Инженерный вестник Дона, №11 (2025)
ivdon.ru/ru/magazine/archive/n11y2025/10533

Онтология методов и стратегий защиты радиоканалов от преднамеренных помех

К.С. Григорян, Е.С. Басан

Южный федеральный университет, Ростов-на-Дону

Аннотация: Целью настоящего исследования является анализ методик защиты радиоканала от преднамеренных помех посредством управления ресурсами беспроводного канала, с акцентом на выявление ключевых проблем и направлений дальнейших исследований в данной области. В качестве основного метода применён онтологический подход к инженерии знаний. В работе собраны и систематизированы основные подходы к противодействию глушению каналов связи, а также проанализированы исследования, направленные на формализацию проблем радиосетей с целью их моделирования и анализа. Результаты позволили определить актуальные направления развития, выявить существующие пробелы, сформулировать требования к разрабатываемой модели и обосновать выбор методов, которые будут использоваться в дальнейшем исследовании.
Ключевые слова: помехи, радиоканал, радиосвязь, телекоммуникации, глушение, сеть, моделирование, связь, противодействие, безопасность.

Введение

Классическая модель системы, предлагаемая для исследования, изображена на рисунке 1. В представленной модели присутствуют передатчик и приемник, а также различные виды помех, включая преднамеренные, сгенерированные злоумышленником. В рассматриваемом сценарии легитимные пользователи системы могут сталкиваться с различными типами преднамеренных помех: как интеллектуальных (когда злоумышленник анализирует частотный спектр приема и передачи легитимных узлов), так и с неинтеллектуальными, представляющими собой широкополосные и многотоновые помехи. На рисунке 2 изображены некоторые возможные типы атак на спектральном водопаде. На данном рисунке изображён спектральный водопад устройства, находящегося под атакой глушения канала. Жёлтым и красным цветом окрашены радиосигналы, исходящие от устройства. Промежутки синего цвета обозначают отсутствие сигнала, что является признаком глушения.

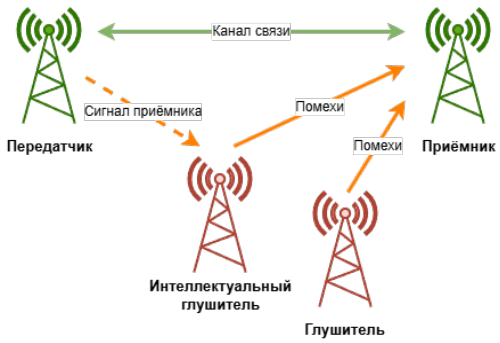

Рис. 1. – Модель системы передачи информации с глушителем

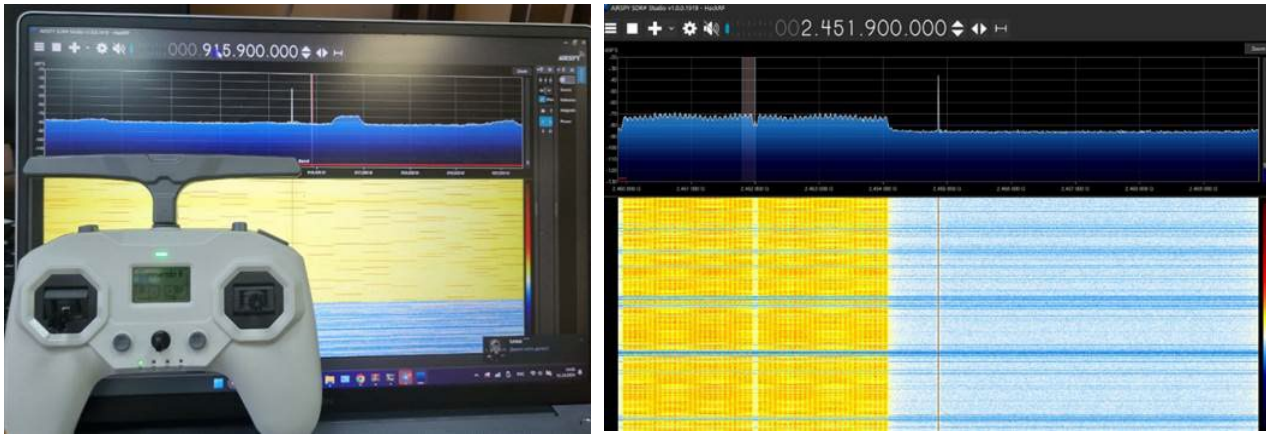

Рис. 2. – Спектральные водопады при помехах в диапазонах 915МГц и 2.4ГГц

Модель нарушителя

В ходе анализа работ, посвященных данной тематике, были выявлены основные стратегии атаки злоумышленником при помощи метода глушения [1].

Реактивный глушитель - Злоумышленник прослушивает канал связи и излучает помехи только в момент обмена информацией в канале.

Постоянный глушитель - Устройство глушения излучает электромагнитные волны или случайную последовательность бит на постоянной основе. Недостатком такой стратегии может являться необходимость в постоянном высоком расходовании энергии.

Маскированный глушитель - Отличается от стратегии постоянного глушения тем, что передает не случайную последовательность, а специально подготовленный набор бит, который делает передающее устройство похожим на один из честных узлов сети.

Импульсный глушитель – глушитель, прослушивающий радиоканал и генерирующий помехи в момент обнаружения служебных пакетов (например: ACK в сетях 802.11 с целью создания коллизий сети или предотвращения принятия данных).

Корреляционные помехи – вид помех, когда устройство злоумышленника генерирует шум, которое имеет те же характеристики что и легитимный передатчик (схожий алгоритм фильтрации, вид модуляции сигнала и т.д.) [2] [3].

Гребенчатый глушитель – способ подавления, который атакует несколько частотных каналов одновременно, создавая "гребенку" из помех. В отличие от широкополосных или точечных глушителей, он распределяет мощность помех дискретно, что делает его эффективным против систем с частотным разнообразием.

Сканирующий глушитель – способ подавления, который последовательно перебирает частотный диапазон, создавая помехи на разных каналах в разное время.

Многотоновые помехи – это тип электронного устройства противодействия, предназначенного для нарушения или блокирования сигналов связи в широком диапазоне частот. Он работает путем одновременного излучения нескольких сигналов разной частоты, которые создают помехи целевым сигналам и создают эффект "глушения" [4].

Основные количественные показатели, которые используются в системах защиты от помех:

- BER/SNR (Bit error rate to signal to noise ratio) вероятность битовой ошибки от отношения сигнала к шуму. Данная характеристика может быть представлена аналитически через формулу 1:

$$BER = Q\left(\sqrt{\frac{E_b}{N^0}}\right), \quad (1)$$

где Q – интегральная функция распределения; E_b– энергия на один бит информации; N^0– спектральная плотность шума.

– BER/SJR (Bit error rate to signal to jammer ratio) вероятность битовой ошибки от отношения сигнала к помехам от глушителя при фиксированном SNR (signal to noise ratio) или SINR (signal to interference plus noise ratio). Данная характеристика может быть представлена формулой 2:

$$BER = Q\left(\sqrt{\frac{E_b}{N^0 + J}}\right), \quad (2)$$

где J – Спектральная плотность помех глушителя.

Формализация проблемы

В общем случае система с использованием ПСПЧ (псевдослучайной перестройки частот) имеет такой набор возможных частот Ω, что $\Omega = \{f1, f2, \dots f_i\}$, где i – количество возможных частот. Тогда в случае с классическим методом ПСПЧ с одной последовательностью информационный сигнал $s(t)$ может быть представлен через формулу 3:

$$s(t) = \sqrt{2E_s/T_s} \cdot e^{j2\pi f_i t}, \quad (3)$$

где E_s – энергия на один символ,

T_s – длительность символа,

f_i – i-ая частота.

В итоге получается baseband сигнал $s(t)$, который в дальнейшем подвергается фильтрации и преобразуется к частоте радиопередачи.

На стороне приемника, после фильтрации и переноса спектра в область baseband сигнала, получается сигнал $r(t)$, представленный формулой 4:

$$r(t) = \sqrt{\frac{2E_s}{T_s}} \cdot \cos(2\pi f_i t + \delta) + n(t) + J(t), \quad (4)$$

где:

$n(t)$- аддитивный шум АБГШ (аддитивный белый гауссовский шум),

$J(t)$ - преднамеренные помехи от злоумышленника,

δ - случайная фаза сигнала.

Рассмотрим Систему, использующую метод DFH (differential frequency hopping). Ее можно описать, добавив в структурную схему G-функцию. Итоговая структурная схема системы с использованием DFH изображена на рисунке 3. Таким образом, G-функция – элемент схемы, который преобразует биты пользовательских данных в номер частоты, в результате чего перестройка частот зависит от пользовательских данных. Синтезатор частот – генерирует частоту в соответствии с результатом G-функции. Радиопередатчик – элемент, осуществляющий модуляцию и перенос спектра на радиочастоту для передачи по радиоканалу. На рисунке 4 изображена структурная схема приёмника с использованием схемы DFH. АЦП – аналого-цифровой преобразователь. БПФ – Быстрое преобразование Фурье. Детектор – блок, получающий цифровые данные в соответствии с видом модуляции. На приёмной стороне также имеется G-функция, которая получает номер канала из пользовательских данных для вычисления следующего частотного скачка.

Метод MPFH, в отличие от DFH, меняет не номер частоты, а номер канала, как это изображено на рисунке 5. На рисунке 6 изображён приёмник с системой MPFH [5]. Как видно из представленной схемы, приёмник осуществляет приём на нескольких каналах, каждый из которых имеет собственный квадратурный детектор. Сигналы с каждого квадратурного детектора подаются на сумматор, после чего происходит декодирование сигнала.

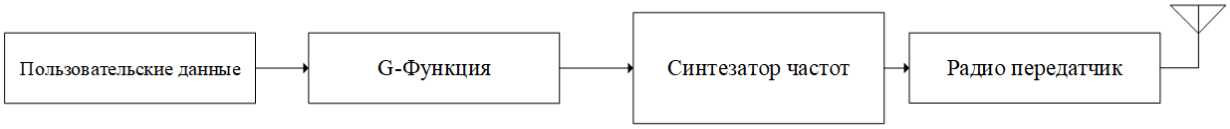

Рис. 3. – Передатчик с системой DFH

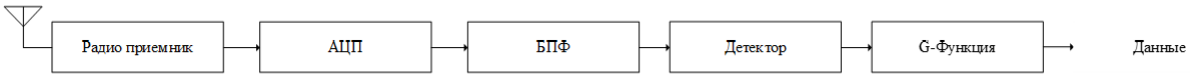

Рис. 4. – Приёмник с системой DFH

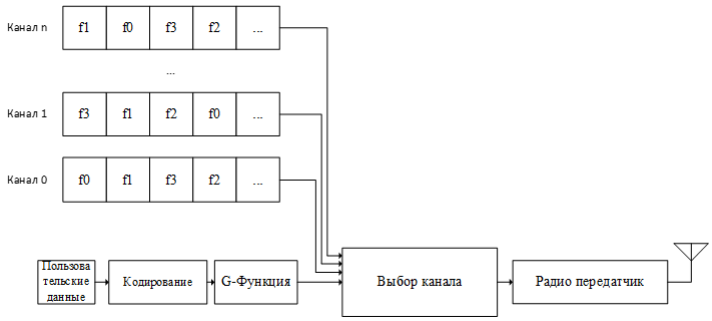

Рис. 5. – Передатчик с системой MPFH

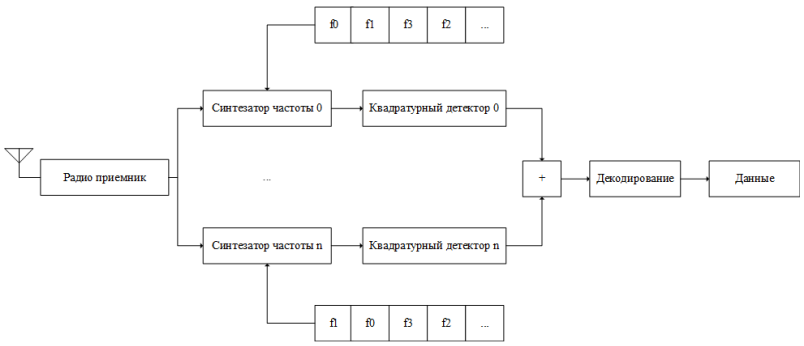

Рис. 6. – Приемник с системой MPFH

Соответственно, baseband сигнал $s(t)$ будет формироваться по другому закону, представленному в формуле 5:

$$s(t) = \sqrt{2E_s/T_s} \cdot e^{j2\pi f_{(i,t)}t}, \quad (5)$$

а на стороне приемника в соответствии с формулой 6:

$$r(t) = \sqrt{\frac{2E_s}{T_s}} \cdot \cos\left(2\pi f_{(i,t)}t + \delta\right) + n(t) + J(t), \quad (6)$$

где $f_{(i,t)}$ – частота на i-ом канале.

Кодеры на стороне передатчика и декодер на стороне приемника – элементы, которые необходимы для получения мягких значений (soft decision) и вычисления значения бит при помощи логарифмических отношений правдоподобия.

В данном разделе были рассмотрены технические аспекты управления частотным спектром. В следующем разделе приведены работы, в которых рассматриваются практические реализации каждого из рассмотренных техник, а также обзор полученных авторами результатами.

Методы регулирования параметров радиоканала

В источнике [6] авторы считают, что псевдослучайного изменения параметров на физическом уровне недостаточно для защиты информации, так как злоумышленник может использовать уязвимости протоколов более высокого уровня. В таблице 1 представлена сравнительная таблица методов регулирования параметров радиоканала.

В источнике [7] авторы Georgios Michalis и др. Предлагают собственную систему перестройки частоты с централизованным узлом генерации случайной последовательности на основе QRNG (Quantum Random Number Generator). Авторы провели моделирование сети из 4

устройств с топологией «кольцо» и впервые доказали возможность использования квантового шума для генерации случайных частот при помощи вычисления критерия хи-квадрат, Колмогорова-Смирнова, а также вычисления корреляции всех используемых частот. Кроме того, авторы предлагают систему распределения последовательности через передачу с использованием шифрования AES + HMAC.

В источнике [8] авторы Tao Huang и др. Предлагают новую систему ПСПЧ, которая основана на использовании активной защиты (IMSFH). Разработанная система позволяет бороться против интеллектуальных реактивных систем глушения при помощи глубокого обучения, которое совмещено с использованием алгоритмом смены частоты с несколькими последовательностями (MSFH). В качестве данных для обучения модели были использованы отношения сигнала к шуму, уровень помех, а также история смены частот. Моделирование показало, что IMSFH имеет лучшие показатели BER чем MPFH и WGMPFH при отношении мощности сигнала к мощности глушителя 0дБ (в случае с IMSFH вероятность битовой ошибки равна 10^{-4}, в то время как у выше названных методов она близка к 0,5). Также авторы утверждают, что при SJR 0дБ вероятность обнаружения частоты передачи равна 0,95 (против 0,65 у WGMPFH и 0,6 у MPFH). Также стоит отметить, что при различных значениях SJR график BER в случае с IMSFH является практически линейным что может говорить о возможности системы приспосабливаться к глушителям при различных условиях эксплуатации.

В источнике [9] авторы Quan Houde и др. предлагают использовать многопрофильную перестройку частот (MPFH). Суть предлагаемой системы состоит в том, что принятый сигнал попадает на два разных канала, где происходит параллельная обработка сигнала. Каждый канал имеет частотный синтезатор, который генерирует частоту из последовательности частот,

хранящейся в памяти канала. После этого сигнал поступает на квадратурный детектор, после чего сигналы каналов суммируются и попадают на декодер Витерби. Результаты, полученные в результате симуляции, показали, что при отношении мощности сигнала к мощности глушителя 0дБ предложенный алгоритм может обеспечить вероятность битовой ошибки не хуже 10^{-4}, что сильно лучше стандартного метода ПСПЧ.

В источнике [10] авторы Yao-bei Wang предлагают систему защиты от реактивных помех на основе метода WGMPFH (Wide Gap Multi-Pattern Frequency Hopping). Данный метод основан на ранее описанном методе MPFH. При этом авторы добавляют дополнительное условие - разнос между двумя каналами должен быть достаточно большим чтобы максимально уменьшить вероятность глушения основного и побочного канала. Схема предлагаемая схема приемника схожа с ранее рассмотренной схемой из MPFH, за исключением того, что для детектирования информации используется блок hard-decision, что требует меньше вычислительных мощностей. В результате моделирования системы при различных разносах по частоте, при SJR 0дБ, BER равен 10^{-3}. Для достижения того же BER WGMPFH требует чтобы SJR был примерно на 4 дБ ниже, чем у FH/BFSK, и на 1 дБ ниже чем у MPFH.

В источнике [11] Yaobei Wang и др. проводят анализ устойчивости метода MSFH (Multi sequence frequency hopping) к реактивным помехам с учетом обмена информацией в канале с АБГШ. В результате симуляций было доказано, что разработанный MSFH метод способен обеспечивать выигрыш 2,47–2,7 дБ по сравнению с классическим ПСПЧ при ОСШ = 13,35 дБ и BER = 10^{-4}.

В источнике [12] авторы предложили реализацию MDFH (Message-Driven Frequency Hopping) метода перестройки частоты. Авторы предлагают

систему, которая состоит из двух основных этапов. Первый – синхронизация приемника и передатчика путем обмена ключа шифрования. Далее: и обе стороны выполняют генерацию ID последовательности с помощью шифра AES с общим ключом и начальным вектором. На следующем этапе передатчик передает ID символ на n-ом канале, где n соответствует десятичному представлению передаваемых пользовательских данных. Приёмник имеет n фильтров, согласованных с ожидаемым ID-символом, что позволяет отфильтровать помехи, не коррелирующие с ID символом. В последующих итерациях передачи и приема обе стороны симметрично обновляют свой ID символ. В результате симуляции, было доказано, что при JSR равному 0дБ вероятность битовой ошибки равна 10^{-4} против 0,5 у MDFH. Моделирование было проведено в условиях маскирующего глушителя.

В источнике [13] Jiawei Zhu и др. делается акцент на обеспечении эффективного поиска и приёма сигнала приемником. Авторы предлагают новый метод восстановления последовательности смены частоты приемником при помощи машинного обучения. В данной работе используются рекуррентные и сверточные нейронные сети для восстановления последовательности скачков. Авторы используют STFT для преобразования сигнала во временно-частотную область. В результате, полученное изображение используется как вход в нейронную сеть.

В источнике [14] Авторы предлагают протокол для вероятностного доступа к каналу в системах с временным разделением каналов. Особенность данного алгоритма заключается в том, что узлам не нужно различать причину недоступности канала в определенный момент времени. Каждый узел может отправить сообщение в канал с вероятностью p_v. Данная

вероятность ограничена пороговой вероятностью p. Каждый определенный момент времени устройство может выполнять два действия:

- Отправить сообщение в канал с вероятностью p_v.

- Если сообщение не отправлено, то выполнить прослушивание канала:

1. Если канал пуст, то увеличить вероятность p_v.

2. Иначе уменьшить вероятность p_v.

Выводы по главе

Методы регулирования параметров радиоканала эволюционируют от простого ПСПЧ к схемам, сочетающим криптографию, машинное обучение и многопрофильную перестройку частот. Алгоритмы MPFH, WGMPFH, MSFH, MDFH и IMSFH показали существенное снижение вероятности ошибок и высокую устойчивость к реактивным глушителям, включая интеллектуальные. В результате комбинация частотной перестройки с ИИ и криптографическими механизмами обеспечивает значительно более надёжную защиту радиоканала от помех и атак.

Перестройка частоты FH (Frequency Hoping) – стандартный методы защиты канала, который заключается в простой перестройке частоты на основе заранее известного алгоритма перестройки, который известен приемнику и передатчику.

DFH (Differential Frequency Hoping) – методы перестройки частоты, в котором выбор канала происходит по детерминированному алгоритму, известному как приемной, так и передающей части.

IMSFH (Intelligent Multi-Sequence Frequency) – Это способ, при котором перестройка происходит при помощи машинного обучения, которое позволяет распознавать закономерности реактивных помех.

DSFH (Dual-Sequence Frequency Hopping) – Метод, при котором используются две взаимодополняющие последовательности для передачи

информации. Существуют как более простые разновидности данного метода, при которых на втором канале передается копия основного канала передачи, так и более сложные, при которых по вспомогательному каналу передаются метаданные, предназначенные для коррекции ошибок.

MDFH (Message-driven Frequency Hopping) – Метод расширения спектра, в котором выбором несущей частоты управляет не псевдослучайная последовательность, а часть информационных битов.

MPFH (Multi-Pattern Frequency Hopping) – Заключается в использовании одновременно нескольких частот для повышения устойчивости к реактивным атакам глушения. Данные метод, также как и DSFH может использоваться вместе с суммированием сигналов нескольких каналов для дальнейшего детектирования при помощи получения мягких значений через получение максимального значения правдоподобия и специальных кодов, таких, как коды Витерби.

WGMPFH (Wide-Gap Multi-Pattern Frequency Hopping) – Алгоритм использования нескольких частот для приема и передачи, который заключается в большом частотном разнесении побочных каналов.

Таблица № 1

Сравнение рассмотренных методов повышения защиты радиоканала

№ п/п	Критерий	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
1	Используемый метод	QRNG + FHSS	IMSFH	MPFH	WGMPFH	MSFH	MDFH	Deep Learning (CNN-GRU)	MAC protocol

2	Цель	Усиление устойчивости к глушению за счёт истинно случайных частотных скачков.	Защита от следящих помех	Защита от следящих и частично-полосных помех	Защита от следящих помех	Борьба с реактивным глушением через множественные FH-последовательности	Защита от маскированных помех	Восстановление FH-последовательностей в условиях глушения с помощью ИИ	Разработка MAC-протокола, устойчивого к адаптивным глушителям в одношаговых беспроводных сетях.
3	Метод	Использование квантового генератора случайных чисел (QRNG) для FHSS	Глубокое обучение + MSFH	Множественные FH-шаблоны	Широкие частотные интервалы	Использование нескольких последовательностей для смены частот	Защищенной ID-последовательности для аутентификации сигнала и подавления маскированных помех.	Гибридная CNN-GRU сеть для анализа time-frequency диаграмм сигналов	Использование вероятностного доступа к каналу с адаптацией вероятностей передачи на основе наблюдений за состоянием канала

4	Преимущества	Высокая устойчивость к предсказанию и глушению за счёт истинной случайности	Лучшая BER при высоком JSR	Универсальность в борьбе против нескольких методов глушения	Повышение BER на 1–3 дБ по сравнению с MPFH	Высокая устойчивость против реактивных глушителей (выигрыш 2,4-2,7дБ в сравнении с FHSS)	- Высокая спектральная эффективность - Устойчивость к сильным помехам с высоким JSR	- Обобщение на новые типы помех - Точность более 95% при SNR более -6 дБ	- Локальный контроль без централизованного управления - Энергоэффективность
5	Ограничения	Зависимость от аппаратного QRNG, сложность синхронизации	Высокие вычислительные затраты	Сложность синхронизации	Снижение спектр. эффективности	Сложность синхронизации	- Дополнительная сложность из-за генерации ID-последовательности	Требует больших вычислительных ресурсов для обучения	Требует дополнительных затрат на оценку параметров сети

Методы построения модели защищенной системы

Построение модели системы на основе некооперативных игр широко применяется в проблемах перестройки частоты [15]. Существуют различные решения, позволяющие моделировать процесс работы канала связи в условиях глушения:

- Байесовская игра — некооперативная игра с неполной информацией, в которой игроки имеют лишь вероятностные представления о характеристиках противника. Вместо точных данных используются априорные распределения вероятностей [16].
- Игра Штакельберга - Иерархическая игра, в которой один игрок (легитимный узел) первым выбирает стратегию, а другой (злоумышленник) реагирует на его действиях [17].
- Марковская игра - динамическая игра, в которой состояние системы меняется случайным образом в зависимости от действий игроков. Это расширение марковских процессов принятия решений (MDP) для многопользовательских сценариев [18].
- Игра с нулевой суммой - антагонистическая игра, в которой выигрыш одного игрока равен проигрышу другого (например: функция полезности легитимного узла зависит от пропускной способности, а функция полезности злоумышленника зависит от эффективности подавления легитимных узлов) [19].

Ключевой задачей при построении игровой модели – определение так называемой функции полезности (utility function). Легитимные узлы и злоумышленники имеют стратегии T и J соответственно, а также функции полезности u_T и u_J. Задача игроков – максимизировать функцию полезности. Задача злоумышленника противоположна – минимизировать полезность легитимного узла. В качестве функции полезности могут

выступать различные характеристики канала. В источнике [20] авторы используют функцию SINR в качестве u_T. Выбор именно SINR в качестве u_T, а не пропускной способности авторы объясняют тем, что многие технологии передачи голосовой информации не требуют предельной пропускной способности по Шеннону, а используют кодеки, адаптирующиеся к SINR. Формула u_T в таком случае будет иметь вид, представленный в формуле 8:

$$u_T(T,J) = \frac{\alpha T}{N^0 + \beta J} - C_T T, \tag{8}$$

Где a – коэффициент усиления канала,

β- коэффициент усиления сигнала глушителя,

N^0-шум в канале,

C_T-стоимость передачи узла.

В источнике [21] авторы выбрали в качестве u_T пропускную способность по формуле Шеннона. Вид u_T представлен в формуле 9:

$$u_T(T,J) = \ln\left(1 + \frac{\alpha T}{N^0 + \beta J}\right) - C_T T. \tag{9}$$

В источнике [22] авторы рассматривают систему со случайным доступом, в которой узлы сети конкурируют за доступ к общей среде. В данной работе u_T задана в виде вектора действий всех передающих сенсоров $a = (a_1, a_2, \dots, a_n)$,

где a_i принимает значение 1 или 0, в зависимости от наличия или отсутствия передачи информационным сенсором. Таким образом, функция u_T имеет вид, представленный в формуле 10:

$$u_T(a) = \begin{cases} 0, \text{если } a_i = 0 \\ 1, \text{если } a_i = 1 \\ -c_i, \text{штраф за неудачу, состояние коллизии.} \end{cases} \quad (10)$$

Равновесие Нэша в игре легитимных узлов и глушителя – состояние, в котором полезности легитимного узла и злоумышленника не могут быть увеличены при изменении стратегий T и J, что может быть выражено формулой 11:

$$\begin{aligned} u_T(\check{T}, J) \leq u_T(T, J), \\ u_J(T, \check{J}) \leq u_T(T, \check{J}). \end{aligned} \quad (11)$$

Методы оптимизации стратегий

Взаимодействие легитимных узлов и злоумышленника в канале связи представляет собой многоступенчатую динамическую игру, в которой участники игры могут дополнять свои субъективные вероятности. Существуют различные способы организации обучения в ходе многоступенчатой игры, такие как Q-learning, Deep Q-Learning, генетический алгоритм.

В источнике [23] авторы предлагают систему противодействия к глушению в когнитивном радио при помощи Q-learning. Взаимодействие легитимных узлов и злоумышленника рассматривается как Марковский процесс принятия решений. В качестве состояния используется SINR каналов. Действие (action) злоумышленника – выбор канала передачи. Награда (Reward) – даётся на основе пропускной способности. Q-таблица обновляется при помощи

уравнения Беллмана со стратегией исследования ε-greedy. Алгоритм позволяет бороться против 4 видов глушителей: случайный, сканирующий, гребенчатый спектральный и трекинговый.

В источнике [24] авторы предлагают систему на основе Deep Q-learning. В этом методе Q-таблица заменяется нейронной сетью для работы с большим пространством состояний. Авторы используют приоритетное воспроизведение опыта с использованием метода Парето, которое основано на TD-ошибке (Temporal difference error) и мгновенной награде за высокий SINR. Кроме того, предусмотрено уменьшение веса старых образцов в памяти, что снижает риск переобучения сети. Авторы утверждают, что система позволяет бороться с 4 типами глушителей: случайные, следящие, гребенчатые, сканирующие. Достоинство данного алгоритма – возможность применения в крупных динамических системах за счёт обучения на данных используемого канала.

В источнике [25] авторы предлагают многодоменную стратегию, объединяющую частотный и энергетический домен. Ключевым методом в данной работе служит генетический алгоритм, который решает задачу оптимизации для легитимного узла и злоумышленника через обратную индукцию. Генетический алгоритм позволяет максимизировать SINR в условиях игры Штаклберга с лидером в виде легитимного узла и ведомым в виде злоумышленника. Система позволяет бороться против адаптивных глушителей. Достоинство алгоритма – отсутствие высоких требований к вычислительным ресурсам.

Игровые модели

В источнике [26] авторы описывают уменьшение влияния глушения с точки зрения теории игр. В качестве так называемых игроков выступает сеть из n-

ого количества честных узлов, обменивающихся данными по каналу с временным разделением, и глушащее устройство. Процесс обмена информацией представляется как процесс игры, которая имеет некоторые точки равновесия Нэша, среди которых есть состояние, при котором энергия глушащего устройства максимальна, а вероятность обмена информацией p равна нулю. Цель честных узлов - сместить игру в точку равновесия Нэша в пользу сети для того, чтобы исключить случай нулевой вероятности обмена данными. В первую очередь, данный способ предназначен против глушащего устройства с ограниченным запасом энергии. Для реализации метода предлагается использовать дополнительный узел анти-глушитель с вероятностью передачи q. Данный узел является приманкой для устройства заглушения, которая заставляет это устройство расходовать больше энергии.

В источнике [27] Yalin Evren Sagduyu и др. Предлагают модель на основе Байесовской игры с целью противодействия атакам глушения типа DoS на уровне управления доступом MAC. Байесовская игра заключается в том что ни легитимный пользователь, ни злоумышленник не обладают о полной информации о противнике и вынуждены строить свои стратегии на не полной информации. Авторы предложили два подхода, для скрытия информации: Контроль мощности передачи и введение метода вероятностного доступа к каналу. Данные подходы позволяют затруднить получение информации о канале и, как следствие, снизить эффективность глушителя.

В источнике [28] Dejun Yang и др. получили аналитические выражения для оптимальных стратегий как пользователя, так и глушителя, используя игру Штакельберга. Авторы доказали, что используя модель, рассмотренную в данной работе, легитимные узлы, следуя равновесию Штакельберга, могут нивелировать преимущества интеллектуального глушителя. Основной

параметр, который изменяет пользователь в данной игре – это мощность передачи.

В источнике [29] Fuqiang Yao и Luliang Jia предлагают модель защиты от глушения на основе Марковской игры с использованием метода Q-Learning. Авторы получили результаты симуляции, представив зависимости коэффициента нормализации, коэффициента ложного срабатывания (когда легитимный узел принял другой узел за помеху или наоборот), а также коэффициент ложных тревог. В результате метод на основе Марковской игры имеет наилучшие показатели по сравнению с другими предложенными методами на основе Q-Learning. Данный результат может быть обоснован тем, что Марковские игры обладают полезным свойством – они хорошо подходят для систем с высокой динамикой, в которых необходимо учитывать зависимость взаимодействий участников системы [30].

В источнике [31] Tianlong Song и др. предлагают модель защиты от атаки глушения на основе антологической игры с нулевой суммой. Была исследована проблема защиты от помех при регулировании мощности между законным пользователем и источником помех, и мощность была определена как функция полезности.

В источнике [32] Zhang и др. предлагают модель на основе многоуровневой игры Штаклберга. В этой модели имеется множество легитимных узлов и один злоумышленник. В этой игре легитимные узлы действуют сообща для того чтобы оптимизировать общую пропускную способность канала. В статье предлагается подход “No Pains, No Gains”, который предполагает жертвование узлом частью своих ресурсов для улучшения пропускной способности всей сети.

Сравнительный анализ работ, используемых методы оптимизации стратегий, представлен в таблице 2, в которой отражены основные преимущества и цели используемого метода. В таблице 3 представлена

сводная информация о рассмотренных игровых моделях. В ней отражаются условия применения, функция выигрыша и метода, используемая для защиты канала. Также отражён вид равновесия, рассмотренного в каждой работе.

Таблица № 2

Сравнение рассмотренных методов оптимизации стратегий

№ п/п	Критерий	[23]	[24]	[25]
1	Используемый метод	Q-learning, Марковский процесс принятия решений, эпсилон-жадная стратегия	Интеллектуальный алгоритм генерации бивариативных FH-паттернов на основе DQN с PER и Pareto.	Игра Штаклберга и генетический алгоритм (GAED)
2	Цель	Максимизация пропускной способности канала	Улучшение свойств системы перестройки частоты через адаптивные параметры (скорость и интервал скачков)	Оптимизация частотного и энергетического домена в системе с перестройкой частоты
3	Преимущества	- Устойчивость к нескольким видам глушения (случайный, сканирующий, гребенчатый, отслеживающий)	Устойчивость к комплексным электромагнитные помехи (широкополосные, узкополосные, сканирующие)	Использование мультидоменного подхода позволяет улучшить энергоэффективность одновременно с SINR канала

Таблица № 3

Сравнение рассмотренных игровых моделей

№ п/п	Критерий	[26]	[27]	[28]	[29]	[31]	[32]
1	Тип игры	Некооперативная игра с элементами иерархии	Байесовская игра	Одноуровневая игра Штаклберга	Марковская игра	Игра с нулевой суммой	Одноуровневая игра Штаклберга
2	Условия	Многопользовательская игра с энергоограниченным глушителем	Многопользовательская игра с неполной информацией о типах пользователя	Один лидер – пользователь, один ведомый - глушитель	Многопользовательская игра с совместными действиями между легитимными узлами	Один легитимный узел и один глушитель	Многопользовательская игра с энергоограниченным глушителем
3	Функция выигрыша	Для пользователя – пропускная способность. Для злоумышленника – энергозатраты	SINR	SINR	Количество удачных приёмов информации	Пропускная способность канала	Общая пропускная способность канала

4	Равновесие	Два равновесия Нэша: желательное и нежелательное	Байесовское равновесие Нэша	Равновесие Штаклберга	Марковское равновесие	Равновесие Нэша	Равновесие Штаклберга
5	Методика	Активная защита с целью истощения его энергии	Анализ влияния неопределенности на эффективность глушения	Управление мощностью передачи в зависимости от характера глушения	Многоагентное обучение с подкреплением с учётом динамически меняющихся условий среды	Итеративный алгоритм «водонаполнения» (iterative water pouring), для распределения мощности по каналам	Агрегация каналов с целью повышения общей пропускной способности
6	Техника оптимизации	Аналитический поиск равновесия Нэша + градиентный метод + эвристики для вероятности доступа к каналу анти-глушителя	Аналитическое решение + динамические методы (градиентный метод, фиктивная игра)	Аналитическое решение + динамические методы (градиентный метод)	Обучение с подкреплением (Q-learning)	Аналитическое решение + динамические методы (градиентный метод)	Обучение с подкреплением (Q-learning), которое сходится к равновесию Штаклберга

Результаты

В данной статье был проведен обзор методов защиты канала от различных видов глушения. Были рассмотрены разновидности устройств-глушителей, методы регулирования параметров радиоканала для борьбы с глушением, а также способы построения моделей на основе разных форм теории игры: игра Штакельберга, Байесовская игра и игры с нулевой суммой. Были рассмотрены методы оптимизации стратегий, которые могут использоваться в игровой модели. На рисунке 7 изображены модели и методы, используемые в построении системы для защиты от радиопомех. На рисунке 8 изображена онтология методов и стратегий защиты радиоканалов от преднамеренных помех.

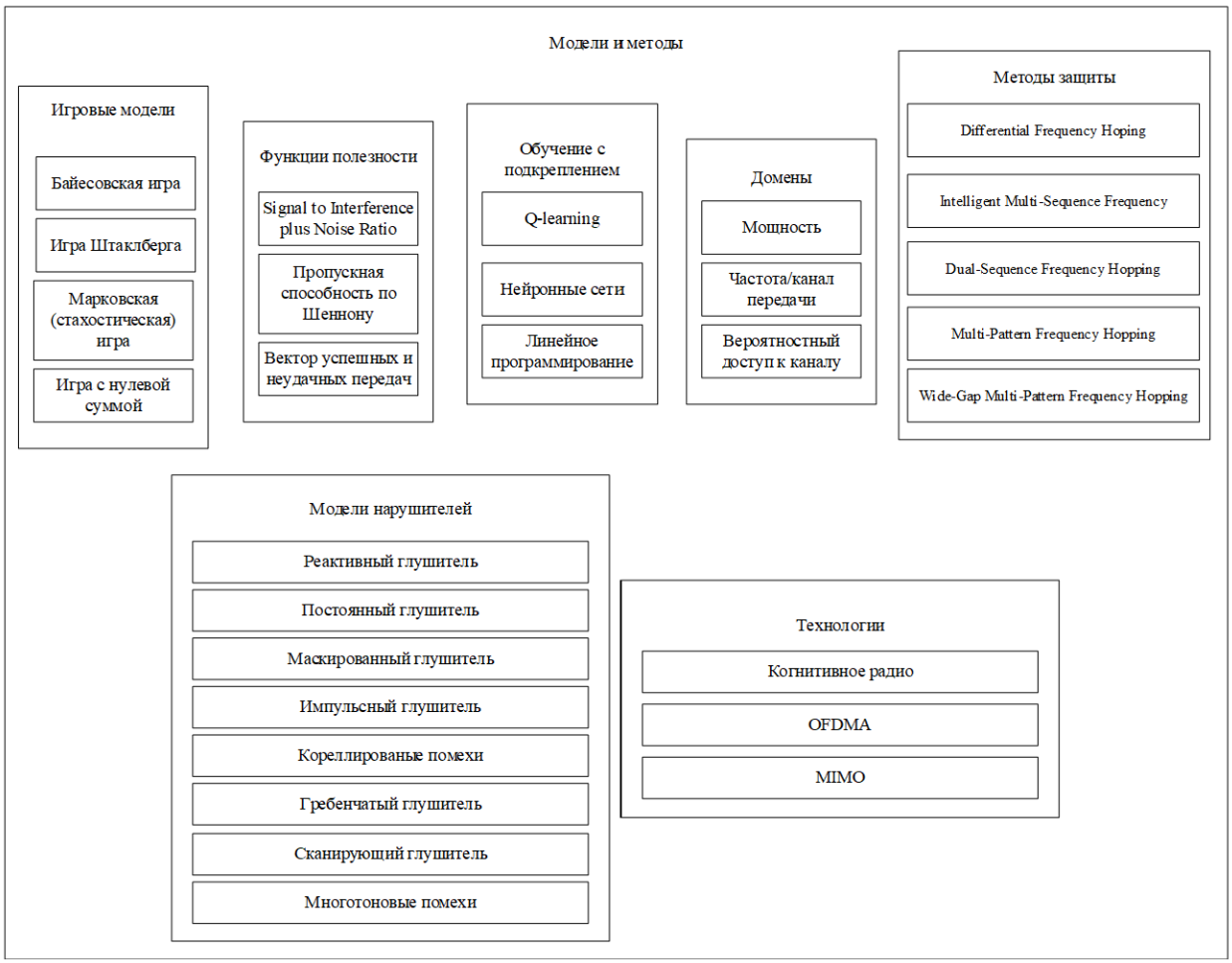

Рис. 7. – Модели и методы, используемые в построении системы для защиты от радиопомех

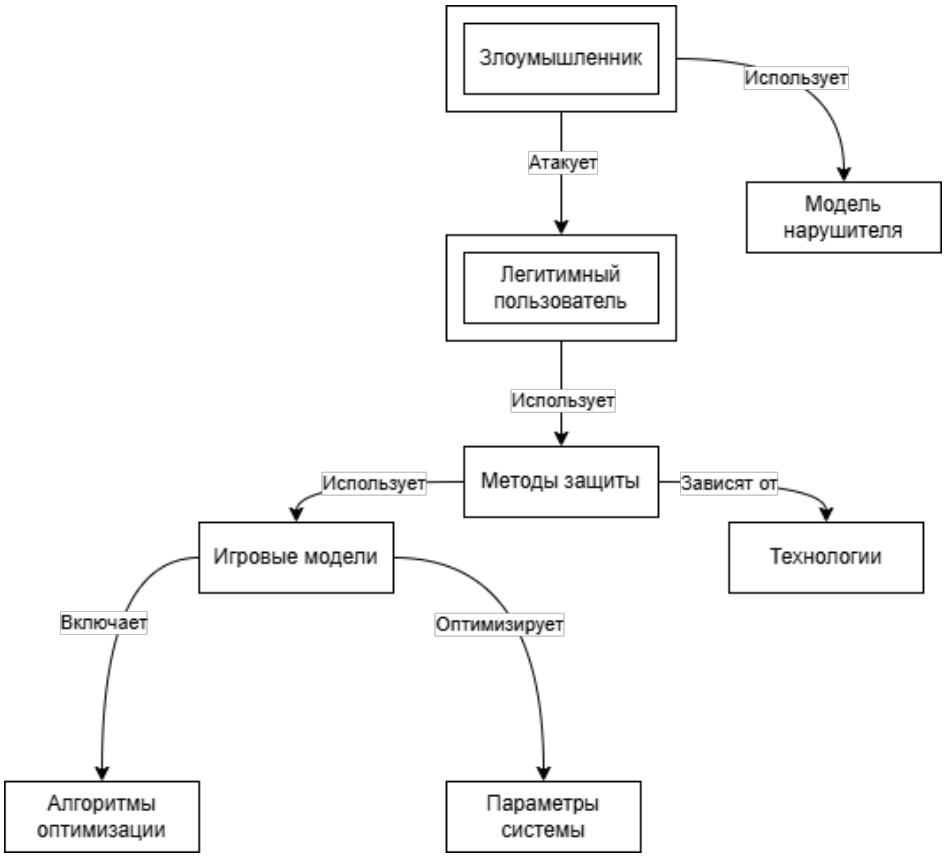

Рис. 8. – Онтология методов и стратегий защиты радиоканалов от преднамеренных помех

Выводы

Анализ показал, что методы регулирования параметров радиоканала, основанные на перестройке частоты (ПСПЧ, MPFH, WGMPFH, MSFH, MDFH, IMSFH), обеспечивают значительное снижение вероятности ошибок и повышают устойчивость к преднамеренным помехам.

Сравнение методов на основе ПСПЧ с игровыми моделями показывает, что первые ориентированы преимущественно на случайность и устойчивость к глушению в фиксированных сценариях, но уязвимы при адаптивных атаках. Игровые модели, напротив, учитывают поведение злоумышленника и позволяют формализовать стратегическое противодействие на основе теории

игр, что открывает возможности для построения динамически адаптивных систем защиты. Таким образом, ключевой проблемой остаётся интеграция сильных сторон обоих подходов: высокой помехоустойчивости ПСПЧ и адаптивности игровых моделей.

Литература (References)

1. Vadlamani S., Eksioglu B., Medal H., and Nandi A. Jamming attacks on wireless networks: A taxonomic survey. International Journal of Production Economics, vol. 172, 2016, pp. 76–94.

2. Basar T. and Wu Y. W. Solutions to a class of minimax decision problems arising in communication systems. Journal of Optimization Theory and Applications, vol. 51, 1986, no. 3, pp. 375–404

3. Zhou K., Song T., Ren J., and Li T. Robust CDMA receiver design under disguised jamming. IEEE Signal Processing Society SigPort, 2016, pp. 2179-2183.

4. Ahmed A. M., Begum Z., Sultana A., Samreen S., Maheen L., and Afreen I. Multitone jammer, ISL Engineering College, Department of Electronics and Communication Engineering, Hyderabad, India, Technical Report, 2016, pp. 132-150

5. Chao Z., Zhu X., He W., Ban Y., and Chen S. A frequency-hopping communication system based on multiple parallel hopping. IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2018, pp. 1564–1568, IEEE

6. Liu X., Noubir G., Sundaram R., and Tan S. SPREAD: Foiling smart jammers using multi-layer agility. IEEE INFOCOM 2007 – 26th IEEE International Conference on Computer Communications, Anchorage, AK, USA, 2007, pp. 2536–2540, IEEE

7. de Curto J., de Zarza I., Cano J. C., and Calafate C. T. Enhancing communication security in drones using QRNG in frequency hopping spread spectrum. Future Internet, vol. 16, 2024, no. 11, p. 412, art. 412

8. Huang T., Liu Y., Liu X., and Wang M. A new improved multi-sequence frequency-hopping communication anti-jamming system. Electronics, vol. 14, 2025, no. 3, p. 523

9. Quan H., Zhao H., and Cui P., Anti-jamming frequency hopping system using multiple hopping patterns. Wireless Personal Communications, vol. 81, 2014, no. 3, pp. 1159–1176

10. Wang Y. B., Quan H.D., Sun H.X., and Cui P. Z. Anti-follower jamming wide gap multi-pattern frequency hopping communication method. Defence Technology, vol. 16, 2020, no. 6, pp. 1067–1076

11. Wang Y., Quan H., Sun H., and Cui P. Anti-follower jamming analysis of multi-sequence frequency hopping in AWGN channel. IOP Conference Series: Materials Science and Engineering, vol. 563, 2019, pp. 453-459

12. Zhang L., Wang H., and Li T., Anti-jamming message-driven frequency hopping—part i: System design. IEEE transactions on wireless communications, vol. 12, 2012, no. 1, pp. 70–79.

13. Zhu J., Wang A., Wu W., Zhao Z., Xu Y., Lei R., and Yue K. Deep-learning-based recovery of frequency-hopping sequences for anti-jamming applications. Electronics, vol. 12, 2023, no. 3, p. 496

14. Awerbuch B., Richa A. W., and Scheideler C., A jamming-resistant MAC protocol for single-hop wireless networks. 27th ACM Symposium on Principles of Distributed Computing (PODC), Toronto, ON, Canada, 2008, pp. 45–54, ACM

15. Jia L., Qi N., Su Z., Chu F., Fang S., Wong K. K., and Chae C. B., Game theory and reinforcement learning for anti-jamming defense in wireless communications: Current research, challenges, and solutions. IEEE Communications Surveys & Tutorials, in press, 2024, pp. 1798-1838

16. Slimeni F., Scheers B., Le Nir V., Chtourou Z., and Attia R. Learning multi-channel power allocation against smart jammer in cognitive radio networks.

2016 International Conference on Military Communications and Information Systems (ICMCIS), 2016, pp. 1–7, IEEE.

17. Yang D., Xue G., Zhang J., Richa A., and Fang X. Coping with a smart jammer in wireless networks: A stackelberg game approach. IEEE Transactions on Wireless Communications, vol. 12, 2013, no. 8, pp. 4038–4047

18. Wang X., Chen X., Wang M., and Dong S. Decentralized reinforcement learning based anti-jamming communication for self-organizing networks. IEEE Wireless Communications and Networking Conference (WCNC), 2021, pp. 1–6, IEEE

19. Pelechrinis K., Koufogiannakis C., and Krishnamurthy S. V. On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks. IEEE transactions on wireless communications, vol. 9, 2010, no. 10, pp. 3258–3271

20. Garnaev A., Petropulu A. P., Trappe W., and Poor H. V. A jamming game with rival-type uncertainty. IEEE Transactions on Wireless Communications, vol. 19, 2020, no. 8, pp. 5359–5372

21. Xiao L., Chen T., Liu J., and Dai H. Anti-jamming transmission stackelberg game with observation errors. IEEE communications letters, vol. 19, 2015, no. 6, pp. 949–952

22. Garnaev A., Liu Y., and Trappe W. Anti-jamming strategy versus a low-power jamming attack when intelligence of adversary's attack type is unknown. IEEE Transactions on Signal and Information Processing over Networks, vol. 2, 2015, no. 1, pp. 49–56

23. Xiao Y., Ren H., Wu S., Liu L., Meng X., and Ding P. Anti-jamming method of cognitive radio based on Q-learning. 12th International Conference on Electronics, Communications and Networks (CECNet 2022), Frontiers in Artificial Intelligence and Applications, vol. 363, 2022, pp. 97–104, IOS Press

24. Zhu J., Zhao Z., and Zheng S., Intelligent anti-jamming decision algorithm of bivariate frequency hopping pattern based on DQN with PER and Pareto. International Journal of Information Technology and Web Engineering (IJITWE), vol. 17, 2022, no. 1, pp. 23–37

25. Li Y., Bai S., and Gao Z. A multi-domain anti-jamming strategy using stackelberg game in wireless relay networks. IEEE Access, vol. 8, 2020, pp. 173609–173617

26. Chen L. and Leneutre J. Fight jamming with jamming–a game theoretic analysis of jamming attack in wireless networks and defense strategy. Computer Networks, vol. 55, 2011, no. 9, pp. 2259–2270

27. Sagduyu Y. E., Berry R. A., and Ephremides A. Jamming games in wireless networks with incomplete information. IEEE Communications Magazine, vol. 49, 2011, no. 8, pp. 112–118

28. Yang D., Zhang J., Fang X., Richa A., and Xue G. Optimal transmission power control in the presence of a smart jammer. IEEE Global Communications Conference (GLOBECOM), 2012, pp. 5506–5511, IEEE

29. Yao F. and Jia L., A collaborative multi-agent reinforcement learning anti-jamming algorithm in wireless networks. IEEE wireless communications letters, vol. 8, 2019, no. 4, pp. 1024–1027

30. Slimeni F., Chtourou Z., Scheers B., Nir V. L., and Attia R., Cooperative q-learning based channel selection for cognitive radio networks. Wireless Networks, vol. 25, 2019, no. 7, pp. 4161–4171

31. Song T., Stark W. E., Li T., and Tugnait J. K. Optimal multiband transmission under hostile jamming. IEEE Transactions on Communications, vol. 64, 2016, no. 9, pp. 4013–4027

32. Zhang Y., Wang H., Han T., and Zhang X. A multi-leader one-follower Stackelberg game approach for cooperative anti-jamming: No pains, no gains. IEEE Communications Letters, vol. 22, 2018, no. 8, pp. 1680–1683.

Дата поступления: 22.09.2025

Дата публикации: 28.10.2025