Защита от атаки Сибиллы без использования распределения криптографических ключей

А.В. Аксенов

МИРЭА – Российский технологический университет

Аннотация: Актуальность статьи обусловлена необходимостью создания легковесных и масштабируемых решений для децентрализованных систем (блокчейн, IoT), где традиционные криптографические методы неэффективны или избыточны. Разработан теоретико-практический метод защиты беспилотных транспортных систем от атаки Сибиллы, основанный на анализе роботом-сервером уникальной сигнатуры карты мощности направленного электромагнитного сигнала каждого клиента-робота. Показаны экспериментальные решения для защиты от атаки Сибиллы на двух воздушных серверах, расположенных на квадрокоптерах. Предлагаемая методика защиты от атак Сибиллы без криптографических ключей использует анализ параметров WiFi-сигнала (например, рассеяние мощности и изменяемую диаграмму направленности антенн) для выявления поддельных роботов-клиентов. Эксперименты подтверждают, что контроль уникальных характеристик радиоканала эффективно ограничивает возможность фальсификации сигнатур. Этот физический подход также применим для обнаружения инъекций пакетов в Wi-Fi-сетях роботов. Ключевыми преимуществами разработанного метода являются: отказ от криптографии снижает вычислительные затраты; физические параметры сигнала служат «отпечатком» легитимных устройств; метод масштабируется на другие угрозы, такие как инъекция трафика.
Ключевые слова: защита от атаки Сибиллы, беспилотные транспортные системы, карта мощности электромагнитного сигнала, WiFi-сигнал, фальсификация сигнатур, спуфер, синтетический апертурный радар.

Введение

Мульти-роботные сети используют беспроводную связь для предоставления широкого спектра услуг, таких как воздушное наблюдение и беспилотная доставка. Однако эффективная координация между несколькими роботами требует доверия, что делает их особенно уязвимыми к кибератакам. В частности, такие сети могут быть серьезно нарушены атакой Сибиллы (Sybil attack), при которой даже один злонамеренный робот может подделать большое количество фальшивых клиентов.

Атака Сибиллы – это тип кибератаки, при которой злоумышленник создает множество поддельных идентификаций или узлов в сети, чтобы получить непропорциональное влияние на систему. Название атаки

происходит от персонажа книги "Сибилла", который страдал от диссоциативного расстройства идентичности.

В контексте мульти-роботных систем или распределенных сетей злоумышленник может использовать один физический узел (например, робот или компьютер), чтобы представлять себя как множество различных узлов.

Атака Сибиллы является серьезной угрозой для многих систем, особенно тех, которые зависят от доверия и децентрализованного управления. Для защиты от таких атак разработаны различные механизмы, включая алгоритмы аутентификации и методы обнаружения спуферов.

"Спуферы" (spoofers) – это устройства или программы, которые подделывают свою идентичность или информацию для обмана систем или пользователей. В контексте беспроводных сетей и кибербезопасности спуферы могут имитировать другие устройства, чтобы получить доступ к сети, манипулировать данными или осуществлять атаки, такие как атака Сибиллы. Например, спуфер может выдавать себя за множество различных клиентов, что затрудняет обнаружение и защиту от него. Это создает угрозу для доверия и безопасности в сетях, особенно в мульти-роботных системах.

Будем рассматривать проблему защиты от атак Сибиллы в сетях с несколькими роботами. Сосредоточимся на общем классе проблем, когда группа роботов-серверов координирует свои действия для предоставления некоторой услуги, используя транслируемые местоположения группы роботов-клиентов.

Сети с несколькими роботами полагаются на беспроводную связь для решения широкого спектра задач и приложений: покрытие [1, 2], борьба со стихийными бедствиями [3], наблюдение [4, 5]. В этом направлении уже используются дроны-доставщики, которые перевозят товары (например, Яндекс доставка [6]), алгоритмы перенаправления трафика (например, Google Maps Navigation). Однако эффективная координация роботов требует

доверия. Для того, чтобы эти мультироботные системы могли оптимально выполнять свои задачи, часто предполагается, что передаваемые данные являются точными и заслуживающими доверия. Особенно сложной атакой на это предположение является так называемая “атака Сивиллы”.

При атаке Сивиллы злоумышленник генерирует (или подделывает) большое количество ложных идентификационных данных, чтобы получить непропорционально большое влияние в сети. Эти атаки, как известно, просты в реализации [7] и могут нанести ущерб сетям с несколькими роботами. Примером этого является покрытие, когда враждебно настроенный клиент может обмануть группу клиентов, находящихся поблизости от него, чтобы создать высокий местный спрос, в свою очередь отказывая в обслуживании законным клиентам. Хотя кибербезопасности многоузловых сетей (например, проводной локальной сети) в целом посвящено огромное количество литературы, этого нельзя сказать о сетях с несколькими роботами [8], что делает их в значительной степени уязвимыми для атак. Это связано с тем, что многие характеристики, уникальные для роботизированных сетей, усложняют безопасность; например, традиционную передачу ключей или криптографическую аутентификацию сложно поддерживать из-за высокодинамичного и распределенного характера команд из нескольких роботов, где клиенты часто входят в сеть и выходят из нее.

Постановка проблемы

Знание позиций агентов в сети облегчает выполнение некоторых совместных задач. Зададимся в сети наличием двух групп агентов: роботами-клиентами, которым требуется некоторый тип услуг на основе местоположения, такой как покрытие площади электромагнитными волнами или доставка товаров, и роботами-серверами, позиции которых оптимизированы для предоставления услуг своим роботам-клиентам.

Необходимо по приблизительным оценкам расположения роботов-клиентов выявить в них поддельного робота-клиента, потенциально имеющий осуществить атаку Сивиллы.

Синтетический апертурный радар широко используется для радиолокационной визуализации и позиционирования внутри помещений [9]. Синтетический апертурный радар – Synthetic Aperture Radar (далее SAR) – это технология радарной съемки, которая используется для получения высококачественных изображений поверхности Земли и других объектов. SAR работает на основе принципа синтетической апертуры, что позволяет создавать изображения с высоким разрешением, даже если антенна радара имеет небольшие размеры.

Основные принципы работы SAR:

- Измерение времени задержки: радар излучает радиоволны, которые отражаются от объектов на поверхности и возвращаются обратно. Измеряя время, за которое сигнал возвращается, можно определить расстояние до объекта.
- Движение платформы: SAR обычно устанавливается на движущихся платформах. Движение платформы позволяет "синтетически" увеличивать размер антенны, что улучшает разрешение изображения.
- Обработка сигналов: полученные данные обрабатываются с использованием сложных алгоритмов, которые позволяют создавать двумерные изображения с высоким разрешением. Она работает на основе радиоволн и позволяет получать детализированные изображения, независимо от погодных условий и времени суток.

С помощью SAR можно обеспечить кибербезопасность многоагентную сеть с несколькими роботами-клиентами. При этом она предоставляет теоретические гарантии безопасности, которые подтверждены экспериментально [2]. Они легко интегрируются с гарантиями

производительности существующих контроллеров с несколькими роботами-клиентами, таких как известные контроллеры покрытия роботов-клиентов [2] и контроллеры доставки дронов [10].

Теоретико-практическая метод защиты от атаки Сибиллы

Поскольку для реализации решения защиты от атаки Сибиллы без использования распределения криптографических ключей не используется специализированное оборудование или обмен зашифрованными ключами, тогда предлагается использовать только Wi-Fi-адаптер и программное обеспечение. На роботах-серверах будут использоваться Wi-Fi-адаптеры в качестве Wi-Fi-анализатора, который будет анализировать физическую информацию, уже присутствующую в беспроводных сигналах. При распространении беспроводных сигналов они взаимодействуют с окружающей средой посредством рассеивания и поглощения объектами вдоль своего пути распространения. Тщательно проанализированные физические характеристики беспроводных сигналов позволят получить уникальную сигнатуру для каждого робота-клиента, посредством измерения мощности принимаемого сигнала в каждом пространственном направлении, что показано на рис. 1. В отличие от содержимого сообщений, такого как сообщаемые идентификаторы или местоположения, которыми могут манипулировать спуферы, пространственные уникальные сигнатуры основаны на взаимодействии физических сигналов, которое невозможно точно предсказать спуферам [11]. Wi-Fi-анализатор необходимо встроить в SAR с активной фазированной решеткой.

Используя уникальные сигнатуры на рис. 1 для каждого клиента в сети, можно получить метрику доверия $M_д \in (0, 1)$ для каждого роботов-клиента. У легитимных роботов-клиентов ожидаемая метрика доверия близка к 1, а у поддельных роботов-клиентов ожидаемая метрика доверия близка к нулю.

Особенно привлекательной особенностью метрики доверия M_∂ является то, что ее можно легко интегрировать в различные решения для борьбы с киберугрозами в сетях [8].

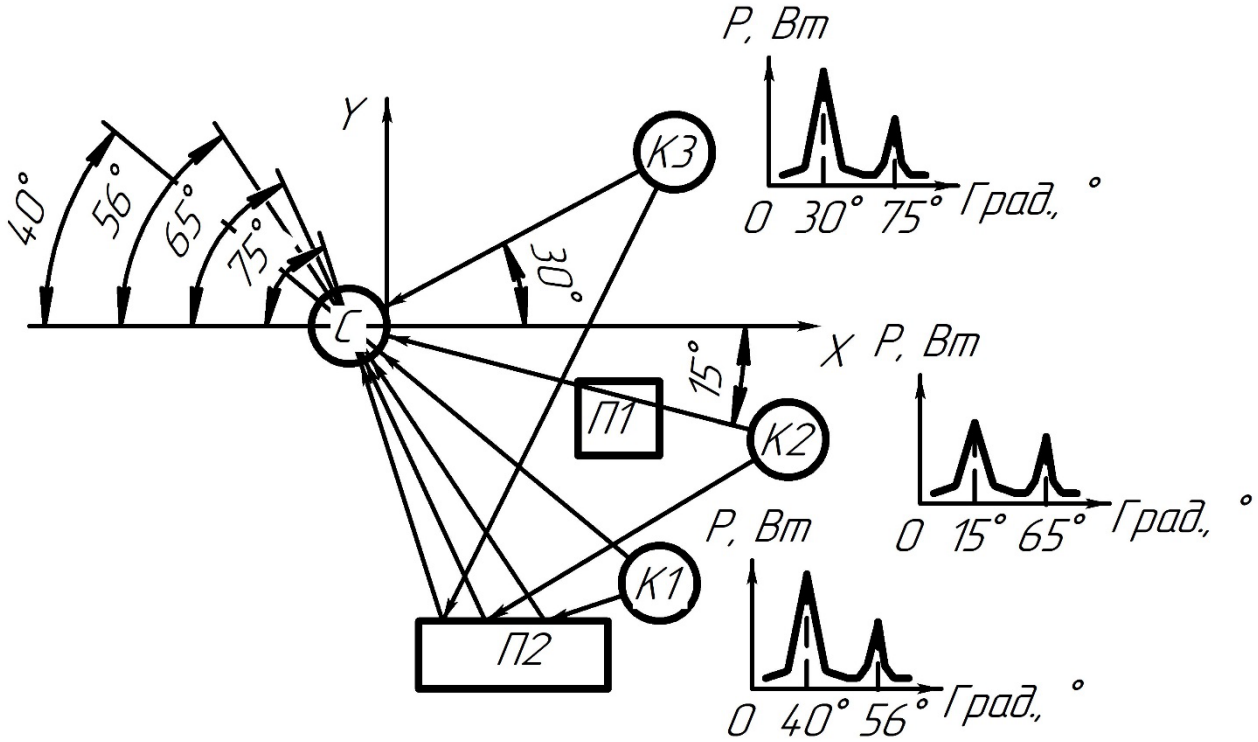

Рис. 1. Получение уникальной сигнатуры роботом сервером путем измерения мощности направленного сигнала каждого клиента: *С* – робот-сервер; *К1*, *К2* и *К3* – соответственно роботы-клиенты, *П1* и *П2* – соответственно препятствия для электромагнитной волны

При этом если спуфер будет установлен очень близко к роботу-клиенту по горизонтали или вертикали, тогда для более надежной защиты от атаки Сибиллы необходимо использовать поворотное устройство в роботе клиенте, которое будет с определенной частотой вращать его розу электромагнитного излучения Wi-Fi радиопередатчика. В этом случае уникальную сигнатуру роботов-клиентов невозможно подделать.

Такое решение учитывает физические свойства беспроводных сигналов и, следовательно, не требует распределенного управления ключами, также

оно основано на недорогих обычных Wi-Fi радиопередатчиках, встроенных в роботы-клиенты, в отличие от аппаратных решений [12], а в роботе-сервере может быть установлена пассивная ФАР. Также данное решение устойчиво к мобильности роботов-клиентов и атакам на масштабирование мощности.

Система робота-сервера основывается на синтетической апертурной радарной технологии (SAR) для создания уникальных сигнатур.

Пусть $P_k = (p_{k1}, ..., p_{kn})$ обозначает позиции роботов-клиентов в трехмерном пространстве. Пусть $P_c = (p_{c1}, ..., p_{cm}\}$ – позиции роботов-серверов в трехмерном пространстве. Записи $[n] = (1, ..., n)$ и $[m] = (1, ..., m)$ обозначает соответственно индексы роботов-клиентов и роботов-серверов. Рассматривается случай, когда подмножество поддельных роботов-клиентов $P_{k.s}$ имеют неопределенные позиции $P_{k.s} = (p_{k.s1}, ..., p_{k.sl})$ в трехмерном пространстве.

Модель угроз. В модели угроз рассматривается один или несколько поддельных роботов-клиентов с одной WiFi-антенной у каждого. Поддельные роботы-клиенты могут быть мобильными и наращивать мощность для каждого пакета передачи данных, переданных по беспроводным каналам. В модели рассматриваются только поддельные роботы-клиенты. Поддельные роботы-серверы в данной модели не рассматриваются. Поддельные роботы-клиенты выполняют атаку Сивиллы для подделки пакетов данных, переданных по беспроводным каналам, и имитирующих $p_{k.sl}$ несуществующих роботов-клиентов, где l может превышать количество законных роботов-клиентов.

Допущение по поддельным роботам-клинтам. Один поддельный (вредоносный) робот-клиент может генерировать несколько уникальных идентификаторов. Каждый поддельный робот-клиент может находиться в поддельной позиции трехмерного пространства. Каждый сгенерированный идентификатор роботов-клиентов считается, что его подделал поддельный

робот-клиент. Подделывая нескольких клиентов, поддельный робот-клиент получает право влияние на работоспособность сети. Все роботы-клиенты, которые не подделаны, считаются законными роботами-клиентами.

Допущение по атаке Сивиллы. «Атакой Сивиллы» называется атакой поддельных клиентов $P_{k.s}$, входящих в множество P_k, и предполагаем, что множество P_k известно, но неизвестно, какие клиенты подделываются $P_{k.s}$.

Чтобы противостоять атаке Сивиллы необходимо:

1. Определить отношение, фиксирующее направленную силу сигнала между клиентом n и сервером m. Здесь рассчитывается отображение, такое, что для любого трехмерного направления (θ , φ), определенного на рис. 2, значение $F_{nm}(\theta, \varphi)$ является мощностью принятого сигнала от клиента n вдоль этого направления. Используя такое отображение, необходимо рассчитать метрику доверия, ожидание которой в пределах $\sigma^2 \ldots 1{,}0$ для законных клиентов и $0 \ldots \sigma^2$ для поддельных клиентов. Порог σ^2 (дисперсию ошибок) необходимо определить аналитически из параметров, таких как отношение сигнал/шум принятого беспроводного сигнала WiFi.

2. Применить рассматриваемый в данном разделе диссертации метод обнаружения спуферов в качестве весов, которые могут ограничить влияние спуферов в задачах с несколькими роботами. В этом случае рассматриваем задачу покрытия, изложенную в [2]. Рассматриваем задачу покрытия, где функция доверия определена параметрами среды и где позиции роботов-клиентов соответствуют пикам в функции доверия. Далее необходимо построить уникальную сигнатуру роботов-клиентов, т.е. профиль направленной мощности сигнала для взаимодействующей пары сервер-клиент. Это позволяет:

1) фиксировать направленную информацию источника передаваемого сигнала и, таким образом, хорошо подходят для маркировки ложно сообщенных позиций клиента;

2) могут быть получены для одной пары сервер-клиент, в отличие от методов оценки местоположения, таких как триангуляция, которые требуют координации нескольких серверов;

3) не могут быть изменены клиентом, поскольку возникновение каждого пути сигнала обусловлено отражениями окружающей среды;

4) применимы в сложных многолучевых средах, где передаваемый сигнал рассеивается от стен и объектов, а такие рассеянные сигналы проявляются как измеримые пики в уникальной сигнатуре, что вносит значительный вклад в уникальность изображения сигнатуры.

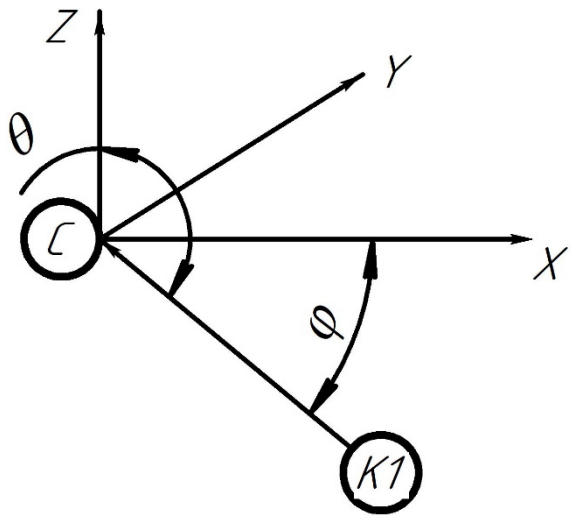

Рис. 2. Назначение углов между роботом-сервером и роботом-клиентом

Уникальная сигнатура роботов-клиентов, строится на основе использования беспроводных каналов h_i, каждый из которых задается и заранее определен для робота сервера. Беспроводной канал измеряется на любом беспроводном устройстве, который имеет сигнатуру в виде затухания мощности электромагнитного сигнала и его поворот фазы. Беспроводные каналы также фиксируют тот факт, что беспроводные сигналы рассеиваются окружающей средой, достигая приемника по (потенциально) нескольким различным путям, что демонстрирует рис. 1. Однако далее в теоретической и

практической части используем 3D-профиль (трехмерное пространство) уникальной сигнатуры роботов-клиентов, который может помочь различать разных роботов-клиентов. Направленные антенны состоят из больших массивов множества антенн, которые слишком громоздки для небольших гибких роботизированных платформ. Выбираем технологию SAR для эмуляции антенны с использованием обычного Wi-Fi-передатчика. Ее ключевая идея заключается в использовании небольшого локального вращения, для получения нескольких снимков беспроводного канала, которые затем обрабатываются как направленный массив антенн. SAR реализована с использованием алгоритма обработки сигнала MUSIC [13] для получения пространственных уникальных сигнатур от роботов-клиентов на каждом роботе-сервере.

Математическая формализация уникальной сигнатуры от робота-клиента следующая:

$$F_{nm}(\theta,\varphi) = \frac{1}{\left| E_n(\boldsymbol{h}_{n.m}\boldsymbol{h}_{n.m}^T) exp\left(\sqrt{-1}\frac{2\pi r}{\lambda} cos(\varphi-\Phi) sin(\theta-\Theta)\right)\right|^2},$$

где E_n – собственные векторы шума антенны; $\boldsymbol{h}_{n.m}$ – вектор отношения сигнатуры беспроводного канала между двумя антеннами, установленными на корпусе робота-сервера m; $\boldsymbol{h}_{n.m}^T$ – транспонированный вектор отношения сигнатуры беспроводного канала; λ – длина волны сигнала, r - расстояние между антеннами; Φ и Θ – соответственно угловая ориентация сервера.

$$\boldsymbol{h}_{n.m} = \frac{h_{1.n.m}}{h_{2.n.m}},$$

где $h_{1.n.m}$ и $h_{2.n.m}$ – соответственно каналы первой и второй антенны.

Однако на практике пики рассеиваемой мощности на уникальных сигнатурах могут иметь небольшие сдвиги из-за шума. Таким образом,

любое сравнение между пиковыми положениями должно допускать некоторую дисперсию из-за этих сдвигов. Электромагнитный шум в беспроводных средах можно близко смоделировать как аддитивный белый-гауссовский [14]. Это приводит к пиковым смещениям, которые также являются гауссовыми, что означает, что их дисперсию легко моделировать и учитывать. Можно утверждать, что сдвиги нормально распределены с нулевым средним и четко определенной дисперсией на основе отношения сигнал/шум (S_{NR}) беспроводной среды:

$$\sigma_{\phi}^2 = \sigma_{\theta}^2 = \frac{1{,}125\lambda^2}{K\pi^2 r^2 S_{NR}},$$

где S_{NR} – отношение сигнал/шум в сети; K – количество пакетов за один такт передачи данных; r – расстояние между антеннами.

Вышеуказанная формула выведена на основе границ Крамера–Рао [15] для линейных перемещений антенн в системах радиолокации с синтезированной апертурой (SAR) [16]. Из данного уравнения следует, что связь между расстоянием антенны rrr и разрешением уникальной сигнатуры σ\sigmaσ становится очевидной. Чем больше расстояние rrr между двумя установленными антеннами, используемыми при расчёте соотношения каналов, тем ниже дисперсия ошибок оценки параметров сигнала и, следовательно, тем выше пространственное разрешение уникальной сигнатуры, формируемой от роботов-клиентов. Это позволяет более точно различать близко расположенные источники сигнала, а значит, и надёжнее выявлять поддельных клиентов. Таким образом, оптимальное размещение антенн существенно влияет на точность и устойчивость всей системы аутентификации. Показатель доверия M_g определяется по следующей формуле:

$$M_{g.n} = \left(\prod_{m} \left[g\left(\varphi_{n.m} - \varphi_{F_{n.m}}, 0, \sigma'^{2}_{\varphi},\right) \times g\left(\theta_{n.m} - \theta_{F_{n.m}}, 0, \sigma'^{2}_{\theta},\right) \right] \right) \cdot$$

$$\cdot \left(\prod g\left(\varphi_{n.i} - \varphi_{n,j}, 0, 2\sigma^{2}_{\varphi},\right) \right) \cdot \left(\prod g\left(\theta_{n.i} - \theta_{n,j}, 0, 2\sigma^{2}_{\theta},\right) \right)$$

где $g\left(\varphi_{n.m} - \varphi_{F_{n.m}}, 0, \sigma'^{2}_{\varphi},\right)$ – нормализованная гауссовская плотность вероятности $f(x, \mu, \sigma^2)$; σ' – дисперсионная ошибка.

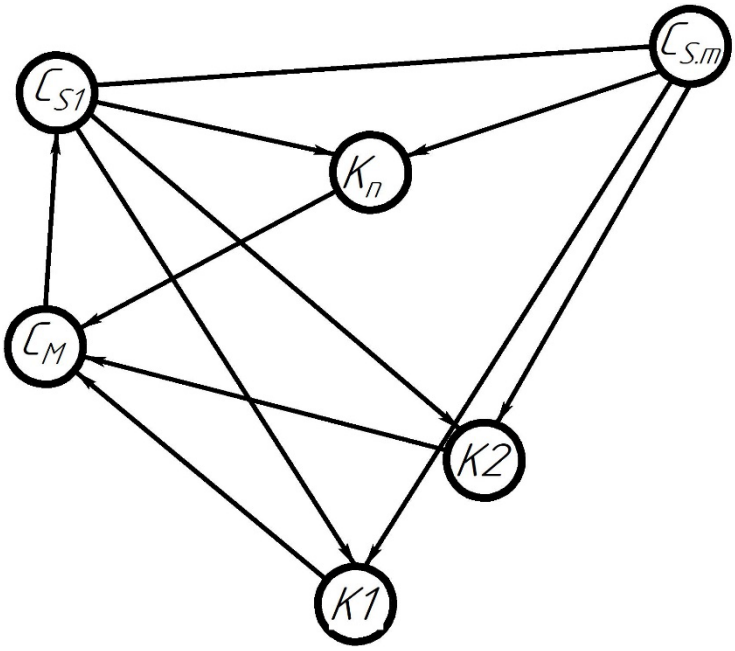

Рис. 3. Схема работы роботов и их направления коммуницирования

За основу ИНС возьмем архитектуру, разработанную в источнике [17, рис. 1], показавшую высокую эффективность в задачах классификации с ограниченным объёмом входных данных. Кроме того, возможно использование более сложных глубоких искусственных нейронных сетей, в частности сверточных сетей на базе стандартной архитектуры VGG [18], которая хорошо себя зарекомендовала в задачах извлечения пространственных признаков из сигналов и изображений. Такие сети

способны эффективно обрабатывать сигнатуры, полученные с учетом временных и амплитудных характеристик электромагнитного сигнала.

Вывод: многолучевые отражения от стен и препятствий четко отличают поддельных роботов-клиентов от легитимных роботов-клиентов даже при φ = 0°.

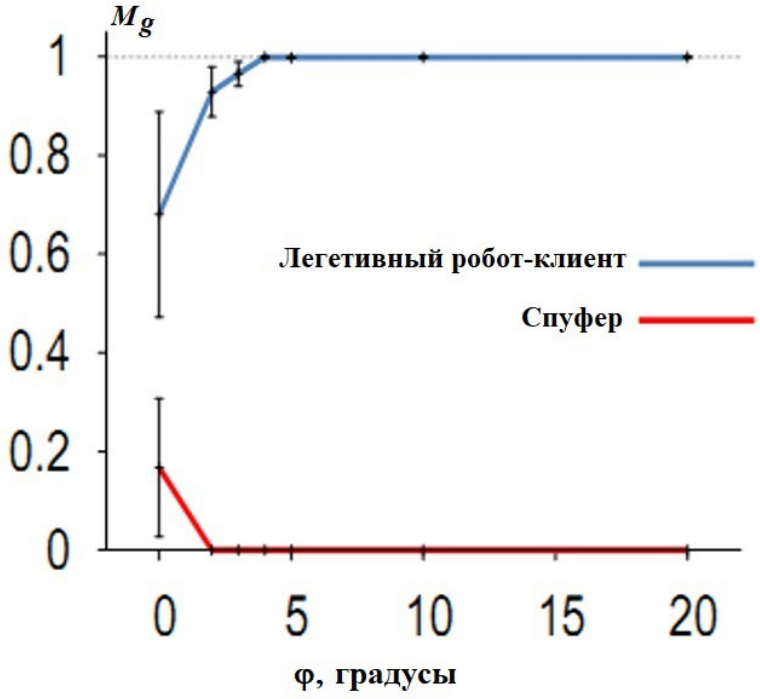

Рис. 4. Взаимосвязь параметра M_g от угла φ расположения робота-клиента от master робота-сервера в безэховой камере без использования неравномерной розы электромагнитного сигнала

Для увеличения быстродействия системы аутентификации роботов-клиентов будем использовать нейронную сеть в качестве показателя Mg. Методика аутентификации роботов-клиентов, входящих в систему роботов согласно рис. 3, будет описана далее. В системе роботов имеются несколько роботов-серверов (назовём их slave роботы-серверы), передающих данные роботам-клиентам, один робот-сервер (master робот-сервер), принимающий сигналы от всех роботов-клиентов и передающий данные о роботах-клиентах одному slave роботу-серверу, несколько роботов-клиентов, принимающих

сигналы только от slave роботов-серверов и имеющих индивидуально настроенную розу электромагнитного сигнала, посылаемого на master робот-сервер, и свой уникальный канал передачи данных. Такая архитектура обеспечивает централизованную обработку информации и позволяет детектировать аномалии на уровне всей системы. Использование нейронной сети в роли анализатора параметра Mg способствует сокращению времени принятия решения и повышению точности аутентификации что демонстрирует рис.4.

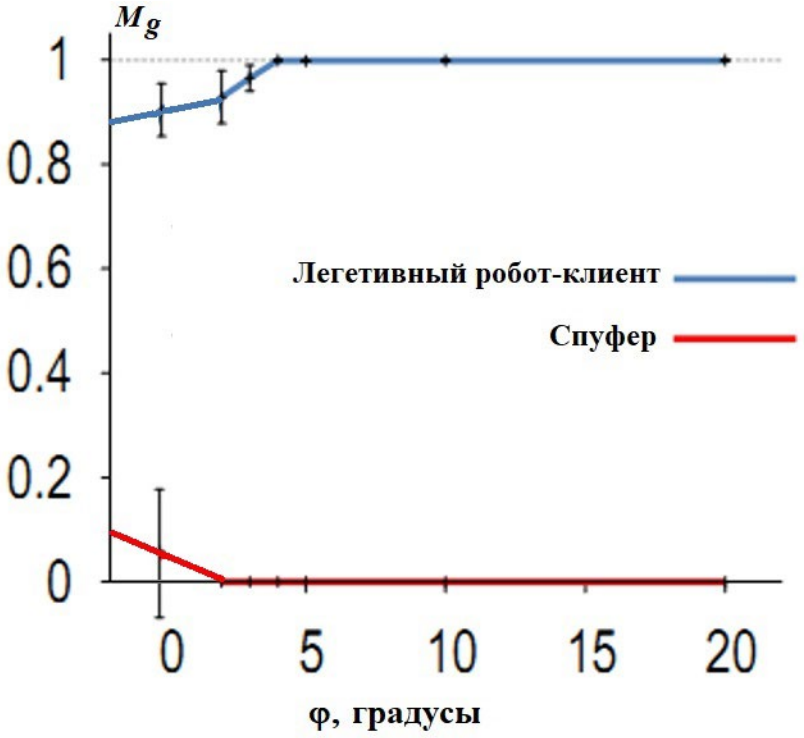

Рис. 5. Взаимосвязь параметра M_g от угла φ расположения робота-клиента от master робота-сервера в безэховой камере с использованием неравномерной розы электромагнитного сигнала

После установки роботов-клиентов в исходные положения они начинают передавать эталонные электромагнитные сигналы связи на master робот-сервер. Master робот-сервер для каждого канала связи от робота-клиента создает таблицу уникальных сигнатур, отражающих характерные особенности передаваемых сигналов. Для каждой такой таблицы master

робот-сервер рассчитывает параметр $M_{g.n.}$, характеризующий поведение конкретного клиента. Значения таблиц уникальных сигнатур служат входными данными для искусственной нейронной сети (ИНС), а параметр $M_{g.n.}$, вычисленный по теоретической формуле, используется в качестве эталонного выхода. На основе этой обучающей пары — входов и соответствующих выходов — осуществляется обучение ИНС. Процесс позволяет сети выявлять закономерности в сигналах и точно определять соответствующий параметр $M_{g.n}$. После успешного обучения система может использоваться для анализа новых клиентов и выявления аномалий или подделок на основе их сигнатур.

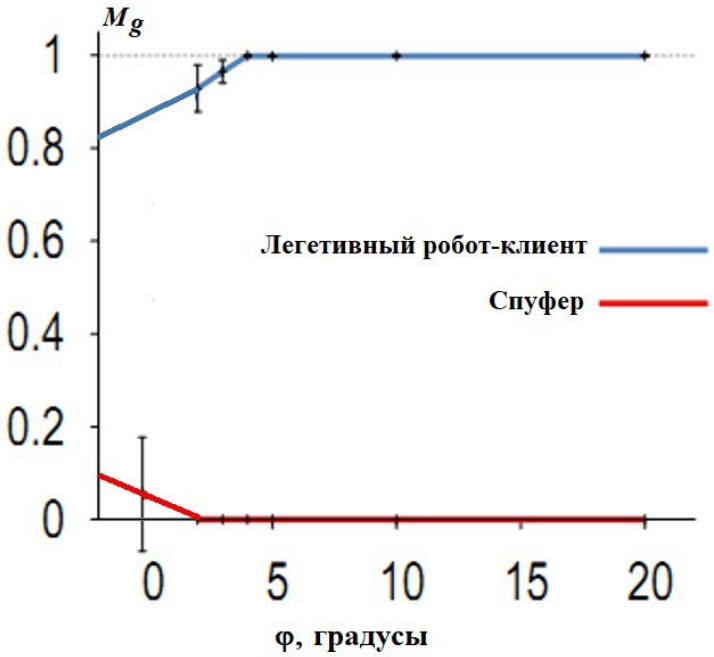

Рис. 6. Взаимосвязь параметра M_g от угла φ расположения робота-клиента от master робота-сервера в безэховой камере с применением препятствия без использования неравномерной розы электромагнитного сигнала

В систему искусственной нейронной сети (ИНС) вводятся поддельные роботы-клиенты, имитирующие легитимных участников сети. Такой тип вмешательства представляет собой атаку Сивиллы — ситуацию, при которой

злоумышленник создает множество фальшивых сущностей (узлов), чтобы получить непропорциональное влияние на распределённую систему. Master робот-сервер, выступающий в качестве управляющего узла, отслеживает подключение каждого клиента и для каждого канала связи формирует таблицу уникальных сигнатур, отражающих поведенческие и/или сетевые характеристики соответствующего робота-клиента. Эти сигнатуры могут включать параметры трафика, временные метки, характеристики сообщений, частотные и статистические данные и другие признаки, способные дифференцировать клиентов.

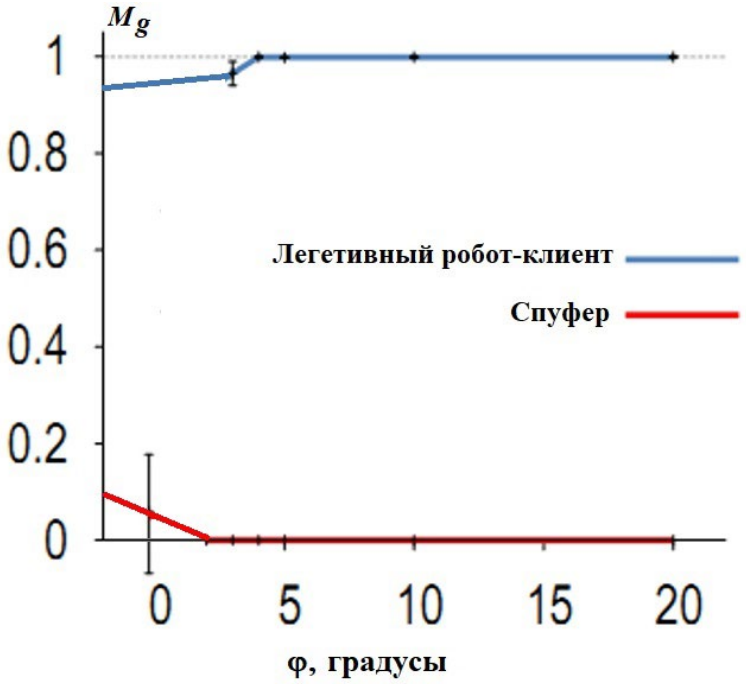

Рис. 7. Взаимосвязь параметра M_g от угла φ расположения робота-клиента от master робота-сервера в безэховой камере с применением препятствия с использованием неравномерной розы электромагнитного сигнала

Для каждой таблицы сигнатур Master робот-сервер рассчитывает параметр $M_{g.n.}$, который служит агрегированным показателем поведения клиента и формируется как для поддельных, так и для неподдельных (настоящих) роботов-клиентов. Таким образом, формируется выборка,

содержащая как входные данные — сигнатуры клиентов и параметр $M_{g.n.}$, так и выходную метку — классификацию клиента как поддельного или неподдельного. На основе этой обучающей выборки производится обучение искусственной нейронной сети, задача которой — научиться отличать поддельных роботов-клиентов от настоящих, выявляя скрытые закономерности и различия в поведении между ними.

После завершения этапа обучения искусственной нейронной сети (ИНС) проводится тестирование её работоспособности и качества полученной модели. На этом этапе система проверяется на ранее не использовавшихся в обучении данных, что позволяет объективно оценить её способность к обобщению и применению знаний в новых ситуациях. Тестирование охватывает различные сценарии с участием как легитимных, так и поддельных роботов-клиентов, в том числе в условиях изменяющейся мощности и подвижности. Это позволяет убедиться в устойчивости модели к внешним помехам и её способности корректно реагировать на сложные атаки.

Эксперименты с учетом статических, мобильных и масштабируемых по мощности поддельных роботов-клиентов.

Методика. Эксперимент проводился в многолучевом испытательном стенде, расположенном в помещении со стенами, препятствиями и неравномерной розой электромагнитного сигнала от легитимных роботов-клиентов. Такая среда моделирует реальные условия эксплуатации, включая многолучевое распространение, отражения и затухание сигнала. Каждый запуск включал один master робот-сервер и группу случайно размещённых роботов-клиентов, что обеспечивало разнообразие топологий и сетевых условий. Были проведены две основные конфигурации: (1) только десять легитимных

роботов-клиентов и (2) смешанная группа, состоящая из десяти легитимных и десяти поддельных роботов-клиентов.

Атаки Сивиллы имитировались в трёх различных вариантах поведения поддельных клиентов:

1. стационарный поддельный робот-клиент с постоянной мощностью передачи сигнала;
2. мобильный поддельный робот-клиент, перемещающийся либо случайным образом, либо прямолинейно по заданной траектории;
3. группа стационарных поддельных роботов-клиентов, масштабирующая мощность пакета данных в диапазоне от 1 до 31 мВт.

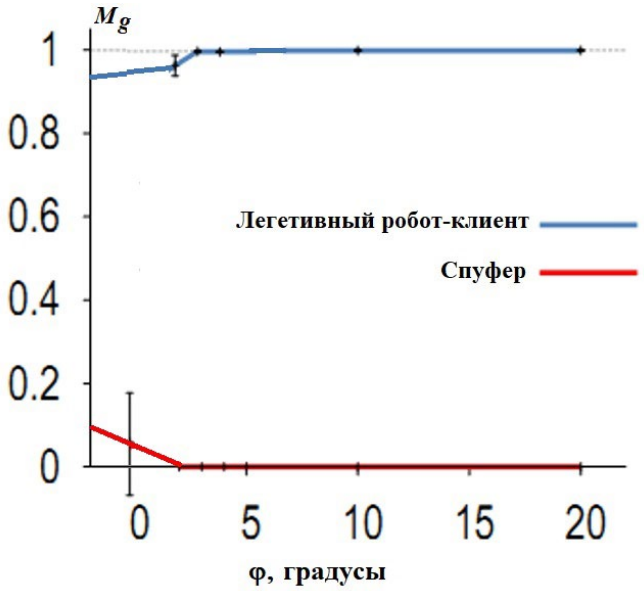

Рис. 8. Взаимосвязь параметра M_g от угла φ расположения 20-и роботов-клиентов, десять из которых поддельных роботов-клиентов двигаются случайным образом, от master робота-сервера в безэховой камере с применением препятствия с использованием неравномерной розы электромагнитного сигнала

Для каждого сценария регистрировались изменения в сигнатурах каналов связи, что позволяло оценить устойчивость системы и нейронной сети к различным формам атак. Дополнительно отслеживалось влияние

различных типов перемещений и масштабирования мощности на способность ИНС различать поддельных и легитимных клиентов. Эти данные использовались при обучении и валидации модели, обеспечивая высокую обобщающую способность нейросети.

Сравнение эффективности предлагаемой системы проводилось с базовым классификатором, основанным на анализе уровня RSSI (Received Signal Strength Indicator) и использующим метод порогового минимального различия [19]. В данном классификаторе роботы-клиенты считаются легитимными, если разница в уровне RSSI между ними и эталонными значениями не превышает заданного порога. Такой подход отличается простотой реализации, но слабо устойчив к многолучевому распространению сигнала и активным атакам, таким как атака Сивиллы.

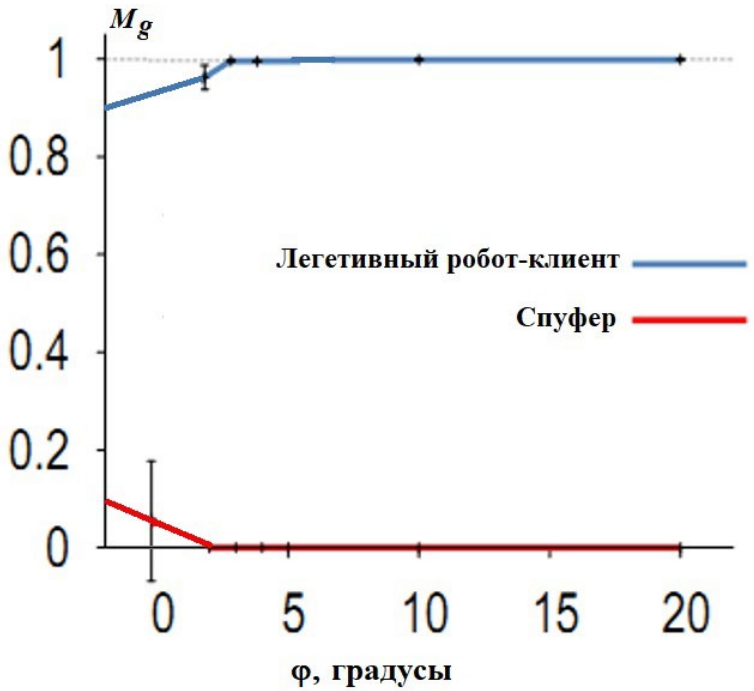

Рис. 9. Взаимосвязь параметра M_g от угла φ расположения 20-и роботов-клиентов, десять из которых поддельных роботов-клиентов двигаются прямолинейно, от master робота-сервера в безэховой камере с применением препятствия с использованием неравномерной розы электромагнитного сигнала

В рамках эксперимента измеренные отношения сигнал/шум (SNR) для роботов-клиентов находились в диапазоне от 5 дБ до 25 дБ, что отражает широкий спектр условий связи — от слабых, зашумлённых каналов до стабильных, с высокой мощностью сигнала. Низкие значения SNR характерны для поддельных клиентов, пытающихся имитировать легитимное поведение в условиях подавления или помех, тогда как высокие значения чаще наблюдаются у настоящих клиентов с прямой видимостью к серверу.

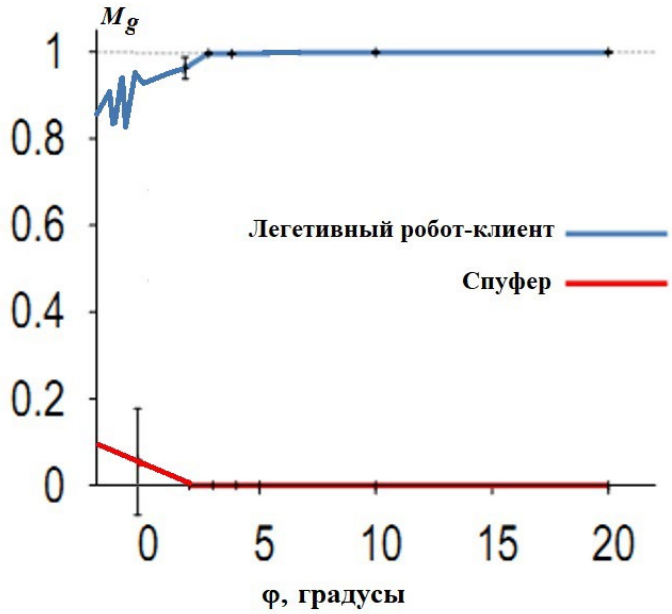

Рис. 10. Взаимосвязь параметра M_g от угла φ расположения 20-и роботов-клиентов, десять из которых стационарных поддельных роботов-клиентов масштабируют мощность пакета данных в предеах от 1 до 31 мВт, от master робота-сервера в безэховой камере с применением препятствия с использованием неравномерной розы электромагнитного сигнала

В таких условиях базовый классификатор RSSI демонстрирует ограниченную точность, особенно при пересечении диапазонов значений для поддельных и легитимных узлов. Наша система на основе ИНС, напротив, использует комплексную сигнатуру канала и параметр $M_{g.n}$., что позволяет ей учитывать множество факторов, влияющих на передачу сигнала. В

результате система демонстрирует более высокую чувствительность к аномалиям в поведении клиентов и устойчивость к манипуляциям с мощностью или положением поддельных узлов.

В нашей системе master робот-сервер выполнял оценивание параметра M_g ценности для всех роботов-клиентов. На рис. 5…10 показаны измерения истинно-положительных результатов в зависимости от угла φ.

Эмпирические данные позволяют с уверенностью утверждать, что пороговым значением параметра M_g для кластеризации роботов клиентов на легитимных и поддельных будет 0,56.

Методика защиты от атаки Сибиллы без использования распределения криптографических ключей позволяет установить доказуемые границы в ожидании влияния поддельных роботов-клиентов.

Экспериментально подтверждено, что, используя группу квадрокоптеров AscTec и наземных клиентов iRobot Create, уровень обнаружения подделок не менее 96%.

Заключение

Расчет показателя доверия в методике защиты от атаки Сибиллы по каждому роботу-клиенту ограничивает вероятность подделывания роботами-клиентами эталонные уникальные сигнатуры рассевания мощности радиоканала связи.

Эмпирические данные позволяют уверенно утверждать, что наиболее эффективно как с точки зрения информационной безопасности, так и с финансовой точки зрения защищаться от атаки Сивиллы с использованием WiFi передатчиков, контролирующих параметр M_g, а также при наличии у легитимных роботов-клиентов изменяемой неравномерной розы электромагнитного WiFi-сигнала.

Метод, заложенный в экспериментальном решении защиты от атаки Сибиллы без применения распределения криптографических ключей и

основаный на фундаментальной физике беспроводных сигналов, применим и к другим проблемам безопасности Wi-Fi в роях роботов-клиентов в обнаружение атак путем инъекции пакетов передачи данных.

Литература

1. Кофнов О.В., Потрясаев С.А., Соколов Б.В., Трефилов П.М. Специальное модельно-алгоритмическое и программное обеспечение проактивного управления групповым поведением робототехнических средств // Известия ЮФУ. Технические науки. 2021. № 1 (218). С. 138-149. URL: doi.org/10.18522/2311-3103-2021-1-138-149.
2. Cortes J., Martinez S., Karatas T., Bullo F. Coverage control formobile sensing networks // IEEE Transactions on Robotics and Automation, 2004, 20(2), pp. 243–255. DOI: 10.1109/TRA.2004.824698.
3. Daniel K., Dusza B., Lewandowski A., Wietfeld C. AirShield: A system-of-systemsMUAV remote sensing architecture for disaster response // In: Systems Conference, 2009 3rd Annual IEEE, pp. 196–200. DOI: 10.1109/SYSTEMS.2009.4815797.
4. Курочкин С.Ю., Тачков А.А. Методы управления групповым движением мобильных роботов (обзор). Мехатроника, автоматизация, управление. 2021. №22(6). С. 304-312. URL: doi.org/10.17587/mau.22.304-312.
5. Beard R., McLain T., Nelson D., Kingston D., Johanson D. Decentralized Cooperative Aerial Surveillance Using Fixed-Wing Miniature UAVs. // Proceedings of the IEEE 94(7), 1306–1324 (2006). DOI: 10.1109/JPROC.2006.876930.
6. Алхимова Д.С., Салпагаров С.И. О программных средствах реализации доставки товаров // Современные наукоемкие технологии. 2023. № 2. С. 9-16. DOI: doi.org/10.17513/snt.39517.

7. Sheng Y., Tan K., Chen G., Kotz D., Campbell A. Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength. // IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, Phoenix, AZ, USA, 2008, pp. 1768-1776, DOI: 10.1109/INFOCOM.2008.239.

8. Sargeant I., Tomlinson A. Modelling malicious entities in a robotic swarm. // 2013 IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC), East Syracuse, NY, USA, 2013, pp. 7B1-1-7B1-12. DOI: 10.1109/DASC.2013.6712635.

9. Kumar S., Gil S., Katabi D., Rus D. Accurate Indoor Localization with Zero Start-up Cost. // In Proceedings of the 20th annual international conference on Mobile computing and networking (MobiCom '14). Association for Computing Machinery, New York, NY, USA, pp. 483–494. URL: doi.org/10.1145/2639108.2639142.

10. Pavone M., Frazzoli E., Bullo F. Adaptive and distributed algorithms for vehicle routing in a stochastic and dynamic environment. // in IEEE Transactions on Automatic Control, vol. 56, no. 6, pp. 1259-1274, June 2011, DOI: 10.1109/TAC.2010.2092850.

11. Malmirchegini M., Mostofi Y. On the Spatial Predictability of Communication Channels. // in IEEE Transactions on Wireless Communications, vol. 11, no. 3, pp. 964-978, March 2012. DOI: 10.1109/TWC.2012.012712.101835.

12. Xiong J., Jamieson K. SecureArray: Improving Wifi Security with Fine-grained Physical-layer Information. // In: Proceedings of the 19th Annual International Conference on Mobile Computing & Networking, MobiCom '13, pp. 441–452. ACM, New York, NY, USA (2013). DOI: 10.1145/2500423.2500444.

13. Hayes M.H. Statistical Digital Signal Processing and Modeling, 1st edn. JohnWiley & Sons, Inc., New York, NY, USA (1996), 624 c.

14. Tse D., Viswanath P. Fundamentals of wireless communication. Cambridge University Press, USA. 2005, 586 c.

15. Gazzah H., Marcos S. Cramer-Rao bounds for antenna array design. // IEEE Transactions on Signal Processing, 2006, Iss. 54, pp. 336–345. DOI: 10.1109/TSP.2005.861091.

16. Stoica P., Arye N. MUSIC, maximum likelihood, and Cramer-Rao bound. Acoustics, Speech and Signal Processing. // in IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 37, no. 5, pp. 720-741, May 1989, DOI: 10.1109/29.17564.

17. Ерохин В.В. Жадное послойное обучение сверточных нейронных сетей // Мягкие измерения и вычисления. 2021. № 11. Т. 48. С. 66–83; URL: doi.org/10.36871/2618-9976.2021.11.004.

18. Simonyan, K., Zisserman, A. (2014). Two-Stream Convolutional Networks for Action Recognition in Videos. Paper presented at the 28th Conference on Neural Information Processing Systems (NIPS), Vol. 27, pp. 568-576.

19. Wang T., Yang Y. Analysis on perfect location spoofing attacks using beamforming. // 2013 Proceedings IEEE INFOCOM, Turin, Italy, 2013, pp. 2778-2786. DOI: 10.1109/INFCOM.2013.6567087.

References

1.Kofnov O.V., Potriasaev S.A., Sokolov B.V., Trefilov P.M. Izvestiya YuFU. Tekhnicheskie nauki. 2021. № 1 (218). pp. 138–149. URL: doi.org/10.18522/2311-3103-2021-1-138-149.

2. Cortes J., Martinez S., Karatas T., Bullo F. IEEE Transactions on Robotics and Automation. 2004. 20(2). Pp. 243–255. DOI: 10.1109/TRA.2004.824698.

3. Daniel K., Dusza B., Lewandowski A., Wietfeld C. Systems Conference, 2009 3rd Annual IEEE. Pp. 196–200. DOI: 10.1109/SYSTEMS.2009.4815797.

4. Kurochkin S.Yu., Tachkov A.A. Mekhatronika, avtomatizatsiya, upravlenie. 2021. № 22(6). pp. 304–312. URL: doi.org/10.17587/mau.22.304-312.

5. Beard R., McLain T., Nelson D., Kingston D., Johanson D. Proceedings of the IEEE. 2006. 94(7). Pp. 1306–1324. DOI: 10.1109/JPROC.2006.876930.

6. Alkhimova D.S., Salpagarov S.I. Sovremennye naukoemkie tekhnologii. 2023. № 2. pp. 9–16. DOI: doi.org/10.17513/snt.39517.

7.Sheng Y., Tan K., Chen G., Kotz D., Campbell A. IEEE INFOCOM 2008 - The 27th Conference on Computer Communications. Phoenix, AZ, USA. 2008. Pp. 1768–1776. DOI: 10.1109/INFOCOM.2008.239.

8. Sargeant I., Tomlinson A. 2013 IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC). East Syracuse, NY, USA. 2013. Pp. 7B1-1–7B1-12. DOI: 10.1109/DASC.2013.6712635.

9.Kumar S., Gil S., Katabi D., Rus D. Proc. 20th Annual International Conference on Mobile Computing and Networking (MobiCom '14). ACM. New York, NY, USA. 2014. Pp. 483–494. URL: doi.org/10.1145/2639108.2639142.

10. Pavone M., Frazzoli E., Bullo F. IEEE Transactions on Automatic Control. 2011. Vol. 56. No. 6. Pp. 1259–1274. DOI: 10.1109/TAC.2010.2092850.

11. Malmirchegini M., Mostofi Y. IEEE Transactions on Wireless Communications. 2012. Vol. 11. No. 3. Pp. 964–978. DOI: 10.1109/TWC.2012.012712.101835.

12. Xiong J., Jamieson K. Proc. 19th Annual International Conference on Mobile Computing and Networking (MobiCom ’13). ACM. New York, NY, USA. 2013. Pp. 441–452. DOI: 10.1145/2500423.2500444.

13. Hayes M.H. Statistical Digital Signal Processing and Modeling. 1st ed. John Wiley & Sons, Inc. New York, NY, USA. 1996. 624 p.

14. Tse D., Viswanath P. Fundamentals of wireless communication. Cambridge University Press. USA. 2005. 586 p.

15. Gazzah H., Marcos S. IEEE Transactions on Signal Processing. 2006. Iss. 54. Pp. 336–345. DOI: 10.1109/TSP.2005.861091.

16. Stoica P., Arye N. IEEE Transactions on Acoustics, Speech, and Signal Processing. 1989. Vol. 37. No. 5. Pp. 720–741. DOI: 10.1109/29.17564.

17. Erokhin V.V. Myagkie izmereniya i vychisleniya. 2021. T. 48. № 11. pp. 66–83. URL: doi.org/10.36871/2618-9976.2021.11.004.

18. Simonyan K., Zisserman A. Proc. 28th Conference on Neural Information Processing Systems (NIPS). Vol. 27. 2014. Pp. 568–576.

19. Wang T., Yang Y. 2013 Proceedings IEEE INFOCOM. Turin, Italy. 2013. Pp. 2778–2786. DOI: 10.1109/INFCOM.2013.6567087.

Дата поступления: 12.08.2025

Дата публикации: 25.10.2025