан Capkun
ETH Zürich

Аннотация

Мы представляем LTrack - новую атаку на LTE, которая позволяет злоумышленникам скрытно извлекать идентификаторы пользователей (UE) и их местоположение. Чтобы оставаться незаметной, локализация UE в LTrack полностью пассивна. Она опирается на нашу новую реализацию сниффера восходящего/нисходящего канала, который записывает как время прибытия LTE-сообщений, так и содержимое команд Timing Advance, на основе которых LTrack рассчитывает местоположение UE. LTrack впервые демонстрирует осуществимость пассивной локализации UE посредством реализации на программно-определяемом радио.

Атаки пассивной локализации позволяют получить информацию о местоположении UE, но в лучшем случае могут связать это местоположение с псевдонимным временным идентификатором UE (TMSI), что делает отслеживание в густонаселенных районах сложной задачей. LTrack решает эту проблему путем внедрения и реализации нового типа IMSI Catcher под названием IMSI Extractor. Он извлекает постоянный идентификатор UE (IMSI) и привязывает его к его текущему TMSI. Вместо того чтобы полагаться на поддельные базовые станции, как существующие IMSI Catchers (которые можно обнаружить благодаря их выходной мощности), IMSI Extractor полагается на наш сниффер восходящего/нисходящего канала, усовершенствованный хирургическим затенением сообщений. Это делает наш IMSI Extractor самым скрытным IMSI Catcher на сегодняшний день.

Мы оценили работу LTrack в ходе серии экспериментов и показали, что в условиях прямой видимости злоумышленник может определить местоположение телефона с ошибкой менее 6 м в 90 % случаев. Кроме того, мы успешно протестировали наш IMSI Extrac- tor на наборе из 17 современных смартфонов, подключенных к промышленной тестовой площадке LTE.

1 Введение

LTE - одна из наиболее широко распространенных и используемых технологий сотовой связи. Она была разработана не только для обеспечения связи, но и для защиты безопасности и конфиденциальности пользователей путем шифрования связи между устройствами (UE) и базовыми станциями (eNodeB). В отличие от данных пользователя, управляющие сообщения физического и MAC-уровня LTE передаются открытым текстом, идентификаторы абонентов (IMSI) заменены на временные идентификаторы (TMSI) для защиты конфиденциальности пользователей.

Безопасность LTE и, в частности, безопасность и конфиденциальность на беспроводном канале связи между базовыми станциями и пользовательскими устройствами - активная область исследований. В целом атаки на LTE можно классифицировать как активные и пассивные. Активные атаки (например, IMSI Catcher [18, 35]) обычно основаны на использовании поддельных базовых станций, к которым подключаются UE-жертвы. Недавно в качестве новой активной, но более скрытной техники манипулирования появилась перегрузка сообщений [12, 43].

С другой стороны, пассивные атаки основаны на использовании встроенных снифферов. В [7, 22] было показано, что злоумышленник может построить пассивный сниффер трафика нисходящего канала (от eNodeB до UE), используя программно-определяемые радиостанции. Снайперы нисходящего канала затем использовались в качестве инструментов для локализации [31], для взлома шифрования телефонных звонков [33] и для создания отпечатков трафика [19]. Идея пассивного сниффинга восходящих и нисходящих каналов была предложена для локализации пользователей [31], но не была реализована. В отличие от сниффинга нисходящего канала, сниффинг восходящего канала до сих пор реализовывался только с помощью активных методов и опирался на поддельные базовые станции [32, 36].

В этой работе мы сосредоточимся на крупномасштабном скрытном отслеживании UE. Для успешного проведения такой атаки противнику :
(i) определить местоположение UE (ii) получить идентификатор UE, который связывает наблюдаемые местоположения в трассировку, и (iii) избежать обнаружения. До сих пор ни одна атака не выполняла все вышеперечисленные задачи одновременно. Пассивная локализация сама по себе может обеспечить утечку следов UE в некоторых районах с низкой плотностью населения, но в городских районах с высокой плотностью UE эта задача будет сложнее без идентификатора, который связывает наблюдаемые местоположения вместе [37].

Ловцы IMSI, которые используются для утечки IMSI UE противнику и, следовательно, идентификации UE, полагаются исключительно на поддельные базовые станции. Однако, чтобы заставить UE подключиться к поддельной базовой станции (одно из требований атаки), злоумышленник должен передавать сигнал на высокой мощности, поэтому он может быть обнаружен правоохранительными органами и операторами [23, 25, 29].

В данной статье рассматриваются эти вопросы и показывается, что скрытная локализация и идентификация (а значит, и слежение)

UE в LTE действительно возможны. Мы представляем LTrack, новую систему отслеживания

Атака на LTE, сочетающая в себе пассивные и скрытные активные атаки. Для пассивной локализации мы используем LTEPROBE, наш сниффер восходящих/нисходящих каналов, а для привязки собранных следов к IMSI - наш активный, но скрытный IMSI Extractor.

Наша работа посвящена восстановлению следов долговременной мо-бильности пользователей. То, как эта информация в дальнейшем используется противниками, хорошо изучено и не входит в сферу нашей работы. Предыдущие исследования показали, что следы могут быть использованы для деанонимизации пользователей с помощью маршрутов передвижения [24], маршрутов мобильности [13, 28, 41, 44], домашних адресов [14, 17, 20], совместного местонахождения с другими пользователями [26, 39] или онлайн-меток [16].

В итоге мы сделали следующие выводы:

- Мы демонстрируем осуществимость полностью пассивной рекламной локализации UE в сети LTE. Мы показываем, что в условиях прямой видимости злоумышленник может определить местоположение телефона с ошибкой менее 6 м в 90 % случаев.

- Мы предлагаем новый тип ловца IMSI, названный IMSI Extractor. Наш IMSI Extractor не полагается на поддельные базовые станции, а использует комбинацию маломощного хирургического затенения сообщений и сниффинга восходящего/нисходящего канала. Даже если наш ловец вводит сообщение, он делает это в соответствии со спецификацией протокола LTE, что делает его трудно обнаруживаемым с помощью существующих методов обнаружения IMSI Catcher. Мы обсуждаем методы, которые потребуются для обнаружения этой атаки. Мы успешно протестировали наш IMSI Extractor на 17 смартфонах, подключенных к промышленной сети eN- odeB.

- Мы объединили нашу пассивную локализацию и наш IMSI Ex- tractor в систему отслеживания UE, которую мы назвали LTrack, которая обеспечивает одновременную идентификацию и локализацию UE, что позволяет злоумышленникам отслеживать пользователей более настойчиво и с большей точностью, чем в предыдущих атаках. LTrack делает это путем перекрестной проверки пар IMSI-TMSI, полученных с помощью нашего IMSI Extractor, с данными о ло- кации, идентифицированными по TMSI, которые были получены в результате наших атак на локализацию.

- Мы реализуем первый "белый ящик" для сниффера восходящих и нисходящих каналов LTE под названием LTEPROBE. До сих пор в открытых исследованиях были представлены только снифферы нисходящих каналов. Этот сниффер является одним из основных компонентов LTrace. Наш сниффер записывает как информацию на уровне протокола, например, параметры синхронизации или сообщения, специфичные для модели телефона, так и тайминги сообщений на физическом уровне.

- Используя наш сниффер, мы реализуем функцию отпечатка пальцев мобильного телефона, которая позволяет злоумышленнику определить марку и модель телефона. Это позволяет нам в некоторых сценариях дополнительно увеличить точность локализации и отслеживания телефона на целых 20 метров.

2 Фон

2.1 LTE

Сеть радиодоступа в LTE управляется базовыми станциями (eNodeB). eNodeB направляют трафик по защищенному каналу в ядро сети, которое выполняет большинство функций мобильной сети. Наш сниффер перехватывает и анализирует обмен данными между базовой станцией и мобильным телефоном (UE): нисходящий канал от eNodeB к UE и восходящий канал от UE к eNodeB. Большинство провайдеров реализуют разделение восходящего и нисходящего каналов с помощью FDD-LTE (Frequency Division Duplex). В FDD восходящая и нисходящая линии используют две отдельные радиочастотные несущие, по одной для каждого направления. Мультиплексирование осуществляется с помощью OFDMA в нисходящем канале и SC-FDMA в восходящем канале.

Передача данных на физическом уровне планируется в кадрах длиной 10 мс как для нисходящей, так и для восходящей линии связи [2]. Кадры индексируются от 0 до 1023 и разбиваются на десять подкадров, каждый из которых имеет длительность 1 мс. Каждый подкадр состоит из двух слотов. По умолчанию слот состоит из 7 OFDM-символов с одним циклическим префиксом на символ.

В OFDMA и SC-FDMA данные модулируются на ортогональные поднесущие. Модулированные значения данных называются частотными выборками. С помощью обратного быстрого преобразования Фурье частотные выборки преобразуются во временной сигнал и передаются по радиоканалу. Приемник LTE преобразует входящий сигнал в выборки временной области. Быстрое преобразование Фурье по временным выборкам выводит частотные выборки. Наименьшим индексированным элементом является ресурсный блок [2], который охватывает 12 поднесущих и длится один слот.

Каналы физического уровня. Данные на физическом уровне передаются по различным каналам [2]. Каждый канал занимает заранее определенные блоки ресурсов. Физические каналы общего доступа используются для передачи данных, а каналы управления управляют потоком и доступом к ним. Физический канал случайного доступа используется для установления новых соединений UE.

Все распределения ресурсных блоков передаются UE в элементах информации управления нисходящей линии связи (DCI), передаваемых по каналу управления нисходящей линии связи. 16-битный номер RNTI адресует каждый DCI и определяет получателя сообщения. В зависимости от функции номер RNTI указывает на один UE или несколько UE. Формат DCI определяет его функцию.

DCI Format 0 выделяет UE блоки ресурсов в восходящем канале. UE может передавать по общему каналу восходящей линии связи только в том случае, если он получил соответствующее распределение ресурсов. Формат DCI 0 также определяет параметры, используемые для кодирования сообщений, например схемы модуляции.

Формат DCI 1 или 2 определяет, какие блоки ресурсов UE должно декодировать и какие параметры оно должно использовать для декодирования сообщений в общем канале нисходящей линии связи. По общему каналу нисходящей линии связи передаются пользовательские данные и другие

системная информация, например, конфигурация базовой станции.

Установление соединения. UE использует два номера для идентификации в сети: IMSI, уникальный, постоянный идентификатор, и TMSI, временный идентификатор. Каждое соединение UE начинается с запроса на соединение RRC, содержащего TMSI UE. Если TMSI недоступен, UE выбирает случайное значение и включает его вместо TMSI.

Существует два способа, как UE запрашивает услугу у сети. Если UE подключается впервые после потери состояния (например, перезапуска), оно инициирует процедуру присоединения, отправляя запрос присоединения, содержащий TMSI, если он был назначен ранее, или IMSI в противном случае. Если сеть не распознает TMSI, она попросит UE предоставить свой IMSI в процедуре идентификации. В конце процедуры присоединения, после создания контекста безопасности, сеть присваивает UE новый TMSI. В этот момент TMSI шифруется и защищает целостность.

Если UE уже подключено к сети, но простаивает, переходя из состояния простоя в состояние подключения, оно вступает в процедуру запроса услуги, отправляя защищенный по целостности запрос услуги, после чего связь немедленно восстанавливается.

2.2 Соответствующие атаки

Атаки на локализацию. Наблюдая только за пейджинговыми сообщениями, злоумышленник может узнать, находится ли жертва в данный момент в той же зоне слежения или в той же соте (если развернута интеллектуальная пейджинговая система), как показано в [35].

Если жертва подключена к той же базовой станции, что и злоумышленник, можно осуществить более сложные атаки. Как предложено в [31], злоумышленник может наблюдать за управляющими сообщениями на MAC-уровне, которые содержат информацию о коррекции задержки распространения. Только эта информация ограничивает местоположение жертвы кольцом шириной 78 метров вокруг eNodeB, периметр которого определяется коррекцией задержки распространения.

Атаки на локализацию, основанные на поддельных базовых станциях [18], еще более точны. Однако мы не считаем их достаточно скрытными, чтобы использовать в крупномасштабной атаке слежения.

Ловцы IMSI. Как уже говорилось в разделе 1, в зонах с высокой плотностью UE злоумышленнику необходимо иметь возможность получить идентификационные данные жертв, чтобы отслеживать их. Наиболее мощными атаками в этой области являются IMSI Catchers [18, 35], которые раскрывают уникальный номер IMSI злоумышленнику. Однако все эти атаки основаны на использовании поддельных базовых станций.

3 LTEPROBE

Ключевым компонентом, обеспечивающим возможность скрытного слежения, является реализация комбинированного спускового/вспомогательного LTE-снайфера, который мы назвали LTEPROBE. Далее мы опишем LTEPROBE и его возможности. Как уже говорилось, сниффинг нисходящего канала (см., например, [7, 22]) позволяет злоумышленнику записывать незашифрованную информацию управления нисходящим каналом и управляющие элементы на MAC-уровне. Однако при использовании сниффера восходящего канала поверхность атаки существенно увеличивается. Незашифрованные сообщения, такие как сообщения инициализации, могут быть использованы злоумышленником для утечки идентификаторов пользователей. Все сообщения восходящей линии связи, даже зашифрованные, могут быть использованы для точного определения времени прибытия.

3.1 Архитектура системы

Мы разработали LTEPROBE как полностью пассивное устройство и поэтому практически не обнаруживаемое. LTEPROBE принимает радиочастотные образцы как в восходящем, так и в нисходящем канале. Он записывает все коммуникации между мобильными телефонами и базовыми станциями, но не взламывает шифрование. LTEPROBE имеет стабильные часы и синхронизирует свой прием с базовой станцией. Дрейф часов между часами базовой станции и LTEPROBE пренебрежимо мал, поскольку все устройства используют часы, синхронизированные по GPS.

LTEPROBE состоит из двух основных компонентов. Первый компонент - DOWNLINKPROBE, анализатор нисходящего канала, а второй - UPLINKPROBE, анализатор восходящего канала. DOWNLINKPROBE может работать как автономный анализатор нисходящего канала, но UPLINKPROBE для своей работы нуждается в информации о планировании, DOWNLINKPROBE. Снайпинг восходящего и нисходящего каналов возможен благодаря незашифрованным сообщениям DCI, передаваемым по каналу управления нисходящим каналом.

DOWNLINKPROBE сначала синхронизируется с базовой станцией и записывает идентификаторы подключенных UE. Протокол LTE определяет временные номера RNTI для идентификации UE на физическом уровне на время соединения. С помощью RNTI DOWNLINKPROBE находит и декодирует сообщения, предназначенные для UE-жертв.

На физическом уровне, когда UE подключается к eNodeB, eNodeB отвечает ответом Random Access Response. В ответе случайного доступа eNodeB указывает новый RNTI для UE. Поскольку ответ случайного доступа отправляется в виде обычного текста, он виден DOWNLINKPROBE. Однако этот метод можно использовать только для новых соединений. Для уже подключенных UE назначенный RNTI не передается открытым текстом, а кодируется в CRC сообщений DCI. работе [22] описан метод извлечения RNTI из DCI, однако для наших случаев это не требуется.

Для декодирования каналов нисходящей линии связи DOWNLINKPROBE выполняет обратное преобразование OFDMA для получения частотных образцов. Он выполняет коррекцию канала и коррекцию смещения частоты. Затем он перебирает все возможные местоположения DCI для набора записанных RNTI и пытается их декодировать. В зависимости от формата декодированного DCI, DOWNLINKPROBE либо использует его для декодирования сообщения PDSCH, либо передает его UPLINKPROBE. Наконец, DOWNLINKPROBE анализирует

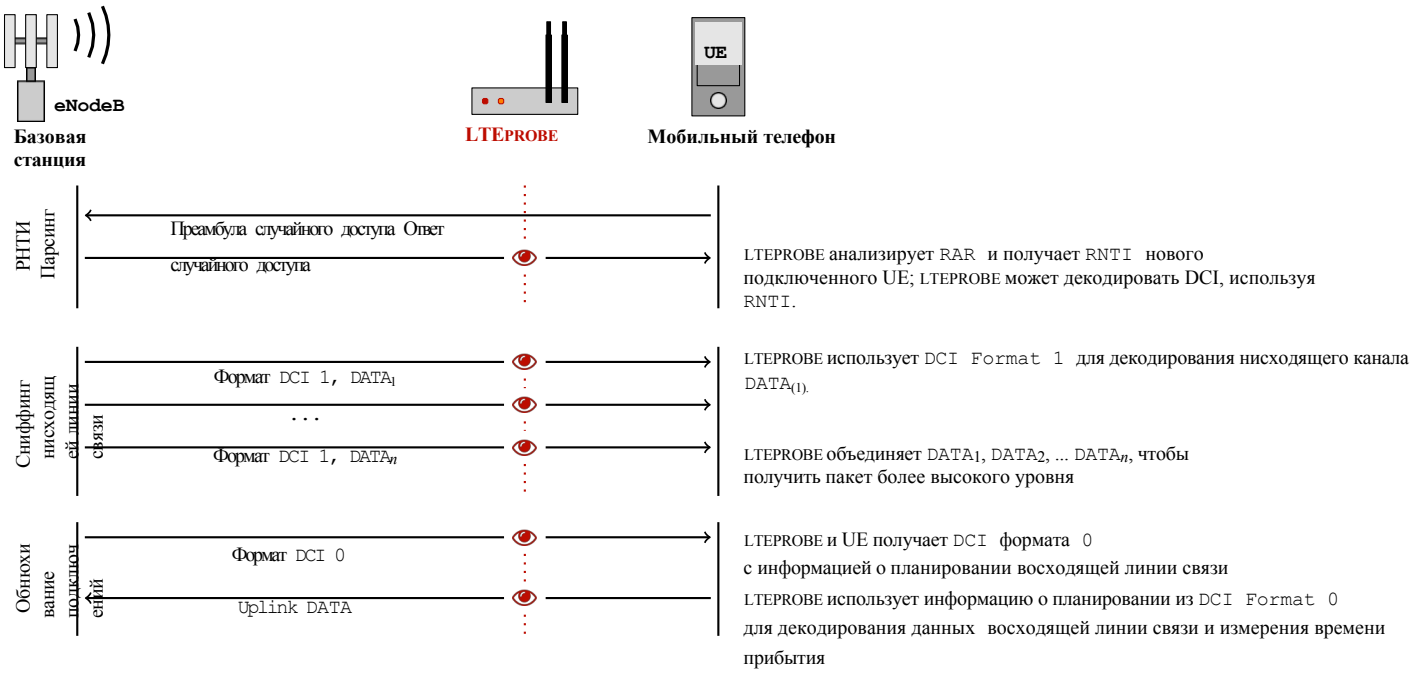


Рисунок 1. Декодирование восходящего и нисходящего каналов с помощью LTEPROBE. Сначала LTEPROBE записывает RNTI UE. Затем он использует его для декодирования DCI. DCI определяет местоположение данных нисходящего или восходящего канала в сетке ресурсов.

Сообщения PDSCH для получения сообщений более высокого уровня, например, сообщений NAS-уровня, содержащих выделенную конфигурацию UE. На рис1 показано, как DOWNLINKPROBE получает RNTIs в Random Access Response и затем получает данные общего канала.

UPLINKPROBE принимает образцы, передаваемые от нескольких UE. Как и eNodeB, он демодулирует их и применяет коррекцию канала. После этого он пытается декодировать общие каналы восходящей линии связи и каналы управления.

Физический общий канал восходящей линии связи декодируется в соответствии с информацией о планировании. eNodeB управляет планированием в протоколе LTE, поэтому он знает запланированное распределение ресурсов. В нашем случае UPLINKPROBE должен получить информацию о расписании из сообщений DCI тем же способом, каким UE получает их. UPLINKPROBE использует переданные сообщения DCI Format 0 от сниффера нисходящего канала, содержащие информацию о расписании. Поскольку сообщения DCI Format 0 содержат информацию о распределении ресурсов для будущих передач по восходящему каналу, без сниффера нисходящего канала UPLINKPROBE не сможет декодировать каналы восходящего канала. На рисунке 1 показана процедура работы UPLINKPROBE.

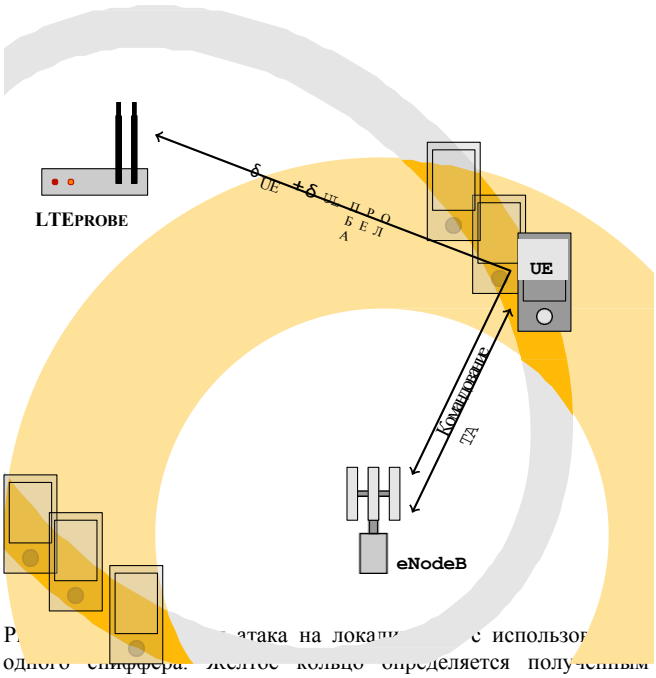
Чтобы правильно декодировать общие и управляющие каналы восходящей линии связи, UPLINKPROBE должен применить специальную конфигурацию UE, отправленную через сообщение RRC-уровня нисходящей линии связи. UPLINKPROBE снова использует информацию, записанную DOWNLINKPROBE. Как и в DOWNLINKPROBE, сообщения физического уровня анализируются для получения сообщений более высокого уровня.

Реализация LTEPROBE

Мы основываем нашу реализацию на srsLTE [15], библиотеке с открытым исходным кодом для протокола LTE. Два основных компонента, DOWNLINKPROBE и UPLINKPROBE, работают на двух отдельных совместно расположенных устройствах USRP, которые используют одни и те же часы, обеспечиваемые модулем распределения часов. Эти два компонента выполняются как два потока родительской программы LTEPROBE.

Подкадры нисходящей и восходящей линии связи планируются одновременно. UE узнают тайминги субкадров из сигналов синхронизации, передаваемых eNodeB. Однако только DOWNLINKPROBE получает сигналы синхронизации. Восходящий и нисходящий потоки LTEPROBE должны совместно использовать тайминги и номера субкадров; в противном случае UP-LINKPROBE не сможет получать субкадры восходящего канала в нужное время. Для точной синхронизации два USRP должны иметь одинаковый временной эталон. Это можно решить с помощью GPSDO на обоих USRP, чтобы иметь одинаковые часы GPS, или с помощью Octoclock, модуля распределения часов.

Для каждого субкадра и UPLINKPROBE, и DOWN- LINKPROBE записывают индекс субкадра и точное время его приема. Если временные метки для одного и того же ин-декса субкадра не совпадают, UPLINKPROBE должен скорректировать свое время приема, отбросив временные выборки. Таким образом, достигается идеальная синхронизация двух компонентов.



Р[illegible] атака на локали[illegible] с использов[illegible] одного сниффера. Желтое кольцо определяется полученным параметром синхронизации (команда Timing Advance), а серый - временем прибытия, измеренным LTEPROBE. Пересечение двух колец определяет возможное местоположение мобильного телефона.

4 Пассивная атака на локализацию

Пассивная локализация UE в сетях LTE была предложена в ряде предыдущих работ [22, 31, 35]. В частности, Рот и др. [31] предложили атаку на пассивную локализацию, которая использует параметры синхронизации, передаваемые на MAC-уровне (Timing Advance Command), и время прибытия сообщений в восходящем и нисходящем каналах.

В частности, атака, предложенная в [31], работает на основе наблюдения за командой Timing Advance Command, содержащей информацию о коррекции задержки распространения. Из-за грубой гранулярности команды Timing Advance Command атака ограничивает местоположение жертвы кольцом шириной 78 метров вокруг eNodeB. Кроме того, в LTE-Advanced UE имеет возможность подключаться к нескольким сотам одновременно. Информация о множественной коррекции задержки ограничивает местоположение жертвы пересечением колец. Наконец, Рот и другие [31] предлагают идею локализации UE на основе времени прихода сообщений восходящего канала, что позволит злоумышленнику ограничить местоположение жертвы дополнительным кольцом шириной 78 метров вокруг атакующего устройства. Однако авторы не приводят подробностей, моделирования или реализации этого предложения.

Наша пассивная атака на локализацию также использует нешифрованную команду Timing Advance Command и время прибытия восходящего канала связи.

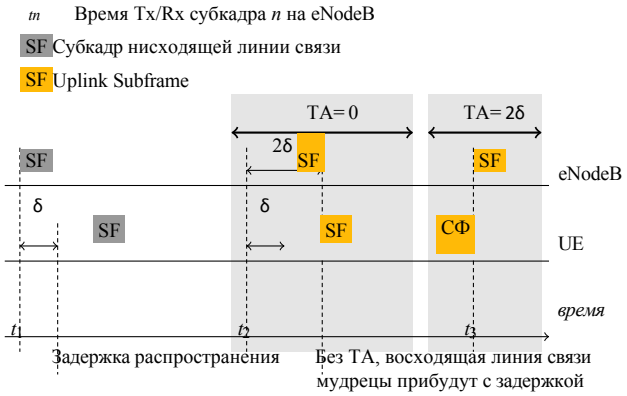


Рисунок 3. Timing Advance используется для выравнивания передач восходящей линии связи. Передача и прием на eNodeB синхронизируются.

мудрецов. Однако, в отличие от их работы, мы преобразуем геометрию задачи из круга в эллипс. Это преобразование позволяет нам устранить систематическую ошибку, вызванную командой Timing Advance. дополнительного кольца шириной 78 м вокруг сниффера мы получаем точный эллипс с фокусами на базовой станции и сниффере, как показано на рис. 2.

Наиболее значительным вкладом нашей атаки является фактическая реализация и ее оценка в разделе 7. Наша реализация выявила неточность аппаратного обеспечения мобильных телефонов. Чтобы решить эту проблему, мы трансформировали активную атаку по отпечаткам пальцев, представленную в [36], в полностью пассивную атаку в подразделе 4.4. Знание модели мобильного телефона может увеличить точность локализации на 20 метров.

В этом разделе мы разработаем пассивную атаку на локализацию, дадим ее математическое обоснование и опишем ее реализацию. Злоумышленник может ограничить местоположение жертвы двумя возможными областями, как показано на рис. 2, используя только одно устройство сниффинга и базовую станцию. Две возможные области - это межсекционный участок широкого кольца, определяемый Timing Advance Com- mand, и эллипс, определяемый временем прихода сообщений восходящей линии связи. Использование двух или более сниффинг-устройств приводит к тому, что злоумышленник узнает местоположение жертвы. В качестве альтернативы противник может исключить возможное местоположение, сверяясь, например, с подробной картой местности.

4.1 Команда опережения зажигания

Несколько UE подключаются к eNodeB. Каждое UE находится на разном расстоянии. Из-за задержки распространения, без какого-либо корректирующего механизма, сообщения восходящей линии связи будут приниматься с разной задержкой. Таким образом, eNodeB должен помочь скорректировать

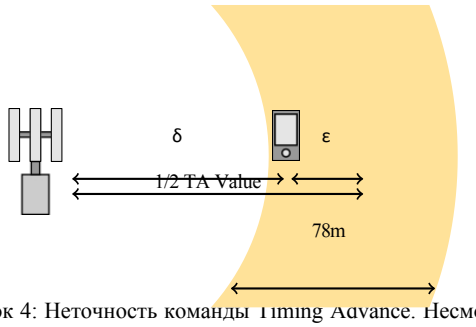


Рисунок 4: Неточность команды Timing Advance. Несмотря на то что задержка распространения между eNodeB и UE составляет δ, полученное значение TA соответствует расстоянию в середине желтого кольца. Разница между этими двумя значениями является систематической ошибкой процедуры синхронизации протокола LTE.

синхронизации каждого UE для обеспечения выравнивания всех сообщений восходящей линии связи в пределах ресурсной сетки, наблюдаемой eNodeB.

На рисунке 3 показана ситуация, когда задержка распространения между UE и eNodeB составляет δ. Из-за задержки распространения нисходящего сообщения кадровая синхронизация UE сдвигается на δ относительно времени eNodeB. Задержка распространения сообщения восходящего канала снова равна δ. Поэтому сообщение восходящего канала поступает на eNodeB с задержкой 2δ. eNodeB измеряет задержку и сигнализирует об этом UE командой Timing Advance (TA).

В спецификации LTE [3] определено, что значение Timing Advance выражается как $T_A \times 16 \times T_{(S)}$, где $T_S = 1/30720ms$. T_A - это значение, сигнализируемое eNodeB. Значение T_A отправляется как часть элемента управления MAC. Оно отправляется eNodeB на MAC-уровень без шифрования.

Таким образом, гранулярность TA составляет $T_S \times 16 = 0{,}5208$ мкс. UE не получает более точного значения задержки распространения δ. Учитывая, что скорость распространения равна скорости света, UE может оценить свое расстояние до eNodeB в диапазоне $78{,}07$ м ($156{,}14$ *м*, деленное на 2 кругового пути). На рисунке 4 показана разница между фактическим расстоянием UE и eNodeB и расстоянием, которое UE вычисляет по команде TA.

4.2 Время прибытия сообщений восходящей и нисходящей линий связи

Атаки на локализацию, основанные на разнице во времени прибытия сообщений жертвы, ограничивают ее местоположение пересечением нескольких гипербол. Атакующий может использовать разницу во времени прибытия между восходящими и нисходящими сообщениями для определения гиперболы между атакующим и базовой станцией. В случае LTE из-за систематической ошибки, вносимой в значение Timing Advance, злоумышленник, использующий этот классический подход, в итоге получает ошибку 78m. Однако мы показываем, как злоумышленник может сформулировать задачу, используя эл. губы и устраняют систематическую ошибку. Для объяснения уникальной проблемы локализации в LTE мы определяем следующие переменные:

t_n начало субкадра n на eNodeB. Это время, когда eNodeB начинает передачу нисходящего подкадра n. UE пытается отправить восходящий подкадр n таким образом, чтобы он прибыл на eNodeB в момент времени t_n.

δ_{UE} задержка распространения между eNodeB и UE.

$\delta_{DLPROBE}$ задержка распространения между eNodeB и LTEPROBE. Мы предполагаем, что это значение известно злоумышленнику, поскольку он знает местоположение eNodeB и LTEPROBE.

$\delta_{ULPROBE}$ задержка распространения между LTEPROBE и UE.

δ_{TA} время, соответствующее значению TA, полученному в команде Timing Advance Command.

ε систематическая ошибка, которую вносит значение TA из-за дискретизации задержки распространения. Это разница между задержкой распространения и значением TA, показанная на рисунке 4, и ее значение находится в диапазоне от -0.1302 мкс до 0.1302 мкс. Мы знаем, что $\delta_{TA} = 2\delta_{UE} + 2\varepsilon$.

Злоумышленник измеряет время прихода сообщений по нисходящей и восходящей линии связи с помощью LTEPROBE с точностью до подвыборки.

Сообщение нисходящей линии связи.

TX на eNodeB	t_n
RX в UE	$t_n + \delta_{UE}$
RX в LTEPROBE	$t_n + \delta_{DLPROBE}$

Поскольку $\delta_{DLPROBE}$ известно злоумышленнику, он может вычислить t_n из времени приема нисходящего сообщения. Время передачи последующих субкадров злоумышленник может определить как $t_{n+k} = t_n + k$, поскольку длина субкадра равна 1 мс.

Сообщение Uplink без команды TA.

TX в UE	$t_n + \delta_{UE}$
RX на eNodeB	$t_n + 2\delta_{UE}$
RX в LTEPROBE	$t_n + \delta_{UE} + \delta_{ULPROBE}$

UE получает все сообщения нисходящей линии связи с задержкой δ_{UE}, поэтому его синхронизация сдвигается, как объясняется в подразделе 4.1. Оно будет передавать сообщения восходящего канала в момент времени $t_n + \delta_{UE}$ вместо t_n. Злоумышленник вычисляет t_n из сообщения нисходящей линии связи. Он может измерить $\delta_{UE} + \delta_{ULPROBE}$ из времени приема сообщения восходящей линии связи, вычитая t_n.

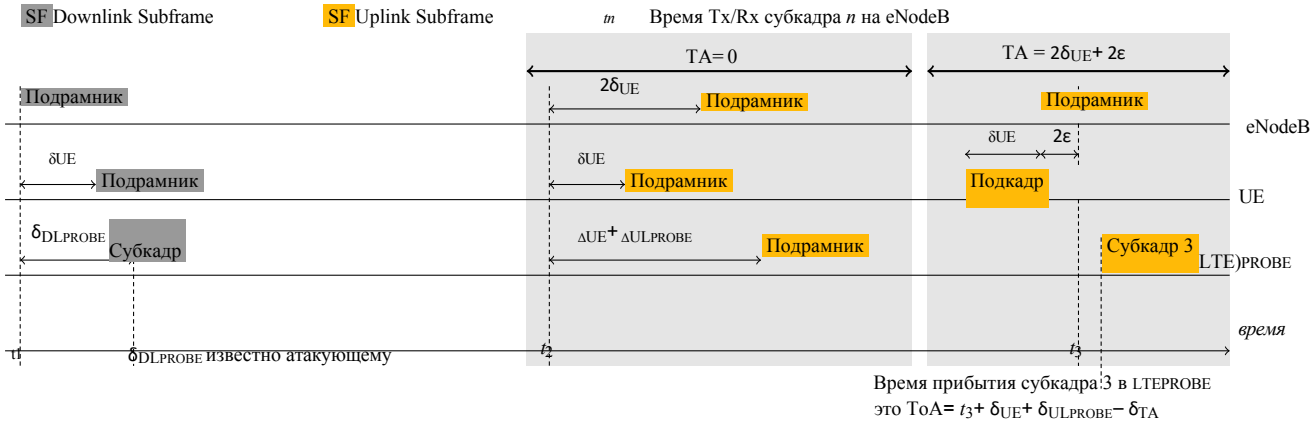


Рисунок 5: Визуализация времени прибытия и задержки восходящих и нисходящих сообщений.

Сообщение Uplink с командой TA.

TX на UE	$t_n + \delta_{UE} - \delta_{TA} = t_n - \delta_{UE} - 2\varepsilon$ RX
на eNodeB	$t_n + 2\delta_{UE} - \delta_{TA} = {}_{t(n)} - 2\varepsilon$
RX в LTEPROBE	$t_n + \delta_{UE} + \delta_{ULPROBE} - \delta_{(TA} =$ $= {}_{tn} - \delta UE + {}_{\delta ULPROBE} - 2\varepsilon$

Злоумышленник больше не может точно вычислить $\delta_{UE} + \delta_{ULPROBE}$ путем вычитания t_n из-за ошибки 2ε, которая может составлять от$-0{,}2604$ мкс до $0{,}2604$ мкс.

4.3 Локализация

В предыдущих двух подразделах мы рассмотрели два набора информации, которые злоумышленник может использовать для локализации жертвы: Timing Advance Command, отправляемая базовой станцией на MAC-уровне, и время прихода восходящих и нисходящих сообщений на LTEPROBE. На рис. 2 показана схема атаки и возможное местоположение телефона жертвы в окружающей среде.

Простая атака на локализацию работает путем прослушивания команд TA, поскольку они передаются без шифрования на MAC-уровне протокола LTE. Поэтому команда TA может быть записана нашим DOWNLINKPROBE. Из-за грубой гранулярности, обусловленной дискретизацией значения TA, локализация TA-команды сужает возможное местоположение до кольца вокруг сниффера нисходящей линии связи шириной 78 м (желтое кольцо на рис2).

В подразделе 4.2 мы рассмотрели, как злоумышленник узнает время передачи подкадров t_n из времени прибытия сообщений нисходящей линии связи. Когда LTEPROBE получает управляющую информацию нисходящего канала с расписанием для передачи по восходящему каналу жертвы, он декодирует сообщение восходящего канала и измеряет время его прибытия. Время прибытия сообщения восходящей линии связи для LTEPROBE составляет:

$$\text{ToA} = t_n - \delta_{UE} + \delta_{ULPROBE} - 2\varepsilon$$

Вычитая время передачи подкадра t_n, злоумышленник получает разницу во времени прихода сообщения по восходящей и нисходящей линии связи. После этого злоумышленник может определить гиперболу возможных местоположений с погрешностью 2ε. В нашем подходе мы вычитаем время субкадра t_n и добавляем значение, от команды TA, чтобы узнать сумму расстояний:

$$\delta UE + {}_{\delta ULPROBE} = \text{ToA} - {}_{tn} + {}_{\delta TA}$$

Таким образом, мы можем полностью исключить систематическую ошибку ε из уравнения. Измеренная сумма двух задержек распространения δ_{UE} и $\delta_{ULPROBE}$ ограничивает набор возможных местоположений UE жертвы как:

$$DUE + {}_{DULPROBE} = c \times (\Delta UE + {}_{\Delta ULPROBE})$$

где d_{UE} - расстояние между UE и eNodeB, $d_{ULPROBE}$ - расстояние между UE и LTEPROBE, а c - скорость света в воздухе. Это ограничение определяет с двумя фокусными точками: LTEPROBE и базовая станция.

Теперь местоположение ограничено пересечением кольца и эллипса, как показано на рисунке 2. Используя только один сниффер, злоумышленник получает две узкие области расположения.

Злоумышленник может значительно повысить точность TA Attack, используя несколько LTEPROBE в разных точках. Конечное местоположение UE находится на пересечении нескольких точных . Однако это вносит дополнительные сложности и увеличивает стоимость атаки.

4.4 Пассивная атака на отпечатки пальцев

Аппаратная ошибка. В системе имеется четыре аппаратных устройства: eNodeB, DOWNLINKPROBE, UPLINKPROBE, и UE жертвы. Все четыре добавляют небольшую ошибку синхронизации, обусловленную конструкцией схемы, длиной кабелей, антенн и т. д. Мы предполагаем, что аппаратная ошибка постоянна для конкретной модели

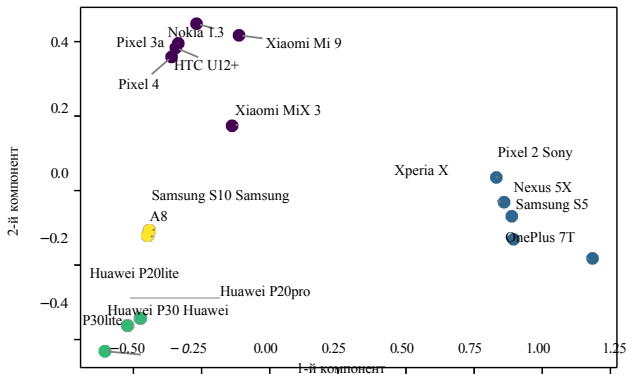


Рисунок 6: Первые две компоненты PCA-разложения вектора признаков.

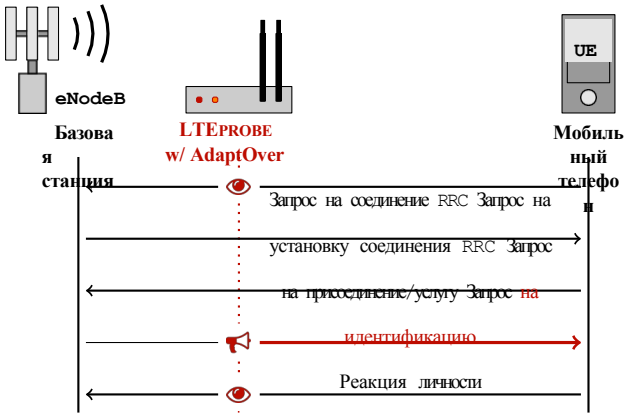


Рисунок 7: Сначала злоумышленник прослушивает запрос RRC-соединения, содержащий TMSI UE. После получения RRC Connection Setup от eNodeB злоумышленник затеняет сообщение, базовой станцией, сообщением Identity Request. Затем злоумышленник перехватывает ответ Identity Response от UE и узнает его IMSI. Злоумышленник может связать временный идентификатор TMSI с уникальным постоянным IMSI.

устройства (она может меняться под воздействием окружающей среды, например, внешней температуры, но мы предполагаем, что это незначительно). В ходе экспериментальной оценки атаки в разделе 7 мы не столкнулись с ошибкой переменной. Оба программно-определяемых радиоприемника в LTEPROBE выбираются злоумышленником, и аппаратная ошибка базовой станции незначительна. Единственное устройство, которое злоумышленник не может контролировать в системе, - это UE жертвы. Однако злоумышленник может создать базу данных с различными телефонами и соответствующими аппаратными ошибками. Если он сможет определить тип телефона жертвы, то сможет найти соответствующую аппаратную ошибку.

Пассивное снятие отпечатков пальцев. Чтобы узнать аппаратную ошибку, вносимую моделью телефона, мы модифицируем и расширяем атаку Шайка и других [36]. Эта атака анализирует восходящий трафик и классифицирует baseband-модем телефонов, подключенных к соте. Базовый модем - это чип, отвечающий за связь в мобильной сети. Атака в [36] использует ретрансляционную базовую станцию для декодирования информации восходящей линии связи, поэтому она является активной атакой. Вместо этого мы используем LTEPROBE для получения информации о восходящей линии связи. Наше усовершенствование делает атаку абсолютно пассивной, и мы показываем, как она может быть использована для дактилоскопии модемов и телефонов с помощью модели дерева решений. В качестве вектора признаков, используемого для отпечатков пальцев, мы используем основные возможности, отправленные в открытом виде вместе с запросом на присоединение. В каждом телефоне реализованы разные возможности, поэтому они сообщения значительно отличаются друг от друга.

На рисунке 6 показано PCA-разложение вектора характеристик для всех протестированных телефонов, за исключением iPhone. Видно, что телефоны с модемом одного производителя имеют схожие основные возможности (список телефонов и соответствующих им модемов в таблице 2). Мы не включаем iPhone в ви- суализацию для прозрачности, так как iPhone сгруппированы вместе на большом расстоянии от других телефонов. На рисунке 6 мы видим четыре кластера. Зеленым цветом выделены телефоны с модемом Huawei, желтым - с Модем Samsung, а синие и фиолетовые кластеры - телефоны Qual- comm. Синие телефоны - это старые телефоны, в то время как фиолетовые соответствуют последним моделям. Единственное исключение OnePlus 7T, который был объединен в кластер со старыми моделями телефонов Qualcomm. Четыре модели телефонов, изображенных на рисунке 6, имеют один и тот же модем: Xiaomi Mi9, Xiaomi MiX 3, Google Pixel 4 и OnePlus 7T. OnePlus 7T - это выброс, однако остальные три телефона все равно не имеют одинакового вектора характеристик, поскольку они лишь тесно сгруппированы друг с другом. Таким образом, объект возможностей зависит как от модема, так и от модели телефона. Таким образом, злоумышленник может узнать точный отпечаток пальца каждой модели телефона.

5 Извлекатель IMSI

Чтобы связать UE с уникальным ключом и тем самым облегчить их отслеживание, мы предлагаем новую идентификационную атаку, основанную на затенении сообщений и LTEPROBE. Для затенения сообщений мы используем AdaptOver [12], недавно предложенную атаку на затенение в LTE. В AdaptOver злоумышленник посылает сообщение, полностью совпадающее по времени и частоте с сообщением базовой станции, но с мощностью на 3 дБ выше, тем самым заменяя оригинальное сообщение на сообщение злоумышленника. Для UE сообщения злоумышленника неотличимы от легитимных сообщений.

В этом разделе мы покажем, что, комбинируя сниффинг на восходящем канале связи и AdaptOver с инъекцией всего одного вредоносного сообщения, мы можем заставить UE слить IMSI. Поскольку каждая SIM-карта имеет уникальный, постоянный номер IMSI, злоумышленник идеально

выделяет жертву с помощью этой атаки. Несмотря на то что атака активна, злоумышленник может выбирать время ее проведения, а также выбирать только определенные UE. Наша атака запускается, когда eNodeB отправляет RRC Connection Setup, как показано на рисунке 7. Это происходит, когда UE переходит из выключенного или незанятого состояния в состояние соединения (например, телефон получает пейджинговое сообщение или должен передать данные).

Идентификация жертвы. Как показано на рисунке 7, UE отправляет первоначальный запрос на подключение RRC, содержащий его номер TMSI. Однако, поскольку сеть LTE может изменить этот идентификатор в любое время, у злоумышленника нет никакой уверенности в долгосрочной идентичности UE. Вместо этого, номер IMSI удовлетворяет этому, но UE не передает IMSI в открытом тексте в обычном поведении протокола. Тем не менее, протокол LTE позволяет ядру сети запрашивать номер IMSI в любое время (например, когда сеть теряет номер TMSI), отправляя запрос идентификации.

5.1 Затенение с помощью запроса на идентичность

Как указано в [4], запрос идентификации для получения номера IMSI может быть отправлен eNodeB без какой-либо защиты целостности до создания контекста безопасности. Поскольку контекст безопасности не создается до запроса на обслуживание или присоединение, злоумышленник может внедрить запрос идентификации в качестве ответа на эти запросы. UE ответит на запрос идентификации сообщением Identity Response, содержащим его уникальный номер IMSI, который получает LTEPROBE. На рисунке 7 показан обмен сообщениями. Несмотря на то, что легитимная базовая станция продолжает процедуру подключения, AdaptOver посылает сообщение с более высокой мощностью, заслоняя его. Таким образом, UE декодирует только запрос идентификации, отправленный злоумышленником. Базовая станция не получает ответ Identity Response, отправленный UE, поскольку AdaptOver также изменяет распределение восходящего канала во время атаки. В целом атака требует от злоумышленника ограниченного количества передач, при этом его мощность лишь немного выше, чем у базовой станции.

Важно отметить, что использование Identity Request - это лишь один из конкретных подходов к работе IMSI Extractor. Однако злоумышленник не ограничен этим и может создавать другие трассировки связи по жалобе протокола, которые вызывают передачу IMSI в открытом виде UE (например, Service Reject с причиной 9, "Идентификация UE не может быть получена сетью").

Мы представляем первую атаку, которая сочетает в себе атаку overshadowing со снифингом восходящего канала для нарушения конфиденциальности пользователей. Предыдущие атаки на затенение, такие как SigOver [43] и AdaptOver [12], были направлены на отказ в обслуживании.

Скрытность нашей атаки. Для UE сообщение с поддельным запросом на идентификацию выглядит доброкачественным. Согласно спецификации LTE [4], сеть может начать процедуру идентификации в любое время, даже сразу после получения запроса на прикрепление или запроса на обслуживание. Таким образом, с точки зрения протокола на уровне UE, наша атака не вызывает никаких тревог. Базовая станция также не замечает никаких проблем. С точки зрения eNodeB, соединение с UE прервалось (например, из-за плохого приема на UE). Таким образом, и для UE, и для базовой станции следы, сообщениями злоумышленника, соответствуют протоколу.

Существующие механизмы обнаружения ловцов IMSI работают на основе выявления поддельных базовых станций [6, 8, 23, 25, 29]. Эти механизмы работают либо путем сравнения местоположения базовых станций, предоставленных в открытых источниках, с отчетами пользователей или специальных устройств, либо путем обнаружения аномалий в поведении базовых станций со стороны UE. В случае нашей атаки эти методы не работают, поскольку UE подключается к реальной базовой станции. Поэтому для UE поведение и местоположение соты являются легитимными. Как предложено в [11], детектор аномалий на основе сигнатур с сигнатурой: "если запрос идентификации, то атака", успешно обнаруживает нашу атаку. Однако, поскольку запросы на идентификацию также отправляются во время легитимного потока протоколов, такое решение будет неизбежно выдавать ложные срабатывания во время легитимных процедур идентификации. Более того, злоумышленник не ограничен отправкой запросов идентификации для выполнения IMSI Extractor, как упоминалось выше.

Как объясняется в [6, 8], в большинстве для отлова IMSI Catcher, основанных на аномалиях, учитываются другие признаки (например, количество соседних ячеек). Оценивая их, наш ловец не классифицируется как IMSI Catcher. Поэтому мы считаем нашу атаку незаметной, по крайней мере, по отношению к существующим и предлагаемым методам.

6 LTrack

В этом разделе мы обсудим, как методы, представленные в разделе 4 и разделе 5, могут быть объединены для поддержки крупномасштабных атак слежения, подобных тем, что описаны, например, в [37]. Цель таких атак - получить следы всех пользователей, оставаясь при этом как можно более скрытными.

На рисунке 8 показана ситуация в городе, где злоумышленник пытается локализовать пользователей. Злоумышленник использует атаку пассивной локализации для определения местоположения отдельных пользователей во время их подключения к базовым станциям. Однако без идентификации все UE выглядят одинаково, и после каждого повторного подключения UE могут анонимизировать себя с помощью нового TMSI. Если пользователь перемещается по менее посещаемым районам, когда TMSI обновляется, злоумышленник все равно может связать два временных идентификатора. Однако, UE входит в зону, где находится множество других UE, эта зона будет выступать в качестве естественной зоны смешения. LTrack решает эту проблему, используя комбинацию пассивного отслеживания и IMSI Extractor, что позволяет злоумышленнику различать UE.

Для того чтобы осуществить нашу атаку в крупных масштабах, злоумышленнику необходимо развернуть как минимум один, а лучше два LTEPROBE для каждой базовой станции, которую он решил контролировать. LTEPROBEs

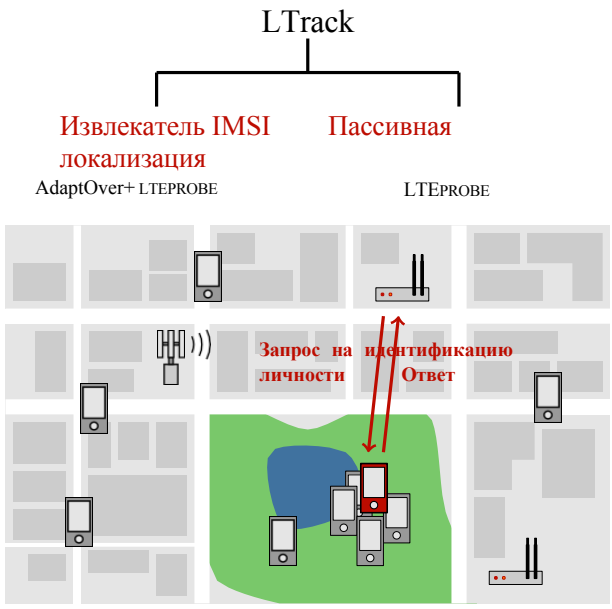


Рисунок 8: Визуализация LTrack, атаки слежения на основе пассивной локализации и IMSI Extractor. Когда злоумышленник теряет след жертвы в естественной микс-зоне, он использует IMSI Extractor, чтобы отличить жертву от других UE в этой зоне.

располагаются вдали от базовых станций таким образом, чтобы злоумышленник мог выполнить атаку на локализацию, изображенную на рисунке 2. Наша атака состоит из следующих четырех этапов:

(i) Запись трафика. Злоумышленник использует LTEPROBE для пассивной записи всего трафика на множестве базовых станций, за которыми он следит. Все сообщения восходящего и нисходящего каналов связи с соответствующим временем прибытия от всех LTEPROBE хранятся в базе данных злоумышленника. Все сообщения во время соединения UE с eNodeB адресуются на физическом уровне уникальным значением RNTI, как объясняется в разделе 3, связывая сообщения воедино. Более того, каждое подключение UE к сети начинается с запроса на подключение RRC, содержащего TMSI пользователя. Злоумышленник хранит список TMSI, замеченных во время выполнения атаки, и связывает их с соответствующими соединениями. Чтобы связать соединения одного и того же пользователя, чей TMSI изменился во время выполнения атаки, злоумышленник запускает программу IMSI Extractor, описанную ниже.

(ii) Экстрактор IMSI. IMSI Extractor извлекает и сохраняет пары TMSI-IMSI пользователей, связывая наблюдаемые коммуникации с уникальным, постоянным идентификатором UE (IMSI), как объясняется в разделе 5. После того как LTEPROBE регистрирует запрос RRC-соединения, злоумышленник проверяет, знает ли он уже IMSI, соответствующий вложенному TMSI в запрос RRC-соединения. Если пара TMSI-IMSI существует в базе данных, злоумышленник не вступает в бой, пассивно записывает сообщение и связывает его с сохраненной парой. Однако если TMSI ранее не встречался, он запускает IMSI Extractor, чтобы узнать номер IMSI, и сохраняет новую пару TMSI-IMSI в базе данных.

(iii) Пассивная локализация. Наконец, у злоумышленника есть записи всех пользователей на нескольких базовых станциях под разными парами TMSI-IMSI. Злоумышленник использует записанные данные, чтобы получить время прибытия каждого сообщения UE в восходящем канале и команды Timing Advance Commands, отправленные базовой станцией. Как показано на рис. 2, каждое измерение восходящего сообщения ограничивает возможное местоположение пользователя.

Более того, злоумышленник проводит пассивную атаку по отпечаткам пальцев на сохраненных записях запросов на прикрепление, чтобы узнать модель телефона. Зная модель телефона, злоумышленник может повысить точность атаки на локализацию. Кроме того, поскольку злоумышленник хранит все записанные сообщения, он может ретроактивно компенсировать аппаратные ошибки, чтобы повысить точность атаки локализации.

измеренное время прибытия сообщений восходящей линии связи для данного пользователя. Поэтому, даже если TMSI пользователя изменится, мы обновим его в базе данных во время последующего запроса на обслуживание/присоединение. Мы можем еще больше повысить точность локализации, выбирая более вероятные места, например, пользователь, скорее всего, движется по улице, а не по стенам зданий. В целом злоумышленник может визуализировать перемещение жертвы. Наконец, злоумышленник собирает полный след передвижения пользователя.

(iv) Особые случаи. При определенных условиях (например, при наличии отхода) UE остается подключенным к сети, но меняет обслуживающую соту на соту с более сильным сигналом. Затем UE отключается от старой соты и выполняет процедуру случайного доступа к новой соте. Поскольку оно все еще подключено к сети, нет необходимости в сообщении Service Request. Таким образом, злоумышленник может наблюдать новый случайный доступ без запроса на обслуживание и сопоставить его с соединением, которое прервалось на соседней соте. Если применяется атака локализации, злоумышленник может улучшить соответствие между старыми и новыми соединениями на основе местоположения UE.

Даже если злоумышленник потеряет UE, он обнаружит его снова во время следующего запроса на обслуживание, который он сформирует. Например, при таймере бездействия в 10 секунд в среднем UE подключается к сети более одного раза в минуту при фоновом трафике (т. е. пользователь не использует телефон активно) [1], что является обычным сценарием во время движения человека. Злоумышленник также может принудительно переподключиться с помощью пейджингового сообщения или звонка.

В данной работе мы не рассматриваем деанонимизацию пользователей. Исследования в этой области уже достаточно обширны, и взломщик может использовать множество существующих методов для получения истинных идентификационных данных пользователей. Пользовательские следы, восстановленные с помощью LTrack, могут быть использованы для идентификации пользователей [21, 42],

например, на основе транс-.

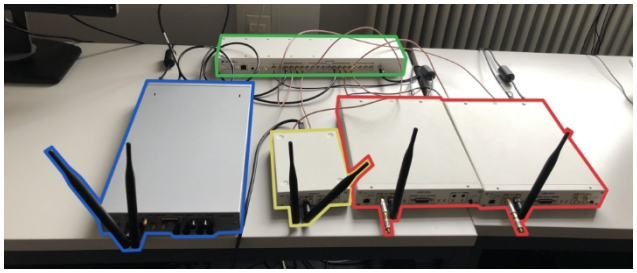


Рисунок 9: Наша установка, используемая для оценки пассивной локализации и экстрактора IMSI.

рутины [24], следы мобильности [13, 28, 41, 44], дом Адреса [14, 17, 20], знакомые [26, 39] или онлайн-медиа с геометками [16]. В [9, 10] показано, что даже грубые пространственно-временные следы деанонимизируют пользователей на основе их уникальных моделей мобильности.

Атака, представленная в этом разделе, может также использоваться более , например для слежения за отдельными людьми. В некоторых сценариях злоумышленник может напрямую сопоставить записанные запросы на прикрепление с жертвой (например, наблюдая, как жертва выключает режим полета в аэропорту или подзаряжает разряженный телефон) и выбрать для отслеживания только жертву, игнорируя других пользователей.

7 Экспериментальная оценка

7.1 Экспериментальная установка

Для экспериментальной оценки нашей атаки мы использовали установку, изображенную на рисунке 9. Она состоит из:

eNodeB, работающая на программно-определяемом радио USRP N310, выделена синим цветом на рисунке 9. В качестве альтернативы мы используем базовую станцию начального уровня AMARI Callbox Mini [5] для оценки атаки IMSI Extractor. Однако из-за того, что она имеет более низкий класс часов, ее временные характеристики не соответствуют действительности. Поэтому мы не используем ее для атаки на локализацию, где необходима точность.

LTEPROBE работает на двух SDR USRP X310, выделенных красным цветом на рисунке 9. Один X310 используется в качестве DOWNLINKPROBE, а другой - в качестве UPLINKPROBE. К TX-порту ra- dios не подключена антенна, что свидетельствует о том, что это пассивное устройство. Оба устройства подключены к Octoclock для совместного использования одного и того же тактового генератора.

Модель **Octoclock** CDA-2990, выделенная зеленым цветом, распространяет один и тот же сигнал синхронизации на все подключенные устройства. В качестве входного сигнала он принимает сигнал GPS. Все подключенные устройства имеют одинаковое чувство времени. Два сниффинга USRP всегда подключены к Octoclock.

AdaptOver работает на программно-определяемом радио USRP B210, выделенном желтым цветом на рисунке 9.

В ходе экспериментальной оценки в качестве **UE** мы использовали несколько мобильных телефонов. Полный список UE приведен в таблице 2 и таблице 1 в приложении.

7.2 Пассивная атака на локализацию

Для экспериментальной оценки нашей атаки на локализацию мы разместили eNodeB и LTEPROBE и варьировали уровень локализации UE. Вместо местоположения мы оценили расстояние LTEPROBE от UE. В нашем эксперименте мы узнали ошибку измерения LTEPROBE, которую можно использовать для количественной оценки ошибки локализации при различных разбавлениях точности. Поскольку eNodeB и LTEPROBE находятся в одном и том же месте, расстояние UE от LTEPROBE составляет:

$$_{\text{dULPROBE}} = c \times (_{\delta\text{UE}} + _{\delta\text{ULPROBE}})/2$$

Мы провели эксперимент с пятью различными UE: USRP B210, Huawei P20 Pro, Huawei P30, iPhone X и iPhone 8. Эксперимент проводился в помещении. Поскольку получить GPS-привязку было невозможно, к октоклоку подключили eNodeB и LTEPROBE. Мы расположили UE в зоне прямой видимости на шести различных расстояниях в длинном коридоре: *0* м, 7,5 *м*, *15* м, *30* м, *45* м и *60* м. Для каждого расстояния и UE мы подключались шесть раз, чтобы измерить расстояние при нескольких подключениях. Для каждого измерения расстояния и UE мы перезапускали LTEPROBE по крайней мере один раз, чтобы сбросить ошибки синхронизации.

Одна точка данных соответствует медианному измерению расстояния во время одного соединения UE с нашей eNodeB. Мы не рассматриваем соединения, для которых у нас есть десяти измерений. Для каждого UE существует постоянная аппаратная ошибка, которая обусловлена свойствами модема UE, радиостанции LTEPROBE и радиостанции eNodeB. Мы оцениваем постоянную аппаратную ошибку как среднюю разницу между расчетным и фактическим расстояниями. Перед построением графика мы удаляем аппаратную ошибку из этих оценок расстояний. Наконец, мы визуализируем точки данных с помощью боксплотов для каждого UE на рисунке 10.

В таблице 2 мы количественную оценку постоянной аппаратной ошибки для всех тестовых телефонов. Мы оцениваем аппаратную ошибку с помощью одного измерения расстояния в *0* м. Мы видим, что аппаратная ошибка одинакова для всех UE с одним и тем же модемом LTE baseband. Более того, все модемы Intel имеют одинаковую погрешность.

Для количественной оценки ошибки оценки расстояния мы вычисляем ошибки между оцененными переменными (с исправленным постоянным смещением) и фактическими расстояниями. Ошибка оценки расстояния может быть напрямую переведена в ошибку локализации при идеальном разбавлении точности. Мы наблюдаем, что для всех мобильных телефонов ошибка 90-го процентиля составляет~ *6* м. Конкретно, 90-й процентиль ошибок составляет: 5,659 м для Huawei P20 Pro, 5,214 м для Huawei P30, 7,238 м для iPhone X и 4,672 м для iPhone 8.

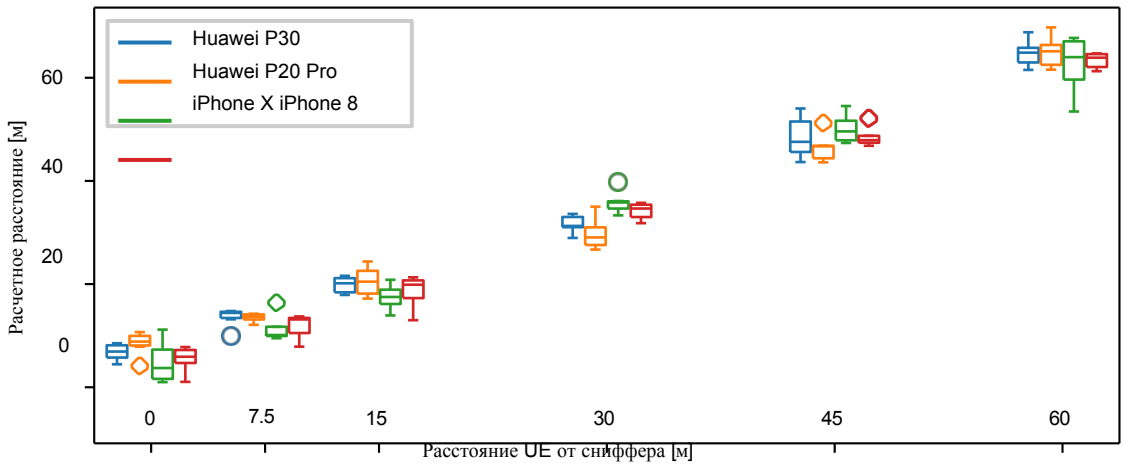


Рисунок 10: Измерения расстояния для четырех различных телефонов на шести расстояниях.

Для USRP B210 90-й процентиль равен 10,474, однако без GPS-фиксации производительность часов B210 ограничена. Очевидно, что при более низких процентилях значения становятся значительно лучше. Медианная ошибка составляет~ 2m для телефонов и~ 7m для B210. Одной из проблем, которую мы наблюдали, была ошибка, возникающая из-за того, что UE не получает команду TA Command. Если UE не получает команду TA Command, eNodeB отправляет ее повторно. Однако LTEPROBE получает ее дважды и применяет команду снова, что приводит к несоответствию. Поскольку N310 не является профессиональным устройством eNodeB, его TX-мощность ниже. Мы можем ожидать лучшей производительности в реальном мире. Возможным исправлением в будущем может стать мониторинг ACK, отправленных UE. Тогда LTEPROBE будет применять только те команды TA, которые UE подтвердило. Мы удалили выбросы соединений, которые более чем в десять раз превышали интерквартильный размах от медианной точки. Из 186 соединений мы удалили 4 точки данных.

7.3 Извлекатель IMSI

Поскольку IMSI Extractor - это атака на уровне протокола, мы оценили ее с помощью программного обеспечения базовой станции промышленного уровня от Amarisoft на аппаратном обеспечении AMARI Callbox Mini [5]. Базовая станция, AdaptOver USRP и Octoclock были синхронизированы с часами GPS.

Мы провели атаку на 17 современных телефонов для сообщений Attach Request и Service Request. Для всех 17 телефонов мы получили IMSI-номер в ответ на запрос прикрепления. Для всех телефонов, кроме одного, iPhone 7, нам удалось получить номер IMSI в качестве ответа на запрос услуги. После передачи Identity Response UE успешно подключались сети. Для пользователя атака была незаметна. Полный список телефонов, использованных в оценке, и пример файла захвата пакетов в нашей атаке можно найти в приложении в таблице 1 и на рисунке 11.

8 Меры противодействия

Как показано в работе [30], атаки на утечку данных о местоположении, представленные в данной работе, невозможно предотвратить, если сообщения и время их передачи/приема не будут полностью рандомизированы. связи с высокой синхронизацией работы LTE эти требования не могут быть реализованы.

Вместо этого мы предлагаем решение, которое требует только изменений в UE и совместимо с текущим протоколом LTE. В нашей контрмере UE отправляет начальное сообщение Random Access со случайным смещением. Поскольку UE знает это смещение, оно изменяет полученную команду Timing Advance Command, добавляя примененное случайное смещение. Таким образом, значение Timing Advance, записанное LTEPROBE, не имеет значения, и его использование в атаке на локализацию приводит к неверным оценкам местоположения. Однако наше предложение не позволяет полностью предотвратить атаку на локализацию. Злоумышленник может использовать больше снифферов и определить случайное смещение, которое применяет UE. Однако это также увеличивает сложность и стоимость атаки.

С другой , мы предлагаем три типа противодействия нашему IMSI Extractor: (i) Противодействие на базе UE развертывается на UE и работает путем наблюдения за запросами идентификации для номера IMSI. UE уведомляют пользователей о неполных идентификационных запросах или сообщают в сеть о нестандартном количестве идентификационных запросов. Сообщение оператору требует доверия к UE в том, что они честно сообщают номера.

(ii) Сетевые контрмеры используют большое количество подслушивающих устройств в покрытия. Они сравнивают подслушанные запросы идентификации с запросами, отправленными базой.

станции. Поскольку операторы устанавливают подслушивающие устройства, они имеют доступ ко всем передаваемым запросам идентификации. Ни контрмеры на базе UE, ни контрмеры на базе сети не предотвращают IMSI Extractor, а лишь обнаруживают его. (iii) Наконец, контрмеры на основе протокола являются наиболее надежными и работают даже против IMSI Extractor, основанных на других процедурах; однако они требуют наиболее масштабных изменений в LTE, что, скорее всего, не модернизировать существующие устройства. В 5G перехват IMSI уже невозможен, поскольку IMSI шифруется с помощью открытого ключа сети. Таким образом, злоумышленник не сможет расшифровать номера IMSI.

9 Связанные работы

Первая работа, в которой был реализован сниффер нисходящего канала управления, была написана Кумаром и другими [22]. В последующей работе Bui et al. [7] реализован сниффер нисходящего канала управления с помощью библиотеки с открытым исходным кодом srsLTE [15]. Мы улучшаем эти две работы, создавая сниффер нисходящего канала, который декодирует каналы данных и восстанавливает дейтаграммы верхнего уровня. Это позволяет нам получать команды TA на MAC-уровне или получать выделенную UE конфигурацию для восходящего канала на уровне RRC. Однако ни в одной из этих работ не реализована функциональность снифера восходящего канала, которая является одним из основных вкладов нашей работы, позволяя нам выполнять локализацию и IMSI Extractor.

Доступны три коммерческих сниффера. Airscope [38] это сниффер, работающий только с нисходящими каналами, в то время как Wavejudge [34] и thinkRF
[40] охватывают функциональность сниффера как для восходящих, так и для нисходящих линий связи. Эти продукты имеют высокую цену и закрытый исходный код, поэтому мы не смогли сравнить наш сниффер с этими продуктами или использовать их для проведения атак.

Что касается отслеживания и локализации пользователей, в работе Shaik et al. [35] показано, как противник может прослушивать пейджинговые сообщения на разных eNodeB. Сначала оператор передает пейджинговое сообщение для конкретного пользователя с последней используемой eNodeB. Из этого сообщения злоумышленник узнает грубое местоположение UE.

В работе LTEye [22] авторы используют радар с синтезированной апертурой для определения кратчайшего и наиболее прямого пути радиосигнала от пользовательского оборудования. Местоположение пользователей определяется по пересечению прямых путей, оцененных несколькими радарами в разных местах.

Наиболее близкой к нашей работе (в контексте локализации UE) является работа [31]. В [31] также предлагается использовать как команду Tim- ing Advance Command от eNodeB, так и время прибытия сообщений восходящей линии связи для приблизительного определения геолокации UE. Однако в [31] не приводится подробная информация об измерении времени прибытия сообщений восходящей линии связи, не реализуется атака и не связывается полученное местоположение с идентификатором UE, как это делается в данной работе. В частности, в нашей работе мы также повышаем точность локализации за счет отпечатка модели телефона и исправления его аппаратных ошибок. В работе [31] используется аппроксимация времени передачи UE из команды Timing Advance Command, что вносит существенную погрешность. Мы преобразуем геометрию задачи в Эллипс с двумя точками фокусировки, что нивелирует большую системную ошибку, вносимую командой Timing Advance Command. В [31] также подчеркивается, что их работа успешна в условиях, когда UE находится вблизи нескольких eNodeB. В нашей атаке достаточно одного eNodeB вблизи жертвы с двумя развернутыми снифферными устройствами.

В работе [27] показана реальная атака на локализацию на основе команды Timing Advance Commands против сетей WiMax со сценарием с несколькими базовыми станциями. Для выполнения атаки использовалось коммерческое устройство Wave-Judge 4900A [34]. Они улучшили оценку расстояния между мобильными телефонами и базовой станцией, используя измерение времени прихода. Однако, по сравнению с этой работой, наша оценка времени прихода обеспечивает точность на уровне подвыборки. В [27] также не оценивались современные смартфоны и соответствующие им аппаратные ошибки.

До сих пор основным инструментом для идентификации UE были IMSI Catchers, которые опираются на поддельные базовые станции [18, 35] и поэтому легко обнаруживаются. Другие подходы включают в себя инициирование повторных подключений путем принуждения UE жертвы к действию, например, путем отправки сообщения в WhatsApp или Facebook [19, 35]. Когда UE снова подключается к сети, злоумышленник может определить модель и марку устройства и сравнить его с UE жертвы [36]. Однако такие атаки направлены в основном против конкретных UE и недостаточны для масштабного отслеживания.

10 Заключение

В этой работе мы предложили и показали возможность масштабного отслеживания пользователей в сети LTE. Кроме того, мы создали LTEPROBE, надежный сниффер восходящего и нисходящего каналов связи, основанный на компонентах srsLTE. Реализация LTEPROBE является "белым ящиком" и не зависит от каких-либо дорогостоящих или проприетарных модулей, кроме готовых программно-определяемых радиостанций. Используя наш сниффер, мы смогли разработать атаку слежения, которую мы назвали LTrack. LTrack улучшает современный уровень, комбинируя сниффер Timing Advancement и измеряя время прибытия сообщений LTE по нисходящей и восходящей линии связи. LTrack также содержит специально разработанный IMSI Catcher, который не полагается на поддельную базовую станцию, а заслоняет пакеты с хирургической точностью и очень малым количеством энергии. Эта работа является первым исследованием отслеживания UE в практических условиях и с помощью доступного оборудования.

Ссылки

[1] 3GPP. 3rd Generation Partnership Project; Technical Specifica- tion Group Radio Access Network;LTE Radio Access Network (RAN) enhancements for diverse data applications. Техническая спецификация (TS) 36.822, Проект партнерства 3-го поколения (3GPP), 2020.

[2] 3GPP. Эволюционный универсальный наземный радиодоступ (e-utra); физические каналы и модуляция. Техническая спецификация (TS) 36.211, Проект партнерства 3-го поколения (3GPP), октябрь 2020 г.

[3] 3GPP. Эволюционный универсальный наземный радиодоступ (e-utra); физический уровень; измерения. Техническая спецификация (TS) 36.214, Проект партнерства 3-го поколения (3GPP), июль 2020 г.

[4] 3GPP. Универсальная система мобильной связи (UMTS); LTE; 5G; протокол Non-Access-Stratum (NAS) для Evolved Packet System (EPS);. Техническая спецификация (TS) 24.301, Проект партнерства 3-го поколения (3GPP), 2020 г.

[5] Амарисофт. AMARI Callbox Series.

[6] Равишанкар Боргаонкар, Эндрю Мартин, Шинджо Парк, Альтаф Шаик, Жан-Пьер Зейферт и ТУ Берлин. White-Stingray: Оценка приложений для обнаружения IMSI-ловушек. *In11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17) 2017*, page 12, 2017.

[7] Никола Буи и Йорг Видмер. OWL: надежный онлайн-наблюдатель для измерений контрольного канала LTE. В *материалах 5-го семинара по операциям, приложениям и задачам сотовой связи - ATC '16*, стр. 25-30, Нью-Йорк, Нью-Йорк, 2016. ACM Press.

[8] Адриан Дабровски, Никола Пьянта, Томас Клепп, Мартин Мулаццани и Эдгар Вайпль. IMSI - поймай меня, если сможешь: IMSI-ловушки. В *материалах 30-й ежегодной конференции по компьютерной безопасности*, ACSAC '14, стр. 246- 255, Нью-Йорк, США, декабрь 2014 г. Association for Computing Machinery.

[9] Ив-Александр де Монжуа, Сезар А. Идальго, Мишель Вер-лейсен и Винсент Д. Блондель. Уникальность в толпе: Границы важности человеческой мобильности. *Scientific Reports*, 3(1):1376, март 2013 г. Номер: 1 Издатель: Nature Publishing Group.

[10] Йони де Малдер, Джордж Данезис, Лейла Батина и Барт Пре-нел. Идентификация с помощью профилирования местоположения в сетях GSM. *Труды 7-го семинара ACM по конфиденциальности в электронном обществе*, WPES '08, стр. 23-32, Нью-Йорк, штат Нью-Йорк, США, октябрь 2008 г. Ассоциация вычислительной техники.

[11] Митсиу Эчеверрия, Зеешан Ахмед, Бинчен Ванг, М. Фа- рид Ариф, Сайед Рафиул Хуссейн и Омар Чоудхури. PHOENIX: Device-Centric Cellular Network Protocol Mon- itoring using Runtime Verification. *arXiv:2101.00328 [cs]*, January 2021. arXiv: 2101.00328.

[12] Симон Эрни, Марк Рёшлин, Патрик Леу, Мартин Котуляк и Срджан Капкун. AdaptOver: Адаптивное затенение сигналов LTE. *arXiv*, август 2021.

[13] Себастьен Гамбс, Марк-Оливье Киллиджиан и Мигель Нуньес дель Прадо Кортес. Атака на деанонимизацию геолокационных данных. *Журнал компьютерных и системных наук*, 80(8):1597-1614, декабрь 2014.

[14] Филипп Голле и Курт Партридж. Об анонимности пар местоположений дом/работа. Хидеюки Токуда, Майкл Бейгл, Адриан Фрайд, А. Дж. Бернхайм Браш и Йошито Тобе, редакторы, *Первазивные вычисления*, том 5538, страницы 390-397. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. Название серии: Lecture Notes in Computer Science.

[15] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sut- ton, Pablo Serrano, Cristina Cano, and Doug J. Leith. srsLTE: open-source platform for LTE evolution and experimenta- tion. В *материалах десятого международного семинара ACM on Wireless Network Testbeds, Experimental Evaluation, and Characterization - WiNTECH '16*, pages 25-32, New York City, New York, 2016. ACM Press.

[16] Бенджамин Хенне, Кристиан Сзонготт и Мэтью Смит. SnapMe if you can: угрозы конфиденциальности чужих геометок и то, что мы можем с этим сделать. В *материалах шестой конференции ACM по безопасности и конфиденциальности в беспроводных и мобильных сетях*, WiSec '13, стр. 95-106, Нью-Йорк, США, апрель 2013 г. Ассоциация вычислительной техники.

[17] Байк Хох, М. Грутсер, Хуэй Сьонг и А. Альрабади. Повышение безопасности и конфиденциальности в системах мониторинга трафика. *IEEE Pervasive Computing*, 5(4):38-46, октябрь 2006. Название конференции: IEEE Pervasive Computing.

[18] Роджер Пикерас Жовер. Эксперименты по обеспечению безопасности LTE, использованию протоколов и отслеживанию местоположения с помощью дешевого программного радио. *arXiv:1607.05171 [cs]*, июль 2016. arXiv: 1607.05171.

[19] Катарина Кольс, Дэвид Руппрехт, Торстен Хольц и Кристина Пёппер. Шифрование потерянного трафика: отпечатки пальцев LTE/4G-трафика на втором уровне. В *материалах 12-й конференции по безопасности и конфиденциальности в беспроводных и мобильных сетях*, стр. 249-260, Майами, Флорида, май 2019 г. ACM.

[20] Джон Крумм. Атаки на умозаключения по отслеживанию местоположения. Энтони Ламарка, Марк Лангейнрих и Кхай Н. Труонг, редакторы, *Первобытные вычисления*, том 4480, страницы 127-143. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007. Название серии: Lecture Notes in Computer Science.

[21] Джон Крумм. Обзор вычислительной конфиденциальности местоположения. *Personal and Ubiquitous Computing*, 13(6):391-399, август 2009.

[22] Сварун Кумар, Эззельдин Хамед, Дина Катаби и Ли Эрран Ли. Радиоаналитика LTE стала простой и доступной. В *материалах конференции ACM 2014 SIGCOMM - SIGCOMM '14*, стр. 211-222, Чикаго, Иллинойс, США, 2014. ACM Press.

[23] Чжэньхуа Ли, Вэйвэй Ван, Кристо Уилсон, Цзянь Чэнь, Чэнь Цянь, Тэхо Чжун, Лань Чжан, Кебин Лю, Сянъян Ли и Юньхао Лю. FBS-Radar: Обнаружение фальшивых базовых станций в дикой природе. В *материалах 2017 Network and Dis- tributed System Security Symposium*, San Diego, CA, 2017. Internet Society.

[24] Лин Ляо, Дональд Дж. Паттерсон, Дитер Фокс и Генри Каутц. Обучение и вывод транспортных маршрутов. *Artificial Intel- ligence*, 171(5-6):311-331, апрель 2007.

[25] Накарми Праджвол Кумар, Ноамен Бен Хенда и Власиос Ци-ацис. 3GPP Release 15 и борьба с ложными базовыми станциями, январь 2019 г. Последнее изменение: 2020-04-27T11:21:46+00:00.

[26] Александра-Михаэла Олтеану, Кевин Угенин, Реза Шокри и Жан-Пьер Юбо. Количественная оценка влияния информации о совместном местоположении на конфиденциальность местоположения. Эмилиано де Кристо-фаро и Стивен Дж. Мердок, редакторы, *Технологии повышения конфиденциальности*, Лекции по , стр. 184-203, Чам, 2014. Springer International Publishing.

[27] Бенджамин А Пиментел. *Пассивная геолокация в сценарии 4G WIMAX с одной базовой станцией*. Докторская диссертация, Военно-морская аспирантура, Монтерей, Калифорния, 2013.

[28] Апостолос Пиргелис, Кармела Тронкосо и Эмилиано Де Кристофаро. Тук-тук, кто там? Выявление принадлежности к группе по агрегированным данным о местоположении. In *Proceedings 2018 Net- work and Distributed System Security Symposium*, San Diego, CA, 2018. Internet Society.

[29] Купер Квинтин. *Обнаружение поддельных базовых станций 4G в реальном времени*. DEF CON, 2020.

[30] Каспер Бонне Расмуссен и Срджан C˘ апкун. Важность протоколов с ограничением расстояния. *Труды 15-й конференции ACM по компьютерной и коммуникационной безопасности*, CCS '08, стр. 149-160, Нью-Йорк, штат Нью-Йорк, США, октябрь 2008 г. Association for Computing Machinery.

[31] Джон Д. Рот, Мурали Туммала, Джон К. МакИхен и Джеймс В. Скрофани. О конфиденциальности местоположения в сетях LTE. *IEEE Transactions on Information Forensics and Security*, 12(6):1358-1368, June 2017. Название конференции: IEEE Trans- actions on Information Forensics and Security.

[32] Дэвид Руппрехт, Катарина Колс, Торстен Хольц и Кристина Пёппер. Взлом LTE на втором уровне. *Симпозиум IEEE по безопасности и конфиденциальности (SP), 2019*, стр. 1121-1136, май 2019. ISSN: 2375-1207.

[33] Дэвид Руппрехт, Катарина Кольс, Кристина Пёппер и Торстен Хольц. Подслушивание зашифрованных звонков LTE с помощью REVOLTE. В *материалах 29-й конференции USENIX по безопасности*, стр. 17, 2020.

[34] Sanjole. WaveJudge 5000 Беспроводная тестовая система для LTE и WiMAX.

[35] Альтаф Шайк, Равишанкар Боргаонкар, Н. Асокан, Валттери Ниеми и Жан-Пьер Сейферт. Практические атаки против конфиденциальности и доступности в системах мобильной связи 4G/LTE. *arXiv:1510.07563 [cs]*, август 2017. arXiv: 1510.07563.

[36] Альтаф Шайк, Равишанкар Боргаонкар, Шинджо Парк и Жан-Пьер Сейферт. Новые уязвимости в протоколах сетей сотового доступа 4G и 5G: раскрытие возможностей устройств. В *материалах 12-й конференции по безопасности и конфиденциальности в беспроводных и мобильных сетях*, стр. 221-231, Майами, Флорида, май 2019 г. ACM.

[37] Реза Шокри, Джордж Теодоракопулос, Жан-Ив Ле Будек и Жан-Пьер Юбо. Количественная оценка конфиденциальности местоположения. *Симпозиум IEEE 2011 по безопасности и конфиденциальности*, стр. 247-262, Окленд, Калифорния, США, май 2011. IEEE.

[38] Программные радиосистемы. Продукция| SRS.

[39] Мудхакар Шриватса и Майк Хикс. Деанонимизация следов мобильности: использование социальной сети в качестве побочного канала. *Труды конференции ACM 2012 по компьютерной и коммуникационной безопасности*, CCS '12, стр. 628-637, Нью-Йорк, США, октябрь 2012 г. Association for Computing Machinery.

[40] ThinkRF. Лидер в области программно-определяемого спектрального анализа.

[41] Хуандун Ван, Чэнь Гао, Юн Ли, Ган Ван, Депенг Цзинь и Цзинбо Сунь. Деанонимизация трасс мобильности: Dissecting the Gaps between Theory and Practice. В *материалах 2018 Network and Distributed System Security Symposium*, San Diego, CA, 2018. Internet Society.

[42] Мариус Вернке, Павел Скворцов, Франк Дюрр и Курт Ротер-мель. Классификация атак и подходов к обеспечению конфиденциальности местоположения. *Personal and Ubiquitous Computing*, 18(1):163-175, January 2014.

[43] Ходжун Ян, Сангвук Бэ, Минчеол Сон, Хонгиль Ким, Сонг Мин Ким и Йонгдэ Ким. Прятки в обычном сигнале: Атака на затенение физического сигнала LTE. В *материалах 28-й конференции USENIX по симпозиуму по безопасности*, SEC'19, стр. 19, 2019.

[44] Хуэй Цанг и Жан Болот. Анонимизация данных о местоположении не работает: масштабное измерений. В *материалах 17-й ежегодной международной конференции по мобильным вычислениям и сетям*, MobiCom '11, страницы 145-156, Нью-Йорк, штат Нью-Йорк, США, сентябрь 2011 года. Ассоциация вычислительной техники.

A Приложение

Модель UE	Идентификация Прикрепить запрос	Идентификация Запрос на услугу
Samsung Galaxy s10	да	да
Samsung Galaxy a8	да	да
Huawei P20 Pro	да	да
Huawei P30 Lite	да	да
Huawei P30	да	да
Xiaomi Mi9	да	да
Xiaomi MiX 3	да	да
Google Nexus 5X	да	да
Google Pixel 2	да	да
Google Pixel 3a	да	да
HTC U12+	да	да
OnePlus 7T	да	да
iPhone 6s	да	да
iPhone 7	да	нет
iPhone 8	да	да
iPhone X	да	да
iPhone 11	да	да
iPhone 11 Pro	да	да

Таблица 1: Мобильные телефоны, использовавшиеся в экспериментах по извлечению IMSI.

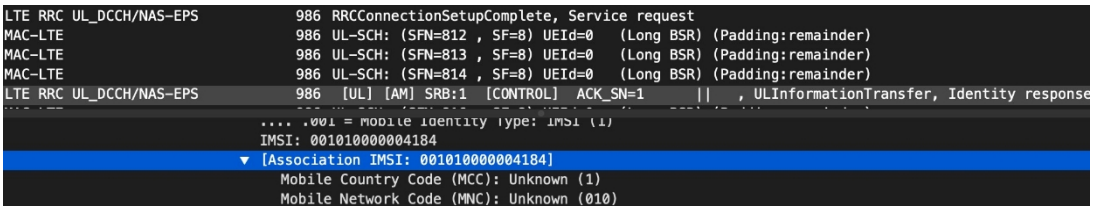


Рисунок 11: Файл захвата пакетов из программы IMSI Extractor.

Модель UE	Модем	Аппаратная ошибка [$м$]	std [m]
Samsung Galaxy s10	Exynos 9820	11.29	7.22
Samsung Galaxy a8	Exynos 7885	-26.62	4.77
Samsung Galaxy s5	Qcom. Gobi 4G	-	-
Huawei P20 Lite	Кирин 659	-24.47	2.13
Huawei P20 Pro	Кирин 970	-9.34	2.90
Huawei P30 Lite	Кирин 710	-10.27	0.98
Huawei P30	Кирин 980	-24.51	1.49
Xiaomi Mi9	Qcom. X24 LTE	10.44	2.20
Xiaomi MiX 3	Qcom. X24 LTE	11.57	1.60
Nokia 1.3	Qcom. X5 LTE	-	-
Sony Xperia X	Qcom. X8 LTE	-11.20	4.78
Google Nexus 5X	Qcom. X10 LTE	5.08	2.51
Google Pixel 2	Qcom. X16 LTE	-13.52	2.32
Google Pixel 3a	Qcom. X12 LTE	4.46	2.14
Google Pixel 4	Qcom. X24 LTE	12.88	1.67
HTC U12+	Qcom. X20 LTE	-13.66	1.55
OnePlus 7T	Qcom. X24 LTE	12.66	1.42
iPhone 7	Intel XMM7360	-23.86	0.88
iPhone 8	Intel XMM 7480	-23.65	2.28
iPhone X	Intel XMM7480	-25.64	3.75
iPhone 11	Intel XMM 7660	-23.19	2.49
iPhone 11 Pro	Intel XMM 7660	-25.35	2.46

Таблица 2: Мобильные телефоны, использовавшиеся в экспериментах по локализации и отпечатку пальцев.