AdaptOver : Адаптивное затенение сигналов LTE

Симон Эрни, Патрик Леу, Мартин Котуляк, Марк Рёшлин, Срджан Čапкун
Факультет компьютерных наук ETH
Zurich

Аннотация

Мы представляем AdaptOver, новую атаку на затенение сигнала LTE, которая позволяет противнику реактивно и адаптивно затенять любое сообщение нисходящего канала между сетью и пользовательским оборудованием (UE). Мы демонстрируем влияние AdaptOver, используя ее для проведения целевых атак типа "отказ в обслуживании" (DoS) на UE.

Мы реализуем AdaptOver с помощью коммерчески доступного программно-определяемого радио. Наши эксперименты показали, что DoS-атаки вызывают стойкую потерю соединения продолжительностью более 12 часов для широкого спектра смартфонов. DoS-атаки на основе AdaptOver более скрытны, чем атаки, основанные на использовании поддельных базовых станций, и более устойчивы, чем существующие атаки с затенением, которые приводили к потере соединения всего на 9 минут. Учитывая, что AdaptOver может реактивно затенять любое сообщение в нисходящем канале, его применение не ограничивается DoS-атаками - он может использоваться для широкого спектра других атак, например, для извлечения IMSI из UE более скрытным способом, чем традиционные IMSI-ловушки. Мы считаем, что AdaptOver является важным строительным блоком для многих атак на реальные сети LTE. В частности, любая атака на поддельную базовую станцию, использующая поддельные нисходящие сообщения, может быть перенесена на представленный метод атаки, что приведет к гораздо более надежному, стойкому и скрытному эффекту.

1 Введение

Технология LTE была разработана для создания инфраструктуры сотовой связи, устойчивой к помехам, но не всегда подходящей для устойчивой к помехам связи. Поэтому неудивительно, что радиосвязь между базовой станцией (eNodeB) и пользовательским оборудованием (UE) уязвима для беспроводных помех [12]. Учитывая отсутствие аутентификации базовой станции, LTE еще более уязвима для атак на поддельные базовые станции, что приводит к атакам типа "отказ в обслуживании" (DoS) [19] или "человек посередине" (MITM) [18]; при такой атаке UE подключаются к поддельной базовой станции, в результате чего злоумышленник может подменить любые сообщения, не прошедшие аутентификацию/защиту целостности. В частности, поддельная базовая станция может вызвать DoS, ответив на процедуру обслуживания/присоединения отказом [7, 8, 19], выступить в роли перехватчика IMSI [8] или подделать ключевой поток пользовательских данных, не защищенных целостностью [17, 18]. Хотя эти атаки обладают высокой эффективностью, они требуют от злоумышленника длительной активности и высокой выходной мощности, что чревато обнаружением со стороны регулирующих органов и правоохранительных органов.

Совсем недавно появился новый, более сложный метод атаки на LTE, основанный на затенении сообщений [21]. В ходе этой атаки, получившей название SigOver, нисходящий сигнал базовой станции затеняется (т. е. заменяется по воздуху) синхронизированным по времени и частоте сигналом атаки большей силы. В отличие от использования (глушения) или поддельной базовой станции, эта атака требует гораздо меньшей мощности (3 дБ против 30 дБ) для достижения высокого уровня успеха в создании DoS для UE. Однако конструкция SigOver позволяет применять затенение только к каналам с предсказуемым планированием, таким как канал управления широковещательной передачей (BCCH) и канал управления пейджингом (PCCH). Учитывая это, SigOver может вызвать DoS, ограниченный одной сотой, и отключить UE от сети не более чем на 9 минут. Если UE находится в зоне действия других базовых станций, он попытается подключиться снова, что потребует от атакующего одновременного проведения атаки на все базовые станции, находящиеся поблизости от UE-жертвы.

В этой работе мы представляем новую технику атаки под названием AdaptOver, которая позволяет затенять *произвольные* сообщения нисходящего канала и вмешиваться в любые протокольные процедуры между любым из компонентов LTE (базовой станцией и опорной сетью) и UE в активном соединении. По своей конструкции AdaptOver является реактивным и соединен с декодером нисходящего канала, что позволяет ему реагировать на трафик нисходящего канала. Чтобы успешно заслонить сообщение, AdaptOver необходимо достичь мощности всего на 1,8 дБ выше, чем у легитимного сигнала. Хотя это кажется улучшением по сравнению с SigOver, мы можем списать это на различия в наших экспериментальных установках и поэтому не будем утверждать о каком-либо преимуществе.

Для того чтобы продемонстрировать влияние AdaptOver, мы осуществили ряд DoS-атак на несколько процедур установления соединения LTE. Наши результаты показывают, что

Затеняя одно нисходящее сообщение (присоединение, обслуживание или аутентификация) от eNodeB и базовой сети к UE, AdaptOver способен создать постоянный DoS длительностью >12 часов (по сравнению с DoS длительностью 9 минут при использовании существующих методов затенения). Атака не зависит от количества базовых станций в непосредственной близости от UE - вице-тим UE не будет пытаться переподключиться ни к одной из соседних базовых станций. AdaptOver может совершить DoS на UE в любой момент, когда телефон восстанавливает обслуживание после некоторого простоя (что происходит в худшем случае не чаще, чем раз в 6 минут, когда пользователь не взаимодействует с телефоном [1]), перезагружается или переключается в авиарежим.

Влияние AdaptOver не ограничивается DoS-атаками. AdaptOver может быть использован для манипулирования протокольными процедурами LTE и утечки информации, подобно атакам на поддельные базовые станции, но более хирургическим и скрытным способом. В [10] AdaptOver используется для улучшения отслеживания пользователей путем раскрытия постоянного идентификатора (IMSI) пользователя, подключающегося к сети. Эта проблема известна как *IMSI catcher* или *Stingray* attack. Традиционно для этой атаки требуется установить поддельную базовую станцию с высокой выходной мощностью, которая заманивает находящиеся поблизости UE-жертвы для подключения к ней. LTE не предназначен для предотвращения этой атаки, но, учитывая заметность поддельных базовых станций, были сделаны предложения по их обнаружению [3, 4, 11, 14, 16, 20]. Используя AdaptOver, злоумышленник может победить методы, основанные на обнаружении поддельных базовых станций, и таким образом раскрыть IMSI более скрытным способом.

В итоге мы сделали следующие выводы:

- Мы разрабатываем реактивную и протокольно-ориентированную атаку, позволяющую внедрять нисходящие сообщения в радиоканал в любой момент времени и на любом коммуникационном уровне LTE.
- Мы продемонстрировали влияние AdaptOver, реализовав DoS-атаки, более скрытные, чем предыдущие атаки, которые основывались на использовании поддельной базовой станции, и более продолжительные (12 часов), чем существующие атаки с затенением, которые приводили к потере соединения всего на 9 минут.
- Наконец, мы обсуждаем меры противодействия, которые могут быть реализованы производителями baseband для предотвращения предлагаемых DoS-атак.

Остальная часть статьи организована следующим образом. В разделе 2 мы приводим необходимые сведения о LTE и предыдущих работах по затенению сигнала. В разделе 3 мы представляем наш подход и демонстрируем атаку Service Reject. В разделе 4 представлены все атаки, перенесенные на AdaptOver, а в разделе 5 приведена их оценка. Наконец, в разделе 6 рассматриваются меры противодействия.

2 Общие сведения: LTE и затмение

В следующем разделе представлены исходные данные, необходимые для понимания дизайна атаки AdaptOver.

Читатели, знакомые с внутренним устройством LTE, могут пропустить эту часть.

2.1 LTE

Сеть LTE состоит из двух основных компонентов: базовой сети, называемой Evolved Packet Core (EPC), и сети радиодоступа (RAN), которая включает набор базовых станций, называемых Evolved Node B (eNodeB), и пользовательского оборудования (UE), например смартфонов, маршрутизаторов или устройств Интернета вещей (IoT).

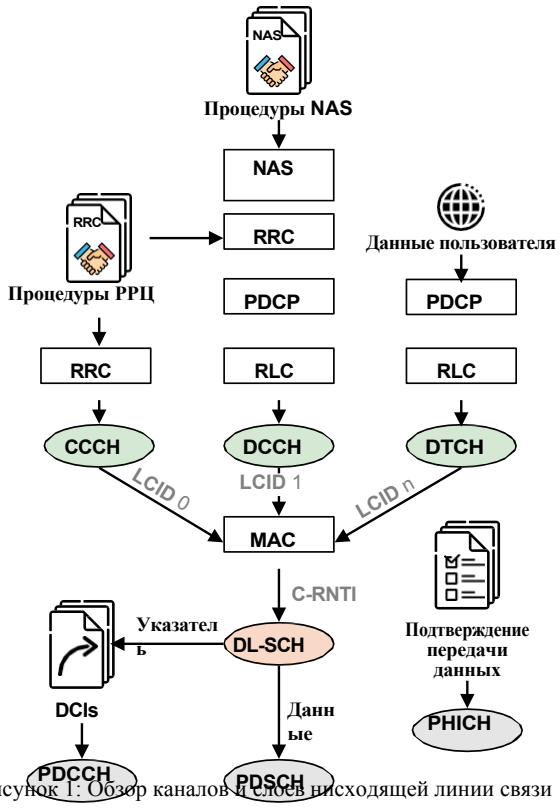


Рисунок 1: Обзор каналов и слоев нисходящей линии связи

Беспроводной сигнал LTE имеет следующую структуру. Во временной области сигнал LTE состоит из кадров длительностью 10 мс, каждый из которых делится на 10 подкадров длительностью 1 мс. Каждый субкадр в LTE имеет одинаковую базовую структуру и не зависит от других субкадров. В частотной области сигнал LTE делится на 72 - 1200 ортогонально расположенных поднесущих, в зависимости от настроенной полосы пропускания соты.

Отдельные единицы данных, подлежащие передаче, затем модулируются на выделенные поднесущие и преобразуются с помощью IFFT во временную область. Распределение определяется с помощью так называемой сетки ресурсов, где ось y соответствует поднесущим в частотной области, а ось x - слотам во временной области. Каждая область (под)сетки отводится под определенную функцию. В данной статье мы сосредоточимся на нисходящей линии связи.

На рисунке 1 нижние овалы (PDCCH, PDSCH и PHICH) представляют собой каналы нисходящей линии связи, которым отведена определенная область на сетке повторного источника. Как эти каналы используются для передачи пользовательских и управляющих данных, объясняется в следующем разделе.

2.1.1 Каналы и слои

Физический канал управления нисходящим каналом (PDCCH) В начале субкадра находится физический канал управления нисходящим каналом (PDCCH). Он содержит сообщения Downlink Control Informa- tion (DCI), которые имеют две основные цели. Во-первых, они служат метаданными для данных, передаваемых в остальной части субкадра, указывая, какому UE предназначаются данные, где они расположены в сетке ресурсов и как они закодированы. Во-вторых, сообщения DCI распределяют ресурсы восходящей линии связи между UE, указывая, что UE может отправлять данные в определенное время и в определенном диапазоне частот в канале восходящей линии связи.

(Физический) Downlink Shared Channel (PDSCH / DL- SCH) Данные, инкапсулированные на уровне управления доступом к среде (MAC), поступают в виде транспортных блоков на Downlink Shared Channel (DL-SCH). Там они обрабатываются вместе с цепочкой обработки физического общего канала нисходящей линии связи (PDSCH) и затем помещаются в сетку ресурсов. Любые параметры, используемые при обработке, такие как схема модуляции, прекодирование или сопоставление уровней, помещаются в сообщение DCI и отправляются вместе с ним.

Временный идентификатор радиосети (RNTI) С помощью временных идентификаторов радиосети (RNTI) можно передавать данные для разных UE в одном субкадре. Сообщения, предназначенные для UE, помечаются уникальным идентификатором ячейки, называемым C-RNTI, а сообщения конфигурации широковещания используют специальные RNTI, называемые системными информационными RNTI (SI-RNTI).

Управление доступом к среде (MAC) Внутри UE пользовательские данные и управляющие сообщения, относящиеся к текущим процедурам, мультиплексируются и размещаются вместе на DL-SCH. Чтобы различать различные процедуры, уровень MAC назначает каждому каналу логический идентификатор канала (LCID).

Физический канал индикации HARQ (PHICH) Через 4 субкадра после передачи распределения по восходящей линии связи с помощью сообщения DCI UE отправляет данные. Еще через 4 субкадра она подтверждается 1-битным сообщением гибридного автоматического запроса повтора (HARQ), передаваемым по нисходящему каналу по PHICH. Это служит механизмом с низкой задержкой для обнаружения и исправления ошибок передачи по восходящей линии.

Сообщения **(Radio Resource Control, RRC)** передаются между UE и базовой станцией и используются для управления соединением между UE и базовой станцией. В процедуре установления соединения (показана в Раздел 2.1.2), сообщения RRC Connection Request и RRC Connection Setup передаются по общему каналу управления (CCCH). В сообщении RRC Connection Setup конфигурируется выделенный канал управления (DCCH), по которому передаются все дальнейшие сообщения RRC. После установления соединения пользовательские данные передаются по выделенному каналу трафика (DTCH).

Сообщения **уровня без доступа (NAS)**, которыми обмениваются UE и компоненты опорной сети, такие как узел управления мобильностью (MME) во время установления соединения (см. раздел 2.1.2), передаются на уровне NAS, где они по желанию шифруются и/или защищаются от повреждений. Они упаковываются в сообщение RRC, которое может быть пустым или содержать отдельное сообщение RRC. Задача MME - распределять пейджинговые сообщения, управлять хэндоверами и обрабатывать процедуры присоединения и обслуживания.

Управление радиоканалом (RLC) Уровень RLC используется для сегментации, надежной транспортировки и передачи в порядке очереди. В нисходящем и восходящем каналах каждый отправленный сегмент RLC подтверждается. Это делается путем включения наибольшего порядкового номера сегмента, который был успешно получен. Такие подтверждения могут передаваться и в сегментах данных.

Конвергенция пакетных данных (PDCP) PDCP несет ответственность за сжатие, а также за функции безопасности, такие как защита целостности и шифрование. Целостность и шифрование являются необязательными для каждого сообщения и могут быть включены в заголовке PDCP.

2.1.2 Процедуры

Когда UE подключается к сети, он выполняет процедуру, показанную на рисунке 2. Независимо от того, ли оно просто бездействующим, сначала оно выполняет прикрепление к базовой станции. После этого UE продолжает процедуру присоединения к базовой сети, которая в конечном итоге предоставляет UE услуги сети или телефонии.

Присоединение базовой станции. После получения конфигурации соты путем декодирования сообщений блока системной информации (SIB), отправленных по широковещательному каналу управления (BCCH), UE запрашивает выделение восходящей линии связи по физическому каналу случайного доступа (PRACH) с помощью преамбулы PRACH. eNodeB выделяет RNTI и необходимые ресурсы восходящей линии связи и сигнализирует об этом UE с помощью ответа PRACH. Затем UE инициирует запрос соединения RRC и получает сообщение RRC Connection Setup, содержащее выделенную конфигурацию для UE. Наконец, UE подтверждает соединение с помощью сообщения RRC Connection Setup Complete.

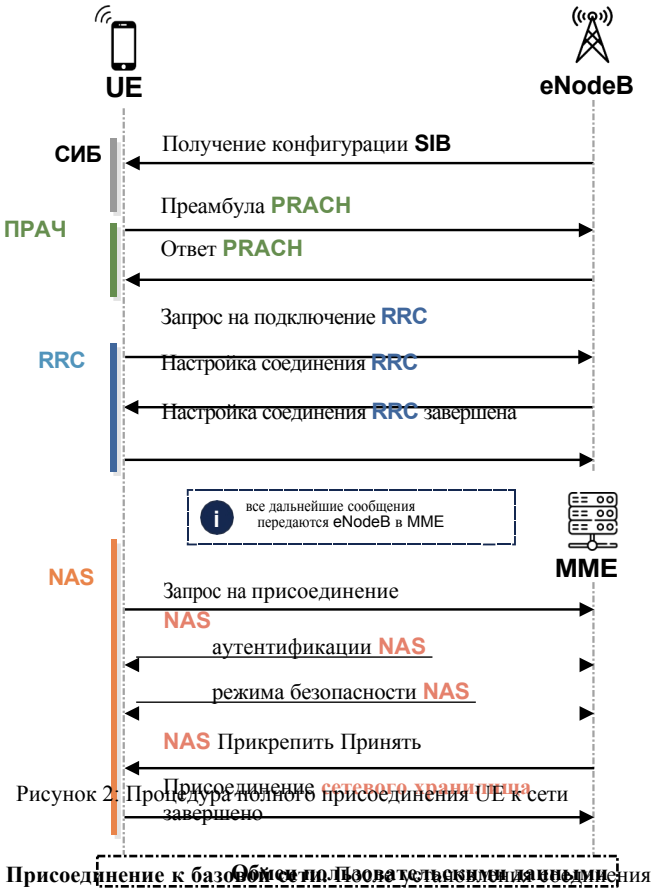


Рисунок 2: Процедура полного присоединения UE к сети

Присоединение к базовой станции. После установления соединения с базовой станцией с помощью процедуры RRC, описанной выше, UE начинает процедуру присоединения NAS. Сначала UE отправляет свой идентификатор вместе с запросом на присоединение NAS в MME. Затем MME и UE выполняют процедуру аутентификации и обмена ключами (AKA). Затем в процедуре режима безопасности активируется безопасность канала. Наконец, они завершают успешное присоединение сообщением NAS Attach Accept and Complete. Если UE и сеть не обмениваются данными в течение некоторого времени, UE переходит в режим ожидания, отсоединяясь от сети. Оно может возобновить соединение, повторив процедуру прикрепления к базовой станции, а затем процедуру запроса услуг NAS, которая будет показана далее в контексте атаки на рисунке 3.

2.2 SigOver Attack

Авторы работы [21] продемонстрировали новый метод атаки под названием SigOver, который заменяет часть легитимного сигнала базовой станции LTE (eNodeB) на сигнал, контролируемый злоумышленником, используя только коммерчески доступные программно-определяемые радиостанции.

(SDR). Они добились этого, заслонив часть сигнала своим атакующим сигналом, который достигает более высокой мощности на UE. Хотя эти два сигнала сталкиваются, более сильный сигнал все равно будет декодирован. Это явление называется *эффектом захвата*.

Синхронизация времени и частоты. Для того чтобы перехватить сигнал, злоумышленник должен отправить его с правильной по времени и частоте. Для этого злоумышленник сначала измеряет смещение между генерируемой частотой генератора в SDR и реальным сигналом eNodeB. Затем он соответствующим образом настраивает частоту выходного сигнала, компенсируя любые неточности внутреннего генератора SDR. Чтобы точно выровнять время сигнала, злоумышленник декодирует сигналы синхронизации eNodeB (PSS и SSS) и выравнивает их с выходом SDR. По этим сигналам синхронизации злоумышленник может определить начальную точку субкадров, которые он стремится заслонить. Поскольку SDR, используемый в атаке, вносит постоянную задержку передачи в диапазоне 5-20
микросекунд (в зависимости от частоты дискретизации), злоумышленнику необходимо дать SDR команду начать передачу раньше, чтобы компенсировать задержку. Однако эта задержка постоянна и зависит от аппаратной модели SDR, а значит, может быть измерена и настроена статически.

PDSCH Overshadowing. SigOver атакует физический общий канал нисходящей линии связи (PDSCH). Чтобы затенять канал PDSCH, необходимо также затенять сигналы PCFICH, PDCCH и сигналы отсылки, используемые для оценки канала, поскольку все они необходимы для декодирования канала PDSCH. При использовании SigOver эти сигналы генерируются злоумышленником и отправляются вместе с подкадром.

Атаки, поддерживаемые SigOver. По каналу PDSCH сота передает конфигурационные сообщения в виде блоков системной информации (SIB) и пейджинговые сообщения, которые используются для уведомления UE о входящих данных или вызовах. Пейджинговые сообщения SIB передаются по фиксированному расписанию: SIB2 передается в 5-м подкадре каждого второго кадра, а пейджинговые сообщения - в 9-м подкадре. SigOver показала, что можно достичь DoS одной ячейки, включив запрет ячеек SIB2, с сохранением около 9 минут после отключения передачи атаки. Кроме того, исследователи добились выборочного DoS целевого UE путем введения пейджинговых сообщений, содержащих IMSI, хотя и без стойкости, поскольку UE немедленно попытается подключиться снова. Кроме того, им удалось выполнить понижение рейтинга с помощью пейджинговых сообщений, предназначенных для принуждения UE к подключению к сети 3G.

Ограничения SigOver. Конструкция SigOver позволяет применять затенение только для каналов с предсказуемым планированием, таких как канал управления широковещательной передачей (BCCH)

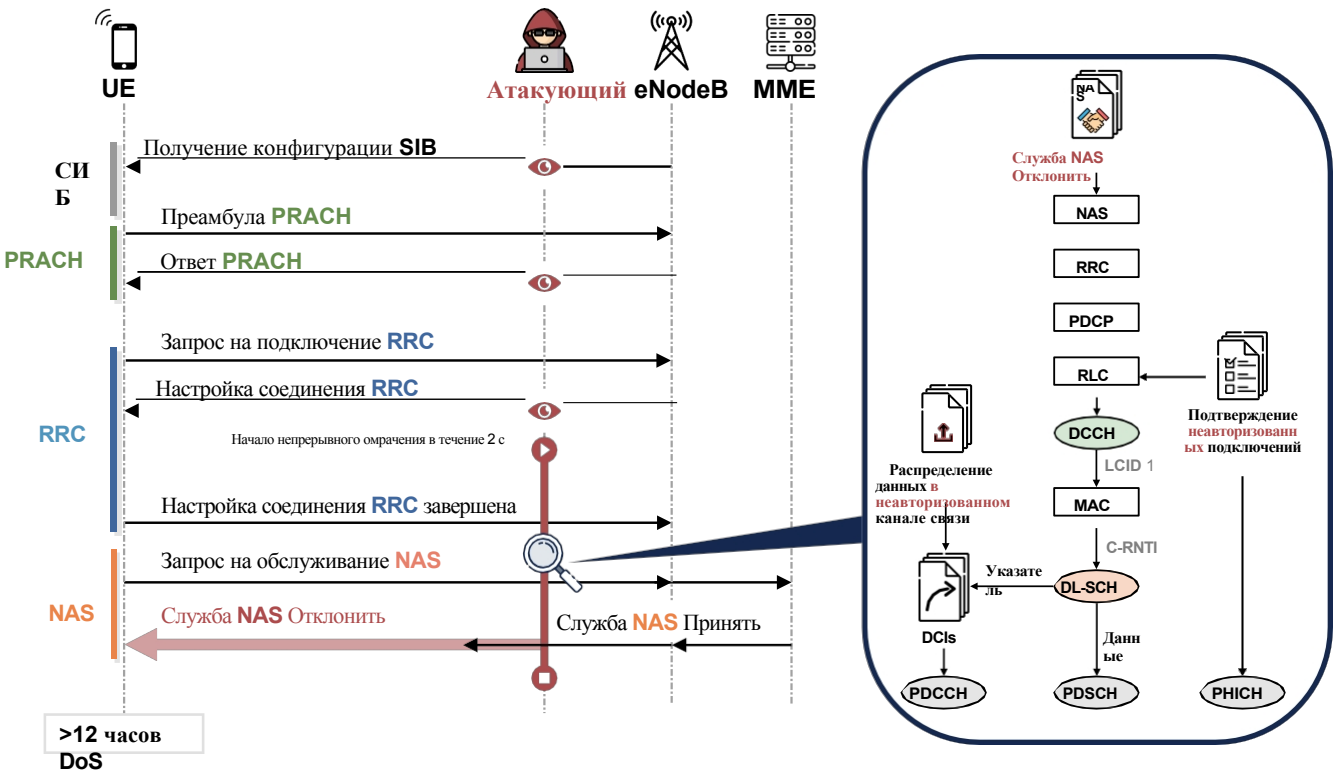


Рисунок 3: объяснение AdaptOver с помощью атаки Service Reject Attack. Для начала атаки злоумышленник прослушивает сообщение RRC Connection Setup. Атакующий посылает NAS Service Reject в каждом субкадре в течение 2 секунд, заслоняя Service Accept Service Reject, вызывая DoS на UE длительностью >12 часов. Во время атаки злоумышленник включает несанкционированное выделение восходящего канала и подтверждение, чтобы позволить UE отправить запрос службы NAS.

и канал управления пейджингом (PCCH). Поэтому SigOver может быть применен только к процедурам пейджинга и получения конфигурации, что приводит к DoS, ограниченному одной сотой и приводящему к отключению UE всего на 9 минут. Однако в реальности UE редко оказывается в ситуации, когда в зоне доступа находится только одна сота, поэтому оно немедленно переключается на следующую доступную соту, что требует от злоумышленника проведения атаки на все базовые станции в непосредственной близости от жертвы, поскольку в противном случае DoS-атака не затронет UE в реальных условиях. Несмотря на то, что эта атака более скрытна, чем атака с поддельной базовой станцией, заслонение сигналов в нескольких нисходящих потоках требует координации и увеличивает стоимость оборудования, а также повышает вероятность обнаружения.

3 Адаптивное затенение сигнала

AdaptOver является реактивным и способен изменять потоки сообщений и процедуры между UE и всеми компонентами LTE, такими как базовая станция или службы опорной сети. AdaptOver способен заслонить любой канал нисходящей линии произвольными данными, а также декодировать каналы нисходящей линии, что делает его способным реагировать на любой трафик нисходящей линии.

Мы показали, что DoS-атаки на LTE, для которых требовалась поддельная базовая станция, могут быть перенесены на AdaptOver, что позволяет проводить постоянные атаки.

(>12 часов) DoS-атаки в любой момент, когда телефон перезагружается, переключается в авиарежим или, что бывает чаще, восстанавливает связь после некоторого простоя. Наконец, мы показываем, как AdaptOver был применен в [10] для создания IMSI-ловушки, которая более скрытна, чем существующие традиционные IMSI-ловушки, основанные на поддельных базовых станциях.

Модель злоумышленника и допущения. Мы рассматриваем следующую модель злоумышленника: **(i)** Отсутствие знаний о ключах и физического доступа к компонентам оператора или пользовательского оборудования (UE). **(ii)** Способность принимать нисходящую связь от базовой станции к UE; отсутствие возможности расшифровывать зашифрованные сообщения. **(iii)** Возможность посылать сигналы LTE на UE таким образом, чтобы мощность сигнала злоумышленника на UE была на 3 дБ выше мощности сигнала, передаваемого базовой станцией. Это может быть достигнуто либо за счет изменения мощности передачи, либо за счет изменения местоположения устройства злоумышленника.

Мы покажем, что эти возможности злоумышленников реалистичны и достаточны для добавления, изменения и удаления сообщений, исходящих не только от eNodeB, но и от компонентов опорной сети, таких как Mobility Management Entity (MME).

Мы подробно проиллюстрируем возможности AdaptOver на примере

пример атаки Service Reject Attack, которая направлена на UE, когда оно восстанавливает обслуживание после простоя. Варианты этой атаки мы рассмотрим в разделе 4.

3.1 Обзор и атака на отказ в обслуживании

Процедура запроса услуги. Если UE не нуждается в обмене данными, он может перейти в режим ожидания для экономии энергии, если на это укажет eNodeB. Выход из режима ожидания осуществляется путем повторного подключения к базовой станции с помощью процедур PRACH и RRC, после чего следует запрос услуги к MME, на который приходит сообщение о принятии услуги. [1, 6], UE переходит в режим ожидания после того, как проведет без трафика не более 60 с. Наши измерения в реальных сетях трех различных операторов мобильной связи подтвердили это наблюдение. Анализ различных моделей трафика, проведенный в [1], показал, что типичное UE с небольшим количеством трафика будет входить в процедуру запроса на обслуживание примерно каждые 6 минут. Теоретически этот период можно сократить еще больше, принудительно прервав активное соединение с помощью глушения активного соединения или вбросив пейджинговое сообщение с TMSI или IMSI жертвы. Однако это не требуется для работы AdaptOver и достигается за счет более высокой обнаруживаемости.

Атака на отказ в обслуживании. Цель нашей атаки Service Reject заключается в том, чтобы заслонить сообщение Service Accept, отправленное MME, и заменить его сообщением Service Reject со значением причины 8 (т. е. *услуги EPS и не-EPS не разрешены*), как показано на рисунке 3. Согласно разделу 5.6.1.5 стандарта 3GPP TS 24.301 [2], это приведет к тому, что UE будет считать SIM-карту недействительной, и, если пользователь не повторит попытку, UE будет отходить от сети более 12 часов, не пытаясь подключиться к ней. В разделе 5.2 мы проверяем эффект атаки на различных телефонах. Мы впервые показываем, что подобная атака может быть осуществлена путем инъекции сообщений. До сих пор было показано, что такие атаки работают только в том случае, если UE подключен к поддельной базовой станции злоумышленника.

Чтобы запланировать и надежно выполнить атаку Service Reject At- tack, AdaptOver реализует следующие шаги, показанные на рисунке 3. Во-первых, чтобы иметь возможность запланировать инжекцию сообщения Attack Reject в нужное время и с нужными параметрами, AdaptOver реализует декодер нисходящего канала, который специально прослушивает и декодирует сообщения eNodeB, а также MME. Получив сообщение RRC Con- nection Setup, AdaptOver начинает непрерывно вводить сообщения Service Reject в каждом субфрейме в течение следующих 2 секунд. Это достаточно консервативный подход, эксперименты показали, что и короткой инжекции в течение 50 мс, ценой небольшого снижения надежности. AdaptOver размещает эти сообщения в канале PDSCH, тем самым затмевая все сообщения, отправляемые eNodeB в UE. В разделе 3.2 мы подробно обсудим, как наша реализация затенения улучшает SigOver.

Основные задачи. В LTE базовая станция выделяет ресурсные слоты, в пределах которых UE могут отправлять свои данные. Без такого распределения восходящих каналов UE не смогут отправлять данные. Если злоумышленник отправит сообщение об отказе в обслуживании слишком рано, т. е. до того, как UE успеет отправить запрос на обслуживание, сообщение об отказе не будет принято UE, и атака провалится. Поскольку AdaptOver временно заслоняет все сообщения нисходящей линии связи для целевого UE, во время атаки теряется распределение восходящей линии связи от eNodeB.

Чтобы исправить это, злоумышленник может подождать, пока запрос Service Re- будет полностью передан UE и подтвержден eNodeB. Однако в этом случае возникают две проблемы:
(i) нам нужен декодер восходящей линии связи в реальном времени, чтобы определить, когда передача по восходящей линии связи будет завершена, и **(ii)** у злоумышленника очень мало времени, чтобы начать затенение, поскольку ответ от MME обычно передается течение нескольких миллисекунд. Хотя теоретически эти проблемы не являются труднопреодолимыми, существует более простое и надежное решение, реализованное в AdaptOver, которое может быть легко выполнено на готовых SDR.

AdaptOver не ждет, пока запрос будет передан и подтвержден. Вместо этого он начинает передачу как можно скорее после получения RRC Connection Setup по нисходящей линии связи, как показано на рисунке 3. Поскольку передача должна начаться до следующего сообщения по нисходящей линии, инъекция должна происходить с задержкой не более 8 мс. Во время атаки, помимо отправки отказа от услуги, AdaptOver также инжектирует выделение и подтверждение восходящего канала, что гарантирует, что UE отправит свой запрос услуги и, таким образом, примет отказ от услуги.

Для этого мы использовали компоненты srsLTE [15] из их реализации eNodeB и адаптировали их к нашим потребностям. Мы достигли задержки менее 6 мс между получением сообщения по нисходящей линии связи и началом затенения.

Как побочный эффект, распределения восходящего канала, отправленные AdaptOver, скорее всего, отличаются от тех, что отправила базовая станция. Таким образом, базовая станция может оказаться не в состоянии декодировать запрос на обслуживание, отправленный UE, и не продолжить процедуру повторного подключения, что делает атаку еще более надежной.

3.2 Компоненты AdaptOver

В следующем разделе рассматриваются все компоненты AdaptOver и их взаимодействие. **(i)** Декодер нисходящего канала непрерывно декодирует сообщения низкого и высокого уровня, передаваемые базовой станцией. Он используется для определения временного и частотного смещения затенения, настройки кодировки и параметров сообщений, а также для инициирования начала атаки. **(ii)** После запуска атаки компонент кодирования сообщений кодирует и упаковывает сообщения атаки таким образом, чтобы UE декодировал их должным образом. **(iii-iv)** Во время атаки непрерывно подаются управляющие сообщения, которые изменяют надежные транспортные механизмы. Это делается для того, чтобы UE-жертва смог...

успешно передаст свой запрос. В противном случае он не принимает ответ злоумышленника. **(v)** Сообщения непрерывно передаются путем размещения их в канале PDSCH, заслоняя реальный нисходящий канал. Для этого используется реализация, вдохновленная SigOver, в которую мы внесли ряд существенных улучшений.

(i) Декодер нисходящей линии связи. Декодирование данных по нисходящей линии связи - задача, которую должен решать каждый UE. Мы используем компоненты с открытым исходным кодом из srsLTE [15], которые уже обеспечивают синхронизацию и получение сигнала от базовой станции. В нашей реализации мы специально прослушиваем *ответные* сообщения *PRACH* от базовой станции. Это сообщение несет временный идентификатор сети Ra- dio (RNTI) для UE, который будет идентифицировать все дальнейшие сообщения на PDSCH. Все дальнейшие сообщения на PDSCH затем декодируются независимо параллельно для каждого UE и могут служить триггером для дальнейших действий, таких как начало атаки.

(ii) Кодирование сообщений. Мы снова используем компоненты srsLTE [15] для кодирования нужных сообщений от уровня процедур NAS до физического уровня, как показано на рис. 3. Используя конфигурационные сообщения, полученные нашим декодером нисходящего канала **(i)**, мы настраиваем уровни, через которые должно пройти сообщение.

(iii) Распределение каналов связи (Uplink Allocation). В LTE базовая станция выделяет UE ресурсные слоты, когда они могут отправлять свои данные. Без такого выделения UE не сможет отправить данные, и последующий Service Reject не будет обработан. оригинальные распределения от eNodeB заслоняются злоумышленником, ему необходимо отправить и эти распределения. Мы воспользовались компонентами srsLTE и отправляем распределения восходящей линии связи в первом подкадре каждого кадра, как показано на рисунке 4. Мы используем внутренний буфер для хранения отправленных распределений, поскольку от него зависят подтверждения HARQ (которые отправляются 8 субкадров спустя).

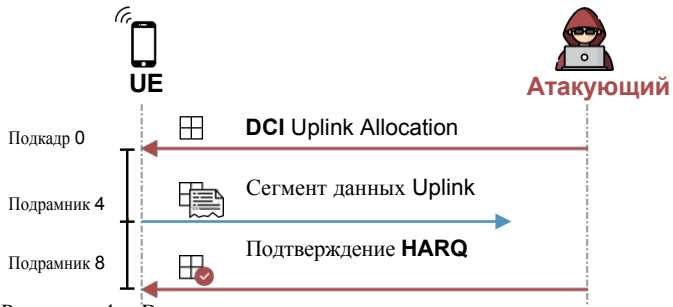


Рисунок 4. В каждом кадре в определенных подкадрах отправляется DCI Uplink Allocation и соответствующее ему HARQ Acknowledgement. UE передает данные в субфрейме 4, но они никем не принимаются, поскольку злоумышленник не прослушивает их, а исходный eNodeB, скорее всего, не отправлял такое же распределение.

(iv) Надежная транспортная модификация. UE должен полностью передать и подтвердить свой запрос, прежде чем принять ответ на него. Поскольку злоумышленник также перехватывает подтверждения для данных восходящего канала, ему необходимо включить подтверждения в перехват. В LTE квитанции передаются на двух разных уровнях: MAC и RLC.

(RLC) Уровень RLC использует подтверждения с номерами последовательности как в направлении вверх, так и вниз. Он также может разделять сообщения на несколько сегментов, которые затем передаются в нескольких субкадрах. Поэтому для подтверждения запроса присоединения необходимо отправить подтверждение для самого высокого номера сегмента всего запроса. Поскольку наша модель атакующего не предполагает возможности декодирования восходящего канала, атакующий не знает этот наибольший номер сегмента, но может ограничить его узким диапазоном. В начале каждого соединения номера последовательностей RLC начинаются с 0. Атакующий посылает подтверждения для всех номеров последовательностей в порядке возрастания из интервала $[0,\Delta]$, причем Δ - это максимальное количество сегментов, на которые может быть разбито сообщение. В наших экспериментах мы обнаружили, что для всех протестированных моделей смартфонов достаточно $\Delta \leq 8$. Как показано на рисунке 5, во время атаки мы увеличиваем номер последовательности на единицу каждые 250 мс и отправляем подтверждение RLC в каждом субфрейме вместе с сообщением NAS Service Reject.

(MAC) На уровне MAC подтверждения предыдущего транспортного блока, отправленного UE, передаются в гибридном канале индикации ARQ (PHICH) физического канала примерно через 8 субкадров после выделения восходящей линии. Как показано на рисунке 4, наш злоумышленник отправляет квитанции в каждом кадре на 8-м подкадре, после того как отправил распределение восходящей линии связи в первом подкадре. Квитанции HARQ содержат 1-битный ACK/NACK без порядкового номера и зависят от местоположения соответствующей квитанции восходящей линии связи сетке ресурсов LTE, которая ищется в буфере, созданном в (iii).

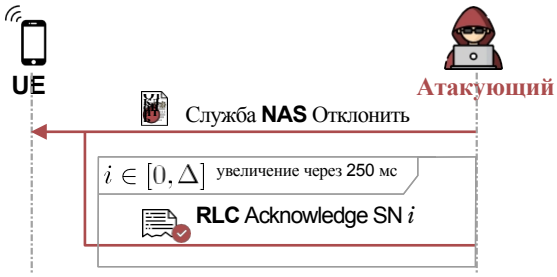


Рисунок 5: В каждом субфрейме отправляется подтверждение RLC вместе с полезной нагрузкой атаки NAS Service Reject. Наибольший порядковый номер неизвестен и угадывается путем увеличения порядкового номера на единицу каждые 250 мс или через 250 субкадров.

(v) Затенение. Перезатенение LTE требует точной синхронизации частоты и времени, что было исследовано в SigOver. AdaptOver вносит несколько ключевых улучшений. Во-первых, сообщения можно отправлять в каждом субкадре, а только в одном. Во-вторых, высокоуровневые сообщения кодируются менее чем за 1 мс до передачи на радиоустройство, что обеспечивает высокую реактивность системы. В-третьих, несколько сообщений могут передаваться по каналу PDSCH , что позволяет проводить параллельные атаки на несколько UE-жертв. Наконец, каждый канал PDSCH для UE адаптивно модулируется в соответствии с конфигурационными сообщениями, декодированными из нисходящего канала непосредственно перед началом атаки. Эти конфигурационные сообщения включают параметры физического канала, выделенные для каждого UE. Затеняя PDSCH, SigOver и AdaptOver должны также затенять PDCCH для передачи управляющих сообщений. В качестве побочного эффекта любые легитимные управляющие сообщения, предназначенные для UE, включая выделение восходящей линии связи, также затеняются.

4 Другие атаки, основанные на AdaptOver

В этом разделе мы представим различные атаки, использующие возможности AdaptOver. Мы фокусируемся на DoS-атаках, направленных доступность системы LTE с высокой стойкостью, очень низкими требованиями к энергопотреблению и обнаруживаемостью. Для достижения этой цели мы, подобно представленной в разделе 3.1 атаке Service Reject, модифицируем ответ от MME в беспроводном канале, затеняя его. За исключением специального сообщения, вводимого во время атаки, процедура и компоненты AdaptOver идентичны представленной атаке Service Reject.

Мы приводим краткое описание атаки на перехват IMSI основе AdaptOver, представленной в [10].

4.1 Прикрепить Отклонить

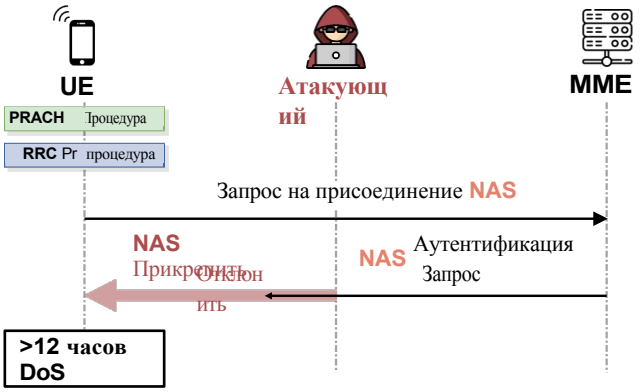


Рисунок 6: Атака с отклонением прикрепления - злоумышленник заменяет запрос аутентификации NAS на отклонение прикрепления NAS, вызывая DoS на UE более чем на 12 часов.

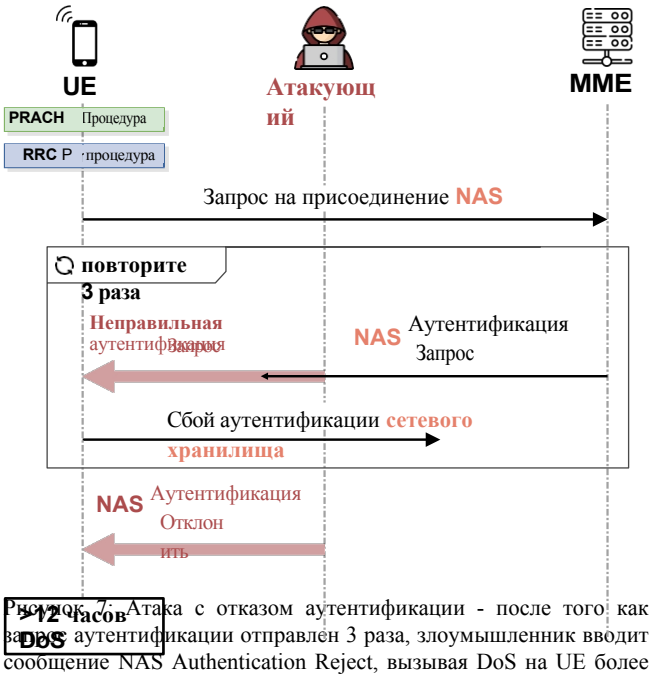


Рисунок 7: Атака с отказом аутентификации - после того как запрос аутентификации отправлен 3 раза, злоумышленник вводит сообщение NAS Authentication Reject, вызывая DoS на UE более чем на 12 часов.

Как показано на рисунке 6, UE сначала отправляет сообщение Attach Request на MME. Используя AdaptOver, злоумышленник заменяет доброжелательный ответ MME в беспроводном канале сообщением Attach Reject. Это заставляет UE считать вставленную SIM-карту недействительной, что приводит к DoS на UE. Если с ней не взаимодействовать, UE не будет переподключаться более 12 часов. Мы провели эту атаку на 20 различных моделях смартфонов от 10 разных производителей и наблюдали одинаковый результат для всех из них. Подробная процедура и результаты эксперимента приведены в разделе 5.3.

4.2 Атака на отклонение аутентификации

На рисунке 7 показан поток процедур, приводящий к отказу в аутентификации. Он вызывает сбой аутентификации MME на UE путем трехкратной отправки неверного запроса аутентификации. После этого, в соответствии с 3GPP TS 24.301 [2], сеть может завершить процедуру с помощью сообщения Authentication Reject, отправленного на UE. Мы оценили влияние сообщения об отказе в аутентификации на UE, реализовав атаку с помощью AdaptOver. Мы заметили, что почти для всех протестированных моделей смартфонов после повторных попыток не более 2 раз не было зарегистрировано ни одной повторной попытки подключения в течение более 12 часов после прекращения атаки.

Атака также может быть выполнена, если подождать, пока UE отправит (корректный) ответ аутентификации, но к этому времени UE установит корректные сеансовые ключи, что может помочь

идентифицировать наш неавторизованный Authentication Reject. Поэтому предпочтительнее атаковать процедуру, как показано на рисунке.

Ограничения. Хотя мы продемонстрировали высокую атаки Authentication Reject, практическая применимость ее остается довольно низкой, поскольку та же процедура может быть атакована на один шаг раньше с помощью атаки Attach Reject, продемонстрированной в разделе 4.1, и требует значительно большего инженерного обеспечения.

4.3 Ловец IMSI на основе AdaptOver

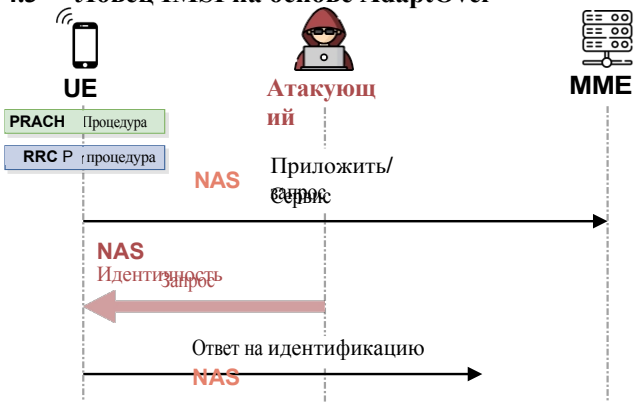


Рисунок 8: IMSI Catcher, построенный с использованием Uplink Sniffer и AdaptOver. После того как злоумышленник записывает запрос на обслуживание или присоединение, отправленный UE-жертвой, он внедряет сообщение NAS Identification Request, заставляя UE раскрыть свой IMSI в открытом виде.

Ловцы IMSI [8] позволяют злоумышленнику создать поддельную базовую станцию, к которой подключаются UE и передают свои IMSI (постоянные идентификаторы). Из-за особенностей конструкции LTE полное предотвращение IMSI-ловушек не представляется возможным. В 5G этот вектор атаки решен, однако до полного отказа от LTE атаки на понижение статуса остаются серьезной проблемой.

В работе [10] показано, что IMSI-ловушка может быть реализована путем объединения AdaptOver с пользовательским снифером восходящего канала LTE и победить существующие методы обнаружения IMSI-ловушек. Это связано с тем, что обнаружение IMSI-ловушек в основном основано на распознавании присутствия поддельных базовых станций [3, 4, 11, 14, 16, 20]. Ниже мы приводим краткую информацию об этом и иллюстрируем ее на рисунке 8.

В ходе атаки противник с помощью AdaptOver вводит сообщение Identity Request после того, как базовая станция отправила сообщение RRC Connection Setup. Неважно, отправило ли UE сообщение Attach или Service Request, в соответствии с 3GPP TS
24.301 [2], UE ответит своим IMSI в виде обычного текста. Этот ответ затем перехватывается снифером восходящей линии связи злоумышленника, как показано в [10].

5 Экспериментальная оценка

В этом разделе мы сначала представим нашу экспериментальную аппаратную установку, а затем покажем результаты оценки трех DoS-атак, реализованных в AdaptOver. Результаты по всем трем DoS-атакам мы обобщили в таблице 1.

Наконец, мы представили нашу оценку требуемой мощности и диапазона работы AdaptOver.

5.1 Настройка оборудования

Рисунок 9: Экспериментальная установка

Чтобы оценить наши атаки в реальных условиях, мы создали частную сеть LTE в защищенном пространстве, используя коммерчески доступный Amarisoft Callbox Mini в качестве базовой станции и опорной сети. Для выполнения атак мы использовали ноутбук Lenovo T490, подключенный к программно-определяемому радио Ettus Research USRP B210. Для отладки мы использовали ноутбук Lenovo X230T для декодирования нисходящего канала с помощью нашей реализации, srsUE из srsLTE [15] для работы качестве UE, и, наконец, установили QCSuper [13] на некоторые телефоны для проверки приема сообщений.

5.2 Оценка атак на отказ в обслуживании

Мы провели атаку на отказ от сервиса, описанную в разделе 3.1, в защищенной среде с помощью нашей реализации AdaptOver. Для этого мы сначала регулярно подключали смартфоны к сети и ждали, пока они перейдут в режим ожидания. Затем мы начали атаку и взаимодействовали со смартфонами, чтобы они вышли из режима ожидания и вошли в процедуру запроса сервиса, которую мы затем атаковали с помощью нашей атаки AdaptOver, отправив сообщение Service Reject.

Результаты. Только iPhone X подключился самостоятельно спустя почти 10 часов. Все остальные протестированные смартфоны не восстановили соединение в течение 12 часов. Для большинства моделей для восстановления соединения было достаточно переключить режим полета или перезагрузить устройство. Для LG Nexus 5X потребовалась повторная установка SIM-карты.

Телефон	Отказ в обслуживании			Отклонение вложений			Отклонение аутентификации		
	Продолжительность[1]	Действие[2]	GUI[3]	Продолжительность[1]	Действие[2]	GUI[3]	Продолжительность[1]	Действие[2]	GUI[3]
Pixel 2	>12h	R		> 12h	R		> 12h	R	
Pixel 3a	>12h	T		> 12h	T		> 12h	T	
Huawei P20 Pro	>12h	T		> 12h	T		> 12h	T	
Huawei P30	>12h	T	□	> 12h	T	□	>12h	T	□
Huawei P30 Lite	>12h	T		> 12h	T		> 12h	T	
Samsung Galaxy A8	>12h	T	□	> 12h	T	□	> 12h	T	
Samsung Galaxy S10	>12h	T	□	> 12h	T	□	> 12h	T	
LG Nexus 5X	>12h	S	□	> 12h	R		> 12h	R	
iPhone 6S	>12h	R	□	> 12h	R	□	> 12h	R	□
iPhone 7	>12h	T		> 12h	T		> 12h	T	
iPhone 8	>12h	T		> 12h	T		> 12h	T	
iPhone 11	>12h	T		> 12h	T		> 12h	T	
iPhone 11 Pro	>12h	T		> 12h	T		> 12h	T	
iPhone X	9.78h	T		> 12h	T		> 12h	T	
HTC U12+	>12h	T		> 12h	T		> 12h	T	
OnePlus 7T Pro	>12h	T		> 12h	T	□	> 12h	T	
Xiaomi Mi 9	>12h	T		> 12h	T		> 12h	T	
Xiaomi Mi Mix 3 5G	>12h	T		> 12h	T		> 12h	T	

[1] Продолжительность, пока UE самостоятельно не восстановит соединение

[2] Действие, которое немедленно переподключит телефон, **T**: переключение режима полета, **R**: перезагрузка телефона, **S**: повторная установка SIM-карты

[3] Присутствует ли индикатор на графическом интерфейсе

Таблица 1: Результаты DoS-атаки, осуществленной с помощью AdaptOver

карту, чтобы восстановить соединение. Кроме того, некоторые смартфоны выводили на сообщение, указывающее на проблему с SIM-картой. Подборка таких сообщений показана на рисунке 10; аналогичные сообщения отображались на Huawei P30, Samsung Galaxy S10 и LG Nexus 5X.

5.3 Прикрепить Отклонить Оценка атаки

Используя схему из раздела 3, мы реализовали атаку Attach Reject с помощью AdaptOver. Сначала мы перевели UE в режим полета, после чего начали атаку, а затем выключили режим полета для каждого UE, запустив процедуру присоединения и, соответственно, атаку. Через несколько минут мы отключили атаку. Используя журналы Amarisoft Callbox Mini, мы убедились, что с момента первого отклонения прикрепления от UE больше не было попыток подключения.

Результаты. Ни один из телефонов не пытался восстановить соединение с сетью в течение 12 часов. В таблице 1 приведены результаты для каждого протестированного смартфона.

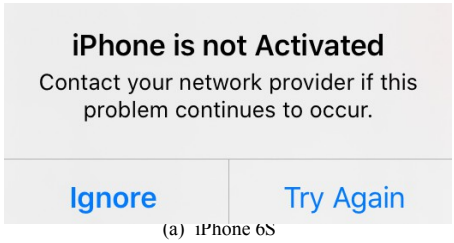
5.4 Аутентификация Отклонение атаки Оценка

Чтобы оценить эффект нашей атаки Authentication Reject, мы реализовали ее в AdaptOver. Сначала мы перевели UE в режим полета, после чего начали атаку, а затем выключили режим полета для каждого UE, запустив процедуру прикрепления и, соответственно, нашу атаку. После того как каждый телефон подвергся атаке, атакующий был отключен, а телефоны оставлены в покое.

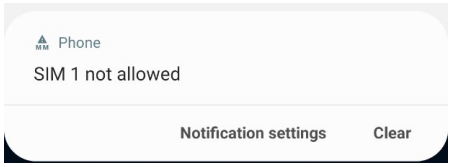
Результаты. Все протестированные телефоны не восстановили связь в течение 12 часов. В таблице 1 приведены результаты, включая необходимые меры по исправлению ситуации. Для Huawei P30 потребовалось дважды отправить сообщение Authentication Reject, чтобы атака прошла успешно, так как на первый Authentication Reject он Authentication Failure.

5.5 Требования к питанию

Чтобы оценить мощность, необходимую для работы атаки, мы выполнили ее в экранированной среде, при этом at-такер и eNodeB находились на расстоянии ровно 1 м от



(a) iPhone 6S



(b) Samsung Galaxy A8

Рисунок 10: Индикаторы графического интерфейса смартфонов, подвергшихся атаке Service Reject

UE. Затем мы изменяли выходное усиление атакующего и измеряли, сколько затененных сообщений было правильно декодировано от атакующего, а сколько - от легитимного eNodeB. Сообщения, которые вообще не могли быть декодированы, отбрасывались. Затем мы подключили выход eNodeB и атакующего к осциллографу Keysight и измерили разницу в мощности в дБ. Хотя мы обнаружили, что относительное преимущество по мощности (J/S) в 1,8 дБ достаточно для достижения 100-процентного успеха атаки, что является улучшением по сравнению с [21], это может быть связано с различиями в экспериментальных установках. В таблице 2 приведены результаты измерений J/S и соответствующий коэффициент успешности. Приведены как стандартное отклонение ($\sigma_{J/S}$), так и среднее значение ($\mu_{J/S}$).

мкДж/с	*σJ/S*	Показатель успешности
-2,049 дБ	0.627	0%
-1,1202 дБ	0.675	1.325%
-0,117 дБ	0.665	30.625%
0,639 дБ	0.619	96.825%
1,870 дБ	0.641	100%
2,559 дБ	0.733	100%

Таблица 2: Сводные данные по успешности затенения и результативности J/S

Результирующая дальность атаки. Исходя из числа 3 дБ, мы можем определить максимальное расстояние $d_{Attacker}$ атакующей стороны до UE по отношению к расстоянию от UE до базовой станции $d_{\leftrightarrow}$ и выходной мощности атакующей стороны $P_{Attacker}$ и базовой станции P_{eNodeB}. Предполагая модель потерь на пути в свободном пространстве, получаем:

$$d_{Attacker} \leq d_{\leftrightarrow} - 10^{\frac{P_{Attacker} - P_{eNodeB} - 3dB}{20}} \quad (1)$$

В связи с нормативными требованиями тестирование вне экранированной среды не представляется возможным. Если мы консервативно предположим, что мощность передачи, включая любые усиления антенн, составляет 40 дБм eNodeB и 20 дБм для атакующего, мы сможем получить представление о том, насколько велик радиус атаки, как показано в таблице 3.

$d_{\leftrightarrow}$	Максимум **нисходящей линии связи** $d_{Атакующий}$ 100 м
	7.1m
500m	35.4m
1 км	70.8m

Таблица 3: Расчетная дальность атаки для мощности передачи злоумышленника 20 дБ. Базовая станция излучает свой нисходящий сигнал с мощностью 40 дБ. $d_{\leftrightarrow}$ обозначает расстояние между UE и базовой станцией. max $d_{Attacker}$ - расстояние между атакующим и жертвой UE.

6 Меры противодействия

В следующем разделе мы рассмотрим возможные меры противодействия представленным DoS-атакам AdaptOver и способы их реализации.

6.1 Механизм повтора

Гарантировать доступность в LTE , так как канал без проводов всегда может быть достаточно нарушен, чтобы связь стала невозможной. Однако для этого требуется высокая выходная мощность и постоянная передача атакующего, в то время как наши атаки вызывали постоянный отказ в обслуживании при сравнительно низкой мощности. Однако наши атаки были успешными только потому, что смартфоны не пытались восстановить соединение даже спустя несколько часов.

Таким образом, наша рекомендация разработчикам baseband заключается в том, чтобы чаще повторять попытки установления соединения, независимо от причины неудачи. Это заставит злоумышленника постоянно атаковать свою жертву, что потребует больших времени и ресурсов. В идеале затраты и эффективность злоумышленника, применяющего AdaptOver, должны быть схожи с обычными шумовыми атаками. Недостатком такого подхода является то, что повторные запросы UE, не имеющих законных оснований для подключения сети, будут увеличивать нагрузку на опорную сеть своими постоянными попытками. Чтобы сбалансировать эти противоположные потребности, мы предлагаем реализовать механизм повторных запросов в виде экспоненциального отката, распределяя повторные запросы так, чтобы избежать перегрузки основной сети.

6.2 Обнаружение

Обнаружение атак AdaptOver на нижних уровнях не представляет сложности, поскольку мы постоянно заслоняем нисходящий канал идентичной информацией, чтобы исключить любой легитимный нисходящий трафик, представляющий собой легко идентифицируемую характеристику. На более высоком уровне отделить легитимный отказ от фиктивного можно, определив отсутствие кода аутентификации сообщения. В работе [5] Эчеверрия и др. попытались идентифицировать атаку отказа в подключении, обслуживании или аутентификации, исходящую от поддельной базовой станции, но, кроме наличия сообщения об отказе, они не смогли определить никаких характеристик, которые бы четко отделяли атаку от легитимного отказа.

6.3 Защита целостности

Когда требуется целостность сообщений между участниками, к сообщению добавляется код аутентификации сообщения (MAC), доказывающий получателю, что оно не было подделано. Ни одно из отправленных нами сообщений не содержало такого валидного MAC, поскольку наша модель злоумышленника исключала знание злоумышленником общего ключа между UE и оператором. Однако наши атаки все равно увенчались успехом. Техническая спецификация 3GPP [2] требует, чтобы сообщения без защиты целостности не принимались UE после установления аутентифицированной сессии. Очевидно, что это требование было реализовано неправильно, но его можно легко исправить с помощью меры повторной попытки, предложенной в разделе 6.1.

7 Связанные работы

Обнаружение атак на поддельные базовые станции. Атаки на поддельные базовые станции требуют значительно большей мощности, чем атаки с затенением, как показано в SigOver [21]. Благодаря высокой выходной мощности и требованию постоянно транслировать свою конфигурацию, атаки на поддельные базовые станции очень легко обнаружить, что было исследовано в многочисленных работах [3, 4, 11, 14, 16, 20]. В этих работах авторы обнаруживают поддельные базовые станции по их необычной конфигурации вещания, местоположению или другим признакам. В работе [5] авторы не используют индикаторы нижнего уровня для обнаружения присутствия поддельной базовой станции, а полагаются на трассировку протокола взаимодействия с поддельной базовой станцией.

Влияние атак на поддельные базовые станции. Несмотря на высокую защищаемость, атаки на поддельные базовые станции имеют высокую степень воздействия и, как было показано, могут быть полезны как для DoS-, так и для MITM-атак. В работах [17, 18] авторам удалось манипулировать обычным пользовательским трафиком, используя поддельную базовую станцию в качестве MITM. В [9] авторы исследовали реализацию нескольких реальных MME, обнаружив множество дефектов реализации операторов, приводящих к DoS и SMS-фишингу. В данной работе мы сосредоточились на атаках типа "отказ в обслуживании", поддерживаемых стандартом 3GPP, и, соответственно, использовали атаки типа "отказ в обслуживании" NAS. Принцип

Эти атаки на аутентификацию, присоединение и отказ от услуг NAS были рассмотрены в [7, 8, 19], причем все они использовали поддельную базовую станцию.

Затенение нисходящего канала. Затенение сигнала в LTE впервые было рассмотрено в SigOver [21]. В SigOver авторы реализовали DoS-атаку с использованием IMSI-пейджинга и затенения SIB. Далее они реализовали шторм сигнализации, падение сети и крупномасштабное отслеживание атак на LTE. Наша работа значительно дополняет и улучшает их работу, позволяя осуществлять интерактивные и адаптивные атаки на процедуры более высокого уровня, что приводит к более стойким DoS-атакам. Эта работа была использована в [10] для создания очень секретного устройства извлечения IMSI, позволяющего осуществлять постоянное отслеживание в течение неограниченно долгого периода времени.

8 Заключение

В этой статье мы разработали и реализовали новый метод атаки на LTE под названием AdaptOver. Мы реализовали три варианта DoS-атак, способных лишить LTE-сервиса все протестированные современные смартфоны на нескольких базовых станциях в течение более чем 12 часов. Мы предложили простые и эффективные средства защиты от DoS-атак, которые могут реализованы производителями базовых станций без каких-либо изменений в стандарте.

Благодарности

Мы благодарим авторов SigOver за предоставленный код.

Ссылки

[1] 3GPP. 3GPP TS 36.822, сентябрь 2012 г. Последнее обращение: 21.09.2020.

[2] 3GPP. 3GPP TS 24.301, июль 2020. Последнее обращение: 21.09.2020.

[3] CellularPrivacy. CellularPrivacy/Android-IMSI-Catcher-. Детектор, декабрь 2020 г. Последнее обращение: 07.12.2020.

[4] 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 компьютерной безопасности - ACSAC '14*, стр. 246- 255, Новый Орлеан, Луизиана, 2014. ACM Press.

[5] 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.

[6] Джанлука Фоддис, Розарио Г. Гарроппо, Стефано Джордано, Грегорио Прочисси, Симоне Рома и Симоне Топацци. Анализ трафика LTE для компромисса между нагрузкой на сигнализацию и энергопотреблением в мобильных сетях. *Международная конференция по связи (ICC), 2015*, стр. 6005-6010, 2015.

[7] Саид Рафиул Хуссейн, Омар Чоудхури, Шагуфта Мехназ и Элиза Бертино. LTEInspector: Системный подход адверсионному тестированию 4G LTE. В *материалах 2018 Network and Distributed System Security Symposium*, San Diego, CA, 2018. Internet Society. Last accessed: 30.04.2020.

[8] Роджер Пикерас Жовер. Безопасность LTE, эксплойты протоколов и эксперименты по отслеживанию местоположения с помощью недорогого программного радио. *arXiv:1607.05171 [cs]*, июль 2016. arXiv: 1607.05171, Last accessed: 30.04.2020.

[9] Хонгиль Ким, Джихо Ли, Юнкю Ли и Йонгдэ Ким. Прикосновение к неприкасаемым: Динамический анализ безопасности плоскости управления LTE. *Симпозиум IEEE по безопасности и конфиденциальности (SP), 2019*, стр. 1153-1168, май 2019.

[10] Мартин Котуляк, Симон Эрни, Патрик Леу, Марк Рёшлин и Срджан Капкун. LTrack: Скрытное отслеживание мобильных телефонов в LTE. *arXiv*, июнь 2021.

[11] 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 масштабе дикой природы. Январь 2017 г.

[12] Марк Лихтман, Роджер Пикерас Джовер, Мина Лабиб, Рагхунан-дан Рао, Вук Мароевич и Джеффри Х. Рид. Помехи, спуфинг и сниффинг в сетях LTE/LTE-A: оценка угроз и их устранение. *Журнал IEEE Communications*, 54(4):54-61, апрель 2016 г. Название конференции: IEEE Communications Magazine.

[13] Марин Мулинье и Бенуа Мишо. P1sec/QCSuper, Novem- ber 2020. Последнее обращение: 30.11.2020.

[14] Праджвол Кумар Накарми и Карл Норрман. Обнаружение ложных базовых станций в мобильных сетях, июнь 2018 г. Последнее обращение: 07.12.2020.

[15] Андре Пушманн, Исмаэль Гомес, Педро Альварес, Хавьер Артеага, Франциско Пайсана, Пол Саттон и Джастин Таллон. srsLTE/srsLTE, апрель 2020 г. Последнее обращение: 28.04.2020.

[16] Купер Квинтин. *Обнаружение поддельных базовых станций 4G в реальном времени*. 2020. Опубликовано: DEF CON, Последнее обращение: 07.12.2020.

[17] Дэвид Руппрехт, Катарина Колс, Торстен Хольц и Кристина Поппер. Взлом LTE на втором уровне. *Симпозиум IEEE по безопасности и конфиденциальности (SP)*, *2019*, стр. 1121-1136, Сан-Франциско, Калифорния, США, май 2019. IEEE. Last accessed: 30.04.2020.

[18] Дэвид Руппрехт, Катарина Колс, Торстен Хольц и Кристина Пёппер. IMP4GT: атаки IMPersonation Attacks in 4G NeTworks. На *симпозиуме ISOC по безопасности сетей и распределенных систем (NDSS)*. ISOC, февраль 2020 г.

[19] Альтаф Шайк, Равишанкар Боргаонкар, Н. Асокан, Валттери Ниеми и Жан-Пьер Сейферт. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. *arXiv:1510.07563 [cs]*, August 2017. arXiv: 1510.07563, Last accessed: 30.04.2020.

[20] Тхань Ван До, Хай Тхань Нгуен, Николов Момчил и Ван Тхуан До. Обнаружение IMSI-ловушек с помощью мягких вычислений. Майкл В. Берри, Азлина Мохамед и Би Вах Яп, редакторы, *Мягкие вычисления в науке о данных*, том 545, страницы 129-140. Springer Singapore, Singapore, 2015. Название серии: Communications in Computer and Information Science.

[21] Ходжун Ян, Сангвук Бэ, Минчеол Сон, Хонгиль Ким, Сонг Мин Ким и Йонгдэ Ким. Скрытие в обычном сигнале: атака на LTE с затенением физического сигнала. В *материалах 28-й конференции USENIX по безопасности*, SEC'19, стр. 55-72, США, август 2019 г. USENIX Associa- tion. Last accessed: 16.10.2020.