Вопросы обеспечения безопасности абонентов в сетях радиодоступа пятого поколения

В. С. Бельский, А. В. Дрынкин, С. А. Давыдов

Аннотация—**Вопросы обеспечения конфиденциальности абонентов в системах мобильной телефонной связи в настоящее время представляют большой интерес из-за ожидаемого в будущем взрывного роста новых услуг связи (виртуальная реальность, межмашинное взаимодействие [Machine-Type Communications – MTC], взаимодействие средств транспорта [Vehicle-to-Everything – V2X], интернет вещей [Internet-of-Things – IoT] и т. д.), предоставляемых сетями 5G. В обзоре рассматриваются вопросы безопасности в системах связи 5G. В качестве основного релиза спецификаций 5G выбран релиз 15 (Release 15), также добавлена некоторая информация из Release 16 до стадии Stage 3 включительно. В рамках исследования рассматривается только беспроводная компонента (участок между базовой станцией провайдера и мобильным устройством) сетей 5G. Несмотря на то, что сети 5G предлагают дополнительные средства обеспечения безопасности по отношению к предыдущим поколениям связи, представленный обзор демонстрирует, что в указанной области остаются существенные проблемы. В обзоре представлен анализ уязвимостей, которые существовали в предыдущих поколениях мобильной телефонии, приведен обзор предложенных в стандарте 5G мер по повышению безопасности, выделены угрозы, наследованные 5G Release 15 от предыдущих поколений. Для полноты исследований приведены некоторые новые виды атак, которые появились после публикации 5G Release 15, а также предложены направления исследований для устранения выявленных пробелов в обеспечении конфиденциальности сетей 5G.**

Ключевые слова—**5G, анонимность, GSM, LTE, мобильные сети, конфиденциальность, приватность, UMTS**

I. Введение

Персональная информация абонентов мобильной телефонной связи является привлекательной целью для компаний, работающих в сфере онлайн-рекламы и смежных отраслях. Разоблачения Эдварда Сноудена продемонстрировали, что помимо коммерческих фирм, личную информацию абонентов в больших объемах собирают также национальные спецслужбы [1]. Существует опасность, что персональная информация может быть использована как для осуществления различного рода атак, так и для достижения личных целей. В связи с этим, конфиденциальность становится сегодня главным критерием для пользователей при выборе и использовании услуг мобильной телефонной связи.

Статья получена ? ?? 2021

Владимир Сергеевич Бельский, Лаборатория Криптографии АО НПК «Криптонит», (email: v.belsky@kryptonite.ru).

Антон Викторович Дрынкин, Лаборатория Криптографии АО НПК «Криптонит», (email: a.drynkin@kryptonite.ru).

Степан Андреевич Давыдов, Лаборатория Криптографии АО НПК «Криптонит», (email: s.davydov@kryptonite.ru).

3GPP [3rd Generation Partnership Project], международный орган по стандартизации мобильной телефонной связи, в конце 2017 года опубликовал первые документы, относящиеся к 5G. Разработка систем связи 5G планировалась в два этапа: 5G Phase 1 (официально называется Release 15) и 5G Phase 2 (официально – Release 16). Документация 5G [2] для разработки различных требований по вопросам безопасности и конфиденциальности зачастую ссылается на соответствующие технологии предыдущих поколений мобильных сетей. В частности, Release 15 ссылается на рекомендации 3GPP TS 33.102 [3] в отношении перечисленных ниже требований:

- **Конфиденциальность идентификатора пользователя:** постоянный идентификатор пользователя, должен быть защищен от перехвата/подслушивания в радиоэфире.
- **Конфиденциальность местоположения пользователя:** присутствие или прибытие пользователя в определенную местность не может быть определено путем прослушивания радиоэфира.
- **Невозможность сопоставления проведенных операций:** прослушивая радиоэфир злоумышленник не должен иметь возможность узнать, были ли различные услуги предоставлены одному и тому же абоненту. Последнее условие иногда называют криптографическим термином *неотслеживаемость*, однако, авторы статьи не будут использовать указанный термин.

Стоит отметить, что при анализе угроз безопасности в 3GPP рассматриваются модели как пассивных, так и активных злоумышленников. Хорошим примером здесь служит исследование 3GPP TR 33.899 [4], которое было проведено для сбора, анализа и дальнейшего изучения потенциальных угроз безопасности и требований для систем 5G и содержит явные указания на активных злоумышленников.

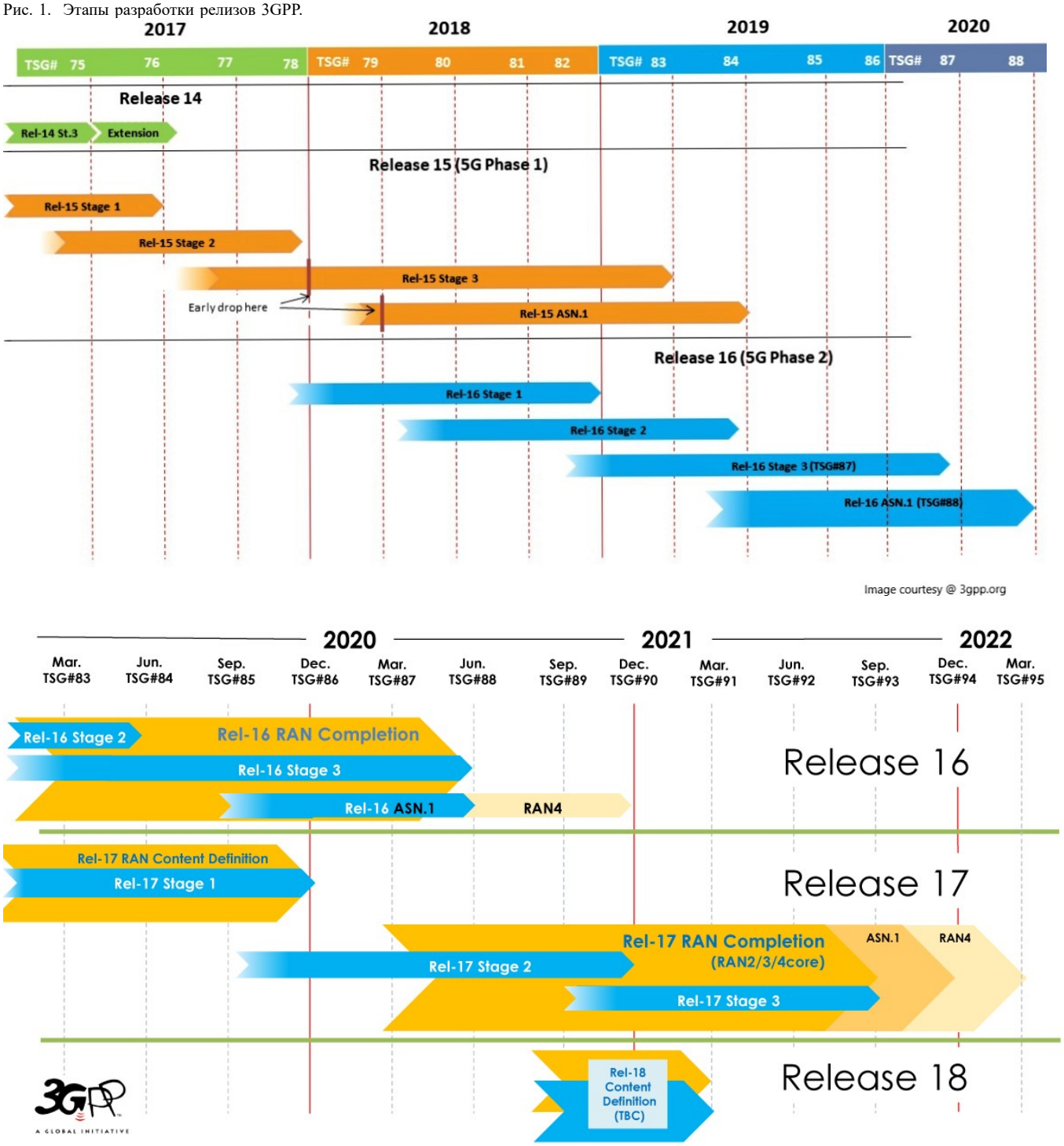
В представленном обзоре рассматриваются вопросы конфиденциальности абонентов в сетях радиодоступа 5G. На рисунке 1 представлена хронология разработки стандартов сети 5G.

Хороший обзор по рассматриваемой тематике вплоть до 5G Release 15 представлен в [5]. Авторы во многом опирались на указанную работу. Также в обзор были добавлены новые документы 3GPP, в частности, документы по Release 16 и постквантовой криптографии.

Объем исследования, проведенного в нашей статье, определяется тремя составляющими:

- **Исследование вопросов обеспечения конфиденциальности беспроводной подсистемы 5G.** Это

Рис. 1. Этапы разработки релизов 3GPP.



связано, прежде всего, с тем, что этот канал вследствие своей доступности легко может быть использован любым злоумышленником и в результате является наиболее уязвимым. Отметим, что в проводном канале также существуют уязвимости, но их рассмотрение не входит в представленный нами обзор.

- **Исследование вопросов конфиденциальности абонента, которые входят в компетенцию 3GPP.** В наши дни смартфоны превратились в мощные многофункциональные устройства, возможности которых выходят за рамки осуществления исключительно телекоммуникаций. Существует множество других источников угроз безопасности пользователей, таких как Wi-Fi [6], Bluetooth [7] и т. д., которые не регулируются 3GPP. В представленном обзоре угрозы конфиденциальности со стороны других источников не рассматриваются.
- **Release 16 рассматривается в обзоре лишь до стадии Stage 3,** поскольку, на момент написания обзора, работа 3GPP над ним не завершена. Представляется целесообразным расширить данное ис-

следование после завершения работ над Release 16, чтобы учесть предложенные в нем улучшения в области обеспечения конфиденциальности (если таковые будут).

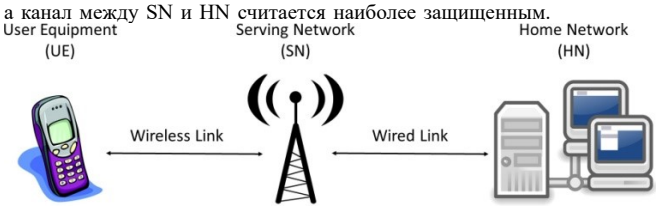
Дальнейшая часть документа организована следующим образом: раздел II содержит необходимую справочную информацию. В разделе III рассматриваются угрозы конфиденциальности, существовавшие до 5G, а также соответствующие им улучшения, предусмотренные в 5G Release 15. В разделе IV обсуждаются нерешенные до сих пор проблемы конфиденциальности в сетях 5G, некоторые предложения из Release 16 и направления будущих исследований. Раздел V посвящен обзору опубликованных работ по рассматриваемой теме. В заключении VI приведены некоторые рекомендации.

II. Механизмы аутентификации в мобильных сетях

Рассмотрим инфраструктуру мобильной связи и ее механизмы безопасности.

A. Архитектура системы

Рис. 2. Архитектура 5G. Канал между UE и SN наименее защищен, а канал между SN и HN считается наиболее защищенным.



Архитектуру мобильной телефонии составляют три основных объекта (см. рисунок 2): домашняя сеть [Home Network, HN], обслуживающие/гостевые сети [Serving Network, SN] и пользовательское оборудование [User Equipment, UE]. Чаще всего в качестве оборудования пользователя используются мобильные устройства [Mobile Equipment – ME], например, телефон, смартфон или планшет. Каждое такое устройство содержит универсальную интегрированную карту [Universal Integrated Circuit Card, UICC], которую обычно называют SIM-картой. Домашняя сеть выполняет первоначальную регистрацию абонентов. Она хранит учетные данные абонентов и отвечает за их аутентификацию.

Зачастую оборудованию пользователя приходится работать в областях, где их домашние сети не имеют базовых станций. Другие поставщики услуг (операторы сотовой связи), которые имеют соглашение с домашней сетью абонента, предоставляют ему услуги связи. В таких случаях говорят, что абоненты находятся в роуминге, а поставщики услуг роуминга называются гостевыми сетями. Согласно стандарту 3GPP [2], гостевые и домашние сети дополнительно делятся на логические подобъекты, однако, вопросы безопасности и конфиденциальности, изучаемые в данном обзоре, не требуют более глубокого уровня детализации.

SIM-карта определяет все условия предоставления связи абоненту со стороны его домашней сети. Во время регистрации абонента домашняя сеть сохраняет его долгосрочный идентификатор MSISDN [Mobile Station International Subscriber Directory Number] (телефонный номер) и другие данные, относящиеся к абоненту, включая 128-битный секретный ключ K и 48-битный постоянно увеличивающийся счетчик SQN [Sequence Number]. Счетчик SQN используется для предотвращения повторного воспроизведения сообщений (см. п. II-E). Хотя состояние счетчика должно быть синхронизировано между пользователем и домашней сетью, иногда возможен сбой синхронизации вследствие потери сообщений в беспроводном канале, и значения могут незначительно отличаться. Эти параметры абонента также хранятся в базе данных домашней сети и образуют основу контекста безопасности между абонентом и домашней сетью, а, в случае роуминга, между абонентом и гостевой сетью. Гостевые сети предоставляют абоненту услуги после установления между ними безопасного канала при посредничестве домашней сети.

B. Типы идентификаторов и терминология

В системах мобильной телефонной связи каждому абоненту присваивается уникальный долгосрочный идентификатор, в предыдущих поколениях называемый IMSI [International Mobile Subscriber Identity – международный идентификатор мобильного абонента], а начиная с 5G – SUPI [Subscription Permanent Identifier – постоянный идентификатор абонента]. Согласно рекомендации 3GPP TS 23.501 [8], SUPI представляет собой набор из 15 десятичных цифр, первые три из которых – мобильный код страны [MCC - Mobile Country Code], следующие две или три – код мобильной сети [MNC - Mobile Network Code], который идентифицирует оператора и определяется национальными стандартами. Остальные цифры, которых девять или десять, обозначают идентификационный номер мобильного абонента [MSIN — Mobile Subscriber Identification Number] и определяют отдельного пользователя этого конкретного оператора. Каждая десятичная цифра SUPI представляется в двоичном виде с использованием двоично-десятичного кода [TBCD, Telephony Binary Coded Decimal] [9].

Аутентификация между пользователем и провайдером основана на использовании общего симметричного ключа (п. II-E), поэтому она возможна только после первоначальной регистрации пользователя. Если передавать значения IMSI / SUPI по радиоканалу в незашифрованном виде, абонент может быть по ним идентифицирован и отслежен злоумышленником. Чтобы избежать этой угрозы конфиденциальности, абонентам назначаются временные идентификаторы – GUTI [Globally Unique Temporary User Equipment Identity – глобальный временный уникальный идентификатор оборудования пользователя].

IMEI [International Mobile Equipment Identity – международный идентификатор мобильного оборудования], который однозначно идентифицирует мобильное устройство, представляет собой строку из 15 цифр. Передача IMEI по радио в открытом виде может поставить конфиденциальность пользователя под угрозу. Поэтому спецификации 3GPP запрещает мобильным устройствам передавать IMEI до тех пор, пока не будет установлен защищенный канал с сетью [10].

C. Постулаты модели безопасности

- В соответствии с 3GPP TS 33.501 (подпункт 5.9.3) [2], канал между гостевыми сетями и домашней се-

тью должен обеспечивать конфиденциальность, целостность, аутентификацию и предотвращение повторного воспроизведения сообщений. Радиоканал между мобильным устройством и гостевой сетью подвержен прослушиванию, перехвату и внедрению сообщений со стороны злоумышленника.

- Мобильное устройство и его домашняя сеть являются полностью доверенными объектами. Предполагается, что совместно используемые секретные данные, хранящиеся этими двумя сторонами, защищены от третьих лиц. В частности, SIM-карта считается защищенным от несанкционированного доступа, и ее содержимое не может быть прочитано злоумышленником. Гостевые сети являются полудоверенными в том смысле, что в процессе установления защищенного канала им предоставляется только SUPI (секретный ключ и текущее значение счетчика не раскрываются). Передача SUPI необходима для правильной тарификации/биллинга.

D. Инициализация процедуры аутентификации

Когда мобильное устройство не участвует в непосредственной передаче данных, оно находится в состояние ожидания [*idle state*]. Если устройству необходимо доставить некоторую сетевую услугу, такую как вызов или SMS, первоначально сеть проверяет состояние телефона: отправляет поисковое [пейджинг, *paging*] сообщение и дожидается соответствующего ответа. Процедура поискового вызова работает, поскольку даже в состоянии ожидания мобильное устройство через определенные интервалы времени, зависящие от его настроек, отслеживает наличие пейджинговых сообщений, декодирует их и, если обнаруживает в них свой идентификатор, то выбирает доступный радиоканал и запрашивает у соответствующей базовой станции установление соединения для обмена дальнейшими сообщениями.

Как будет показано в п. II-E, безопасный канал между абонентом и провайдером устанавливается с помощью протоколов «запрос-ответ», основанных на общем секретном ключе K. До начала выполнения протоколов сети необходимо идентифицировать абонента, с которым устанавливается соединение. Рекомендация 3GPP TS 33.501 (подпункт 6.1.2) [2] подробно определяет процедуры идентификации абонента и выбора метода последующей аутентификации.

Гостевая сеть может инициировать аутентификацию с мобильным устройством в ходе любой процедуры, предусматривающей такое соединение. Мобильное устройство в качестве ответа на запрос идентификатора *(identifier request)* отправляет либо 5G-GUTI, либо SUCI [Subscription Concealed Identifier – скрытый идентификатор абонента, зашифрованная копия SUPI (см. п. III-A)]. В случае 5G-GUTI, гостевая сеть извлекает соответствующий SUPI из своей базы данных и направляет его вместе со своим глобальным идентификатором SN_{name} [Serving Network Name – имя обслуживающей (гостевой) сети] в домашнюю сеть *(authenticate request)*. В противном случае вместо SUPI отправляется SUCI. При получении *authenticate request* домашняя сеть проверяет правомочность использования данного имени гостевой сети, сравнивая его с имеющимся именем. Если гостевая сеть не авторизована для использования полученного имени, домашняя сеть отвечает сообщением «обслуживающая сеть не авторизована». Если в *authenticate request* указан SUCI, домашняя сеть расшифровывает его (получая SUPI) и выбирает метод аутентификации в соответствии со своей политикой безопасности.

E. Метод аутентификации 5G-AKA

Безопасность связи между абонентом и провайдером требует взаимной аутентификации и согласования криптографических ключей. В системах 5G для этой цели предусмотрены протоколы EAP-AKA и 5G-AKA, оба являются протоколами типа AKA [Authentication and Key Agreement – аутентификации и согласования ключей]. EAP-AKA и 5G-AKA различаются лишь способом получения ключей. Рассмотрим их работу на примере 5G-AKA. Его детали определены в рекомендации 3GPP TS 33.501 (подпункт 6.1.3.2) [2]. Безопасность 5G-AKA основана на общем симметричном ключе K.

Для запуска процедуры аутентификации мобильное устройство отправляет в гостевую сеть либо 5G-GUTI в сообщении *registration request*, либо SUCI в качестве ответа на *identifier request* (см. п. II-D).

Таблица I
Описание параметров протокола 5G-AKA.

Параметр	Значение / описание
R	Случайное значение [Random Challenge]
AK	Ключ анонимности [Anonymity Key]
CK	Ключ конфиденциальности [Confidentiality Key]
IK	Ключ целостности [Integrity Key]
RES	Ответ [Response]
MAC	Код контроля целостности сообщения [Message Authentication Code]
CONC	Скрытый счетчик [Concealed Sequence Number]
AUTN	Токен аутентификации [Authentication Token]
AUTS	Токен повторной синхронизации [Resynchronization Token]
XRES	Ожидаемый отклик/ответ [Expected Response]
HRES/HXRES	Значение хэш-функции от RES/XRES
KAUSF	Промежуточный ключ [Intermediate Key]
KSEAF	Мастер-ключ [якорный ключ, Anchor Key]

Схема протокола 5G-AKA приведена на рисунке 4, соответствующие сокращения раскрыты в таблице I. На схеме R – случайное, выбранное равновероятно 128-битное число, а $f_1, ..., f_5, f_1^*$ и f_5^* – функции на основе алгоритмов симметричного шифрования. f_1, f_2 и f_1^* действуют как функции аутентификации сообщений, а f_3, f_4, f_5 и f_5^* используются в качестве функций выработки ключей. Префикс X в обозначениях на схеме протокола означает, что полученное значение подлежит проверке (сравнению с аналогичным значением, полученным другим участником протокола).

Алгоритм состоит из следующих шагов:

1) Домашняя сеть (HN) генерирует случайное 128-битное число R и, с использованием текущего значения счетчика SQN_{HN} и постоянного ключа мобильного устройства K, вычисляет ключи AK, CK, IK и аутентификационные метки MAC и $XRES$.

2) Далее, с использованием функции KDF [Key Derivation Function – функция выработки ключа, см.

Рис. 3. Инициализация процедуры аутентификации.

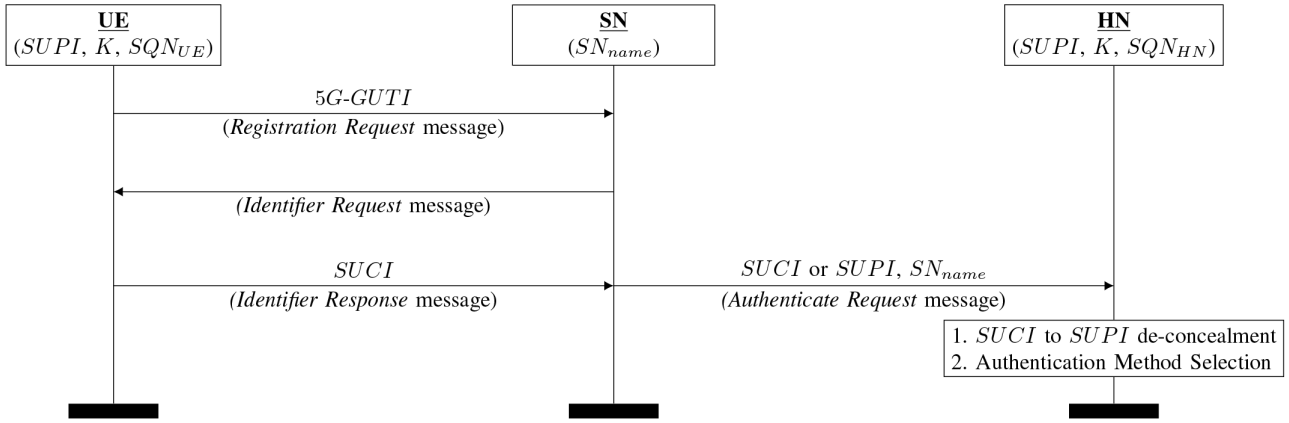
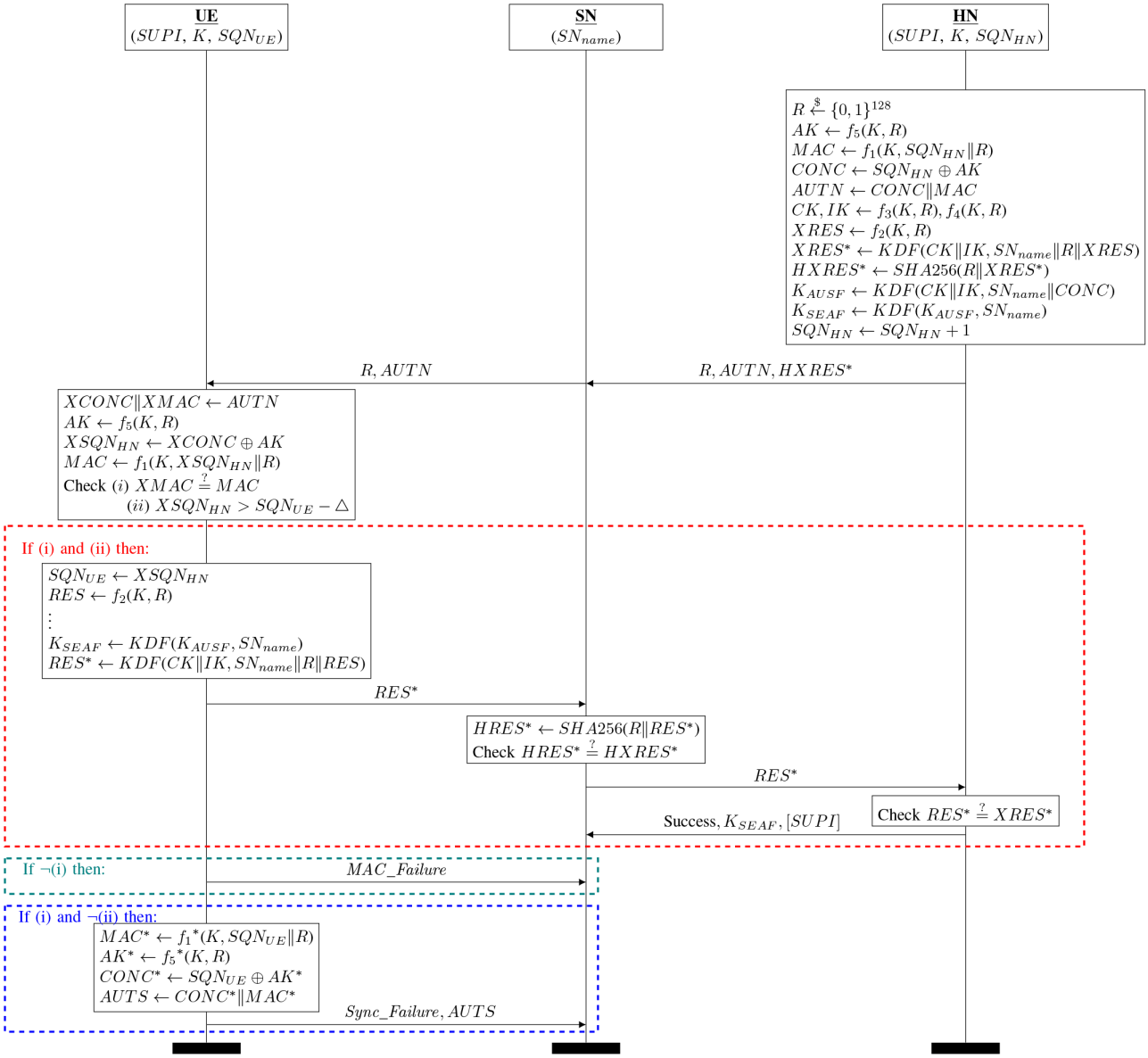


Рис. 4. Протокол 5G-AKA и связанные механизмы отказа.



3GPP TS 33.220 [11] вычисляются ключи K_{AUSF} и K_{SEAF} и, с использованием хэш-функции $SHA256$, вычисляется проверочная метка $HXRES^*$.

3) Домашняя сеть передает гостевой сети (SN):

- сгенерированное число R;
- блок для проведения аутентификации мобильного устройства $AUTN$, содержащий счетчик SQN_{HN}, скрытый XOR-суммой с ключом AK и метку аутентификации MAC ;
- проверочную метку $HXRES^*$.

4) Гостевая сеть передает полученные R и $AUTN$ мобильному устройству и сохраняет у себя проверочную метку $HXRES^*$ и значение R.

5) Мобильное устройство, получив значения R и $AUTN$, по соответствующим размерам выделяет значения $XCONC$ и $XMAC$ и вычисляет ключ AK.

6) Мобильное устройство вычисляет $XSQN_{HN}$ и значение MAC, после чего выполняет проверку на совпадение $XMAC = MAC$ (i). В случае несовпадения (вариант ¬(i) на схеме) мобильное устройство отправляет в гостевую сеть сообщение об ошибке *MAC Failure* и завершает алгоритм.

7) В случае успешной проверки (i) мобильное устройство сравнивает текущее значение своего счетчика SQN_{UE} с вычисленным значением $XSQN_{HN}$ (ii). Значение $XSQN_{HN}$ принимается мобильным устройством, если выполняются два условия:

- $XSQN_{HN} > SQN_{UE} - \Delta$;
- $XSQN_{HN}$ не было получено мобильным устройством ранее.

Последнее условие проверки счетчика защищает протокол от повторного воспроизведения сообщений.

В случае сбоя (вариант (i) и ¬(ii) на схеме) следует ответ *Sync Failure* вместе с токеном повторной синхронизации *AUTS*. С использованием токена *AUTS* домашняя сеть сможет восстановить значение счетчика SQN_{UE} и начать текущий протокол заново.

8) В случае успешной проверки условий (i) и (ii) мобильное устройство повторяет последовательность шагов домашней сети по вычислению всех ключей и проверочной метки RES^* и отправляет такую метку в гостевую сеть.

9) Гостевая сеть вычисляет значение хэш-функции $SHA256$ от сохраненного значения R и полученной метки RES^*, после чего сравнивает полученный хэш-код $HRES^*$ с сохраненным значением $HXRES^*$.

10) В случае успеха гостевая сеть отправляет значение RES^* домашней сети, которая сравнивает его с сохраненным значением $XRES^*$.

11) Успех такого сравнения означает успешное завершение протокола аутентификации. Домашняя сеть отправляет соответствующее сообщение в гостевую сеть, прикрепив выработанный мастер-ключ K_{SEAF} и идентификатор мобильного устройства SUPI.

При успешном выполнении протокола 5G-AKA мобильное устройство и гостевая сеть получают общий мастер-ключ K_{SEAF}, на основе которого в дальнейшем вычисляются дополнительные ключи для защиты данных.

Во время выполнения протокола 5G-AKA важно, чтобы счетчик был защищен от злоумышленника, поскольку воздействие последнего может привести к компрометации личности и местоположения абонента (см. п. IV-B).

В результате успешного завершения протокола 5G-AKA, гостевая сеть получает SUPI мобильного устройства. Это требуется для «законного перехвата» [Lawful Interception – LI]. Правоохранительные органы большинства стран требуют, чтобы местные провайдеры в предусмотренных законом случаях имели возможность определять местонахождение и отслеживать любого конкретного пользователя. В дальнейшем гостевая сеть использует SUPI в качестве входа для функций выработки общих ключей с мобильным устройством.

III. Наследственные проблемы и их устранение в 5G

Определим некоторые понятия, используемые далее.

Под нарушением *«конфиденциальности (приватности)»* пользователя (абонента) будем понимать следующие события:

- события, при которых злоумышленник получает доступ к информации, передаваемой или получаемой пользователем по радиоканалу, имеет возможность изменить или навязать ее;
- события, при которых злоумышленних имеет возможность отслеживать местоположение пользователя, используя данные, передаваемые и получаемые его мобильным устройством.

Под установлением *«контекста безопасности»* между пользователем и гостевой сетью будем понимать состояние, при котором есть возможность защищенной передачи информации по радиоканалу. Например, после успешного завершения протокола 5G-AKA пользователь и гостевая сеть имеют общий мастер ключ, на основе которого вычисляют дополнительные ключи для защиты данных. В этом случае контекст безопасности установлен.

«Ключевая проблема» – это термин, используемый в исследованиях 3GPP для обозначения потенциальной проблемы конфиденциальности пользователей. По каждой ключевой проблеме в стандартах 3GPP можно найти описание проблемы, связанные угрозы и соответствующие рекомендации для уменьшения риска угроз. Некоторые рекомендации являются строгими требованиями, это указывается в соответствующих спецификациях стандартов. Сам по себе термин *«ключевая проблема»* носит, скорее, нестрогий характер и призывает специалистов более внимательно изучить указанные потенциальные уязвимости.

Одной из основных задач при разработке 5G Release 15 было устранение угроз конфиденциальности абонента, существовавших в предыдущих поколениях сетей связи.

В таблице II приведена сводка атак на сети предыдущих поколений. Рассматриваются следующие атаки: перехват IMSI [10], [12] - [18], IMSI-зондирование [19], неаутентифицированный запрос IMEI [12], [14], [16], неизменность GUTI [20], [21], связь между GUTI и MSISDN [21] - [24], атака повторного переназначения GUTI [20], [25], уязвимости протокола RRC [21], [26], IMSI-пейджинг [27], [21], [20], [28], ToRPEDO [29], атака связуемости сообщений о сбоях протокола AKA [20], [27], [30].

5G Release 15 предусматривает несколько новых функций безопасности, которые уменьшают

Таблица II
Обзор атак на конфиденциальность абонента в системах связи предыдущих поколений
+ означает применимо, ± - частично / ограниченно / возможно, – - неприменимо, ? - неизвестно.

Атака	Тип			Возможности атакующего					Поколение связи				Параграф
	Раскрытие идентичности	Утечка местоположения	Отслеживаемость пользователя	Пассивный перехват	Активный перехват	Знание IMSI	Знание MSISDN	Знание TMSI / GUTI	2G	3G	4G	5G (до Release 16 Stage 3)	
Перехват IMSI	+	+	+	+	+	–	–	–	+	+	+	–	III-A
IMSI-зондирование	–	+	+	+	±	–	+	–	+	+	+	+	III-B
Неаутентифицированный запрос IMEI	+	+	+	+	+	–	–	–	+	+	–	–	III-C
Неизменность GUTI	–	+	+	+	–	±	±	–	+	+	+	–	III-D
Связь между GUTI и MSISDN	–	+	+	–	±	–	+	–	+	+	+	–	III-E
Атака повторного переназначения GUTI	–	–	+	+	+	–	–	–	+	+	+	±	III-F
Уязвимости протокола RRC	–	+	+	+	+	?	+	+	–	–	+	–	III-G
IMSI-пейджинг	–	+	+	+	+	±	±	–	+	+	+	–	III-H
ToRPEDO	±	+	+	+	±	–	+	–	+	+	+	–	III-I
Атака связываемости сообщений о сбоях AKA	–	–	+	+	+	–	–	–	–	+	+	+	III-J

вероятность нарушения конфиденциальности абонента в радиоканале [31], [32]. Таблица III является логическим продолжением таблицы II и содержит сводку влияния новых функций безопасности на уязвимости предыдущих поколений.

A. Перехват IMSI

В целях соблюдения конфиденциальности, для идентификации абонента до момента установления безопасного канала используется временный идентификатор абонента GUTI. Однако, существуют определенные ситуации, когда аутентификация с использованием этого временного идентификатора невозможна. Например, когда пользователь регистрируется в сети впервые, и ему еще не назначен временный идентификатор, либо когда сеть не может извлечь постоянный идентификатор IMSI из предъявленного GUTI. Проводя атаку «человек посередине» (man-in-the-middle – MitM) злоумышленник может намеренно смоделировать второй сценарий, чтобы заставить ничего не подозревающего пользователя раскрыть свой постоянный идентификатор. Эти атаки известны как атаки «перехвата IMSI» [IMSI-catching] [17] и применимы к мобильным сетям, вплоть до стандарта LTE [10], [13], [18]. При осуществлении атаки злоумышленник, используя *identifier request* (п. II-D), получает идентификационные данные всех абонентов в зоне атаки. Для проведения атаки злоумышленнику не требуется знать никакой предварительной информации.

Указанные атаки обозначены как *ключевая проблема* в рекомендации 3GPP TR 33.899 (подпункт 5.7.3.2) [4].

1) Сокрытие SUPI: Учитывая серьезность угроз утечки SUPI посредством атак с IMSI-catching, 3GPP уделили много внимания защите от указанной атаки в 5G Release 15 (подпункт 5.2.5 TS 33.501) [2]. В случае сбоя идентификации через 5G-GUTI, спецификации безопасности 5G не допускают передачу SUPI по радиоканалу в незашифрованном виде. Вместо этого передается зашифрованный «скрытый SUPI», обозначаемый SUCI. Для этой цели выбрана схема (см. рисунки 5 и 6), включающая алгоритмы в группе точек эллиптической кривой [Elliptic Curve Integrated Encryption Scheme – ECIES] [35]. Мобильное устройство генерирует SUCI, используя открытый ключ домашней сети (обозначается *pk*). Ниже приведен обзор механизма защиты на основе ECIES из TS 33.501 [2].

ECIES – это гибридная схема шифрования, которая объединяет криптографию в группе точек эллиптической кривой [Elliptic Curve Cryptography – ECC] [36] и симметричную криптографию. Чтобы вычислить новый SUCI, мобильное устройство генерирует новую одноразовую пару открытого / секретного ключа ECC, используя открытый ключ домашней сети, который безопасно предоставляется терминалу при регистрации/установке SIM-карты. Мобильное устройство выполняет операции шифрования, определенные в [37], как показано на рисунке 5. Результатом работы схемы является конкатенация одноразового открытого ключа, значения зашифрованного текста и значения MAC. Предусмотрена также возможность добавления дополнительных параметров.

Домашняя сеть использует полученный одноразовый открытый ключ и свой закрытый ключ для расшифрования полученного SUCI. Обработка на стороне домашней сети показана на рисунке 6. TS 33.501 предусматривает два варианта реализации схемы ECIES. Оба используют алгоритм AES-128 в режиме счетчика [CTR] для шифрования и алгоритм HMAC-SHA-256 для аутентификации в части симметричной криптографии, а в части криптографии с открытым ключом – эллиптические кривые *Curve25519* и *secp256r1*.

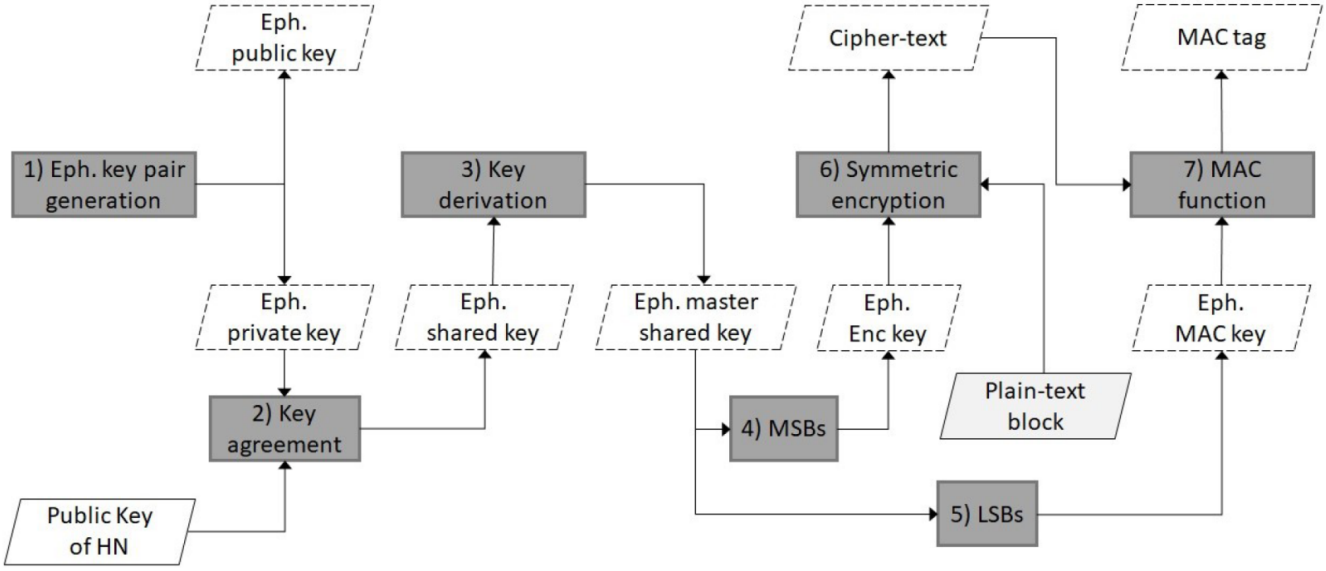
В предложенной схеме защиты скрывается только часть SUPI, содержащая идентификационный номер мобильного абонента MSIN (см. п. II-B), а идентификатор домашней сети (MCC / MNC) передается в открытом виде, поскольку требуется для маршрутизации в случаях нахождения абонента в роуминге. Поля данных, составляющие SUCI:

- **Идентификатор схемы защиты [Protection Scheme Identifier]:** это поле идентифицирует указанную схему защиты.
- **Идентификатор открытого ключа домашней сети [Home Network Public Key Identifier]:** идентификатор *pk*, предоставленного домашней сетью.
- **Идентификатор домашней сети [Home Network Identifier]:** содержит MCC и MNC из SUPI.
- **Выходные данные схемы шифрования [Protection Scheme Output]:** представляет собой результат ра-

Таблица III
Эффективность мер, принятых в рамках 5G, против известных атак
● - противодействует/применимо, ⋆ - частичный / ограниченный эффект, ○ - не противодействует / неприменимо.

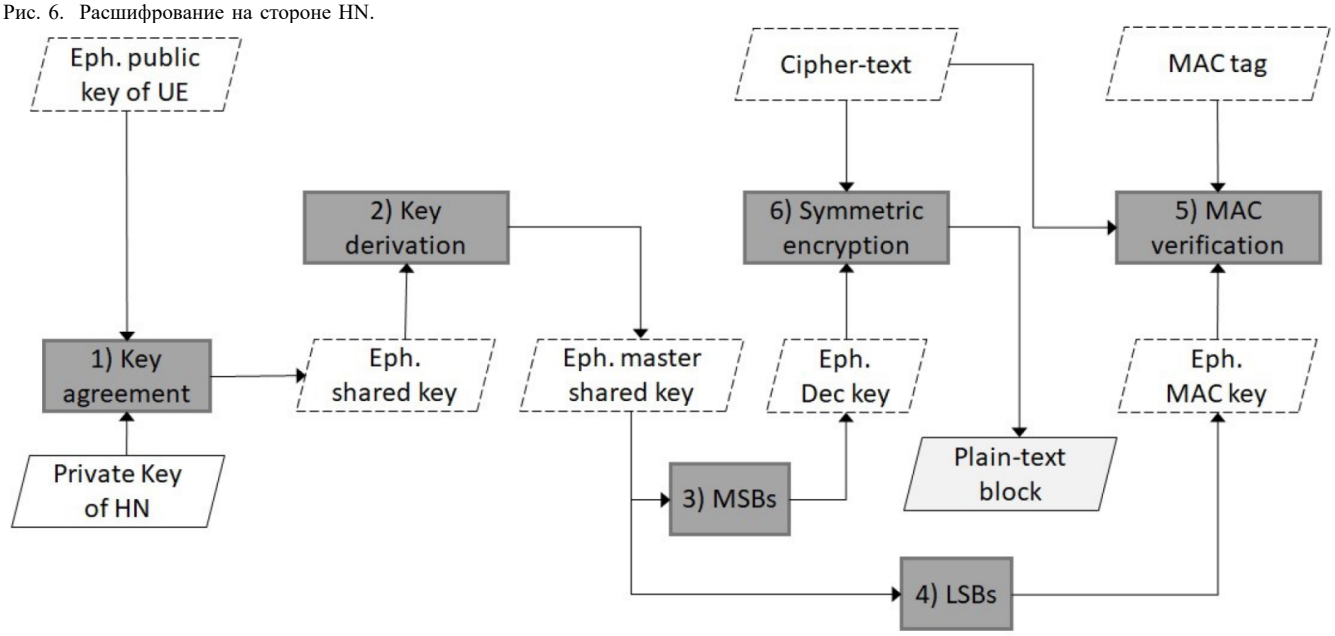
5G Меры по повышению конфиденциальности	Существующие атаки против предыдущих поколений систем связи									Рекомендация 3GPP	Пункт
	IMSI-catching	(Raw) IMSI-probing	GUTI Persistence	GUTI-MSISDN	GUTI Reallocation	Localization via UE	IMSI-paging	ToRPEDO Attack	LFM Attack		
Сокрытие SUPI	●	○	○	○	○	○	○	○	○	TS 33.501 [2] подпункт 5.2.5	III-A1
Строгое обновление GUTI	○	○	●	●	○	○	○	⋆	○	TS 33.501 [2] подпункт 6.12.3	III-D1
Средства выявления ложных баз. станций	⋆	○	○	○	⋆	●	⋆	○	⋆	TS 33.501 [2] приложение E	III-K
Отделение SUPI от механизма пейджинга	○	○	○	○	○	○	●	○	○	TS 33.501 [2] приложение E	III-H1
Пейджинговые сообщения, основанные на GUTI	○	○	○	○	○	○	○	●	○	TS 38.304 [33] подпункт 7.1	III-I1
Безопасные переадресации	⋆	○	○	○	⋆	⋆	⋆	○	○	TS 38.331 [34]	III-G1

Рис. 5. Система защиты на основе ECIES. Зашифрование на стороне UE.



(a) Encryption at UE side

Рис. 6. Расшифрование на стороне HN.



(b) Decryption at HN side

боты указанной схемы.

Поскольку *pk* встроен в защищенную память SIM-карты, инфраструктура открытого ключа не требуется. Кроме того, идентификация абонента осуществляется всего за один проход, что помогает сократить время установления соединения. Эта схема также не чувствительна к десинхронизации идентификаторов между мобильным устройством и домашней сетью [38] и требует простого управления ключами, что приводит к значительному снижению количества ошибок соединения. Тем не менее все еще остаются аспекты, которые требуют дальнейшего совершенствования (см. п. IV-D).

B. IMSI-зондирование

IMSI-зондирование [IMSI-probing] отличается от перехвата IMSI тем, что злоумышленник уже знает идентификатор абонента (например, IMSI или MSISDN) и некоторую связанную информацию и хочет выяснить, присутствует ли абонент с таким идентификатором в заданной географической области. Существует множество возможных способов проведения такой атаки, например, рассылка на соответствующий MSISDN SMS-сообщений (по возможности, незаметных для пользователя [19]) или использование других «триггеров активности» и отслеживание всплеска соответствующего сигнального трафика в проверяемой соте.

В 3GPP сочли противодействие атакам типа IMSI-зондирование нецелесообразными, поскольку такое противодействие потребовало бы больших накладных расходов, например, передачи большого числа фиктивных сообщений сигнализации для скрытия факта осуществления реальной сигнализации. Таким образом, указанная атака применима к 5G Release 15, однако на практике атака требует немалых знаний и возможностей злоумышленника.

C. Неаутентифицированный запрос идентификатора IMEI

В GSM и UMTS злоумышленник может запросить IMEI абонента путем направления ему запроса идентификации (*identity request*, см. п. II-D) без прохождения аутентификации [12], [14], [16]. Начиная с LTE такие возможности были закрыты, и теперь сеть может запрашивать у пользователя его IMEI только после установления между ними защищенного канала.

D. Неизменность идентификатора GUTI

Временные идентификаторы абонентов, такие как GUTI, используются в качестве меры обеспечения конфиденциальности для уменьшения возможности идентификации и отслеживания конкретного абонента по радиоканалу. В системе LTE обновление GUTI рекомендуется в следующих случаях:

- когда меняется гостевая сеть или во время новой процедуры регистрации;
- во время обновления TA [Tracking Area – зоны слежения];
- когда гостевая сеть отправляет команду переназначения GUTI [GUTI reallocation command].

Поскольку в существующих версиях LTE момент обновления GUTI определяется только политикой конкретной гостевой сети, последняя имеет возможность назначать и переназначать конкретному пользователю одно и то же значение GUTI несколько раз. Мобильное устройство не проверяет, отличается ли вновь выделенное ему значение от прежнего, что создает предпосылки для потенциально уязвимых реализаций или конфигураций, в которых GUTI может оставаться неизменным в течение длительного времени. Подобные случаи встречались на практике у некоторых операторов мобильных сетей [20], [21]. В сетях LTE получение или отслеживание временных идентификаторов абонента было одной из основных стратегий при проведении атак на конфиденциальность абонента [21].

Неизменность GUTI была обозначена как *ключевая проблема* в 3GPP TR 33.899 (подпункт 5.7.3.1) [4].

1) Строгое обновление GUTI: В 5G Release 15 (подпункт 6.12.3 TS 33.501) обязательное обновление 5G-GUTI предписано в следующих случаях:

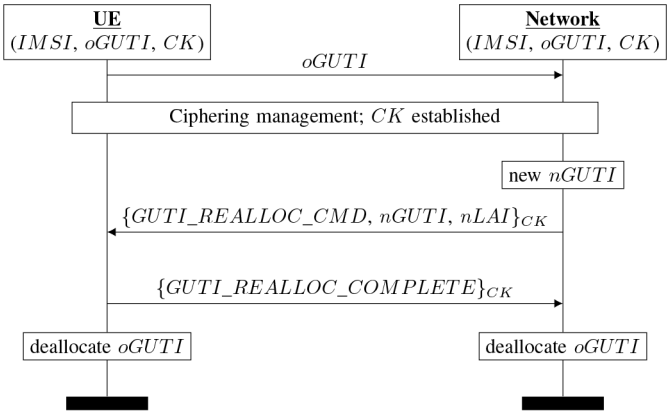
- **Начальная регистрация [Initial Registration]:** если гостевая сеть принимает от мобильного устройства запрос на регистрацию *(Registration Request)* типа «начальная регистрация» *(initial registration)*, она возвращает устройству новый 5G-GUTI в процедуре регистрации.
- **Обновление мобильной регистрации [Mobility Registration Update]:** если гостевая сеть принимает от мобильного устройства *Registration Request* типа «обновление мобильной регистрации» *(mobility registration update)*, она возвращает устройству новый 5G-GUTI в процедуре регистрации.
- **Периодическое обновление регистрации [Periodic Registration Update]:** если гостевая сеть принимает от мобильного устройства *Registration Request* типа «периодическое обновление регистрации» *(periodic registration update)*, она возвращает устройству новый 5G-GUTI в процедуре регистрации.
- **Запрос услуги, инициируемый сетью [Network Triggered Service Request]:** при получении запроса услуги *(Service Request)*, отправленного мобильным устройством в ответ на пейджинговое сообщение, гостевая сеть направляет устройству новый 5G-GUTI.

Эти требования обязательного обновления делают попытки идентификации или отслеживания абонентов на основе 5G-GUTI неэффективными. Кроме того, на усмотрение оператора сети остается более частое переназначение 5G-GUTI, например, после сообщения запроса услуги от мобильного устройства, не инициированного сетью.

E. Связь между идентификаторами GUTI и MSISDN

Атаки этого типа схожи с IMSI-probing (см. п. III-B). Здесь также предполагается, что цель злоумышленника, которому известен один из постоянных идентификаторов абонента, состоит в том, чтобы обнаружить и отслеживать этого абонента. При атаке используются обычные методы – либо осуществление телефонных звонков [22], либо отправка незаметных для пользователя SMS-сообщений [23] на целевой MSISDN, что приводит к

Рис. 7. Процедура переназначения GUTI.



запуску процедур пейджинга (см. п. II-D) и, в конечном итоге, к установлению соответствия между известным идентификатором (обычно MSISDN) и GUTI [24]. Это позволяет злоумышленнику в течение длительного времени отслеживать конкретного абонента благодаря постоянству GUTI в LTE (см. п. III-D). В указанных атаках злоумышленника интересуют именно paging-сообщения, а не любые сообщения сигнализации.

Поскольку проблема постоянства GUTI решена в 5G, указанную в текущем пункте уязвимость можно также считать устраненной.

F. Атака повторного переназначения GUTI (GUTI Reallocation Replay Attack)

При осуществлении соеденения с гостевой сетью (см. рисунок 3), для обеспечения конфиденциальности абоненты используют в качестве своего идентификатора GUTI. Для обновления GUTI в мобильных сетях используют процесс, называемый «Процедура переназначения GUTI» [GUTI Reallocation Procedure] (подпункт 5.4.1 TS 24.301 [39]). На рисунке 7 показан вариант этой процедуры для системы LTE [39].

Здесь *oGUTI* и *nGUTI* обозначают, соответственно, старый и новый GUTI мобильного устройства UE, а CK – ключ конфиденциальности. Процедура состоит в следующем:

- Мобильное устройство идентифицирует себя в сети с помощью текущего присвоенного ему временного *oGUTI*.
- Сеть идентифицирует мобильное устройство и определяет средства шифрования последующей связи.
- После этого сеть направляет зашифрованное с помощью CK сообщение о переназначении GUTI, содержащее *nGUTI*. При необходимости это сообщение также может содержать идентификатор текущей области местоположения (nLAI).
- При получении сообщения о переназначении GUTI мобильное устройство отвечает сообщением о завершении переназначения GUTI, чтобы подтвердить получение нового GUTI.

Если сеть не получает ожидаемое подтверждение от мобильного устройства, она поддерживает оба варианта временного идентификатора (*oGUTI* и *nGUTI*) для соответствующего IMSI. Стандарт определяет два метода установления ключа конфиденциальности CK: (1) новый ключ устанавливается посредством процедуры аутентификации; либо (2) ранее установленный ключ шифрования восстанавливается с помощью процедуры настройки режима безопасности. Возможность использования восстановленных ключей позволяет проводить атаку на процедуру переназначения GUTI [20], [25]. Поскольку *GUTI Reallocation Command* не содержит механизма защиты от воспроизведения, злоумышленник может использовать эту слабость. Сначала злоумышленник перехватывает *GUTI Reallocation Command*. Позже, когда мобильное устройство уже обновило свой GUTI, но еще не добавило ключ шифрования CK, злоумышленник воспроизводит перехваченную команду *GUTI Reallocation Command*. Мобильное устройство не имеет возможности обнаружить повторное воспроизведение команды. Оно успешно расшифровывает *GUTI Reallocation Command* и отвечает сообщением *GUTI Reallocation Complete*. Это позволяет злоумышленнику отличить целевого пользователя от любого другого, поскольку другие пользователи не смогли бы расшифровать *GUTI Reallocation Command* и, следовательно, не стали бы отвечать сообщением о завершении. В результате злоумышленник с минимальными усилиями может отслеживать целевого пользователя.

G. Уязвимости / неправильные реализации протокола RRC

Протокол управления радиоресурсами [Radio Resource Control – RRC] используется для настройки и управления радиосвязью между мобильным устройством и гостевой сетью. Основные функции протокола RRC включают в себя функции установления и разрыва соединения, широковещательную передачу системной информации, установление радиоканала, процедуры управления мобильным соединением, пейджинговые уведомления и т. д. В стеке протоколов (модель ИСО) протокол RRC располагается на сетевом (IP) уровне. Протокол RRC описан в 3GPP TS 25.331 [40] для UMTS и в 3GPP TS 36.331 [41] для LTE.

В системе связи LTE мобильное устройство, находясь в режиме ожидания (*idle state*) RRC, не проверяет подлинность базовой станции. В результате устройство может подключаться к подставной базовой станции. Разработчики систем мобильной телефонной связи в большинстве сосредоточены на обеспечении безопасной связи в состоянии соединения [connected state] RRC, а аспекты безопасности в режиме ожидания не рассматривались должным образом. Указанная уязвимость мобильного устройства к атакам с использованием ложной базовой станции была признана *ключевой проблемой* в TR 33.899 (подпункт 5.4.3.1) [4]. Протокол LTE RRC также содержит функцию «широковещательной передачи сетевой информации», в которой GUTI, связанные с гостевой сетью, передаются по радиоканалу [21]. Эти трансляции не зашифрованы и не подлежат аутентификации, поэтому могут быть легко перехвачены и прочитаны злоумышленником. Поскольку эти широковещательные сообщения зависят от местоположения, для выявления присутствия абонентов в этой конкретной области могут быть применены методы из [22] (атаки типа IMSI-зондирование, см. п. III-B).

Другим типом сообщений RRC, которые содержат конфиденциальную информацию, специфичную для абонента, являются «отчеты об измерениях мобильного устройства». В частности, для компрометации местоположения абонентов в литературе использовались два типа отчетов об измерениях [21]:

- **Отчет об измерениях [measurement report]:** гостевая сеть отправляет мобильному устройству сообщение-запрос [*measurement configuration*], указывающее, какой тип измерения должен быть выполнен. В ответ мобильное устройство составляет и отправляет соответствующий ответ [*measurement report*]. Более ранние спецификации LTE (Версия 12.5.0 TS 36.331 и ранее) позволяли передавать эти сообщения RRC до установления контекста безопасности между мобильным устройством и гостевой сетью, что использовалось для компрометации местоположения абонентов путем декодирования информации о местоположении из этих сообщений [21], [26]. Более поздние спецификации допускают передачу отчета только после установления контекста безопасности.
- **Отчеты о сбое радиолинии [RLF – Radio Link Failure]:** RLF-отчеты используются для устранения проблем с зоной покрытия. Эти отчеты содержат идентификаторы обслуживающей и соседних базовых станций вместе с замерами их мощности, которые могут использоваться в качестве исходных данных для определения точного положения абонента методами трилатерации[42]. Стандарт LTE (Приложение A.6 в [41]) не разрешает передачу *RLF report* до установления контекста безопасности. Тем не менее, практические исследования [21] реальных мобильных сетей показали, что мобильные устройства в действительности передают эти отчеты через сети LTE вне контекста безопасности, что приводит к утечкам информации о местоположении абонентов. Соответствующие принципы в рамках стандарта сформулированы расплывчато, что приводит к их некачественной реализации некоторыми производителями.

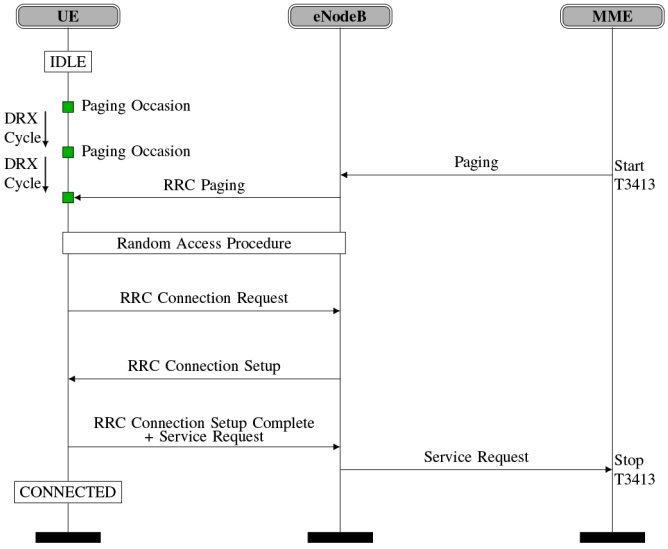
1) Безопасные переадресации: В 5G Release 15 (TS 38.331 [34]) зафиксировано требование защиты сообщений протокола управления радиоресурсами которые переадресовывают устройства. Эта функция делает невозможным использование ложных базовых станций для выполнения мошеннических переадресаций.

H. IMSI-пейджинг

На рисунке 8 показана процедура пейджинга в LTE.

Узел управления мобильностью [Mobility Management Entity – MME] (часть гостевой сети) отвечает за инициирование поиска и аутентификации мобильного устройства, eNodeB – базовая станция LTE (также часть гостевой сети). В начале поискового вызова MME запускает таймер (T3413) и ожидает ответа от мобильного устройства до истечения этого таймера. Для снижения потребляемой мощности мобильного устройства в RRC *idle state* используют прерывистый прием [Discontinuous Reception – DRX], также известный как цикл поискового вызова *(paging cycle)*. DRX-цикл определяет, как часто

Рис. 8. Механизм пейджинга в LTE.



мобильное устройство проверяет наличие пейджинговых сообщений. Мобильное устройство декодирует пейджинговые сообщения RRC и, если находит свой идентификатор в этом сообщении, инициирует получение доступного радиоканала посредством «процедуры произвольного доступа» [Random Access Procedure]. После этого мобильное устройство запрашивает базовую станцию через «запрос соединения RRC» [RRC Connection Request], чтобы настроить радиоресурсы для обмена сигналами. После завершения установки соединения RRC терминал отправляет сообщение запрос на обслуживание [Service Request] и входит в состояние соединения.

В поисковом вызове LTE для оповещения ожидающих мобильных устройств о входящих данных могут использоваться два типа идентификаторов: временный идентификатор GUTI или постоянный идентификатор IMSI. Обычно это GUTI, который используется в качестве идентификатора в пейджинговых сообщениях. Однако, в ситуациях когда гостевая сеть теряет связь с мобильным устройством из-за сбоя или перезапуска, существует условие для отправки IMSI в качестве идентификатора. Использование IMSI в качестве идентификатора мобильного устройства при отправке пейджинговых сообщений считается угрозой конфиденциальности для пользователей [21], [27], [28], [20]. Пассивный противник может просто наблюдать за радиосвязью в интересующем месте и узнать, какие абоненты находятся в этой конкретной области. Так как во время процедуры поискового вызова контекст безопасности между мобильным устройством и гостевой сетью еще не установлен, активный злоумышленник может установить ложную базовую станцию в интересующей области и начать рассылку абонентам пейджинговых запросов на основе IMSI. По полученным ответам злоумышленник может узнать, какие IMSI присутствуют в этой конкретной области. Абоненты сети LTE отвечают на IMSI-триггеры пейджинга, используя свои GUTI, что приводит к корреляции между IMSI и GUTI. В сочетании с инициированием механизма пейджинга посредством совершения телефонных вызовов на MSISDN (п. III-E) злоумышленник имеет возможность дополнительно соотнести нужные IMSI и GUTI

с MSISDN. Таким образом, активные / пассивные нарушители могут с определенной точностью отследить абонентов в конкретной географической области, что нарушает конфиденциальность абонентов. Пейджинг на основе IMSI был определен как *ключевая проблема* в 3GPP TR 33.899 (подпункт 5.7.3.10) [4].

1) Отделение SUPI от механизма пейджинга: Возможности пейджинга мобильного устройства на основе SUPI были удалены из 5G (подпункт 9.3.3.18 в TS 38.413) [43], а вычисление времени проверки пейджинговых сообщений (Paging Occasions, см. п. III-I) теперь завязано на 5G-GUTI вместо SUPI. В сочетании с механизмами принудительного обновления 5G-GUTI данные меры делают идентификацию или отслеживание абонентов с использованием пейджинговых сообщений и ложных базовых станций невозможными.

I. Атака ToRPEDO

В системе LTE моменты времени [Paging Occasions], когда мобильное устройство включает свой приемник и проверяет наличие пейджинговых сообщений, определяются его идентификатором IMSI. Этот механизм может быть использован для проверки наличия (или отсутствия) цели в определенном месте с помощью атаки, называемой ToRPEDO [TRacking via Paging mEssage DistributiOn – отслеживание через рассылку пейджинговых сообщений] [29]. Эта атака эксплуатирует тот факт, что соответствующие моменты времени для конкретного мобильного устройства всегда фиксированы, поскольку зависят от его идентификатора IMSI. Следовательно, путем инициирования последовательных процедур поискового вызова злоумышленник в конечном итоге может с высокой степенью достоверности определить наличие или отсутствие целевого пользователя в заданной области.

1) Пейджинговые сообщения, основанные на GUTI: В отличие от LTE, где пейджинговые сообщения определялись на основе IMSI абонентского устройства, в 5G они основаны на временном идентификаторе (называемом 5G-S-TMSI), который является частью GUTI устройства. В результате, атака ToRPEDO, которая использовала фиксированные пейджинговые сообщения для целевого мобильного устройства, больше не может использовать постоянство в таймингах пейджинга.

J. Атака связываемости сообщений о сбоях протокола AKA

Все поколения мобильной телефонной связи подвержены атаки, известной как «атака связываемости сообщений о сбоях» [Linkability of (AKA) Failure Messages – LFM] [30], [27], [20]. Атака LFM использует тот факт, что в протоколе 5G-AKA (см. п. II-E), в случае завершения процесса аутентификации ошибкой злоумышленник способен перехватить код отказа, то есть получить либо *MAC Failure*, либо *Sync Failure*. Это позволяет ему связать два разных сеанса AKA для идентификации целевого пользователя.

Атака LFM проста для практической реализации и выполняется следующим образом. Сначала атакующий наблюдает за сеансом AKA целевого пользователя и записывает запрос аутентификации *(R, AUTN).* Затем, когда злоумышленник хочет проверить, принадлежит ли другой сеанс AKA тому же целевому пользователю, он воспроизводит записанный запрос аутентификации и отслеживает тип перехваченного сообщения об ошибке. В случае *MAC Failure* это другой пользователь, а в случае *Sync Failure* это тот же пользователь. При атаке LFM не требуются производить дополнительных вычислений, а полученный результат однозначен. Следовательно, это очень эффективная атака, которая позволяет отслеживать абонента, но требует некоторых допущений о возможностях злоумышленника.

K. Система обнаружения ложных базовых станций

В большинстве атак, относящихся к предыдущим поколениям систем мобильной связи, использование ложных базовых станций требуется до того, как мобильное устройство аутентифицирует сеть. В 5G Release 15 (Приложение E к [2]) предложен общий подход для выявления ложных базовых станций с использованием информации о состоянии радиосвязи (*measurement report* III-G), получаемой от мобильного устройства. Информация об уровне принимаемого сигнала и местоположении в *measurement report* может использоваться для обнаружения ложной базовой станции, которая пытается привлечь мобильное устройство, передавая сигнал с более высокой мощностью, чем у подлинных базовых станций. Если ложная базовая станция воспроизводит измененную информацию широковещания с целью предотвращения переключения мобильного устройства жертвы на подлинную базовую станцию (например, путем изменения соседних ячеек, критериев выбора соты, таймеров регистрации и т. п.), обнаружить ее можно, исследуя несоответствия в информации о развертывании. Кроме того, ложные базовые станции, использующие нестандартные частоты или идентификаторы сот, могут быть обнаружены путем анализа соответствующей информации в принятых сообщениях *measurement report.*

Сети и устройства могут использовать другие дополнительные функции безопасности и конфиденциальности на усмотрение оператора. Эффективное обнаружение ложной базовой станции должно привести к уменьшению вероятности нарушения конфиденциальности. Как показано в [44], в случае неповрежденных и нескомпрометированных участников сети мобильной связи протокол 5G-AKA гарантирует конфиденциальность мобильного устройства.

На момент написания обзора в 3GPP продолжается работа по усовершенствованию механизмов обнаружения ложных базовых станций. Итоговые рекомендации (требования) планируют выпустить вместе с окончательной версией Release 16.

IV. Нерешенные проблемы, новые атаки и предлагаемые меры

Успешное развертывание будущих систем 5G требует решения оставшихся проблем с обеспечением конфиденциальности абонента. В этой главе освещены соответствующие угрозы, которые не были устранены в Release 15, а также проанализированы последние публикации, в которых предлагаются улучшения или рассматриваются новые атаки на конфиденциальность абонента в сетях 5G.

A. Неустраненные уязвимости

Изучая раздел III и таблицу III, можно заметить, что главной проблемой конфиденциальности, унаследованной в Release 15 от предыдущих поколений является атака LFM на основе протокола AKA (см. III-J). Последнюю выявили М. Арапинис и соавторы [27], они также предложили варианты ее устранения: домашние сети должны иметь пару открытый/закрытый ключ, каждая USIM-карта должна хранить открытый ключ своей домашней сети. Далее, сообщения об ошибках протокола AKA шифруются с использованием открытого ключа домашней сети. Авторы подтверждают эффективность данного исправления с помощью инструмента автоматического анализа ProVerif [45]. Однако, как было продемонстрировано П. Фоуке и соавторами [46], предложенное исправление по-прежнему не лишено недостатков. Авторы [46] представили собственный улучшенный вариант исправления уязвимости LFM также на основе применения схемы с открытым ключом. С другой стороны, применение таких схем повлечет значительные накладные расходы, поэтому 3GPP не поддерживает эти нововведения. Поскольку между мобильным устройством и домашней сетью изначально предусмотрено разделение общего секрета, решение этой проблемы с помощью схемы с симметричным шифрованием представляется более актуальным. Такие подходы рассмотрены далее в п. IV-C.

B. Новые атаки на конфиденциальность абонента 5G

Некоторое время назад Р. Борганкар и соавторы [47] представили новые атаки против всех вариантов протокола AKA, включая 5G-AKA. Эти атаки используют логическую уязвимость в механизме отказа AKA. Эта уязвимость связана с использованием XOR в токене повторной синхронизации AUTS (см. рисунок 4), который является объединением двух параметров: *CONC** и *MAC**. Параметр *CONC** содержит текущий *SQNUE* в маскированной форме: $SQNUE \oplus AK$*, где *AK** = f_5^**(K, R)*. Во время вычисления маскирующего ключа *AK** значение *R* извлекается из полученного запроса аутентификации *(R, AUTN)*. Следовательно, в случае получения одного и того же запроса аутентификации дважды в два разных момента времени t_1 и t_2 маскированные порядковые номера в их соответствующих токенах *AUTS* будут:

$CONC_1$* = $SQNUE_1 \oplus AK_1$*, где AK_1* = f_5*(K, R),

$CONC_2$* = $SQNUE_2 \oplus AK_2$*, где AK_2* = f_5*(K, R),

где $SQNUE_1$ – номер счетчика *UE* в момент времени t_1, а $SQNUE_2$ – в момент времени t_2. Следовательно, противник может вычислить:

$CONC_1$* $\oplus$ $CONC_2$* = $SQNUE_1 \oplus SQNUE_2$.

В [47] представлены две новые атаки на основе этой логической уязвимости:

- Атака мониторинга активности [Activity Monitoring Attack – AMA].
- Атака на конфиденциальность местоположения [Location Confidentiality Attack – LCA].

В атаке AMA цель противника состоит в том, чтобы узнать *n* младших значащих битов *SQNUE* в моменты времени t_1 и t_2. После этого по разнице между значениями счетчика, соответствующими успешным сеансам аутентификации, злоумышленник определяет «объем активности» (количество вызовов, SMS и т. д.) конкретного пользователя между этими двумя моментами времени. Для осуществления AMA злоумышленнику требуется взаимодействовать как с мобильным устройством, так и с домашней сетью (через гостевую сеть). Следовательно, предварительным условием для запуска AMA является компрометация как идентичности целевого мобильного устройства, так и его местоположения. Онлайн-фаза атаки AMA изображена на рисунке 9.

В ходе этой фазы злоумышленник сначала выбирает $2^{n-1} + 1$ последовательных запросов аутентификации из домашней сети для целевого мобильного устройства. Затем злоумышленник отправляет конкретные $n + 1$ из этих вызовов мобильному устройству, за каждым из которых следует экземпляр первоначально принятого запроса аутентификации $(R_0, AUTN_0)$, и записывает соответствующие $n+1$ токены повторной синхронизации, то есть $AUTS^{'}$ и $AUTS_j$ (для j от 0 до $n-1$).

На офлайн-этапе, используя описанную логическую уязвимость, злоумышленник на основе записанных токенов повторной синхронизации вычисляет следующие значения:

$\delta_i = SQNHN_0 \oplus (SQNHN_0 + 2^i)$ для $0 \leq i \leq n-1$,

где $SQNHN_0$ –значение SQN на стороне домашней сети в начале атаки. В результате приема первого вызова аутентификации $(R_0, AUTN_0)$ от злоумышленника мобильное устройство также синхронизирует свой SQN с этим значением в начале атаки. Кроме того, зная n значений δ_i, при помощи определенного алгоритма злоумышленник вычисляет n младших значащих битов $SQNHN_0$.

В атаке LCA целью злоумышленника является определение присутствия или отсутствия целевого мобильного устройства в конкретном месте. Атака LCA происходит следующим образом:

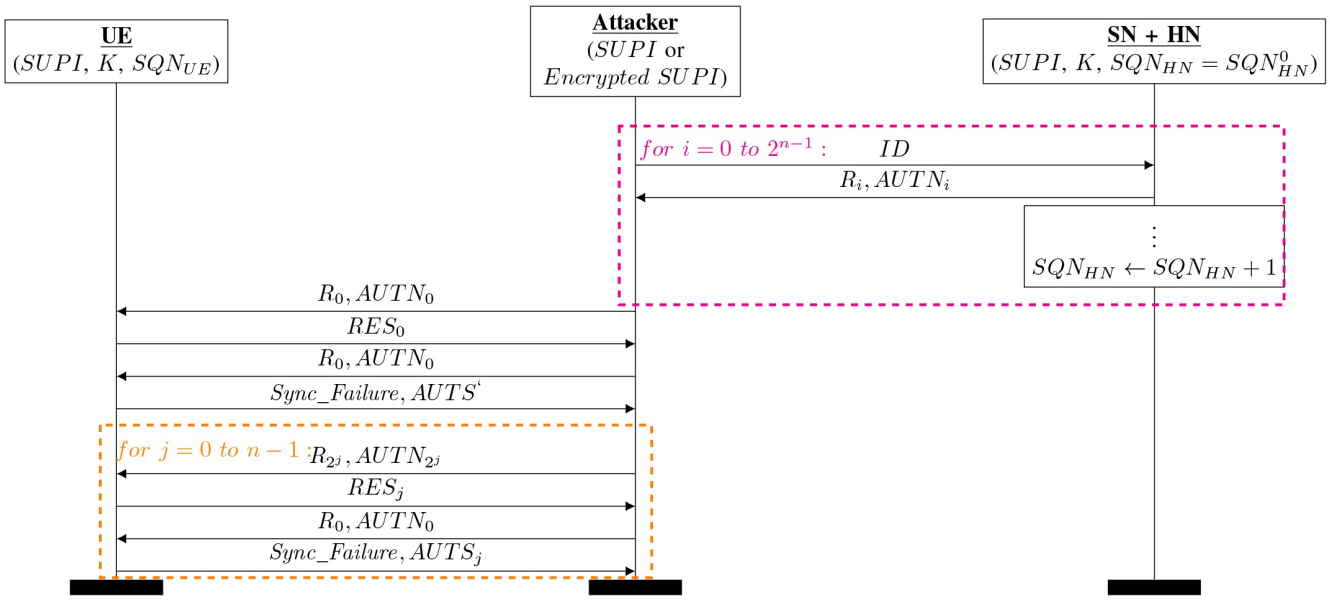
1) Злоумышленник наблюдает за сеансом 5G-AKA некоторого целевого пользователя UE_x и извлекает соответствующее значение $CONC_x$*, воспроизводя перехваченный запрос аутентификации для UE_x.

2) Через некоторое время, если злоумышленник захочет проверить, принадлежит ли другой неизвестный сеанс 5G-AKA пользователю UE_x, злоумышленник вновь направляет перехваченный на предыдущем шаге вызов этому пользователю и получает $CONC_y$*.

3) В случае $x = y$ распределение суммы $CONC_x$* $\oplus$ $CONC_y$* имеет определенный вид, в противном случае распределение близко к равновероятному. На основе имеющихся статистических данных атакующий может с определенной долей вероятности выяснить является ли новый пользователь UE_y пользователем UE_x.

Х. Хан и К. Мартин [48] проанализировали эти атаки на предмет их эффективности, практичности и применимости против 5G. Анализ показал, что AMA не так эффективна против 5G, как против предыдущих поколений (3G / 4G). Очевидно, что LCA является прямым продолжением LFM (п. III-J). Авторы также установили, что любые эффективные контрмеры против атаки LFM, предотвратят также атаки AMA и LCA.

Рис. 9. Онлайн-фаза атаки AMA.



C. Защита от атак LFM, AMA и LCA

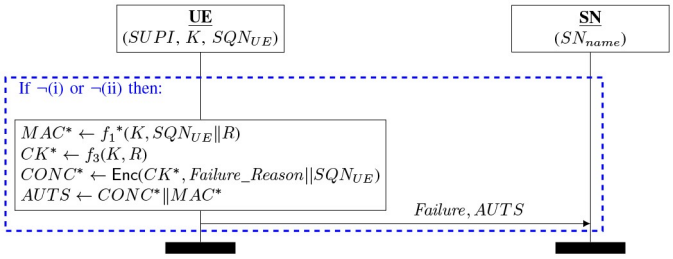
В пункте IV-A была отмечена необходимость решения на основе симметричного шифрования, которое устранило бы все три уязвимости LFM, AMA и LCA. Рассмотрим некоторые из таких решений, предложенных в [47].

1) **Симметричное шифрование *SQNUE*** (рисунок 10(a)): это исправление состоит в изменении механизма маскирования порядкового номера. Вместо использования XOR для сокрытия *SQNUE* предлагается использовать симметричное шифрование. Чтобы противостоять атаке LFM, достаточно скрывать код отказа протокола 5G-AKA внутри зашифрованного *CONC**. Авторы [47] утверждают, что это исправление легко внедрить в существующую систему, поскольку оно требует внесения изменений только в радиомодуль мобильного устройства, не затрагивая SIM-карту. Это решение имеет следующий недостаток: если злоумышленник отправляет сообщение об ошибке, дважды вводя один и тот же запрос аутентификации (пока *SQNUE* не обновился в мобильном устройстве), то ответный *CONC** не изменится, что позволит злоумышленнику понять, что *SQNUE* не менялся.

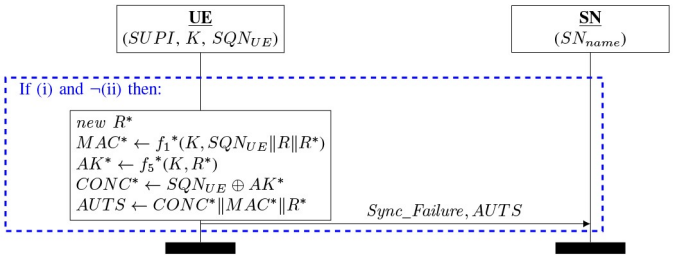
2) **Правильное рандомизирование AUTS** (рисунок 10(b)): другой способ противодействия AMA и LCA – для сокрытия *SQNUE* генерировать новое случайное число *R**, вместо использования числа *R*, полученного в запросе на аутентификацию. Новое случайное число *R** должно быть отправлено обратно в домашнюю сеть вместе с *AUTS* для расшифрования *SQNUE*. Исходное число *R* также должно использоваться при расчете *MAC**, чтобы гарантировать, что ответ получен именно на новый запрос аутентификации. В противном случае злоумышленник сможет воспроизвести старый ответ, заставив домашнюю сеть синхронизировать свой *SQNHN* со старым значением счетчика. Однако, это исправление само по себе не препятствует атаке LFM.

3) **Объединенное исправление** (рисунок 10(c)): оба предложенных выше исправления имеют ограничения. Для комплексного решения достаточно объединить их, как предложено в [47]. Это комбинированное исправление предотвращает LFM, AMA и LCA без каких-либо известных недостатков / ограничений.

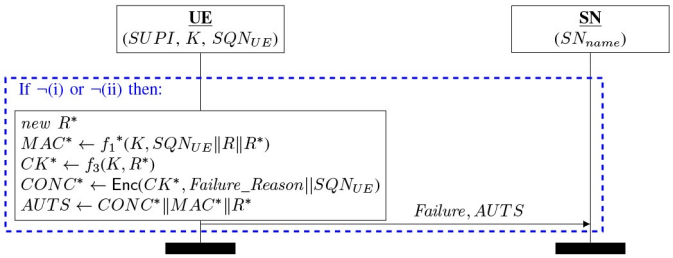
Рис. 10. Предлагаемые исправления для 5G-AKA.



(a) Fix_1: Symmetrically encrypting SQN_{UE}.



(b) Fix_2: Correctly randomizing $AUTS$.



(c) Fix_3: Combining Fix_1 and Fix_2.

D. Недостатки действующего механизма защиты SUPI

Следующие проблемы с существующим механизмом защиты SUPI на основе ECIES (п. III-A) были переданы в 3GPP группой экспертов по алгоритмам безопасности (Security Algorithms Group of Experts – SAGE) ETSI [49]:

- **Квантовая уязвимость:** поскольку схема ECIES использует алгоритмы на основе эллиптических кривых для обеспечения конфиденциальности идентификационных данных, стойкость схемы основывается на сложности решения задачи дискретного логарифмирования [Elliptic Curve Discrete Logarithm Problem – ECDLP]. Противник, обладающий квантовым компьютером, может решить эту задачу, используя квантовый алгоритм Шора [50].
- **Атаки подбора SUPI:** противник может выбрать произвольный SUPI и отправить соответствующий SUCI домашней сети. После этого противник может прослушивать различные ответы от домашней сети, зависящие от того, присутствует ли целевой пользователь в этой конкретной области соты. Любое изменение воспринимаемого результата позволит противнику подтвердить или опровергнуть присутствие соответствующего абонента в этой конкретной ячейке. В основанной на ECIES схеме нет механизма предотвращения подобных атак.
- **Атаки повторного воспроизведения сообщений:** действуя в соответствии со схемой на основе ECIES, домашняя сеть не имеет возможности проверять уникальность поступаемых сообщений. Следовательно, злоумышленник может повторно отправить в домашнюю сеть ранее зашифрованный SUPI и искать различные ответы (например, запрос аутентификации или сообщение об ошибке). На основании полученного ответа, с некоторой вероятностью [51] может быть отслежено устройство, чей SUPI неизвестен злоумышленнику.
- **Атаки понижения поколения связи (Downgrade):** активный злоумышленник, используя ложную базовую станцию, может заставить мобильное устройство переключиться на связь одного из младших поколений (GSM / UMTS / LTE) и затем получить IMSI / SUPI, используя *identity request*. В 3GPP Release 15 [8] SUPI вырабатывается непосредственно из IMSI, поэтому атаки на понижение также ставят под угрозу и 5G SUPI.

E. Защита SUPI на основе личностного шифрования

Как действующий 3GPP механизм защиты SUPI (см. п. III-A), так и предложенная в [52] альтернатива на основе симметричного ключа скрывают в SUPI только часть, содержащую MSIN (см. п. II-B), в то время как MCC и MNC передаются в гостевую сеть по радиоканалу в открытом виде для корректной передачи SUCI к домашней сети. Кроме того, для повышения эффективности поиска операторы мобильной связи разделяют базу данных своих абонентов на поддомены [53]. Значит необходимо, чтобы SUCI доставлялся в нужный поддомен в рамках домашней сети. Как правило, для этого требуется передача в открытом виде от 1 до 3 цифр в MSIN после поля MCC/MNC в качестве информации о маршрутизации [54]. Указанная выше открытая информация доступна для злоумышленников и может быть использована ими при проведении атак.

Другое ограничение механизма защиты 3GPP и предложение [52] заключается в том, что гостевая сеть полностью зависит от домашней сети в вопросе расшифрования SUCI и связанных с ним целей законного перехвата LI (см. п. II-E)[55]. Несколько мер противодействия были предложены на конференциях 3GPP для решения этой проблемы [56], [57], [58], [59], [60]. Все эти предлагаемые контрмеры приводят к издержкам либо из-за дополнительных сообщений сигнализации, либо из-за требования введения новых параметров. Более того, ничто не мешает мобильному устройству и его домашней сети вступить в сговор, чтобы предоставить в гостевую сеть ложный SUPI. Для противодействия упомянутым ограничениям, X. Хан и B. Ниеми [61] предложили схему защиты 5G-SUPI, основанную на личностном шифровании [Identity based Encryption – IBE]. В этой схеме домашняя сеть действует в качестве генератора закрытого ключа. Схемы, основанные на личностном шифровании, по своей сути допускают частичное раскрытие MSIN и обеспечивают лучшие гарантии законного перехвата, поскольку гостевая сеть теперь может извлекать SUPI из SUCI независимо от домашней сети. Предложение [61] может рассматриваться как лучшая альтернатива существующему механизму 3GPP, хотя связанный с ним отзыв ключа довольно сложен. Однако, по сравнению с [52], он не является квантово-безопасным, кроме того, увеличение вычислительных и сигнальных издержек намного выше. Неясно также, может ли указанное решение использоваться в сочетании с предложением по защите от downgrade [62]. Учитывая эти ограничения, в долгосрочной перспективе более предпочтительным выглядит решение [52].

F. Защита от подмены базовых станций

Другим направлением, которое все еще требует дальнейших исследований, является защита от атак с использованием ложных базовых станций. Хотя 5G Release 15 предоставляет структуру для их выявления (см. п. III-K), ее статус на данный момент является только информативным, а предлагаемые механизмы носят общий характер и фокусируются только на аспектах обнаружения. Совсем недавно 3GPP начал комплексное исследование [63], которое сконцентрировано на повышении уровня защиты от ложных базовых станций для будущего 5G Release 16.

G. Постквантовая криптография в 5G

Постквантовым (криптографическим) алгоритмом будем называть криптографический алгоритм, для которого к настоящему моменту времени не предложено эффективных методов анализа с использованием квантового компьютера.

По прогнозам экспертов [64] до создания мощного квантового компьютера, способного за приемлемое время решать задачи по дешифрованию некоторых современных криптоалгоритмов, остается около 10-20 лет. Поскольку внедрение новых стандартов занимает продолжительное время, ITU [International Telecommunication

Union] уже сейчас подготовили рекомендации по использованию постквантовой криптографии в 5G.

Рекомендации основаны на следующих теоретических оценках относительно возможностей квантовых компьютеров по дешифрованию:

1) Стойкость алгоритмов симметричного шифрования, определяемая длиной ключа, уменьшается в 2 раза за счет использования квантового алгоритма Гровера. То есть, для нахождения 128-битного ключа потребуется перебор 2^{64} вариантов, а для нахождения 256-битного ключа - перебор 2^{128} вариантов.
2) Ассиметричные алгоритмы, основанные на проблемах факторизации (например, RSA) и дискретного логарифмирования (например, DSA, ECDSA) теряют свою стойкость и могут быть дешифрованы с использованием квантового алгоритма Шора за полиномиальное время.
3) Алгоритмы хэширования и их производные являются постквантовыми.

Для рассматриваемого в статье беспроводного участка сети рекомендации состоят в следующем:

1) В схеме ECIES (рисунок 5) в качестве алгоритма выработки общего ключа использовать схожие с алгоритмом Диффи-Хеллмана постквантовые алгоритмы, например алгоритм SIKE [supersingular isogeny key encapsulation].
2) В схеме генерации ключа K_{SEAF} (рисунок 4) в качестве корневого ключа K использовать 256-битный ключ и не урезать выходные 256-битные значения функции KDF. На практике некоторые уже выпущенные сим-карты хранят лишь 128-битный корневой ключ и не имеют возможностей расширить его до 256 бит. В этом случае для дополнения корневого ключа рекомендуется использовать ключ K_{SEAF_PRV}, выработанный во время предыдущего соединения. Если соединение устанавливается впервые, рекомендуется сгенерировать дополнительный ключ $K_{SEAF\_INITIAL}$.

H. Использование 256-битных симметричных алгоритмов в сетях 5G

Под *n-битным симметричным алгоритмом* мы будем понимать симметричный алгоритм шифрования с длиной ключа n бит. Постквантовая уязвимость, а также другие уязвимости [65], [66] делают актуальным вопрос о полном переходе на использование 256-битных симметричных алгоритмов шифрования (включая использование более длинных инициализационных векторов [IV] и имитовставок [MAC]) в системе безопасности сетей 5G. Вопрос о возможности такого перехода исследуется уже на протяжении нескольких лет. Однако, до сих пор нет ясности ни по требуемым критериям безопасности, ни по возможному влиянию использования таких алгоритмов на производительность абонентских устройств. Выделим основные моменты, связанные с таким переходом:

1) **Длина вектора инициализации (IV):** В существующих версиях 128-битных алгоритмов шифрования и контроля целостности в радиоинтерфейсе один и тот же ключ используется для шифрования большого числа блоков данных. Для формирования вектора инициализации используются следующие параметры: 32-битный счетчик (COUNT), 5-битный идентификатор несущей (BEARER), 1-бит – направление передачи (DIRECTION). Таким образом, задействовано всего 36 бит для формирования IV. Независимо от используемого алгоритма (128 или 256 бит) это позволяет злоумышленнику провести определенного вида атаки. Например, в работах [65] и [66] приводится пример мультицелевых [multi-target] атак при использовании короткого инициализационного вектора. Очевидно, что для усиления безопасности передаваемых данных по радиоинтерфейсу недостаточно просто заменить алгоритмы на 256-битные. Требуется также увеличивать размер инициализационных векторов, что, в свою очередь, потребует измения сетевых протоколов.
2) **Длина имитовставки (MAC):** Текущая длина имитовставки для защиты передаваемых сообщений в радиоинтерфейсе равна 32 битам. Очевидно, что атакующий может успешно предугадать значение MAC с вероятностью 2^{-32}. Чем большее число попыток будет совершено, тем выше шанс подобрать верное значение. На текущий момент такой уровень риска признается 3GPP приемлемым. Однако, в большинстве современных криптографических протоколов используется длина имитовставки 64 бита или более. В работе [67], приложение A.2 приведен более подробный анализ по данному вопросу.
3) **256-битные модификаций алгоритмов AES, SNOW3G, ZUC:** В 2019 году рабочей группой по безопасности 3GPP (TSG SA3) перед группой экспертов ETSI SAGE были поставлены вопросы об оценке 256-битных версий уже используемых в мобильных сетях алгоритмов шифрования AES, SNOW3G, ZUC (в терминах спецификаций – алгоритмы LTE: 128-EEA1, 128-EEA2, 128-EEA3, 128-EIA1, 128-EIA2, 128-EIA3). В настоящее время ведется активная работа в этом направлении. По алгоритму ZUC-256 есть определенные результаты. В документе [68] приводятся следующие особенности, на которые следует обратить внимание при использовании ZUC-256:

   - По сравнению с ZUC-128 были увеличены длина ключа до 256 бит и длина инициализационного вектора до 184 бит. При этом основной элемент криптоалгоритма, вырабатывающий ключевой поток (keystream) остается тем же самым. Таким образом, подаваемые на вход keystream входные данные сначала сжимаются до значений ZUC-128, а затем конкатенируются. Такой подход не является рациональным с точки зрения производительности, однако, позволяет не производить замену оборудования.
   - ZUC-256 был представлен в 2018 году [69]. На текущий момент в известных публикациях не представлено каких-либо практически реализуемых атак на него. Однако, отмечается, что в алгоритме ZUC-256 отсутствуют ясные и рациональные пояснения от разработчиков, относительно некоторых архитектурных реше-

ний. Такой подход противоречит принципам «отсутствия козыря в рукаве» группы ETSI SAGE (да и вообще всего криптографического сообщества).

- Есть обоснованные сомнения в достаточной производительности при вычислении имитовставки (MAC). Поскольку заявленная скорости передачи данных в сетях 5G может достигать 20 Гб/с, данный вопрос требует существенной проработки.

V. Связанные работы

В таблице IV представлена сводка соответствующей литературы, в которой рассматриваются вопросы безопасности и конфиденциальности в сетях 5G и им подобных. Здесь мы кратко обсудим работу, проделанную в этих публикациях, а также оставим ссылки для возможности дальнейшего ознакомления.

Д. Руппрехт и соавторы [70] классифицировали и систематизировали атаки в существующих поколениях мобильной связи (GSM / UMTS / LTE) по их цели, воздействию и возможностям атакующего. Они также наметили будущие направления исследований для сетей 5G на основе этих существующих проблем безопасности и конфиденциальности. Основное различие между [70] и данной работой заключается в том, что мы также рассматриваем 5G Release 15, тогда как анализ [70] ограничен только предыдущими поколениями. Р. Турани и соавторы [71] проанализировали безопасность, конфиденциальность и контроль доступа в рамках информационной сети [Information-centric Networking – ICN]. ICN – это сетевая парадигма, которая фокусируется на содержании трафика, а не на его происхождении; весьма сходная концепция [79] с концепцией сетевого разделения [*network slicing*, см. Приложение] в 5G.

В [72] и [73] проанализированы общие угрозы безопасности и конфиденциальности для сетей 5G и предложены возможные решения этих угроз на основе опубликованной литературы. Обе эти работы вышли до публикации стандарта 5G. М. Ферраг и др. [74] представили обзор существующих схем аутентификации и обеспечения конфиденциальности для мобильных сетей LTE и 5G. Они представили классификацию моделей угроз в сотовых сетях 4G и 5G по четырем категориям: атаки на конфиденциальность, атаки на целостность, атаки на противодействие возможностям абонента и атаки на процедуру аутентификации. В [74] также представлена классификация соответствующих контрмер по трем типам категорий: криптографические методы, человеческие факторы и методы обнаружения вторжений.

П. Гандотра и Р. Джа [75] представили обзор различных энергоэффективных сценариев для экологически чистой связи в 5G и связанных с ними аспектов безопасности. Для увеличения срока службы батарей пользовательских терминалов [75] предложили передавать информацию путем организации радио-релейной связи и изучили возникающие при этом угрозы безопасности и связанные с ними контрмеры. В [75] не рассматриваются вопросы конфиденциальности в сетях 5G. В [76] исследованы аспекты, связанные с переходом инфраструктуры мобильной сети LTE и 5G на программно-определяемые сети [Software Defined Networking – SDN] и виртуализацию сетевых функций [Network Function Virtualization – NFV]. Кроме того были рассмотрены вопросы безопасности при осуществлении таких переходов и предложены решения на основе SDN.

Г. Чоудри и В. Шарма [77] рассмотрели недавние компьютерные парадигмы как альтернативные механизмы повышения безопасности 5G. Эта работа фокусируется на возможности каталитических и осмотических вычислений в сетях 5G. Х. Хан и соавторы [78] представили обзор безопасности и конфиденциальности 5G, однако указанная работа была составлена до публикации 5G Release 15.

П. К. Накарми и соавторы [80] представили сетевую систему обнаружения ложных базовых станций, не требующую модификации мобильных устройств и позволяющую в полной мере использовать преимущества топологии сети и информацию о конфигурации, доступную для операторов. Представленный в статье подход был одобрен организацией 3GPP.

Джефф Цичонски [81] представил обзор решений, принимаемых в стандартах 5G с целью повышения уровня конфиденциальности абонента. Рассмотрены решения по модернизации протокола аутентификации, защите идентификатора пользователя SUPI, контроля целостности пользовательского трафика, обнаружению ложных базовых станций, модернизации инфраструктуры и др.

Приложение «Работа с сетью в 5G»

Расслоение сети [Network slicing] – это форма архитектуры виртуальной сети, использующая те же принципы, что и программно-определяемые сети [SDN] и виртуализация сетевых функций [NFV] (см. раздел V, [76]) в фиксированных сетях. SDN и NFV обеспечивают большую гибкость сети, позволяя разделить традиционные сетевые архитектуры на виртуальные элементы, которые можно связать с помощью программного обеспечения. Network slicing позволяет создавать несколько виртуальных сетей поверх общей физической инфраструктуры. Виртуальные сети затем настраиваются в соответствии с конкретными потребностями приложений, услуг, устройств, клиентов или операторов. В случае 5G одна физическая сеть разделена на несколько виртуальных сетей, которые могут поддерживать разные сети радиодоступа [Radio Access Networks - RAN] или разные типы услуг, работающие в одной RAN.

Network slicing обеспечивает гибкость сетей 5G, оптимизируя как использование инфраструктуры, так и распределение ресурсов, что обеспечивает более высокую эффективность использования энергии и затрат по сравнению с прежними сетями мобильной связи.

VI. Заключение

Сети 5G открывают огромные перспективы, преобразуя все от домашних приборов до искусственного интеллекта в медицине. Двигаясь в будущем к глобальной связности, необходимо внимательно относиться к вопросам безопасности и конфиденциальности передаваемой информации.

В результате исследования, проведенного в обзоре, выделены некоторые угрозы конфиденциальности, которые

Таблица IV
Важнейшие недавние публикации по вопросам безопасности и конфиденциальности в 5G.

Ссылка	Год публикации	Область применения	Основной вклад	Актуальность для конфиденциальности абонента 5G
[70]	2018	2G, 3G, 4G	Обзор существующей литературы по атакам в предыдущих поколениях (GSM/UMTS/LTE) мобильной телефонии.	Предложены направления исследований для повышения конфиденциальности в сетях 5G.
[71]	2018	ICN	Обзор на тему конфиденциальности и контроля доступа в информационных сетях.	Рассмотрены атаки на конфиденциальность, применимые в рамках концепции сетей 5G.
[72], [73]	2017 / 2018	5G	Обзор проблем и решений в области безопасности сетей 5G.	Обсуждаются проблемы конфиденциальности в 5G с точки зрения пользователя.
[74]	2018	4G, 5G	Исследование существующих схем, решающих задачи конфединиальности и аутентичности в сетях 4G и 5G.	Обсуждаются атаки на конфиденциальность в сетях 5G и даются рекомендации по дальнейшим исследованиям.
[75]	2017	5G	Обзор на тему безопасных коммуникаций и связанных задачах обеспечения безопасности в сетях 5G.	Рассматриваются вопросы конфиденциальности различных технологий сетей 5G (межмашинная связь (M2M) и т.д.)
[76]	2017	SDN	Обзор проблем и задач, возникающих при проектировании сетей 5G на основе SDN.	Рассматриваются решения вопросов безопасности на основе программно определяемых сетей для 4G и 5G.
[77]	2019	5G	Обзор безопасности альтернативных вычислительных парадигм для сетей 5G.	Рассматривается применимость альтернативных вычислительных парадигм для повышения конфиденциальности пользователей.
[78]	2019	5G	Обзор на тему безопасности и приватности в сетях 5G.	Рассмотрение футуристических угроз безопасности в сетях 5G.
[80]	2021	5G	Обнаружение ложных базовых станций.	Предлагается система обнаружения ложных базовых станций, не требующая модификации мобильных устройств.
[81]	2020	5G	Обзор на тему безопасности и приватности в сетях 5G.	Рассматриваются решения, принимаемые в стандартах 5G с целью повышения уровня конфиденциальности абонента.

остаются нерешенными в последних спецификациях 5G. Исследование также позволяет сделать вывод, что для обеспечения надежной конфиденциальности абонента в 5G необходимы новые и более строгие механизмы ее защиты. В частности, на основе [5] и нашего обзора, могут быть предложены следующие рекомендации:

- Для постквантовой безопасности важно заменить существующий механизм защиты идентификации абонента, являющийся единственным механизмом на основе открытого ключа в 5G, альтернативным вариантом на основе симметричного шифрования [52] с использованием алгоритмов с 256-битными ключами. Для защиты от *downgrade*-атак желательно объединить это решение с решением [62].
- Для устранения уязвимостей протокола AKA и воспрепятствования другим новым атакам необходимо принять исправление для сообщений о сбоях 5G-AKA, показанное на рисунке 10(c).
- Как показывает опыт, большинство представителей отрасли не руководствуются стандартами, изданными в виде рекомендаций, поэтому наличие системы обнаружения ложных базовых станций 5G Release 15 необходимо сделать требованием, а не рекомендацией.

Библиография

[1] G. Greenwald, “NSA collecting phone records of millions of Verizon customers daily”, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, Jun 2013.

[2] 3rd Generation Partnership Project, “Security Architecture and Procedures for 5G Systems (3GPP TS 33.501 Version 15.0.0 Release 15)”, Mar 2018.

[3] 3rd Generation Partnership Project, “3G Security; Security Architecture (3GPP TS 33.102 Version 15.0.0 Release 15)”, Jun 2018.

[4] 3rd Generation Partnership Project, “Study on the security aspects of the next generation system (3GPP TR 33.899 Version 1.3.0 Release 14)”, Aug 2017.

[5] Haibat Khan, Keith M. Martin, A Survey of Subscription Privacy on the 5G Radio Interface - The Past, Present and Future, Computer Science IACR Cryptol. ePrint Arch., 2020, https://eprint.iacr.org/2020/101.pdf.

[6] N. Husted and S. Myers, “Mobile Location Tracking in Metro Areas: Malnets and Others”, in Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010, E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds. ACM, 2010, pp. 85–96.

[7] M. Jakobsson and S. Wetzel, “Security Weaknesses in Bluetooth”, in Topics in Cryptology - CT-RSA 2001, The Cryptographer’s Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings, ser. Lecture Notes in Computer Science, D. Naccache, Ed., vol. 2020. Springer, 2001, pp. 176–191.

[8] 3rd Generation Partnership Project, “System Architecture for the 5G System (3GPP TS 23.501 Version 15.1.0 Release 15)”, Mar 2018.

[9] 3rd Generation Partnership Project, “Mobile Application Part (MAP)Specification (3GPP TS 29.002 Version 15.3.0 Release 15)”, Mar 2018.

[10] R. F. Olimid and S. F. Mjølsnes, “On Low-Cost Privacy Exposure Attacks in LTE Mobile Communication”, Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science, vol. 18, pp. 361–370, 2017.

[11] 3rd Generation Partnership Project, “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220 Version 15.2.0 Release 15)”, June 2018.

[12] C. Paget, “Practical Cellphone Spying”, Def Con, vol. 18, 2010.

[13] S. F. Mjølsnes and R. F. Olimid, “Easy 4G/LTE IMSI Catchers for Non-Programmers”, in Computer Network Security - 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings, ser. Lecture Notes in Computer Science, J. Rak, J. Bay, I. V. Kotenko, L. J. Popyack, V. A. Skormin, and K. Szczypiorski, Eds., vol. 10446. Springer, 2017, pp. 235–246.

[14] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. R. Weippl, “IMSI-catch me if you can: IMSI-catcher-catchers”, in Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC 2014, New Orleans, LA, USA, December 8-12, 2014, C. N. P. Jr., A. Hahn, K. R. B. Butler, and M. Sherr, Eds. ACM, 2014, pp. 246–255.

[15] A. Dabrowski, G. Petzl, and E. R. Weippl, “The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection”, in Research in Attacks, Intrusions, and Defenses - 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings, ser. Lecture Notes in Computer Science, F. Monrose, M. Dacier, G. Blanc, and J. García-Alfaro, Eds., vol. 9854. Springer, 2016, pp. 279–302.

[16] K. Nohl, “Mobile Self-defense”, in 31st Chaos Communication Congress 31C3, 2014.

[17] A. Lilly, “IMSI catchers: hacking mobile communications”, Network Security, vol. 2017, no. 2, pp. 5–7, 2017.

[18] D. Fox, “Der imsi-catcher”, Datenschutz und Datensicherheit, vol. 26, no. 4, 2002.

[19] N. J. Croft, “On forensics: A silent SMS attack”, in 2012 Information Security for South Africa, Balalaika Hotel, Sandton, Johannesburg, South Africa, August 15-17, 2012, H. S. Venter, M. Loock, and M. Coetzee, Eds. IEEE, 2012, pp. 1–4.

[20] M. Arapinis, L. I. Mancini, E. Ritter, and M. D. Ryan, “Analysis of Privacy in Mobile Telephony Systems”, Int. J. Inf. Sec., vol. 16, no. 5, pp. 491–523, 2017.

[21] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, “Practical attacks against privacy and availability in 4g/lte mobile communication systems”, in 23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. The Internet Society, 2016.

[22] D. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, “Location Leaks on the GSM Air Interface”, in 19th Annual Network & Distributed System Security Symposium, ISOC-NDSS, 2012.

[23] K. Nohl and S. Munaut, “Wideband GSM Sniffing”, in 27th Chaos Communication Conference, 2010.

[24] B. Hong, S. Bae, and Y. Kim, “GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier”, in 25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018. The Internet Society, 2018.

[25] M. Arapinis, L. I. Mancini, E. Ritter, and M. Ryan, “Privacy through Pseudonymity in Mobile Telephony Systems”, in 21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014. The Internet Society, 2014.

[26] D. Forsberg, L. Huang, T. Kashima, and S. Alanärä, “Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface”, in Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2007, 3-7 September 2007, Athens, Greece. IEEE, 2007, pp. 1–5.

[27] M. Arapinis, L. I. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, “New Privacy Issues in Mobile Telephony: Fix and Verification”, in the ACM Conference on Computer and Communications Security, CCS’12, Raleigh, NC, USA, October 16-18, 2012, T. Yu, G. Danezis, and V. D. Gligor, Eds. ACM, 2012, pp. 205–216.

[28] C. Sørseth, S. X. Zhou, S. F. Mjølsnes, and R. F. Olimid, “Experimental Analysis of Subscribers’ Privacy Exposure by LTE Paging”, Wireless Personal Communications, pp. 1–19, 2018.

[29] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, “Privacy attacks to the 4g and 5g cellular paging protocols using side channel information”, in 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019. The Internet Society, 2019.

[30] R. Borgaonkar, L. Hirshi, S. Park, A. Shaik, A. Martin, and J.-P. Seifert, “New Adventures in Spying 3G & 4G Users: Locate, Track, Monitor”, in Blackhat, Las Vegas, USA 2017, July 2017.

[31] A. Kunz and X. Zhang, “New 3GPP Security Features in 5G Phase 1”, in 2018 IEEE Conference on Standards for Communications and Networking, CSCN 2018, Paris, France, October 29-31, 2018. IEEE, 2018, pp. 1–6.

[32] A. R. Prasad, S. Arumugam, B. Sheeba, and A. Zugenmaier, “3GPP 5G Security”, Journal of ICT Standardization, vol. 6, no. 1, pp. 137–158, 2018.

[33] 3rd Generation Partnership Project, “NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state (3GPP TS 38.304 Version 15.5.0 Release 15)”, Sep 2019.

[34] 3rd Generation Partnership Project, “NR; Radio Resource Control (RRC) protocol specification (3GPP TS 38.331 Version 15.6.0 Release 15)”, Jun 2019.

[35] V. Shoup, “A proposal for an ISO standard for public key encryption”, IACR Cryptology ePrint Archive, vol. 2001, p. 112, 2001.

[36] D. Hankerson and A. Menezes, “Elliptic Curve Cryptography”, in Encyclopedia of Cryptography and Security, 2nd Ed., H. C. A. van Tilborg and S. Jajodia, Eds. Springer, 2011, p. 397.

[37] SECG SEC 1, “Recommended Elliptic Curve Cryptography, Version 2.0”, http://www.secg.org/sec1-v2.pdf, 2009.

[38] M. Khan, K. Järvinen, P. Ginzboorg, and V. Niemi, “On Desynchronization of User Pseudonyms in Mobile Networks”, in Information Systems Security - 13th International Conference, ICISS 2017, Mumbai, India, December 16-20, 2017, Proceedings, ser. Lecture Notes in Computer Science, R. K. Shyamasundar, V. Singh, and J. Vaidya, Eds., vol. 10717. Springer, 2017, pp. 347–366.

[39] 3rd Generation Partnership Project, “Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 16) (3GPP TS 24.301 Version 16.2.0 Release 16)”, Sep 2019.

[40] 3rd Generation Partnership Project, “Radio Resource Control (RRC); Protocol specification (3GPP TS 25.331 Version 15.4.0 Release 15)”, Sep 2018.

[41] 3rd Generation Partnership Project, “Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (3GPP TS 36.331 Version 15.6.0 Release 15)”, Jun 2019.

[42] J. J. Caffery and G. L. Stuber, “Overview of radiolocation in CDMA cellular systems”, IEEE Communications Magazine, vol. 36, no. 4, pp. 38–45, 1998.

[43] 3rd Generation Partnership Project, “NG-RAN; NG Application Protocol (NGAP)(3GPP TS 38.413 Version 15.3.0 Release 15)”, Mar 2019.

[44] M. Lee, N. P. Smart, B. Warinschi, and G. J. Watson, “Anonymity guarantees of the UMTS/LTE authentication and connection protocol”, Int. J. Inf. Sec., vol. 13, no. 6, pp. 513–527, 2014.

[45] B. Blanchet, “Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif”, in Foundations of Security Analysis and Design VII - FOSAD 2012/2013 Tutorial Lectures, ser. Lecture Notes in Computer Science, A. Aldini, J. López, and F. Martinelli, Eds., vol. 8604. Springer, 2013, pp. 54–87.

[46] P. Fouque, C. Onete, and B. Richard, “Achieving Better Privacy for the 3GPP AKA Protocol”, PoPETs, vol. 2016, no. 4, pp. 255–275, 2016.

[47] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols”, PoPETs, vol. 2019, no. 3, pp. 108–127, 2019.

[48] H. Khan and K. M. Martin, “On the Efficacy of New Privacy Attacks against 5G AKA”, in Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2: SECRYPT, Prague, Czech Republic, July 26-28, 2019., M. S. Obaidat and P. Samarati, Eds. SciTePress, 2019, pp. 431–438.

[49] ETSI-SAGE, “First response on ECIES for concealing IMSI or SUPI”, https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=832160, Oct 2017.

[50] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring”, in 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994. IEEE Computer Society, 1994, pp. 124–134.

[51] X. Hu, C. Liu, S. Liu, W. You, Y. Li, and Y. Zhao, “A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security”, IEEE Access, vol. 7, pp. 125, 424–125, 441, 2019.

[52] H. Khan, B. Dowling, and K. M. Martin, “Identity Confidentiality in 5G Mobile Telephony Systems”, in Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings, ser. Lecture Notes in Computer Science, C. Cremers and A. Lehmann, Eds., vol. 11322. Springer, 2018, pp. 120–142.

[53] Vodafone, “Discussion paper on embedded routing information in SUCI”, https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_90Bis_SanDiego/docs/S3-180761.zip, Mar 2019.

[54] Vodafone, “pCR to 33.501 - addition of routing information into SUCI”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180763.zip, Mar 2019.

[55] M. Khan, V. Niemi, and P. Ginzboorg, “IMSI-based Routing and Identity Privacy in 5G”, in Proceedings of the 22nd Conference of Open Innovations Association FRUCT, Jyvaskyla, Finland, 2018.

[56] CATT, “Solution for SUPI privacy and LI requirement”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_SanDiego/Docs/S3-180591.zip, Mar 2019.

[57] KPN, N. DOCOMO, DT, BT, and NEC, “Proposal and Discussion for Privacy and LI Solution”, https://www.3gpp.org/ftp/TSG_SA/WG3_-Security/TSGS3_90Bis _SanDiego/Docs/S3-180684.zip, Mar 2019.

[58] Nokia, “Discussion on LI conformity by verification hash method”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis _SanDiego/Docs/S3-180768.zip, Mar 2019.

[59] Nokia, Gemalto, and IDEMIA, “SUCI and LI – verification hash integrated in 5G AKA”, https://www.3gpp.org/ftp/TSG_SA/WG3_-Security/TSGS3 _90Bis_SanDiego/Docs/S3-180769.zip, Mar 2019.

[60] Ericsson, Q. Incorporated, Samsung, Huawei, Hisilicon, and Intel, “SUCI and LI - verification hash integrated in 5G AKA”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_-SanDiego/Docs/S3-180818.zip, Mar 2019.

[61] M. Khan and V. Niemi, “Concealing IMSI in 5G Network Using Identity Based Encryption”, in Network and System Security - 11th International Conference, NSS 2017, Helsinki, Finland, August 21-23, 2017, Proceedings, ser. Lecture Notes in Computer Science, Z. Yan, R. Molva, W. Mazurczyk, and R. Kantola, Eds., vol. 10394. Springer, 2017, pp. 544–554.

[62] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi, “Defeating the Downgrade Attack on Identity Privacy in 5G”, in Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings, ser. Lecture Notes in Computer Science, C. Cremers and A. Lehmann, Eds., vol. 11322. Springer, 2018, pp. 95–119.

[63] 3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; Study on 5G Security Enhancement against False Base Stations Version 0.6.0 (Release 16)”, Aug 2019.

[64] Draft Recommendation ITU-T X.5GSec-q: Security guidelines for applying quantum-safe algorithms in 5G systems, https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3089.

[65] Jin Hong & Palesh Sarkar, Rediscovery of Time Memory Tradeoffs, https://eprint.iacr.org/2005/090.

[66] Orr Dunkelman & Nathan Keller, Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers, https://eprint.iacr.org/2008/311.

[67] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf.

[68] ETSI SAGE. Observations on ZUC-256, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_99e/docs /S3-200930.zip.

[69] The ZUC-256 Stream Cipher, http://www.is.cas.cn/ztzl2016 /zouchongzhi/201801/W020180126529970733243.pdf.

[70] D. Rupprecht, A. Dabrowski, T. Holz, E. R. Weippl, and C. Pöpper, “On security research towards future mobile network generations”, IEEE Communications Surveys and Tutorials, vol. 20, no. 3, pp. 2518–2542, 2018.

[71] R. Tourani, S. Misra, T. Mick, and G. Panwar, “Security, Privacy, and Access Control in Information-Centric Networking: A Survey”, IEEE Communications Surveys and Tutorials, vol. 20, no. 1, pp. 566–600, 2018.

[72] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. V. Gurtov, “5G security: Analysis of threats and solutions”, in IEEE Conference on Standards for Communications and Networking, CSCN 2017, Helsinki, Finland, September 18-20, 2017. IEEE, 2017, pp. 193–199.

[73] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, “Overview of 5G Security Challenges and Solutions”, IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.

[74] M. A. Ferrag, L. A. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, “Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes”, J. Network and Computer Applications, vol. 101, pp. 55–82, 2018.

[75] P. Gandotra and R. K. Jha, “A survey on green communication and security challenges in 5G wireless communication networks”, J. Network and Computer Applications, vol. 96, pp. 39–61, 2017.

[76] A. K. Rangisetti and B. R. Tamma, “Software Defined Wireless Networks: A Survey of Issues and Solutions”, Wireless Personal Communications, vol. 97, no. 4, pp. 6019–6053, 2017.

[77] G. Choudhary and V. Sharma, “A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks”, CoRR, vol. abs/1909.08844, 2019.

[78] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, “A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions”, IEEE Communications Surveys & Tutorials, 2019.

[79] R. Ravindran, A. Chakraborti, S. O. Amin, A. Azgin, and G. Wang, “5G-ICN: Delivering ICN Services over 5G Using Network Slicing”, IEEE Communications Magazine, vol. 55, no. 5, pp. 101–107, 2017.

[80] Prajwol Kumar Nakarmi, Mehmet Akif Ersoy, Elif Ustundag Soykan, Karl Norrman, “Murat: Multi-RAT False Base Station Detector”, arXiv:2102.08780, 2021, https://arxiv.org/abs/2102.08780.

[81] J. Cichonski, PSCR 2020_5G Security Evolution not Revolution, PSCR Stakeholder Meeting 2020: The Digital Experience, Boulder, CO, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_-id=931275.

A subscriber's Privacy on the 5G Radio Interface

V. Belsky, A. Drynkin, S. Davydov

***Abstract*—The issues of subscriber's privacy in mobile phone systems are currently very interesting due to the expected growth of new communication services (virtual reality, Machine-Type Communications – MTC, Vehicle-to-Everything – V2X, Internet of Things-IoT, etc.) provided by 5G networks. The survey addresses security issues in 5G systems. Release 15 is selected as the main release of the 5G specifications, as well as added some information from Release 16 up to Stage 3. Only the wireless component (the area between the base station and the mobile equipment) of 5G networks is considered in our survey. Despite the fact that 5G networks offer additional security mechanisms, the presented survey demonstrates that many significant problems remain in this area. The paper contains the analysis of security issues in previous mobile phone generations and the survey of countermeasures that improve security in the 5G standard. In addition, we discuss some new types of attacks to 5G Release 15 specifications and suggest some methods to avoid some significant security and privacy issues in 5G networks.**

***Keywords*—5G, anonymity, GSM, LTE, mobile networks, confidentiality, privacy, UMTS**

References

[1] G. Greenwald, "NSA collecting phone records of millions of Verizon customers daily", https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, Jun 2013.

[2] 3rd Generation Partnership Project, "Security Architecture and Procedures for 5G Systems (3GPP TS 33.501 Version 15.0.0 Release 15)", Mar 2018.

[3] 3rd Generation Partnership Project, "3G Security; Security Architecture (3GPP TS 33.102 Version 15.0.0 Release 15)", Jun 2018.

[4] 3rd Generation Partnership Project, "Study on the security aspects of the next generation system (3GPP TR 33.899 Version 1.3.0 Release 14)", Aug 2017.

[5] Haibat Khan, Keith M. Martin, A Survey of Subscription Privacy on the 5G Radio Interface - The Past, Present and Future, Computer Science IACR Cryptol. ePrint Arch., 2020, https://eprint.iacr.org/2020/101.pdf.

[6] N. Husted and S. Myers, "Mobile Location Tracking in Metro Areas: Malnets and Others", in Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010, E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds. ACM, 2010, pp. 85–96.

[7] M. Jakobsson and S. Wetzel, "Security Weaknesses in Bluetooth", in Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings, ser. Lecture Notes in Computer Science, D. Naccache, Ed., vol. 2020. Springer, 2001, pp. 176–191.

[8] 3rd Generation Partnership Project, "System Architecture for the 5G System (3GPP TS 23.501 Version 15.1.0 Release 15)", Mar 2018.

[9] 3rd Generation Partnership Project, "Mobile Application Part (MAP)Specification (3GPP TS 29.002 Version 15.3.0 Release 15)", Mar 2018.

[10] R. F. Olimid and S. F. Mjølsnes, "On Low-Cost Privacy Exposure Attacks in LTE Mobile Communication", Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science, vol. 18, pp. 361–370, 2017.

[11] 3rd Generation Partnership Project, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220 Version 15.2.0 Release 15)", June 2018.

[12] C. Paget, "Practical Cellphone Spying", Def Con, vol. 18, 2010.

[13] S. F. Mjølsnes and R. F. Olimid, "Easy 4G/LTE IMSI Catchers for Non-Programmers", in Computer Network Security - 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings, ser. Lecture Notes in Computer Science, J. Rak, J. Bay, I. V. Kotenko, L. J. Popyack, V. A. Skormin, and K. Szczypiorski, Eds., vol. 10446. Springer, 2017, pp. 235–246.

[14] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. R. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers", in Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC 2014, New Orleans, LA, USA, December 8-12, 2014, C. N. P. Jr., A. Hahn, K. R. B. Butler, and M. Sherr, Eds. ACM, 2014, pp. 246–255.

[15] A. Dabrowski, G. Petzl, and E. R. Weippl, "The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection", in Research in Attacks, Intrusions, and Defenses - 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings, ser. Lecture Notes in Computer Science, F. Monrose, M. Dacier, G. Blanc, and J. García-Alfaro, Eds., vol. 9854. Springer, 2016, pp. 279–302.

[16] K. Nohl, "Mobile Self-defense", in 31st Chaos Communication Congress 31C3, 2014.

[17] A. Lilly, "IMSI catchers: hacking mobile communications", Network Security, vol. 2017, no. 2, pp. 5–7, 2017.

[18] D. Fox, "Der imsi-catcher", Datenschutz und Datensicherheit, vol. 26, no. 4, 2002.

[19] N. J. Croft, "On forensics: A silent SMS attack", in 2012 Information Security for South Africa, Balalaika Hotel, Sandton, Johannesburg, South Africa, August 15-17, 2012, H. S. Venter, M. Loock, and M. Coetzee, Eds. IEEE, 2012, pp. 1–4.

[20] M. Arapinis, L. I. Mancini, E. Ritter, and M. D. Ryan, "Analysis of Privacy in Mobile Telephony Systems", Int. J. Inf. Sec., vol. 16, no. 5, pp. 491–523, 2017.

[21] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4g/lte mobile communication systems", in 23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. The Internet Society, 2016.

[22] D. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, "Location Leaks on the GSM Air Interface", in 19th Annual Network & Distributed System Security Symposium, ISOC-NDSS, 2012.

[23] K. Nohl and S. Munaut, "Wideband GSM Sniffing", in 27th Chaos Communication Conference, 2010.

[24] B. Hong, S. Bae, and Y. Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier", in 25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018. The Internet Society, 2018.

[25] M. Arapinis, L. I. Mancini, E. Ritter, and M. Ryan, "Privacy through Pseudonymity in Mobile Telephony Systems", in 21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014. The Internet Society, 2014.

[26] D. Forsberg, L. Huang, T. Kashima, and S. Alanärä, "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface", in Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2007, 3-7 September 2007, Athens, Greece. IEEE, 2007, pp. 1–5.

[27] M. Arapinis, L. I. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, "New Privacy Issues in Mobile Telephony: Fix and Verification", in the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012, T. Yu, G. Danezis, and V. D. Gligor, Eds. ACM, 2012, pp. 205–216.

[28] C. Sørseth, S. X. Zhou, S. F. Mjølsnes, and R. F. Olimid, "Experimental Analysis of Subscribers' Privacy Exposure by LTE Paging", Wireless Personal Communications, pp. 1–19, 2018.

[29] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4g and 5g cellular paging protocols using side channel information", in 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019. The Internet Society, 2019.

[30] R. Borgaonkar, L. Hirshi, S. Park, A. Shaik, A. Martin, and J.-P. Seifert, "New Adventures in Spying 3G & 4G Users: Locate, Track, Monitor", in Blackhat, Las Vegas, USA 2017, July 2017.

[31] A. Kunz and X. Zhang, "New 3GPP Security Features in 5G Phase 1", in 2018 IEEE Conference on Standards for Communications and

Networking, CSCN 2018, Paris, France, October 29-31, 2018. IEEE, 2018, pp. 1–6.

[32] A. R. Prasad, S. Arumugam, B. Sheeba, and A. Zugenmaier, “3GPP 5G Security”, Journal of ICT Standardization, vol. 6, no. 1, pp. 137–158, 2018.

[33] 3rd Generation Partnership Project, “NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state (3GPP TS 38.304 Version 15.5.0 Release 15)”, Sep 2019.

[34] 3rd Generation Partnership Project, “NR; Radio Resource Control (RRC) protocol specification (3GPP TS 38.331 Version 15.6.0 Release 15)”, Jun 2019.

[35] V. Shoup, “A proposal for an ISO standard for public key encryption”, IACR Cryptology ePrint Archive, vol. 2001, p. 112, 2001.

[36] D. Hankerson and A. Menezes, “Elliptic Curve Cryptography”, in Encyclopedia of Cryptography and Security, 2nd Ed., H. C. A. van Tilborg and S. Jajodia, Eds. Springer, 2011, p. 397.

[37] SECG SEC 1, “Recommended Elliptic Curve Cryptography, Version 2.0”, http://www.secg.org/sec1-v2.pdf, 2009.

[38] M. Khan, K. Järvinen, P. Ginzboorg, and V. Niemi, “On Desynchronization of User Pseudonyms in Mobile Networks”, in Information Systems Security - 13th International Conference, ICISS 2017, Mumbai, India, December 16-20, 2017, Proceedings, ser. Lecture Notes in Computer Science, R. K. Shyamasundar, V. Singh, and J. Vaidya, Eds., vol. 10717. Springer, 2017, pp. 347–366.

[39] 3rd Generation Partnership Project, “Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 16) (3GPP TS 24.301 Version 16.2.0 Release 16)”, Sep 2019.

[40] 3rd Generation Partnership Project, “Radio Resource Control (RRC); Protocol specification (3GPP TS 25.331 Version 15.4.0 Release 15)”, Sep 2018.

[41] 3rd Generation Partnership Project, “Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (3GPP TS 36.331 Version 15.6.0 Release 15)”, Jun 2019.

[42] J. J. Caffery and G. L. Stuber, “Overview of radiolocation in CDMA cellular systems”, IEEE Communications Magazine, vol. 36, no. 4, pp. 38–45, 1998.

[43] 3rd Generation Partnership Project, “NG-RAN; NG Application Protocol (NGAP)(3GPP TS 38.413 Version 15.3.0 Release 15)”, Mar 2019.

[44] M. Lee, N. P. Smart, B. Warinschi, and G. J. Watson, “Anonymity guarantees of the UMTS/LTE authentication and connection protocol”, Int. J. Inf. Sec., vol. 13, no. 6, pp. 513–527, 2014.

[45] B. Blanchet, “Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif”, in Foundations of Security Analysis and Design VII - FOSAD 2012/2013 Tutorial Lectures, ser. Lecture Notes in Computer Science, A. Aldini, J. López, and F. Martinelli, Eds., vol. 8604. Springer, 2013, pp. 54–87.

[46] P. Fouque, C. Onete, and B. Richard, “Achieving Better Privacy for the 3GPP AKA Protocol”, PoPETs, vol. 2016, no. 4, pp. 255–275, 2016.

[47] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols”, PoPETs, vol. 2019, no. 3, pp. 108–127, 2019.

[48] H. Khan and K. M. Martin, “On the Efficacy of New Privacy Attacks against 5G AKA”, in Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2: SECRYPT, Prague, Czech Republic, July 26-28, 2019., M. S. Obaidat and P. Samarati, Eds. SciTePress, 2019, pp. 431–438.

[49] ETSI-SAGE, “First response on ECIES for concealing IMSI or SUPI”, https://portal.3gpp.org/ngppapp/ CreateTdoc.aspx?mode=view&contributionId=832160, Oct 2017.

[50] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring”, in 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994. IEEE Computer Society, 1994, pp. 124–134.

[51] X. Hu, C. Liu, S. Liu, W. You, Y. Li, and Y. Zhao, “A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security”, IEEE Access, vol. 7, pp. 125, 424–125, 441, 2019.

[52] H. Khan, B. Dowling, and K. M. Martin, “Identity Confidentiality in 5G Mobile Telephony Systems”, in Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings, ser. Lecture Notes in Computer Science, C. Cremers and A. Lehmann, Eds., vol. 11322. Springer, 2018, pp. 120–142.

[53] Vodafone, “Discussion paper on embedded routing information in SUCI”, https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_90Bis _SanDiego/docs/S3-180761.zip, Mar 2019.

[54] Vodafone, “pCR to 33.501 - addition of routing information into SUCI”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_-90Bis _SanDiego/Docs/S3-180763.zip, Mar 2019.

[55] M. Khan, V. Niemi, and P. Ginzboorg, “IMSI-based Routing and Identity Privacy in 5G”, in Proceedings of the 22nd Conference of Open Innovations Association FRUCT, Jyvaskyla, Finland, 2018.

[56] CATT, “Solution for SUPI privacy and LI requirement”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis _SanDiego/Docs/S3-180591.zip, Mar 2019.

[57] KPN, N. DOCOMO, DT, BT, and NEC, “Proposal and Discussion for Privacy and LI Solution”, https://www.3gpp.org/ftp/TSG_SA/WG3_-Security/TSGS3_90Bis _SanDiego/Docs/S3-180684.zip, Mar 2019.

[58] Nokia, “Discussion on LI conformity by verification hash method”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis _SanDiego/Docs/S3-180768.zip, Mar 2019.

[59] Nokia, Gemalto, and IDEMIA, “SUCI and LI – verification hash integrated in 5G AKA”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3 _90Bis_SanDiego/Docs/S3-180769.zip, Mar 2019.

[60] Ericsson, Q. Incorporated, Samsung, Huawei, Hisilicon, and Intel, “SUCI and LI - verification hash integrated in 5G AKA”, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_90Bis_-SanDiego/Docs/S3-180818.zip, Mar 2019.

[61] M. Khan and V. Niemi, “Concealing IMSI in 5G Network Using Identity Based Encryption”, in Network and System Security - 11th International Conference, NSS 2017, Helsinki, Finland, August 21-23, 2017, Proceedings, ser. Lecture Notes in Computer Science, Z. Yan, R. Molva, W. Mazurczyk, and R. Kantola, Eds., vol. 10394. Springer, 2017, pp. 544–554.

[62] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi, “Defeating the Downgrade Attack on Identity Privacy in 5G”, in Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings, ser. Lecture Notes in Computer Science, C. Cremers and A. Lehmann, Eds., vol. 11322. Springer, 2018, pp. 95–119.

[63] 3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; Study on 5G Security Enhancement against False Base Stations Version 0.6.0 (Release 16)”, Aug 2019.

[64] Draft Recommendation ITU-T X.5GSec-q: Security guidelines for applying quantum-safe algorithms in 5G systems, https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3089.

[65] Jin Hong & Palesh Sarkar, Rediscovery of Time Memory Tradeoffs, https://eprint.iacr.org/2005/090.

[66] Orr Dunkelman & Nathan Keller, Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers, https://eprint.iacr.org/2008/311.

[67] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf.

[68] ETSI SAGE. Observations on ZUC-256, https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_99e/docs /S3-200930.zip.

[69] The ZUC-256 Stream Cipher, http://www.is.cas.cn/ztzl2016 /zouchongzhi/201801/W020180126529970733243.pdf.

[70] D. Rupprecht, A. Dabrowski, T. Holz, E. R. Weippl, and C. Pöpper, “On security research towards future mobile network generations”, IEEE Communications Surveys and Tutorials, vol. 20, no. 3, pp. 2518–2542, 2018.

[71] R. Tourani, S. Misra, T. Mick, and G. Panwar, “Security, Privacy, and Access Control in Information-Centric Networking: A Survey”, IEEE Communications Surveys and Tutorials, vol. 20, no. 1, pp. 566–600, 2018.

[72] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. V. Gurtov, “5G security: Analysis of threats and solutions”, in IEEE Conference on Standards for Communications and Networking, CSCN 2017, Helsinki, Finland, September 18-20, 2017. IEEE, 2017, pp. 193–199.

[73] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, “Overview of 5G Security Challenges and Solutions”, IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.

[74] M. A. Ferrag, L. A. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, “Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes”, J. Network and Computer Applications, vol. 101, pp. 55–82, 2018.

[75] P. Gandotra and R. K. Jha, “A survey on green communication and security challenges in 5G wireless communication networks”, J. Network and Computer Applications, vol. 96, pp. 39–61, 2017.

[76] A. K. Rangisetti and B. R. Tamma, “Software Defined Wireless Networks: A Survey of Issues and Solutions”, Wireless Personal Communications, vol. 97, no. 4, pp. 6019–6053, 2017.

[77] G. Choudhary and V. Sharma, “A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks”, CoRR, vol. abs/1909.08844, 2019.

[78] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, “A survey on security and privacy of 5G technologies: Potential solutions, recent

advancements and future directions", IEEE Communications Surveys & Tutorials, 2019.

[79] R. Ravindran, A. Chakraborti, S. O. Amin, A. Azgin, and G. Wang, "5G-ICN: Delivering ICN Services over 5G Using Network Slicing", IEEE Communications Magazine, vol. 55, no. 5, pp. 101–107, 2017.

[80] Prajwol Kumar Nakarmi, Mehmet Akif Ersoy, Elif Ustundag Soykan, Karl Norrman, "Murat: Multi-RAT False Base Station Detector", arXiv:2102.08780, 2021, https://arxiv.org/abs/2102.08780.

[81] J. Cichonski, PSCR 2020_5G Security Evolution not Revolution, PSCR Stakeholder Meeting 2020: The Digital Experience, Boulder, CO, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=931275.