БЕЗОПАСНОСТЬ ФИЗИЧЕСКОГО УРОВНЯ ДЛЯ СЕТЕЙ 5G/6G

Петров И.А.[1]

Цель работы: *показать перспективные технологии, которые будут использоваться в новых поколениях систем беспроводной передачи данных, выявить их уязвимости, а также возможные пути их решения.*

Метод исследования: *применен метод системного анализа открытых данных о существующих и перспективных технологиях, обеспечивающих безопасность сетей беспроводной передачи данных.*

Результаты исследования: *Выявлены актуальные проблемы в области информационной безопасности систем беспроводной передачи данных. Сделаны выводы о необходимости использования в ближайшем будущем перспективных технологий передачи данных, а также их недостатки. Поскольку объем передаваемых данных по сетям беспроводной связи постоянно увеличивается, внедрение сетей нового поколение необходимо внедрять в ближайшее десятилетие, но в данной статье выделены определенные проблемы в безопасности и скорости передачи данных, решения которым пока отсутствуют, либо они экономически не целесообразны. Кроме того, выявлены проблемы при использовании машинного обучения и искусственного интеллекта, который может помочь злоумышленникам обходить существующие меры безопасности. Также в статье указаны проблемы с балансом качеством обслуживания абонентов и безопасностью передачи данных.*

Научная новизна: *представленная статья является одной из первых российских работ, посвященной анализу и обобщению проблем информационной безопасности в сетях беспроводной передачи данных в сетях 5/6 поколения. Сформулированы основные проблемы информационной безопасности, а также возможные варианты их решения.*

Ключевые слова: *Беспроводные сети, гетерогенные сети, информационная безопасность, неортогональный множественный доступ, когнитивные радиосети, мультиплексирование с ортогональным частотным разделением, направления развития PLS, проблемы PLS.*

DOI:10.21681/2311-3456-2023-3-101-113

Введение

Требования к скорости и безопасности передачи данных растут с каждым годом. За 40 лет сменилось 4 поколения сетей мобильной связи. На данный момент в мире самым популярным стандартом связи является 4G. Данный стандарт связи основывается на технологиях LTE и IEEE 802.16e (WiMAX). Максимальная скорость восходящего потока в LTE является 50 Мбит/с, нисходящего – 100 Мбит/с. Также, существует стандарт LTE-A, со скоростью восходящего потока 500 Мбит/с, нисходящего – 1 Гбит/с. Однако, для многих задач данной скорости уже не хватает. Проблемы начали возникать и с безопасностью передачи данных. Системы LTE /LTE-A, основанные на подключении по Интернет-протоколу (IP), изначально поддерживали большую пропускную способность сети, низкие задержки и улучшенную спектральную эффективность. Чтобы преодолеть кибератаки, которые были неизбежны в системах 3G, и защитить процесс аутентификации и ключи пользователя, системы LTE-A внедрили механизмы Evolved Packet System-аутентификации и согласования ключей (EPS-AKA) и обмена ключами, аутентифицированными паролем, путем манипулирования (J-PAKE). Но внедрение новых объектов в сетях LTE-A, таких как WiMAX, Machine Type Communication (MTC), Home eNodeB (HeNB) и ретрансляторы, открыло больше возможностей для нарушений безопасности и проблем, чем в сетях 2G /2.5G и 3G.

Каждый год киберпреступность и хакерские атаки наносят значительный ущерб гражданам, учреждениям и компаниям по всему миру. Общий ущерб от действий киберпреступников в России оценивается в

1 Петров Иван Андреевич, ассистент департамента информационной безопасности Финансового университета при Правительстве РФ, Москва, Россия. E-mail: iapetrov@fa.ru

165 млрд рублей. Как подтверждается будущими прогнозами, безопасность и конфиденциальность становятся решающими для Интернета вещей (IoT) [1,2] и 5G [3,4], например, в таких отраслях, как электронное здравоохранение [5] или Индустрия 4.0 [6,8]. Развертывание 5G [8] также привлекает сегодня все больше внимания к своей безопасности [9]; особенно учитывая дополнительные функции, такие как надежные и критически важные сети или мобильные вычисления (MEC) [10, 11], которые особенно уязвимы.

Как показано в недавних отчетах [12, 13], новые хакерские угрозы всегда находятся на горизонте: ботнеты Интернета вещей (например, Mirai 2016 и его варианты, Brickerbot 2017, Hajim 2016); атаки вымогателей (например, WannaCry 2017, SamSam 2016, CryptoLocker 2013), атаки по побочным каналам процессора (например, Spectre 2018, Meltdown 2018, SWAPGS Attack 2019) и даже атаки на модуль идентификации абонента (SIM)-карту (например, Simjacker 2019). Важность повышения осведомленности о безопасности во всем мире очевидна. Стоит напомнить, что большинство уязвимостей и нарушений, вероятно, вызваны недостаточной осведомленностью самих сотрудников или граждан в области безопасности (например, использование слабых паролей или щелчок по фишинговым электронным письмам). Это мотивирует настоятельную необходимость разработки новых надежных решений сегодня для ландшафта безопасности завтрашнего дня.

Различные исследования включает в себя различные модели угроз беспроводные сети, наряду с контрмерами и методами анализа безопасности, используемыми схемами аутентификации и сохранения конфиденциальности, и типами их классификации. Все вышеописанные опросы основаны на криптографических методах, включающих шифрование и согласование ключей. Традиционно меры безопасности на основе шифрования принимались и обеспечивались в стеке протоколов верхнего уровня с использованием сложных методологий, которые были выведены с использованием модели безопасности Шеннона (Shannon, 1949). Шеннон был первым человеком, который заложил основы современной информационной безопасности. Однако модель безопасности Шеннона, основанная на криптографических алгоритмах, предполагала наличие бесшумных каналов как у законных пользователей, так и у подслушивающего устройства. Благодаря недавним технологическим достижениям методы, основанные на шифровании, теперь легко взламываются подслушивающими устройствами, обладающими высокой вычислительной мощностью и стратегиями оптимизации. Более того, такие традиционные схемы требуют наличия надежного объекта, который может эффективно обмениваться секретным ключом между законными пользователями. В предстоящих плотных сетях HetNets поиск такого надежного объекта для секретного ключа управления практически невозможно. Во-вторых, формирование и реализация таких сложных алгоритмов требуют мощных систем, высокой стоимости и ресурсов.

Эти ограничения методов, основанных на шифровании, усилили опасения операторов по поводу безопасности и вынудили исследователей разработать альтернативную схему безопасности, что привело к эволюции безопасности физического уровня (PLS). PLS обеспечивает безопасный обмен информацией между законными пользователями, используя случайность беспроводных каналов, такую как замирание, помехи и шум.

Концепция PLS первоначально была дана Вайнером, который показал в своей работе (Wyner, 1975) что безопасная связь между двумя пользователями была возможна без какого-либо обмена секретными ключами, если канал подслушивающего устройства был сделан более шумным по сравнению с каналом законного получателя. Однако модель Вайнера имела свои недостатки, такие как предполагалось, что канал подслушивающего устройства всегда имеет более низкий ОСПШ (отношение сигнал/помеха-шум) по сравнению с предполагаемым приемником, что было непрактичным сценарием. Но это отвлекло внимание большинства исследователей на PLS из-за его высокозащищенного потенциала передачи, снижения использования ресурсов, сложности и стоимости. Исследователи начали понимать, что, оптимизируя сетевые ресурсы с точки зрения PLS, можно достичь безопасной связи, что открыло совершенно новое направление исследований. Как указано выше, PLS использует внутренние характеристики беспроводных каналов, включая помехи, шум и замирание, для повышения качества сигнала на стороне приемника и ухудшения приема сигнала на подслушивающем устройстве, а также для обеспечения безопасной передачи данных без ключа с помощью дизайна сигнала и методов обработки сигнала. По сравнению с криптографическим подходом, преимущество использования методов PLS для сетей 5G в три раза. Во-первых, механизм PLS не зависит от вычислительной сложности, что означает, что даже если подслушивающие устройства в сети обладают мощными вычислительными устрой-

ствами, связь все равно может быть успешно защищена с помощью PLS. Принимая во внимание, что в случае криптографических методов, основанных на шифровании, безопасность системы связи ставится под угрозу, если подслушивающие устройства оснащены передовыми вычислительными мощностями, которые могут решить любую сложную математическую задачу. Во-вторых, сети 5G основаны на децентрализованных архитектурах, что подразумевает, что устройства могут в любое время подключаться к сети или покидать ее. Из-за этого управление процессом обмена криптографическими ключами может стать очень сложным. Использование PLS в таких случаях может обеспечить безопасную передачу данных прямо или косвенно, действуя в качестве дополнительного уровня безопасности поверх существующих механизмов безопасности. В-третьих, накладные расходы, связанные со схемами PLS для относительно полного выполнения простых алгоритмов обработки сигналов, очень малы по сравнению с методами, основанными на шифровании. Основываясь на этих наблюдениях, очевидно, что PLS является многообещающим решением для обеспечения безопасности для создания конфиденциальной и эффективной сети связи.

Помимо вышесказанного, сети 5G имеют следующие уязвимости:

— Большая поверхность атаки. В нашу жизнь начинают входить такие технологии как SDN(Software Defined Network) и NFV(Network Functions Virtualization), которые требуют огромного количества дополнительного ПО для их работы. Естественно, большое количество разного ПО дает возможность злоумышленникам использовать большое число вариантов развития атак;

— Большое количество устройств Интернета-вещей. У большинства таких устройств зачастую защита оставляет желать лучшего из-за ограниченных криптографических возможностей.

— Децентрализация и расширение границ сети. Периферийные устройства, играющие роль локальных ядер сети, осуществляют маршрутизацию пользовательского трафика, обработку запросов, а также локальное кэширование и хранение пользовательских данных. Таким образом, границы сетей 5-ого поколения расширяются, помимо ядра, на периферию, в том числе на локальные базы данных и радиоинтерфейсы 5G-NR (англ. 5G New Radio). Это создает возможность для атаки на вычислительные ресурсы локальных устройств, которые априори защищены слабее, чем центральные узлы ядра сети, с целью вызвать отказ в обслуживании. Это чревато отключением доступа в интернет целых районов, некорректным функционированием IoT-устройств (например, в системе «умный дом»), а также недоступностью сервиса экстренных оповещений IMS.

Существует несколько подходов к обеспечению безопасности физического уровня беспроводных сетей 5G/6G. В данной статье будет рассмотрены криптографические методы, методы с применением кодирования, методы с использованием мультиантенн. Безопасность физического уровня (PLS) зарекомендовала себя как потенциальное решение для повышения производительности безопасности будущих сетей 5G, которое обещает удовлетворить требования увеличения пользовательского трафика. Предотвратить подслушивание и кражу полезной информации злоумышленниками в условиях такого интенсивного трафика так же сложно, как и исключить их из сети. Многие исследователи представили ряд схем PLS, использующих либо отдельную технологию, такую как

— Multiple-input–multiple-output (MIMO);
— миллиметровую волну (mmWave);
— радиочастоту (RF);
— неортогональный множественный доступ (NOMA);
— связь в видимом свете (VLC) и т.д.,

Возможна также комбинация двух или более технологий для обеспечения безопасности каждой области будущих сетей 5G, таких как гетерогенные сети (HetNets), связь между устройствами (D2D), Интернет вещей (IoT), Когнитивная радиосеть (CRN), беспилотная воздушная сеть (UAV) и т.д.

1. Новые технологии в PLS

Мобильные сети следующего поколения готовятся на основе последних технологических достижений и постоянно растущих требований населения к скорости передачи данных, покрытию, пропускной способности, услугам в режиме реального времени и безопасной связи. В этом разделе мы обсудим методы PLS, которые предлагаются в различных будущих сетях 5G, для повышения безопасности и конфиденциальности полезных информационных сообщений, которыми обмениваются в этих сетях.

1.1 Гетерогенные сети HetNet

Нынешняя однородная сеть (HomNet) больше не способна предоставлять достаточное количество услуг

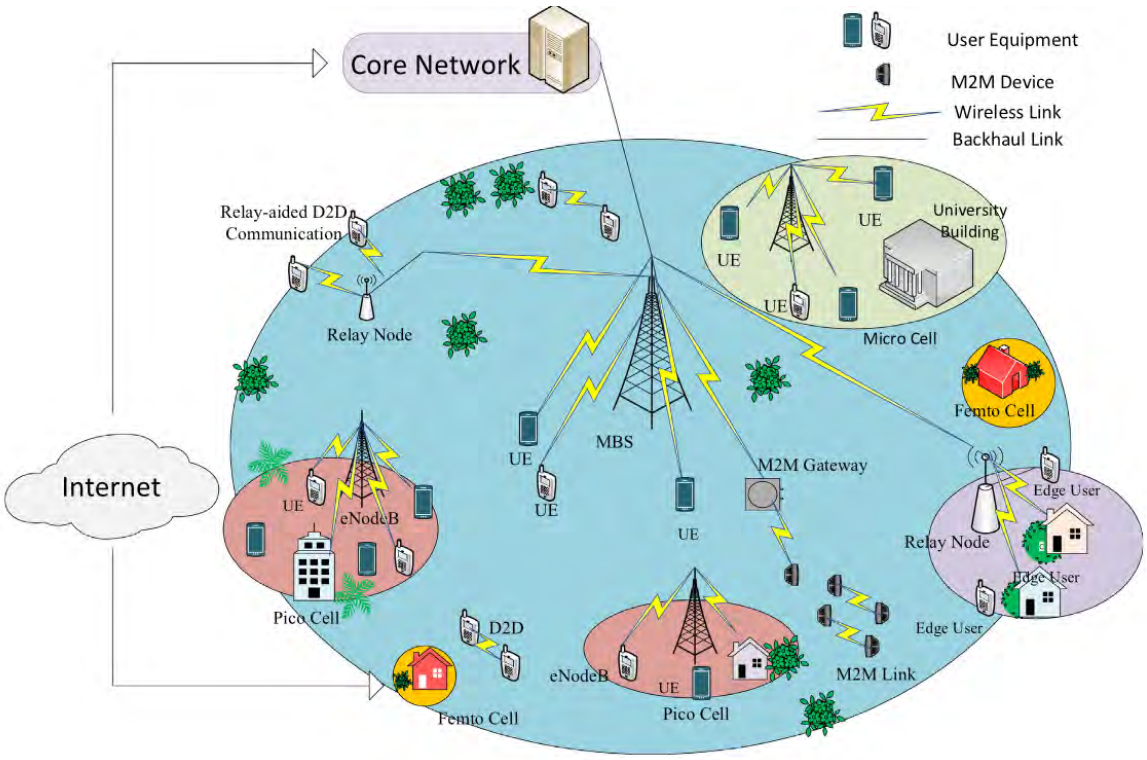

Рис.1 Архитектура гетерогенной сети

постоянно растущему числу пользователей и удовлетворять их запросы. Следовательно, ожидается, что эти обычные сети вскоре будут заменены HetNet, показанной на рис. 1, которые рассматриваются как оптимальное решение для удовлетворения требований пользователей.

Риски безопасности и конфиденциальности, связанные с неоднородной природой сети, в настоящее время находятся в центре внимания многих исследователей. Каждый вклад пытается придумать более практичную и менее сложную технику, это эффективно защищает сеть, потребляя меньше ресурсов. Автор Nasir A.A.[50] представляет некоторые практические сетевые сценарии для улучшения безопасности сети HetNet путем использования каналов помех и гетерогенного характера передаваемых сигналов в приемниках, которые обладают алгоритмами шифрования низкой сложности. Автор Zhong Z.[51] изучал PLS в гетерогенной сотовой сети K-уровня (HCN), где все базовые станции (BSS) (макро, фемто , пико) действуют как источники помех, кроме обслуживающей. Пользователь выбирает базовую станцию, которая обеспечивает максимально достижимый уровень секретности от подслушивающих устройств и получает вероятность обеспечения секретности (SCP) и нагрузку/уровень секретности. Результаты показывают, что по мере увеличения плотности подслушивающих устройств SCP уменьшается из-за увеличения более высокого ОСПШ (отношение сигнал/помеха –шум), получаемого подслушивающим устройством. В исследовании [49] предложена схема распределения ресурсов для совместной оптимизации мощности и поднесущих для достижения PLS в сетях со скрытым подслушивающим устройством. Сначала местоположение подслушивающего устройства определяется с помощью алгоритма локализации на основе уровня принятого сигнала (RSS). Затем, распределение ресурсов выполняется с использованием метода двойной декомпозиции Лагранжа в условиях справедливости, скорости прослушивания и межуровневых помех. Далее будут рассмотрены перспективные технологии безопасности, которые будут или уже используются.

1.2 Когнитивные радиосети (CRN)

CRN - это интеллектуальная системная сеть, которая часто определяет свою рабочую среду и динамически и автоматически настраивает параметры радиосвязи в соответствии с требуемой модификацией системы. Эти модификации включают максимизацию пропускной способности, минимизацию помех, обеспечение интероперабельности и позволяют совмест-

ной среде связи первичного пользователя и вторичного пользователя повышать спектральную эффективность. Ключевые особенности CRN включают в себя осведомленность и адаптацию к своей среде для поддержания сети производительность, более быстрое реагирование за счет извлечения уроков из предыдущих действий и улучшения процесса принятия решений в будущем благодаря наблюдению и сотрудничеству с окружающими устройствами. В CRN происходит обмен информацией и ее сбор локально, на основе чего создается воспринимаемая среда, которая влияет как на текущее, так и на будущее поведение сети. В таких передачах подмена и манипулирование информацией слишком просты для злоумышленников. Это приводит к получению неверной информации, которая вызывает неправильную адаптацию и создание неправильного окружающая среда. Следовательно, злоумышленники будут влиять не только на принятие краткосрочных решений CRN, но и на будущие решения. Этот вопрос занял исследовательское время многих авторов, чтобы повысить безопасность передачи CRN. Одним из потенциальных методов улучшения системы безопасности CRN является защита ее целей, методов и алгоритмов, используемых в процессе принятия решений. В работе Shu Z.[53] автор обобщает атаки безопасности, направленные на физический уровень в CRN, наряду с их существующими контрмерами. Также представлена модель CRN для анализа секретности и вероятности отключения секретности. Автор показывает, что вероятность сбоя уменьшается, а защита увеличивается из-за низкой утечки информации у подслушивающего устройства и помех со стороны вторичных пользователей. В то время как вероятность сбоя увеличивается, а скрытность уменьшается с увеличением вторичных пользователей из-за помех. В работе Bouabdellah M. [54] изучается PLS сети связи на основе CR с двумя переходами, в которой вторичный пользователь передает конфиденциальные данные получателю вторичного пользователя (ВП). с помощью ретранслятора вторичного пользователя. Реле ВП использует технологию объединения максимального коэффициента (MRC) для приема сигналов с задержкой через несколько антенн и пересылает объединенный сигнал к приемнику через единственную антенну, при наличии подслушивающего устройства. Автор определяет показатели секретности путем расчета вероятности нарушения секретности, скрытности и вероятности перехвата, показывающие, что ретрансляция с несколькими антеннами помогает достичь лучшей скрытности, чем ретрансляция с одной антенной. В работе Shah H.A. и Koo I. [55] автор предлагает оптимизированную схему распределения мощности и отображения поднесущих для CRN с поддержкой OFDM, имеющей один узел источника и два реле. Источник ВП передает данные на ретранслятор, который усиливает и пересылает информацию приемнику, в то время как другой ретранслятор посылает сигналы искусственного подавления (AJ), чтобы ухудшить перехват подслушивающего устройства. Мощности источника и реле оптимизированы таким образом, чтобы они не создавали помех для первичного пользователя выше определенного порогового уровня. Кроме того, согласование поднесущих достигается при ретрансляции пересылки, чтобы уменьшить утечку информации при прослушивании. Кроме вышеназванных технологий, используются следующие технологии:

1. Device-to-device (D2D) communication (Связь между устройствами)

При коммуникации D2D устройства напрямую связываются друг с другом друг с другом без необходимости использования какой-либо БС. Пользователи устройств не только повышают спектральную эффективность сети за счет полного использования спектра, но и повышают безопасность всей сети.

2. MIMO/massive MIMO systems

Для повышения аутентификации на физическом уровне против атак на выдачу себя за другого, метод аутентификации на основе канала в работе Baracca P.[54] предложена техника аутентификации на основе канала для двух типов моделей каналов: MIMO и OFDM.

3. OFDM (Orthogonal frequency Division Multiplexing – мультиплексирование с ортогональным частотным разделением)

Технология OFDM является фундаментальным строительным блоком для многих усовершенствованных схем модуляции, используемых в различных системах. Ниже приведены характеристики OFDM:

- Состоит из близко расположенных ортогональных поднесущих, которые перемещаются параллельно друг другу.
- Это повышает высокую спектральную эффективность системы и смягчает эффект селективного замирания, возникающего из-за многолучевого распространения.
- Он может обрабатывать различные сценарии мобильности и передавать данные с высокой скоростью.

4. NOMA (Non-orthogonal Multiple Access - Неортогональный множественный доступ)

Концепция NOMA недавно приобрела безраздельный исследовательский интерес из-за ее большого потенциала для удовлетворения требований к ускоренному трафику и массовых потребностей в подключении в будущих сетях 5G. Эта уникальная технология работает по принципу суперпозиции на передатчике и SIC на приемнике. На стороне передатчика сигналы нескольких пользователей накладываются друг на друга и передаются, причем все пользователи используют одно и то же частотно–временного кода, но они отличаются друг от друга либо по выделенному уровню мощности, либо по коду. На стороне приемника используется механизм SIC (Successive Interference Cancellation – последовательное подавление помех), который позволяет пользователю извлекать желаемый сигнал из наложенного сигнала на основе разности мощностей или разности кодов.

5. SWIPT (Simultaneous Wireless Information and Power–Transfer

Одновременная беспроводная передача информации и энергии) В последнее время большое внимание привлекла концепция SWIPT, которая появилась в области беспроводной передачи энергии (WPT). Это недавно разработанная технология, которая позволяет EH использовать радиочастотные сигналы, известные как сбор радиочастотной энергии (RF-EH). EH — это процесс извлечения неиспользуемой или неважной энергии, такой как тепло, звук или радиочастотные сигналы, и преобразования ее в электричество. При беспроводной связи эта преобразованная мощность сохраняется в батареях принимающих узлов и затем используется для передачи данных.

6. Интеллектуальная сеть

Одним из наиболее технологических достижений, которое будет внедрено в ближайшие годы, является замена обычной электросетевой системы на интеллектуальную сеть. Это интеграция сети беспроводной связи в электрическую сеть для передачи данных о распределении и использовании электроэнергии, а также инструкций по управлению силовыми устройствами, ведущих к созданию интеллектуальной сетевой системы.

2. Проблемы и будущие направления развития PLS

Большинство решений, предлагаемых для PLS, учитывают непрактичные условия среды и труднодоступные аппаратные возможности для систем с ограниченными ресурсами. Из-за этого их реализация остается серьезной проблемой, независимо от того, насколько современная технология предлагается. Такие проблемы безопасности, с которыми сталкиваются на физическом уровне, требуют значительного внимания, чтобы возможности предлагаемых методов можно было практически использовать и обеспечить защищенную от атак связь на физическом уровне. Ниже обсуждаются некоторые из проблем PLS, которые препятствуют процессу внедрения, и связанные с ними будущие направления.

2.1 Проблема мобильности

Почти во всех исследованиях безопасности, которые были изучены до сих пор, рассматривается безопасность пользователя, находящегося где-то с подслушивающим устройством, расположенным поблизости. Мы знаем, что в ближайшие годы большинство окружающих нас объектов будут снабжены датчиками и исполнительными механизмами, способными взаимодействовать с другими устройствами. В недалеком будущем к Интернету будут подключены все устройства, «Интернет-вещей» будет расширятся практически неограниченно. Следовательно, грядущее время требует таких методов обеспечения безопасности, которые смогут обеспечить мобильность в будущих сетях Интернета вещей 5G. Кроме того, для дальнейших исследований можно изучить, как поддерживать идеальный компромисс между качеством обслуживания и безопасностью в этих мобильных устройствах. Кроме того, также может быть исследовано влияние мобильности на запуск атаки физического уровня или защиту от атаки. Пользователь может изменить свое местоположение, чтобы защитить себя от атаки, в то время как злоумышленник может использовать мобильность для получения лучшего места атаки. Поиск решений PLS с точки зрения мобильности может стать интересным направлением исследований.

2.2 Машинное обучение

В настоящее время развертывание большинства эффективных методов обнаружения атак производится на основе машинного обучения. Однако до сих пор существует проблема интеграции таких платформ с высокоразвитым программным обеспечением для мониторинга и управления. В последнее время было проведено множество исследовательских работ по изучению систем безопасности, основанных на алгоритмах, но они основаны на теоретических результатах. Практическая реализация предлагаемых работ для достижения желаемой производительности все еще остается открытым вопросом. Разработка систем, которые могут поддерживать алгоритмы обуче-

ния, требует передовых инструментов и механизмов, отличных от тех, которые уже используются в существующих системах. Поэтому для успешного внедрения машинного обучения в системы безопасности требуется достаточное количество внимания к их практическому развертыванию. Более того, недавние исследования показали, что, хотя разработчики используют машинное обучение для повышения безопасности беспроводной связи, сами эти интеллектуальные системы сталкиваются с некоторыми рисками безопасности из-за обработки и обучения большого объема данных, поступающих от ненадежных и не прошедших проверку подлинности сторон. Следовательно, рано или поздно злоумышленники всегда находят способ быть на шаг впереди защитников. Изучение решений безопасности для машинного обучения, чтобы его можно было эффективно использовать для обеспечения сетевой безопасности, является важным исследовательским подходом. Более того, разработчик системы должен думать не только с точки зрения защитников, но и с точки зрения злоумышленника при проектировании высокозащищенной системы.

2.3 Проблема качества обслуживания

В сфере информационной безопасности существует выражение: «Все что безопасно - неудобно, все что удобно, небезопасно». Данное выражение применимо и к PLS. Большинство исследователей часто рассматривали безопасность и качество обслуживания как отдельные сущности из-за их сложного моделирования компромиссов. Исследования показали, что повышение эффективности безопасности приводит к ухудшению качества обслуживания и наоборот. Однако в работе [58] автор раскрывает взаимозависимость требований безопасности и качества обслуживания, демонстрируя, что неправильный выбор метода защиты может привести к снижению производительности сети, так же как неправильный выбор уровня обслуживания может привести к утечке полезных пакетов данных. Следовательно, требуется оптимальная структура политики, которая может снизить риск конфликтов между этими двумя субъектами. Это приводит к некоторым исследовательским работам, в которых предпринимались попытки создать баланс между двумя наборами, предлагая различные методы. В [57] авторы предлагают алгоритм теории игр (GT) для совместной оптимизации требований пользователей к безопасности и качества обслуживания, позволяя базовой станции максимизировать распределение полосы пропускания в сети HetNet. Автор дополнительно улучшает эту работу в статье [58], нацеленный на решение проблемы поиска и распределения оптимального уровня безопасности для каждого пользователя при одновременном обеспечении требований качества обслуживания с использованием GT-QoSec. В другой работе [59], в которой используется метод азартных игр с учетом нестабильной конфиденциальности (GOLFE), повышается безопасность наряду с качеством обслуживания процесса передачи мобильных устройств путем ранжирования крупных базовых станций на основе уровня конфиденциальности, определенного на этапе анализа передачи, и принятия решения о безопасном выборе. Но все вышеупомянутые три работы основаны на обычных методах шифрования, размера ключа и контроля доступа. Представлено очень мало работ, в которых предлагается сбалансированный компромисс между PLS и качеством обслуживания. В [60] авторы предлагают один ортогональный и два не ортогональных метода формирования луча передачи секретности (STB), которые намеренно создают помехи в совместном канале (CCI) вокруг подслушивающего устройства в двухуровневой сети HetNet для повышения уровня секретности предполагаемого MU и требований качества обслуживания как пользователя фемсоты (FU), так и MU с точки зрения PLS. Однако достижение сбалансированного баланса между PLS и качеством обслуживания по-прежнему остается нерешенной задачей.

2.4 Степень секретности/максимизация пропускной способности

Существует несколько методов подсчета важного параметра для беспроводной передачи данных. Ниже рассмотрим несколько методик. Уровень секретности определяется как разница между достижимой скоростью канала законного пользователя и скоростью канала подслушивания/прослушки. Уровень секретности канала законного пользователя рассчитывается путем вычитания скорости канала m подслушивающего устройства R^{e}_{mn} из скорости канала n приемника пользователя R^{u}_{m}, как показано следующим уравнением:

$$R_n^u = \log(1 + SINR_1) \quad (1)$$

$$R_{m,n}^e = \log(1 + SINR_e) \quad (2)$$

$$R_{s_{(m,n)}} = R_n^u - R_{m,n}^e \quad (3)$$

В работе (63) автор формулирует проблему максимизации уровня секретности как:

$$Function: \max_{w_m\, w_{in}} \{R_{s_{(m,n)}}\} \quad (4),$$

где w_m и w_{in} указывает на пользователей m и n, связанных с малой базовой станцией и пользователя i, связанного с большой базовой станцией. Схема управления помехами, предложенная для решения этой задачи, повышает уровень скрытности наряду со спектральной эффективностью. В работе [62] авторы предлагают проект для совместной оптимизации информации, помех и искусственных помех в большой базовой станции и фемтосотой. Целевая функция Рена и др. (2017) является максимизации уровня секретности при ограничениях качества обслуживания, накопления энергии мощности передачи, заданных как:

$$Function: \max\{\min_{n\in N\ m\in M} R_{s_{(m,n)}}\} \quad (5)$$

В статье [65] усилия авторов были сосредоточены на проблеме безопасности сети 5G и повышении уровня секретности, энергоэффективности и пропускной способности сети, используя технологию PLS в качестве решения для обеспечения безопасности и оптимизировав распределение ресурсов сети. Целевая функция распределения ресурсов была записана в виде

$$Function: \max \sum_{n\in N}\Big(\sum_{k_c\in K_c} r^n_{k_c} + \sum_{k_d\in K_d} r^n_{k_d}\Big) \quad (6),$$

где $r^n kc$ обозначает секретность скорость пользователя сети и r^n_{kd} обозначает скорость устройства пользователей, где k_c и k_d представляют один сотовый канал и один интерфейс D2D связи. Целью уравнения (6) является обеспечение максимальной пропускной способности сети, обеспечиваемой секретностью, как для пользователей сотовой связи, так и для пользователей устройств в двух случаях:

1. Во-первых, когда канал совместно используется между пользователями сотовой связи и пользователями устройств.

2. Во-вторых, когда канал не является общим между ними.

Как можно заметить, вариантов максимизации степени секретности/пропускной способности довольно много, а это означает, что наилучшего варианта еще не найдено.

2.5 Проблема в реализации технологии NOMA

Технология NOMA является одной из важнейших технологий для внедрения сетей 5G, но ее реализация и удобное использование в данное время ограничены. После изучения данной технологии были выявлены следующие сложности:

1. Каждому пользователю до кодирования собственной информации необходимо декодировать информацию всех других пользователей с худшим коэффициентом усиления канала (тех пользователей, которые находятся в одном кластере). Само собой это приводит к сложности приема и дополнительным затратам вычислительных и энергетических ресурсов абонентского устройства на декодирование получаемых данных.

2. Когда в системе последовательного подавления помех возникнет ошибка, то, вероятнее всего, последующее декодирование информации для других пользователей будет выполнено ошибочно. Это означает, что большое количество абонентов не может быть в одном кластере, иначе будет происходить накопление ошибок, декодер на каком-то этапе не сможет исправить все ошибки.

3. Для получения преимуществ мультиплексирования «по мощности» с использованием NOMA (power-domain NOMA), требуется значительная разность коэффициентов усиления канала между сильными и слабыми пользователями. Это ограничивает эффективное количество пар пользователей, что, в свою очередь, уменьшает коэффициент суммарного прироста NOMA.

4. При работе технологии NOMA устройство абонента должно отправлять информацию о коэффициенте усиления своего канала на базовую станцию, однако данная технология чувствительна к точности его определения, вследствие этого могут возникать проблемы с качеством обслуживания.

5. Совместная работа агрегированных каналов и NOMA также может дополнительно увеличить скорость передачи данных конечному пользователю, однако какой тип агрегирования для этого подходит, пока не определено.

6. Также пока не до конца решенной задачей является сам алгоритм выделения мощностных ресурсов для каждого абонента, который должен обладать низкой степенью сложности для наилучшей производительности NOMA.

Вывод

Безопасность физического уровня (PLS) оказалась наиболее оптимальным решением для обеспечения безопасности будущих сетей 5G благодаря своей низкой сложности и легко реализуемым методам по срав-

нению с криптографическими схемами. Существует множество исследовательских работ, направленных на разработку такого метода обеспечения безопасности на физическом уровне, который обеспечивает конфиденциальность 5G и его новых технологий. В этом обзоре мы представили всесторонний обзор исследовательских работ PLS, выполненных до настоящего времени в гетерогенных сетях (HetNets), в отношении различных базовых технологий, а также в других технологиях 5G, таких как MIMO, NOMA, CRN. Данные технологии являются будущими в области беспроводной передачи данных, разрабатываются и оптимизуются более 10 лет, однако до сих пор остается много нерешенных проблем, таких как проблемы с балансом качества обслуживания и безопасностью передачи данных, проблемы использования машинного обучения и искусственного интеллекта, а также проблемы секретности и максимизации пропускного канала.

Но внедрение сетей 5G в мире только наращивает темпы даже с существующими проблемами в безопасности, поэтому вопрос решения выявленных проблем лишь вопрос времени.

Литература

1. L. Chen et al., Reliability, security and privacy in location-based services for the future of the Internet of Things: an overview.
2. I. Andrea, K. Chrysostomou, G. Hadzhihristofi, Internet of Things: vulnerabilities and security problems. IEEE Symposium. Calculation. Commun., 180–187 (2015). https://doi.org/10.1109/ISCC.2015.7405513 .
3. M. Lianaj and others., All-around Safety Management 5 aposematic (aposematic, 2018). isbn: 9781119293071.
4. LaPolla, F. Martinelli, D. Sgandurra, Mobile device Security Review. LIEU Commun. Review. Teacher.15(1), 446-471 (2013). https://doi.org/10.1109/SURV.2012.013012.00028.
5. (2019). https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation .
6. V. Alcazar, V. Cruz-Machado, Scanning Industry 4.0: a review of the literature on technologies for production systems. Eng. The science. Technology. Int. J.22(3), 899-919 (2019).https://doi.org/10.1016/j.jestch.2019.01.006 .
7. K. Huang, K. Zhou, Yu. Qin, U. Tu, Game-theoretic approach to decision-making on inter-level security in industrial cyber-physical systems. IEEE Trans. Ind. Electron.PP (XX), 1-1 (2019). https://doi.org/10.1109/TIE.2019.2907451 .
8. A. Al-Dulaimi et al., 5G networks: Fundamental requirements for technology and Operations management (Wiley, 2018). isbn:978-1-119-33273-2.
9. D. Beisin, J. Dreyer, L. Hirshi, S. Radomirovich, R. Sasse, V. Stettler, in Proc. 2018 ACM SIGMOD Conf. Calculation. Commun. Safety. - CCS '18. Formal Analysis of 5G Authentication, (2018), pp. 1383-1396. https://doi.org/10.1145/3243734.3243846 .
10. European Telecommunications Standards Institute ETSI, Water Technical Document Mobile Peripheral Computing. https://portal.etsi.org/TBSiteMap/MEC/MECWhitePapers.aspx .
11. D. Wang, B. Bai, K. Lei, V. Zhao, Yu Yang, Z. Han, Improving information security using physical layer approaches in heterogeneous IoT using mobile peripheral computing with multiple access in Smart City. IEEE Access. 7:, 54508-54521 (2019). https://doi.org/10.1109/ACCESS.2019.2913438 . Symantec, Отчет об угрозах безопасности в Интернете (ISTR), (2019). https://www.symantec.com/security-center/threat-report .
12. Cisco, Annual Cybersecurity Report for 2018, (2018). https://www.cisco.com/c/m/enau/products/security/offers/annual-cybersecurity-report-2018.html .
13. R. K. M. J. Chakraborty, Handbook of Hardware Cryptography - Algorithms and Analysis (LAP LAMBERT Academic Publishing House, 2018). isbn: 978-6139841653.
14. I. Setiadi, A. I. Kistiyantoro, A. Miyaji, Cryptography on elliptic curves: analysis of algorithms and implementations in coordinate systems. 2015 2nd edition. https://doi.org/10.1109/ICAICTA.2015.7335349 .
15. K. Piotrowski, P. Langendorfer, S. Peter, in the materials of the fourth ACM workshop on peer-to-peer and sensor network security - SASN '06. How Public Key cryptography affects the service life of a wireless sensor node, (2007), p. 169. https://doi.org/10.1145/1180345.1180366 .
16. T. Eisenbart, S. Kumar, K. Par, A. Poshman, L. Ukhsadel, Review of implementations of lightweight cryptography. IEEE Des. Test computing.24(6), 522-533 (2007). https://doi.org/10.1109/MDT.2007.178 .
17. K. L. Matti Latva-aho, Key driving forces and research challenges for ubiquitous wireless intelligence 6G, 6G Flaship (Technical Report, September, University of Oulu, Finland, 2019).
18. R. Roman, K. Alcatraz, J. Lopez, Review of cryptographic primitives and implementations for sensor network nodes with hardware limitations. Crowd. Netw. The app.12(4), 231-244 (2007). https://doi.org/10.1007/s11036-007-0024-2 .
19. S. B. Sadhan, A. O. Salman, Review of the state of Lightweight cryptography and future problems, (2018). https://doi.org/10.1109/ICASEA.2018.8370965 .
20. A. Biryukov, L. P. Perrin, The current state of lightweight symmetric cryptography, University of Luxembourg (University of Luxembourg, 2017).
21. L. Chen et al., NIST: A Report on NIST Post-Quantum Cryptography. https://csrc.nist.gov/publications/detail/nistir/8105/final.
22. Quanta magazine does the law of Non-spring describe the growth of quantum computing (2019). https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618 .
23. IEEE Spectrum, which means Google's quantum superiority requirement for quantum computing, (2019). https://spectrum.ieee.org/tech-talk/computing/hardware/how-googles-quantum-supremacy-plays-into-quantum-computings-long-game.
24. CRYPT CSA, 5.4: Report on Algorithms, Key Size and protocols, (2018). https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.
25. K. Sen, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks [Security and privacy in new wireless networks. IEEE Wireless. Commun.17(5), 56–62 (2010). https://doi.org/10.1109/mwc.2010.5601959 .

26. J. Zhang, T. K. Duong, A. Marshall, R. Woods, Key generation via wireless channels: an overview. IEEE Access. 4:, 614-626 (2016). https://doi.org/10.1109/ACCESS.2016.2521718 .
27. S. Mathur, R. Miller, A. Warshawski, W. Trapp, N. Mandayam, in Proc. 9th Int. Conference. Mob. Syst. Application. The server. - MobiSys'11. ProxiMate, (2011), p. 211. https://doi.org/10.1145/1999995.2000016 .
28. F. Marino, E. Paolini, M. Ciani, in Proc. - IEEE Int. Conf.Extracting a secret key from a UWB channel: Analysis in a Real Environment (Ultra-Wideband, 2014), pp. 80-85. https://doi.org/10.1109/ICUWB.2014.6958955.
29. H. Liu, Y. Wang, J. Yang, Y. Chen, in Proc. IEEE INFOCOM. Fast and practical secret key extraction using channel response, (2013), pp. 3048-3056. https://doi.org/10.1109/INFCOM.2013.6567117 .
30. S. N. Premnat, P. L. Gouda, S. K. Kasera, N. Patvari, R. Ricci, Secret key extraction using Bluetooth wireless signal level measurements. Raising. Annu. IEEE Int. The conference. Probing, communication. Netw., 293-301 (2014). https://doi.org/10.1109/SAHCN.2014.6990365 .
31. J. Wang, A. B. Lopez, M. A. Al-Farouk, in ACM/IEEE 7th Int. The conference. Cyberphysical system. ICCPS 2016 - Proc.Using the randomness of wireless channels to generate keys to ensure the security of an automotive cyber-physical system, (2016), pp. 1-10.
32. https://doi.org/10.1109/ICCPS.2016.7479103 32. A.M. Tonello, A. Pittolo, Physical layer security in power line networks: a new scenario, different from wireless. IET Communun.8(8), 1239-1247 (2014). https://doi.org/10.1049/iet-com.2013.0472 .
33. A. A. E. Hajomer, H. Yang, A. Sultan, U. San, U. Hu, Generation and distribution of keys using phase oscillations in a classical fiber-optic channel. Int. The conference. Transparent selection. Netw.2018-July:, 1-3 (2018). https://doi.org/10.1109/ICTON.2018.8473760 .А. Васкес-Кастро, М. Хаяши, Безопасность физического уровня для радиочастотных спутниковых каналов в режиме конечной длины. IEEE Trans. Inf. Forensics Security.14(4), 981-993 (2019). https://doi.org/10.1109/TIFS.2018.2868538 .
34. B. M. Al Halawani, A. A. A. Al-Banna, K. Wu, Security and privacy at the physical level for access to everything. INSTEAD OF A commune. Wizard.57(10), 84-90 (2019). https://doi.org/10.1109/MCOM.001.1900141 .
35. D. Tian, W. Zhang, J. Sun, K. -H. Wang, Security at the physical communication layer in visible light with interference, 512-517 (2019). https://doi.org/10.1109/ICCChina.2019.8855859
36. Yu. Luo, L. Pu, Z. Peng, Z. Shi, RSS-based secret key generation in underwater acoustic networks: advantages, problems and performance improvements. IEEE Communun. Mag.54(2), 32–38 (2016). https://doi.org/10.1109/MCOM.2016.7402258
37. C. Sanger, Physical layer security for the Internet of Things, doctoral dissertation (University of Bochum, 2017).
38. D. Wang, B. Bai, V. Zhao, Z. Han, Review of approaches to optimizing the security of the wireless physical layer. IEEE Communun. Review. Teacher.21(2), 1878-1911 (2019).
39. https://doi.org/10.1109/COMST.2018.2883144 39. M. Bloch, J. Barros, Physical Layer Security: From Information Theory to Security Engineering (Cambridge Press, 2011). isbn: 978-0521516501.
40. R. Alswede, I. Sissar, Ordinary randomness in Information theory and cryptography - Part I: Sharing Secrets. IEEE Trans. Inf. Theory. 39(4), 1121-1132 (1993).
41. S. N. Premnat, P. L. Gouda, S. K. Kasera, N. Patvari, R. Ricci, Secret key extraction using Bluetooth wireless signal level measurements. Raising. Annu. IEEE Int. The conference. Probing, communication. Netw., 293-301 (2014). https://doi.org/10.1109/SAHCN.2014.6990365 .
42. S. Eberts, M. Strohmeyer, M. Wilhelm, I. Martinovich, A practical man-in-the-middle attack on signal-based key generation protocols. Lecture. Computational Notes. Sci. including Subser. Lecture. Notes Artif. Intelligence. Lecture. Notes Bioinformatics.7459 LNCS:, 235-252 (2012). https://doi.org/10.1007/978-3-642-33167-114 .
43. D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," IEEE Commun. Magazine, vol. 53, pp. 21–27, June 2015.
44. A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in 2011 45th Asilomar Conf. Signals, Systems and Computers, pp. 265–269, Nov 2011.
45. J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," arXiv preprint arXiv:1512.02754, 2015.J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," IEEE Wireless Commun. Letters, vol. 5, pp. 80–83, Feb 2016.
46. Shiqi, G., Chengwen, X., Zesong, F., Jingming, K., 2016. Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper. China Commun. 13 (3), 82–95
47. Nasir, A.A., Tuan, H.D., Nguyen, H.H., Nguyen, N.M., 2019. Physical layer security by exploiting interference and heterogeneous signaling. IEEE Wirel. Commun. 26 (5), 26–31.
48. Zhong, Z., Luo, W., Peng, J., Jin, L., 2017. On the security of K-tier heterogeneous cellular networks. Phys. Commun. 25, 570–576.
49. Baracca, P., Laurenti, N., Tomasin, S., 2012. Physical layer authentication over MIMO fading wiretap channels. IEEE Trans. Wireless Commun. 11 (7), 2564–2573.
50. Shu, Z., Qian, Y., Ci, S., 2013. On physical layer security for cognitive radio networks. IEEE Netw. 27 (3), 28–33.
51. Bouabdellah, M., El Bouanani, F., Ben-Azza, H., 2018. Secrecy outage probability in cognitive radio networks subject to Rayleigh fading channels. In: 2018 Inter- national Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, pp. 1–5.
52. Shah, H.A., Koo, I., 2018. A novel physical layer security scheme in OFDM-based cognitive radio networks. IEEE Access 6, 29486–29498.
53. Cardoso, L.S., Chairman, Q., 2006. Quality and security usability. In: Proc. ITU-T Wksp. End-To-End QoE/QoS.
54. Cardoso, L.S., Chairman, Q., 2006. Quality and security usability. In: Proc. ITU-T Wksp. End-To-End QoE/QoS.
55. Fadlullah, Z.M., Wei, C., Shi, Z., Kato, N., 2017. GT-QoSec: A game-theoretic joint optimization of QoS and security for differentiated services in next generation heterogeneous networks. IEEE Trans. Wireless Commun. 16 (2), 1037–1050.
56. Puska, A., Nogueira, M., Santos, A., 2018. Confidentiality-aware decision on handoffs under uncertainty on heterogeneous wireless networks. In: 2018 IEEE Symposium on Computers and Communications (ISCC). IEEE, pp. 00884–00889.
57. Lv, T., Gao, H., Yang, S., 2015. Secrecy transmit beamforming for heterogeneous networks. IEEE J. Sel. Areas Commun. 33 (6), 1154–1170.
58. Fang, D., Qian, Y., Hu, R.Q., 2017. Interference management for physical layer security in heterogeneous networks. In: 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress. IEEE, pp. 133–138.

59. Ren, Y., Lv, T., Gao, H., Li, Y., 2017. Secure wireless information and power transfer in heterogeneous networks. IEEE Access 5, 4967–4979.
60. Irrum, F., Ali, M., Naeem, M., Anpalagan, A., Qaisar, S., Qamar, F., 2021. D2D-enabled resource management in secrecy-ensured 5G and beyond heterogeneous networks. Phys. Commun. 45, 101275
61. Osipov, A., Pleshakova, E., Gataullin, S., Korchagin, S., Ivanov, M., Finogeev, A., & Yadav, V. (2022). Deep Learning Method for Recognition and Classification of Images from Video Recorders in Difficult Weather Conditions. Sustainability, 14(4), 2420.
62. Krakhmalev, O., Korchagin, S., Pleshakova, E., Nikitin, P., Tsibizova, O., Sycheva, I., ... & Krakhmalev, N. (2021). Parallel Computational Algorithm for Object-Oriented Modeling of Manipulation Robots. Mathematics, 9(22), 2886

PHYSICAL LAYER SECURITY FOR 5G/6G NETWORKS

Petrov I.A.[2]

Purpose: *show promising technologies that will be used in new generations of wireless data transmission systems, to identify their vulnerabilities, as well as possible solutions to them.*

Method: *the method of system analysis of open data on existing and promising technologies that ensure the security of wireless data transmission networks is applied.*

Result: *actual problems in the field of information security of wireless data transmission systems are identified. Conclusions are drawn about the need to use promising data transmission technologies in the near future, as well as their shortcomings. Since the amount of data transmitted over wireless networks is constantly increasing, the introduction of new generation networks must be implemented in the next decade, but this article highlights certain problems in security and data transfer speed, solutions for which are not yet available, or they are not economically feasible. In addition, problems have been identified when using machine learning and artificial intelligence, which can help attackers bypass existing security measures. The article also indicates problems with the balance of the quality of customer service and the security of data transmission.*

The scientific novelty: *the presented article is one of the first Russian works devoted to the analysis and generalization of information security problems in wireless data transmission networks in 5/6 generation networks. The main problems of information security, as well as possible solutions to them, are formulated.*

Keywords: *Wireless networks, heterogeneous networks, information security, orthogonal multiple access, cognitive radio networks, multiplexing with orthogonal frequency division, PLS development directions, PLS problems.*

References

1. L. Chen et al., Reliability, security and privacy in location-based services for the future of the Internet of Things: an overview.
2. I. Andrea, K. Chrysostomou, G. Hadzhihristofi, Internet of Things: vulnerabilities and security problems. IEEE Symposium. Calculation. Commun., 180–187 (2015). https://doi.org/10.1109/ISCC.2015.7405513 .
3. M. Lianaj and others., All-around Safety Management 5 aposematic (aposematic, 2018). isbn: 9781119293071.
4. LaPolla, F. Martinelli, D. Sgandurra, Mobile device Security Review. LIEU Commun. Review. Teacher.15(1), 446-471 (2013). https://doi.org/10.1109/SURV.2012.013012.00028.
5. (2019). https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation .
6. V. Alcazar, V. Cruz-Machado, Scanning Industry 4.0: a review of the literature on technologies for production systems. Eng. The science. Technology. Int. J.22(3), 899-919 (2019).https://doi.org/10.1016/j.jestch.2019.01.006 .
7. K. Huang, K. Zhou, Yu. Qin, U. Tu, Game-theoretic approach to decision-making on inter-level security in industrial cyber-physical systems. IEEE Trans. Ind. Electron.PP (XX), 1-1 (2019). https://doi.org/10.1109/TIE.2019.2907451 .
8. A. Al-Dulaimi et al., 5G networks: Fundamental requirements for technology and Operations management (Wiley, 2018). isbn:978-1-119-33273-2.
9. D. Beisin, J. Dreyer, L. Hirshi, S. Radomirovich, R. Sasse, V. Stettler, in Proc. 2018 ACM SIGMOD Conf. Calculation. Commun. Safety. - CCS '18. Formal Analysis of 5G Authentication, (2018), pp. 1383-1396. https://doi.org/10.1145/3243734.3243846 .
10. European Telecommunications Standards Institute ETSI, Water Technical Document Mobile Peripheral Computing. https://portal.etsi.org/TBSiteMap/MEC/MECWhitePapers.aspx .

2 Ivav A. Petrov, Assistant of the Department of Information Security of the Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: iapetrov@fa.ru

11. D. Wang, B. Bai, K. Lei, V. Zhao, Yu Yang, Z. Han, Improving information security using physical layer approaches in heterogeneous IoT using mobile peripheral computing with multiple access in Smart City. IEEE Access. 7:, 54508-54521 (2019). https://doi.org/10.1109/ACCESS.2019.2913438 . Symantec, Otchet ob ugrozah bezopasnosti v Internete (ISTR), (2019). https://www.symantec.com/security-center/threat-report .
12. Cisco, Annual Cybersecurity Report for 2018, (2018). https://www.cisco.com/c/m/enau/products/security/offers/annual-cybersecurity-report-2018.html .
13. R. K. M. J. Chakraborty, Handbook of Hardware Cryptography - Algorithms and Analysis (LAP LAMBERT Academic Publishing House, 2018). isbn: 978-6139841653.
14. I. Setiadi, A. I. Kistiyantoro, A. Miyaji, Cryptography on elliptic curves: analysis of algorithms and implementations in coordinate systems. 2015 2nd edition. https://doi.org/10.1109/ICAICTA.2015.7335349 .
15. K. Piotrowski, P. Langendorfer, S. Peter, in the materials of the fourth ACM workshop on peer-to-peer and sensor network security - SASN '06. How Public Key cryptography affects the service life of a wireless sensor node, (2007), p. 169. https://doi.org/10.1145/1180345.1180366 .
16. T. Eisenbart, S. Kumar, K. Par, A. Poshman, L. Ukhsadel, Review of implementations of lightweight cryptography. IEEE Des. Test computing.24(6), 522-533 (2007). https://doi.org/10.1109/MDT.2007.178 .
17. K. L. Matti Latva-aho, Key driving forces and research challenges for ubiquitous wireless intelligence 6G, 6G Flaship (Technical Report, September, University of Oulu, Finland, 2019).
18. R. Roman, K. Alcatraz, J. Lopez, Review of cryptographic primitives and implementations for sensor network nodes with hardware limitations. Crowd. Netw. The app.12(4), 231-244 (2007). https://doi.org/10.1007/s11036-007-0024-2 .
19. S. B. Sadhan, A. O. Salman, Review of the state of Lightweight cryptography and future problems, (2018). https://doi.org/10.1109/ICASEA.2018.8370965 .
20. A. Biryukov, L. P. Perrin, The current state of lightweight symmetric cryptography, University of Luxembourg (University of Luxembourg, 2017).
21. L. Chen et al., NIST: A Report on NIST Post-Quantum Cryptography. https://csrc.nist.gov/publications/detail/nistir/8105/final.
22. Quanta magazine, does the law of Non-spring describe the growth of quantum computing (2019). https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618 .
23. IEEE Spectrum, which means Google's quantum superiority requirement for quantum computing, (2019). https://spectrum.ieee.org/tech-talk/computing/hardware/how-googles-quantum-supremacy-plays-into-quantum-computings-long-game.
24. CRYPT CSA, 5.4: Report on Algorithms, Key Size and protocols, (2018). https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.
25. K. Sen, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks [Security and privacy in new wireless networks. IEEE Wireless. Commun.17(5), 56–62 (2010). https://doi.org/10.1109/mwc.2010.5601959 .
26. J. Zhang, T. K. Duong, A. Marshall, R. Woods, Key generation via wireless channels: an overview. IEEE Access. 4:, 614-626 (2016). https://doi.org/10.1109/ACCESS.2016.2521718 .
27. S. Mathur, R. Miller, A. Warshawski, W. Trapp, N. Mandayam, in Proc. 9th Int. Conference. Mob. Syst. Application. The server. - MobiSys'11. ProxiMate, (2011), p. 211. https://doi.org/10.1145/1999995.2000016 .
28. F. Marino, E. Paolini, M. Ciani, in Proc. - IEEE Int. Conf.Extracting a secret key from a UWB channel: Analysis in a Real Environment (Ultra-Wideband, 2014), pp. 80-85. https://doi.org/10.1109/ICUWB.2014.6958955.
29. H. Liu, Y. Wang, J. Yang, Y. Chen, in Proc. IEEE INFOCOM. Fast and practical secret key extraction using channel response, (2013), pp. 3048-3056. https://doi.org/10.1109/INFCOM.2013.6567117 .
30. S. N. Premnat, P. L. Gouda, S. K. Kasera, N. Patvari, R. Ricci, Secret key extraction using Bluetooth wireless signal level measurements. Raising. Annu. IEEE Int. The conference. Probing, communication. Netw., 293-301 (2014). https://doi.org/10.1109/SAHCN.2014.6990365 .
31. J. Wang, A. B. Lopez, M. A. Al-Farouk, in ACM/IEEE 7th Int. The conference. Cyberphysical system. ICCPS 2016 - Proc.Using the randomness of wireless channels to generate keys to ensure the security of an automotive cyber-physical system, (2016), pp. 1-10.
32. https://doi.org/10.1109/ICCPS.2016.7479103 32. A.M. Tonello, A. Pittolo, Physical layer security in power line networks: a new scenario, different from wireless. IET Communun.8(8), 1239-1247 (2014). https://doi.org/10.1049/iet-com.2013.0472 .
33. A. A. E. Hajomer, H. Yang, A. Sultan, U. San, U. Hu, Generation and distribution of keys using phase oscillations in a classical fiber-optic channel. Int. The conference. Transparent selection. Netw.2018-July:, 1-3 (2018). https://doi.org/10.1109/ICTON.2018.8473760 .A. Vaskes-Kastro, M. Hajashi, Bezopasnost' fizicheskogo urovnja dlja radiochastotnyh sputnikovyh kanalov v rezhime konechnoj dliny. IEEE Trans. Inf. Forensics Security.14(4), 981-993 (2019). https://doi.org/10.1109/TIFS.2018.2868538 .
34. B. M. Al Halawani, A. A. A. Al-Banna, K. Wu, Security and privacy at the physical level for access to everything. INSTEAD OF A commune. Wizard.57(10), 84-90 (2019). https://doi.org/10.1109/MCOM.001.1900141 .
35. D. Tian, W. Zhang, J. Sun, K. -H. Wang, Security at the physical communication layer in visible light with interference, 512-517 (2019). https://doi.org/10.1109/ICCChina.2019.8855859
36. Yu. Luo, L. Pu, Z. Peng, Z. Shi, RSS-based secret key generation in underwater acoustic networks: advantages, problems and performance improvements. IEEE Communun. Mag.54(2), 32–38 (2016). https://doi.org/10.1109/MCOM.2016.7402258
37. C. Sanger, Physical layer security for the Internet of Things, doctoral dissertation (University of Bochum, 2017).
38. D. Wang, B. Bai, V. Zhao, Z. Han, Review of approaches to optimizing the security of the wireless physical layer. IEEE Communun. Review. Teacher.21(2), 1878-1911 (2019).
39. https://doi.org/10.1109/COMST.2018.2883144 39. M. Bloch, J. Barros, Physical Layer Security: From Information Theory to Security Engineering (Cambridge Press, 2011). isbn: 978-0521516501.
40. R. Alswede, I. Sissar, Ordinary randomness in Information theory and cryptography - Part I: Sharing Secrets. IEEE Trans. Inf. Theory. 39(4), 1121-1132 (1993).
41. S. N. Premnat, P. L. Gouda, S. K. Kasera, N. Patvari, R. Ricci, Secret key extraction using Bluetooth wireless signal level measurements. Raising. Annu. IEEE Int. The conference. Probing, communication. Netw., 293-301 (2014). https://doi.org/10.1109/SAHCN.2014.6990365 .

42. S. Eberts, M. Strohmeyer, M. Wilhelm, I. Martinovich, A practical man-in-the-middle attack on signal-based key generation protocols. Lecture. Computational Notes. Sci. including Subser. Lecture. Notes Artif. Intelligence. Lecture. Notes Bioinformatics.7459 LNCS, 235-252 (2012). https://doi.org/10.1007/978-3-642-33167-114 .
43. D. Kapetanovic, G. Zheng, and F. Rusek, “Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks,” IEEE Commun. Magazine, vol. 53, pp. 21–27, June 2015.
44. A. Mukherjee and A. L. Swindlehurst, “A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures,” in 2011 45th Asilomar Conf. Signals, Systems and Computers, pp. 265–269, Nov 2011.
45. Xu, L. Duan, and R. Zhang, “Proactive eavesdropping via cognitive jamming in fading channels,” arXiv preprint arXiv:1512.02754, 2015.J. Xu, L. Duan, and R. Zhang, “Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels,” IEEE Wireless Commun. Letters, vol. 5, pp. 80–83, Feb 2016.
46. Shiqi, G., Chengwen, X., Zesong, F., Jingming, K., 2016. Resource allocation for physical
47. layer security in heterogeneous network with hidden eavesdropper. China Commun. 13 (3), 82–95 Nasir, A.A., Tuan, H.D., Nguyen, H.H., Nguyen, N.M., 2019. Physical layer security by exploiting interference and heterogeneous signaling. IEEE Wirel. Commun. 26 (5), 26–31.
48. Zhong, Z., Luo, W., Peng, J., Jin, L., 2017. On the security of K-tier heterogeneous cellular networks. Phys. Commun. 25, 570–576.
49. Baracca, P., Laurenti, N., Tomasin, S., 2012. Physical layer authentication over MIMO fading wiretap channels. IEEE Trans. Wireless Commun. 11 (7), 2564–2573.
50. Shu, Z., Qian, Y., Ci, S., 2013. On physical layer security for cognitive radio networks. IEEE Netw. 27 (3), 28–33.
51. Bouabdellah, M., El Bouanani, F., Ben-Azza, H., 2018. Secrecy outage probability in cognitive radio networks subject to Rayleigh fading channels. In: 2018 Inter- national Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, pp. 1–5.
52. Shah, H.A., Koo, I., 2018. A novel physical layer security scheme in OFDM-based cognitive radio networks. IEEE Access 6, 29486–29498.
53. Cardoso, L.S., Chairman, Q., 2006. Quality and security usability. In: Proc. ITU-T Wksp. End-To-End QoE/QoS.
54. Cardoso, L.S., Chairman, Q., 2006. Quality and security usability. In: Proc. ITU-T Wksp. End-To-End QoE/QoS.
55. Fadlullah, Z.M., Wei, C., Shi, Z., Kato, N., 2017. GT-QoSec: A game-theoretic joint optimization of QoS and security for differentiated services in next generation heterogeneous networks. IEEE Trans. Wireless Commun. 16 (2), 1037–1050.
56. Puska, A., Nogueira, M., Santos, A., 2018. Confidentiality-aware decision on handoffs under uncertainty on heterogeneous wireless networks. In: 2018 IEEE Symposium on Computers and Communications (ISCC). IEEE, pp. 00884–00889.
57. Lv, T., Gao, H., Yang, S., 2015. Secrecy transmit beamforming for heterogeneous networks. IEEE J. Sel. Areas Commun. 33 (6), 1154–1170.
58. Fang, D., Qian, Y., Hu, R.Q., 2017. Interference management for physical layer security in heterogeneous networks. In: 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress. IEEE, pp. 133–138.
59. Ren, Y., Lv, T., Gao, H., Li, Y., 2017. Secure wireless information and power transfer in heterogeneous networks. IEEE Access 5, 4967–4979.
60. Irrum, F., Ali, M., Naeem, M., Anpalagan, A., Qaisar, S., Qamar, F., 2021. D2D-enabled resource management in secrecy-ensured 5G and beyond heterogeneous networks. Phys. Commun. 45, 101275
61. Osipov, A., Pleshakova, E., Gataullin, S., Korchagin, S., Ivanov, M., Finogeev, A., & Yadav, V. (2022). Deep Learning Method for Recognition and Classification of Images from Video Recorders in Difficult Weather Conditions. Sustainability, 14(4), 2420.
62. Krakhmalev, O., Korchagin, S., Pleshakova, E., Nikitin, P., Tsibizova, O., Sycheva, I., ... & Krakhmalev, N. (2021). Parallel Computational Algorithm for Object-Oriented Modeling of Manipulation Robots. Mathematics, 9(22), 2886