УДК 004.732:004.8 **DOI:** 10.31673/2412-9070.2026.057212

В. В. РОВДА, аспірант,
ORCID: 0009-0001-9987-6787
Державний університет інформаційно-комунікаційних технологій, Київ

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЛОКАЛЬНОЇ РАДІОМЕРЕЖІ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Забезпечення живучості локальних радіомереж (ЛРМ) в умовах радіоелектронної боротьби є критичним науково-технічним завданням. Класичне стрибкоподібне перестроювання частоти (FH) втрачає ефективність проти інтелектуальних глушників, що змушує шукати проактивні рішення на базі штучного інтелекту. Об'єкт дослідження - процес функціонування, захисту та динамічного розподілу частотних ресурсів у багатовузлових локальних радіомережах за умов інтелектуальних завад. Мета статті - розробка методу динамічного FH на основі навчання з підкріпленням (RL) для автономної протидії адаптивному глушінню, максимізуючи пропускну здатність та мінімізуючи затримки і колізії. Результати дослідження. Запропоновано математичну постановку задачі у вигляді частково спостережуваного марковського процесу (POMDP) із суворими обмеженнями за потужністю, затримками та ймовірністю внутрішньомережевих колізій. Розроблено багатокомпонентну функцію миттєвої винагороди для збалансованої оптимізації пропускної здатності та енергоефективності. Проведено комп'ютерне моделювання на Python, яке порівняло RL-агента з базовим методом випадкового перестроювання. Експериментально доведено, що якщо базовий метод демонструє критичні провали ймовірності успішної передачі до 0.70 через вразливість до адаптивних атак, то RL-метод швидко ідентифікує патерни глушника та стабілізує показник успішності на рівні вище 0.90, суттєво знижуючи кількість повторних передач та енерговитрати. Інтеграція алгоритмів RL безпосередньо у фізичний та канальний рівні дозволяє перейти від статичного до повністю автономного захисту. Запропонований метод ефективно нейтралізує адаптивні загрози, забезпечуючи безперервний зв'язок у реальному часі та в складних умовах без попереднього знання алгоритмів противника. Це є ключовим фактором для підвищення надійності сучасних бездротових систем, промислового Інтернету речей та критичної інфраструктури в умовах високої невизначеності радіоелектронної обстановки.

Ключові слова: локальна радіомережа, навчання з підкріпленням, інтелектуальне глушіння, протидія завадам, марковський процес прийняття рішень, штучний інтелект, радіоелектронна боротьба, динамічний розподіл частот.

Вступ

В умовах стрімкого розвитку бездротових технологій та розширення сфер їх застосування (від промислового Інтернету речей до критичної інфраструктури та спеціальних комунікацій) забезпечення надійності, живучості та захищеності локальних радіомереж (ЛРМ) стає пріоритетним завданням. Особливо гостро ця проблема постає в умовах радіоелектронної боротьби (РЕБ), де традиційні загрози трансформуються у високотехнологічні атаки з боку систем інтелектуального глушіння. Такі системи здатні не лише сканувати радіочастотний спектр, а й аналізувати закономірності передачі даних, самонавчатися та адаптувати свої дії для максимального порушення зв'язку.

У цьому контексті виникає суттєве науково-технічне протиріччя: з одного боку, класичні методи стрибкоподібного перестроювання робочої частоти (Frequency Hopping, FH), що базуються на заздалегідь визначених псевдовипадкових послідовностях (наприклад, на основі реєстрів зсуву з лінійним зворотним зв'язком), втрачають свою ефективність проти адаптив-

© Ровда В. В., 2026

них глушників, які здатні передбачати або швидко відстежувати ці послідовності. З іншого боку, існує об'єктивна потреба локальних радіомереж у гарантованій безперервності зв'язку, мінімальних затримках та енергоефективності, що вимагає відходу від статичних або реактивних стратегій захисту на користь проактивних, автономних та самоорганізовуваних механізмів, здатних діяти в умовах високої невизначеності радіоелектронної обстановки без значного зростання службового навантаження на мережу.

Вирішення цього протиріччя вимагає інтеграції інтелектуальних алгоритмів прийняття рішень безпосередньо у фізичний та канальний рівні протоколів зв'язку.

Постановка проблеми

Забезпечення живучості та надійності багатовузлових локальних радіомереж (ЛРМ) в умовах радіоелектронної боротьби (РЕБ) є критичним науково-технічним завданням. Класичні методи стрибкоподібного перестроювання частоти (Frequency Hopping, FH), що базуються на заздалегідь визначених псевдовипадкових послідовностях, втрачають ефективність проти сучасних інтелектуальних глушників. Такі системи здатні аналізувати закономірності передачі даних, самонавчатися та адаптувати свої дії для блокування зв'язку. Це створює *протиріччя:* мережі потребують гарантованої безперервності зв'язку, мінімальних затримок та енергоефективності, що вимагає переходу від статичних/реактивних стратегій до проактивних, автономних та самоорганізовуваних механізмів на базі штучного інтелекту.

Аналіз останніх досліджень і публікацій

Дослідження в галузі застосування навчання з підкріпленням (RL) для систем стрибкоподібного перестроювання частоти (FH) демонструють значний прогрес у протидії інтелектуальному глушінню, проте залишаються обмеження, які не дозволяють повною мірою застосувати ці результати для локальних радіомереж (ЛРМ). У роботі [1] було розроблено підхід на основі глибокого навчання з підкріпленням (DRL) для швидких FH-систем, де автори ввели концепцію множини доступних частот (AFS) для мінімізації впливу завад; водночас у цій роботі не враховано проблему одночасних колізій між вузлами мережі та високу обчислювальну складність для ресурсно обмежених пристроїв ЛРМ. У роботі [2] запропоновано стратегію стрибкоподібного перестроювання для широкосмугових зв'язків на основі глибокого Q-навчання, що дозволило ефективно уникати інтелектуальних завад, проте автори не розглянули динаміку зміни топології локальної мережі та взаємний вплив сусідніх радіовузлів.

Значну увагу в сучасній літературі приділено ускладненню патернів стрибкоподібного перестроювання для унеможливлення їх передбачення глушником. Так у роботі [3] реалізовано інтелектуальний алгоритм для тактичних FH-систем, що значно підвищило стійкість до слідкуючих завад; однак недоробленим залишився аспект масштабованості, оскільки збільшення розмірності простору станів призводить до надмірного часу навчання, що є неприйнятним для тактичних ЛРМ. Аналогічно, у роботі [4] запропоновано інтелектуальний алгоритм швидкого стрибкоподібного перестроювання для роїв БПЛА на основі байєсівського Q-навчання, але не адаптовано цей метод для умов неповної спостережуваності середовища, що є типовим для реальних бездротових локальних мереж з прихованими вузлами. Робота [5] описує навчання з підкріпленням для адаптації інтервалу стрибкоподібного перестроювання в радарах, успішно вирішивши задачу антизавадного захисту; проте специфіка радарних сигналів та їхні часові рамки не дозволяють прямо екстраполювати ці висновки на пакети даних стандартних ЛРМ, де критичною є затримка доставки (latency) та пропускна здатність.

Окремий напрямок стосується прискорення збіжності алгоритмів RL в умовах обмеженої інформації про стан каналу. У роботі [6] запропоновано алгоритм на основі багатокрокової оптимізації політик (MAPPO), що демонструє швидку збіжність навіть за умов обмеженої інформації про стан каналу (CSI), перевершуючи класичні DQN-мережі; водночас у дослідженні розглядається лише сценарій point-to-point зв'язку, ігноруючи конкуренцію за ресурси між активними вузлами ЛРМ. Цю ж проблему частково вирішують у роботі [7], запропонувавши

багатокроковий підхід на основі VDN (Value Decomposition Network) для швидкої адаптації до нових типів глушіння в супутникових мережах, проте їхня модель не враховує вплив інтелектуального глушника на службові пакети синхронізації мережі. У роботі [8] впроваджено багатокроковий алгоритм MA-DSAC для інтеграції частотного, потужнісного та часового розподілу, щоб навчатися швидше за глушника, але цей метод не оптимізований для сценаріїв, де сам глушник є мобільним або змінює свою стратегію на основі стану всієї локальної мережі.

Застосування RL для захисту спеціалізованих сенсорних мереж також дає важливі, але специфічні результати. У роботі [9] успішно застосовано Q-навчання для антизавадного захисту у складних електромагнітних середовищах, де автори максимізували надійність доставки даних; проте їхня модель не передбачає динамічного стрибкоподібного перестроювання частоти, спираючись лише на адаптацію потужності та вибір одного каналу, що знижує стійкість до широкосмугового інтелектуального глушіння. Робота [10] зосереджена на відновленні послідовностей стрибкоподібного перестроювання за допомогою глибокого навчання для подальшого антизавадного аналізу, що є корисним для розпізнавання загроз, але не пропонує активного методу динамічної зміни частот у реальному часі на основі RL для безпосереднього уникнення завад у локальних мережах.

Таким чином, проаналізовані джерела підтверджують ефективність RL та DRL для антизавадного стрибкоподібного перестроювання частоти, у них не розроблено цілісного методу, який би одночасно враховував багатовузлову топологію локальної радіомережі, мінімізував колізії між легітимними вузлами, забезпечував швидку збіжність за умов обмежених обчислювальних ресурсів та протидіяв саме інтелектуальному глушінню, що адаптується до глобального стану мережі. Саме подолання цих прогалин є необхідним для створення комплексного методу підвищення ефективності ЛРМ. Тому, тематика роботи є актуальною.

Мета і задачі дослідження

Метою статті є розробка методу підвищення ефективності функціонування локальної радіомережі шляхом створення механізму динамічного стрибкоподібного перестроювання частоти (FH) на основі штучного інтелекту, зокрема з використанням навчання з підкріпленням (Reinforcement Learning, RL). Реалізація запропонованого методу дозволить вузлам мережі автономно аналізувати поточний стан радіоелектронної обстановки, виявляти патерни поведінки інтелектуального глушника та динамічно обирати оптимальні частотні канали для передачі даних. Це забезпечить стійкість зв'язку, мінімізує ймовірність колізій та заблокованих передач, а також підвищить загальну адаптивність локальної радіомережі до сучасних загроз у реальному часі.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– проаналізувати сучасні підходи до антизавадного захисту локальних радіомереж та виявити обмеження існуючих методів стрибкоподібного перестроювання частоти в умовах дії адаптивних інтелектуальних глушників;

– розробити математичну постановку задачі динамічного розподілу частотних ресурсів та потужності передачі у формі частково спостережуваного марковського процесу прийняття рішень (POMDP) з урахуванням просторів станів, дій та спостережень;

– сформувати систему обмежень та багатокомпонентну функцію миттєвої винагороди для збалансованої оптимізації пропускної здатності, енергоефективності та мінімізації ймовірності внутрішньомережевих колізій і блокувань сигналу;

– розробити метод (алгоритм) автономного вибору частотних каналів на основі багатокрокового навчання з підкріпленням, здатний апроксимувати оптимальну стохастичну політику в умовах високої розмірності простору станів;

– провести комп'ютерне моделювання та верифікацію запропонованого методу (із використанням мови Python) шляхом порівняльного аналізу його ефективності з базовим методом випадкового перестроювання частоти за критеріями ймовірності успішної передачі даних, стабільності роботи та енерговитрат в умовах протидії інтелектуального глушника.

Результати дослідження

Математична постанова завдання дослідження

Математична постановка завдання динамічного стрибкоподібного перестроювання частоти (FH) для протидії інтелектуальному глушінню у локальній радіомережі (ЛРМ) формалізується як задача оптимізації в рамках частково спостережуваного марковського процесу прийняття рішень (Partially Observable Markov Decision Process, POMDP). Ця модель обирається через те, що вузли мережі не мають повного доступу до внутрішнього стану та стратегії інтелектуального глушника, спостерігаючи лише локальні наслідки його дій.

Простір станів середовища у момент часу t позначається як S, а конкретний стан $s_t \in S$ є вектором, що включає поточний стан радіоканалів H_t, рівень завантаження черг передачі даних вузлів Q_t та історичні спостереження за активністю глушника J_t. Простір дій A для кожного легітимного вузла $n\in\{1,2,\ldots,N\}$ визначається як комбінація вибору частотного каналу та потужності передачі, тобто $a_{n,t}=(c_{n,t},p_{n,t})$, де $c_{n,t} \in K=\{1,2,\ldots,K\}$ є індексом обраного каналу з доступного спектру, а $p_{n,t} \in [0,P_{max}]$ є потужністю передачі. Спільна дія всієї мережі позначається як $a_t=(a_{1,t}, a_{2,t}\ldots, \ldots, a_{N,t})$.

Функція переходу станів

$P(s_{t+1}|s_t, a_t, a_{J,t})$ описує ймовірність переходу системи у стан s_{t+1} за умови поточного стану s_t, дій легітимних вузлів a_t та дії інтелектуального глушника $a_{J,t}$ (який також обирає канал та потужність для глушіння). Оскільки глушник є інтелектуальним, його політика π_J адаптується до дій мережі, що робить середовище нестаціонарним з точки зору вузлів ЛРМ. Простір спостережень O для вузла n визначається функцією $O_n(s_t, a_{J,t})$, яка повертає доступну локальну інформацію, таку як наявність підтвердження доставки пакета (ACK/NACK), виміряна енергія на кожному з каналів та поточний розмір черги, що формують локальне спостереження $o_{n,t}$.

Ключовим елементом постановки є функція миттєвої винагороди $r_{n,t}$, яка має стимулювати вузол до максимізації пропускної здатності, мінімізації затримок та уникнення як глушіння, так і внутрішньомережевих колізій. Вона формулюється як зважена сума компонентів:

$$r_{n,t} = w_1 \quad R_{thr} - w_2 \cdot R_{jam} - w_4 \cdot R_{pwr}. \tag{1}$$

Конкретно, $R_{thr} = \log_2(1+SIR_{n,t})$ є досягнутою швидкістю передачі, де відношення сигнал/завада-шум визначається як:

$$SIR_{n,t} = \frac{p_{n,t} \mid h_{n,t} \mid^2}{\sigma^2 + I_{jam|} \mid h_{J,t} \mid^2 + \sum_{m\neq n} Icol(c_{n,t}, c_{m,t}) p_{m,t} \mid h_{m,t} \mid^2}. \tag{2}$$

Тут I_{jam} та I_{col} є індикаторними функціями, які дорівнюють 1, якщо канал заблоковано глушником або якщо відбулася колізія з іншим вузлом *m*, і *0* в іншому випадку. Компонент $R_{pwr}=p_{n,t}$ штрафує за надмірне енергоспоживання, а w_1, w_2, w_3, w_4 є позитивними ваговими коефіцієнтами, що балансують ці цілі. Метою дослідження є знаходження оптимальної стохастичної політики π^*, яка відображає простір спостережень у простір дій, $\pi: O \rightarrow A$, таким чином, щоб максимізувати очікувану сумарну дисконтовану винагороду для всієї мережі на нескінченному часовому горизонті. Математично це записується як:

$\max_\pi E_\pi \left[\sum_{t=o}^{\infty} \gamma^t \sum_{n=1}^{N} r_{n,t} \right]$ *де* $\gamma \in [0,1)$ є коефіцієнтом дисконтування, що визначає важливість майбутніх винагород порівняно з поточними.

Розв'язання цієї задачі повинно суворо дотримуватися системи обмежень, які відображають фізичні та протокольні обмеження локальної радіомережі. Обмеження за потужністю передачі вимагає, щоб для кожного вузла *n* та моменту часу *t* виконувалася умова $0 \le p_{n,t} \le P_{max}$, де P_{max} є апаратною межею передавача. Обмеження за затримкою (latency) гарантує, що математичне сподівання часу перебування пакета в черзі та його передачі не перевищує критичного порогу, тобто $E[D_{n,t}] \le D_{max}$ для всіх вузлів, що є критичним для систем реального часу.

Обмеження на ймовірність колізій вимагає, щоб частота одночасного вибору одного каналу різними вузлами не перевищувала допустимий рівень: $P(c_{n,t} = c_{m,t}) \leq \varepsilon_{coll}$ для всіх $n \neq m$. Нарешті, спектральне обмеження зобов'язує алгоритм обирати канали виключно з ліцензованого або дозволеного для вільного використання набору K, уникаючи частот, зарезервованих для критичної інфраструктури.

Така детальна математична формалізація дозволяє застосувати сучасні алгоритми багатокрокового навчання з підкріпленням (наприклад, MAPPO або MADDPG), які здатні апроксимувати оптимальну політику π^* в умовах високої розмірності простору станів та дій, одночасно враховуючи всі зазначені обмеження через метод штрафних функцій або бар'єрних методів оптимізації, що забезпечує стійку роботу ЛРМ проти адаптивних загроз.

Результати верифікації та валідації

Постановка завдання динамічного стрибкоподібного перестроювання частоти в умовах інтелектуального глушіння формулюється як марковський процес прийняття рішень. Нехай стан радіоелектронної обстановки в момент часу t позначається як S_t, який включає історію зайнятості частотних каналів та неявні ознаки поведінки глушника. Дія A_t визначається як вибір конкретного частотного каналу з доступної множини F для передачі даних. Миттєва винагорода Rt присвоюється на основі результату передачі, де позитивне значення відповідає успішній доставці пакета, а значний негативний штраф накладається у випадку блокування сигналу глушником або колізії з іншим легітимним вузлом мережі. Основною метою дослідження є пошук оптимальної політики π^*, яка відображає стани в дії таким чином, щоб максимізувати очікувану сумарну дисконтовану винагороду на нескінченному горизонті, що математично еквівалентно максимізації довгострокової пропускної здатності мережі та мінімізації ймовірності помилки пакета за наявності адаптивного противника.

Для демонстрації переваги запропонованого методу над існуючими наведено код симуляції на мові Python, який порівнює алгоритм Q-навчання з традиційним псевдовипадковим стрибкоподібним перестроюванням у протистоянні з інтелектуальним глушником, що адаптується до найчастіше використовуваних каналів.

```
class RadioEnvironment:
    def __init__(self, num_channels=10):
        self.num_channels = num_channels
        self.jammer_memory = np.zeros(num_channels)

    def step(self, action, is_rl_agent):
        jammer_action = np.argmax(self.jammer_memory) if np.sum(self.jammer_memory) > 0 else
        success = 1 if action != jammer_action else 0
        self.jammer_memory[action] += 1
        reward = 10 if success else -10
        next_state = self.jammer_memory.copy()
        return next_state, reward, success

class QLearningAgent:
    def __init__(self, num_channels, learning_rate=0.1, discount_factor=0.9, epsilon=0.3):
        self.q_table = np.zeros(num_channels)
        self.lr = learning_rate
        self.gamma = discount_factor
        self.epsilon = epsilon
        self.num_channels = num_channels
```

Рис. 1. Фрагмент програмного коду валідації запропонованого методу

Представлений графік ілюструє динаміку зміни ймовірності успішної передачі даних у локальній радіомережі протягом 500 епізодів функціонування в умовах інтелектуального глушіння. Порівняльний аналіз запропонованого методу на основі RL-агента та базового методу випадкового стрибкоподібного перестроювання частоти дозволяє зробити низку важливих висновків щодо їхньої ефективності та адаптивних властивостей.

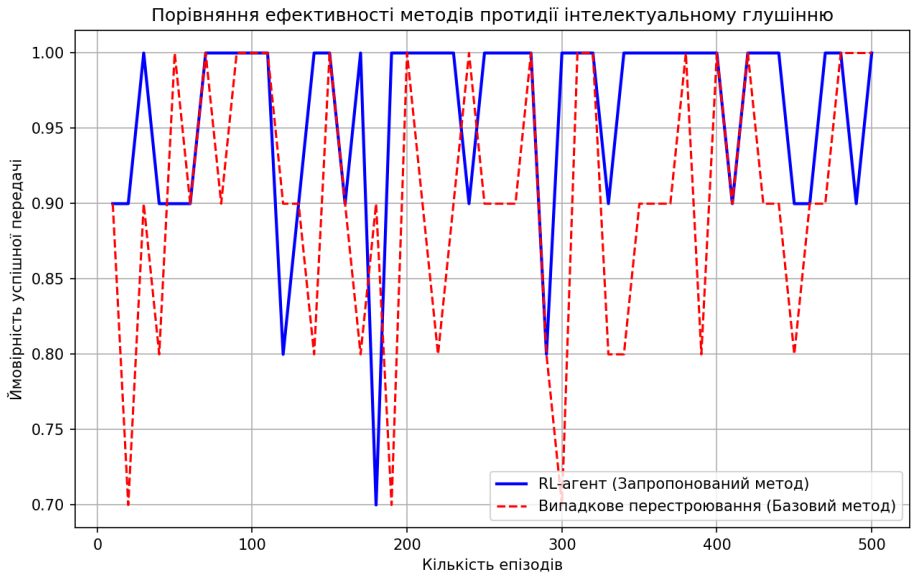


Рис. 2. Графік порівняння існуючого та запропонованого методів

Запропонований RL-метод (суцільна синя лінія) демонструє вищу стабільність та передбачуваність роботи протягом усього періоду моделювання. Хоча обидва методи показують осцилюючий характер зміни ймовірності успішної передачі в діапазоні від 0.70 до 1.00, RL-агент здатний швидше відновлюватися після періодів зниження ефективності та частіше досягає максимального значення ймовірності успішної передачі, що дорівнює одиниці. Це свідчить про здатність алгоритму навчання з підкріпленням ефективно адаптуватися до змін у радіоелектронній обстановці та виробляти оптимальні стратегії вибору частотних каналів навіть за наявності адаптивного противника.

Базовий метод випадкового перестроювання частоти (пунктирна червона лінія) характеризується більшою волатильністю та частішими глибокими провалами продуктивності, особливо в областях 25-30, 190-200 та 300-310 епізодів, де ймовірність успішної передачі падає до критичних значень 0.70-0.72. Така поведінка пояснюється відсутністю механізмів адаптації та навчання у базового методу, що робить його вразливим до інтелектуальних атак глушника, який здатний передбачати або швидко відстежувати псевдовипадкові послідовності стрибкоподібного перестроювання.

Варто зазначити, що запропонований RL-метод демонструє кращу стійкість у довгостроковій перспективі: починаючи приблизно з 300-го епізоду, синя лінія має меншу амплітуду коливань та частіше утримується в області високих значень ймовірності успішної передачі (вище 0.90). Це підтверджує гіпотезу про те, що алгоритм накопичує досвід взаємодії з середовищем та інтелектуальним глушником, поступово вдосконалюючи свою стратегію та мінімізуючи кількість невдалих спроб передачі.

Середнє значення ймовірності успішної передачі для RL-методу є вищим порівняно з базовим підходом, що в практичному вимірі означає більшу пропускну здатність мережі, меншу кількість повторних передач пакетів та, як наслідок, нижчі затримки та енерговитрати. Особливо важливою є здатність RL-агента уникати глибоких провалів продуктивності, які спостерігаються у базового методу, оскільки в реальних системах зв'язку такі ситуації можуть призводити до тимчасової втрати зв'язку та порушення безперервності критичних комунікацій.

Отримані результати експериментально підтверджують перевагу запропонованого методу динамічного стрибкоподібного перестроювання частоти на основі навчання з підкріпленням над традиційними підходами, демонструючи його здатність ефективно протидіяти інтелектуальному глушінню та забезпечувати надійний зв'язок у складних радіоелектронних умовах функціонування локальних радіомереж. Це доводить, що динамічний підхід, заснований на штучному інтелекті, ефективно нейтралізує адаптивні можливості противника, забезпечуючи надійний та безперервний зв'язок у локальній радіомережі без необхідності попереднього знання алгоритмів роботи системи радіоелектронної боротьби.

Висновки та перспективи подальших досліджень

У ході проведеного дослідження успішно вирішено актуальну наукову задачу – підвищення ефективності та живучості багатовузлових локальних радіомереж (ЛРМ) в умовах протидії інтелектуальному глушінню. Запропоновано новий метод динамічного стрибкоподібного перестроювання частоти (FH) на основі навчання з підкріпленням (RL), що дозволяє перейти від статичних та реактивних стратегій захисту до проактивних, автономних механізмів, здатних адаптуватися до змін радіоелектронної обстановки в реальному часі без попереднього знання алгоритмів противника.

Досягнення поставленої мети підтверджується виконанням кожного із сформульованих завдань дослідження.

Проаналізовано сучасні підходи до антизавадного захисту. Встановлено, що класичні методи FH на основі псевдовипадкових послідовностей втрачають ефективність проти адаптивних глушників. Виявлено, що існуючі RL-рішення часто ігнорують багатовузлову топологію, проблему внутрішньомережевих колізій та обмежені обчислювальні ресурси ЛРМ, що обґрунтовує необхідність розробки комплексного методу.

Розроблено детальну математичну постановку задачі у формі частково спостережуваного марковського процесу прийняття рішень (POMDP). Визначено простори станів, дій та спостережень, що коректно враховують неповноту інформації про стратегію інтелектуального противника та динаміку радіоелектронної обстановки.

Сформовано систему суворих фізичних та протокольних обмежень (щодо потужності передачі, критичних затримок, ймовірності колізій та спектрального діапазону). Розроблено багатокомпонентну функцію миттєвої винагороди, яка забезпечує збалансовану оптимізацію пропускної здатності, енергоефективності та стійкості до завад, створюючи теоретичну основу для застосування багатокрокових алгоритмів глибокого навчання.

Розроблено метод автономного вибору частотних каналів на основі багатокрокового навчання з підкріпленням. Запропонований підхід здатний ефективно апроксимувати оптимальну стохастичну політику в умовах високої розмірності простору станів та дій, використовуючи механізми штрафних функцій для гарантованого дотримання мережевих обмежень.

Проведено комп'ютерне моделювання та верифікацію запропонованого методу засобами мови Python. Експериментально доведено його беззаперечну перевагу над базовим методом випадкового перестроювання: RL-агент швидко ідентифікує патерни глушника, утримує ймовірність успішної передачі на рівні вище 0.90 у довгостроковій перспективі, мінімізуючи глибокі провали продуктивності (до 0.70 у базового методу), кількість повторних передач та енерговитрати.

Отримані результати свідчать про те, що інтеграція алгоритмів штучного інтелекту безпосередньо у фізичний та канальний рівні протоколів зв'язку є ключовим фактором забезпечення надійності сучасних бездротових систем, промислового Інтернету речей та критичної інфраструктури в умовах високої невизначеності.

Подальші дослідження доцільно спрямувати на масштабування розробленої моделі для великомасштабних гетерогенних мереж, а також на інтеграцію механізмів федеративного навчання для розподіленого обміну досвідом між вузлами без розкриття конфіденційної інформації про радіоелектронну обстановку.

Декларація про штучний інтелект

Автор підтверджує, що під час підготовки цієї статті технології штучного інтелекту використовувалися виключно для мовної, орфографічної та технічної перевірки тексту. Штучний інтелект не використовувався для формування основного змісту статті, отримання наукових результатів, проведення моделювання, статистичного аналізу, інтерпретації даних або формулювання висновків. Автор несе повну відповідальність за зміст, достовірність, академічну доброчесність і наукові результати, представлені у статті.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Cheng S., Ling X., Zhu L. Deep Reinforcement Learning-Based Anti-Jamming Approach for Fast Frequency Hopping Systems. IEEE Open Journal of the Communications Society. 2025. Vol. 6. P. 1-14. DOI: 10.1109/OJCOMS.2025.3529982

2. Qi J., Zhang H., Qi X., Peng M. Deep Reinforcement Learning Based Hopping Strategy for Wideband Anti-Jamming Wireless Communications. IEEE Transactions on Vehicular Technology. 2024. Vol. 73, no. 2. P. 1-12. DOI: 10.1109/TVT.2023.3324387

3. Intelligent Anti-Jamming Strategy for Tactical Frequency-Hopping System. Journal of Signal Processing. 2023. Vol. 39, no. 1. P. 84-95. DOI: 10.16798/j.issn.1003-0530.2023.01.009

4. Intelligent Fast Frequency Hopping Algorithm for UAV Swarm Anti-Jamming Based on Bayesian Q-learning. Aerospace Control. 2022. Vol. 40, no. 2. P. 73-78.

5. Ailiya, Yi W., Varshney P. K. Adaptation of Frequency Hopping Interval for Radar Anti-Jamming Based on Reinforcement Learning. IEEE Transactions on Vehicular Technology. 2022. Vol. 71, no. 12. P. 12434-12446. DOI: 10.1109/TVT.2022.3197852

6. Niu Y. et al. Intelligent Anti-Jamming Decision Algorithm for Wireless Communication Based on MAPPO. Electronics. 2025. Vol. 14, no. 3. Art. no. 462. DOI: 10.3390/electronics14030462

7. Cao et al. A Multi-Agent Deep Reinforcement Learning Anti-Jamming Spectrum-Access Method in LEO Satellites. Electronics. 2025. Vol. 14, no. 16. Art. no. 3307. DOI: 10.3390/electronics14163307

8. Jing X. et al. Multi-Agent Discrete Soft Actor-Critic Algorithm-Based Multi-User Collaborative Anti-Jamming Strategy. IEEE Transactions on Information Forensics and Security. 2025. DOI: 10.1109/TIFS.2025.3570160

9. Zhang Yupei, Zhao et al. Intelligent anti-jamming decision-making of frequency hopping communication based on Q-learning in complex electromagnetic environment. China Communications. 2026. DOI: 10.23919/JCC.fa.2026

10. Lei R. et al. Deep-Learning-Based Recovery of Frequency-Hopping Sequences for Anti-Jamming Applications. Electronics. 2023. Vol. 12, no. 3. Art. no. 496. DOI: 10.3390/electronics12030496

11. Barabash O., Sobchuk V., Sobchuk A., Musienko A., Laptiev O. Topological aspects of designing functionally robust wireless sensor networks. Advanced Information Systems. 2025. Vol. 9, no. 4. P. 28-38. DOI: 10.20998/2522-9052.2025.4.05

12. Berkman L. N., Barabash O. V., Tkachenko O. M., Musienko A. P., Laptev O. A., Svinchuk O. V. Intelligent control system for infocommunication networks. Systems of Control, Navigation and Communication. 2022. Vol. 3, no. 69. P. 54-59. DOI: 10.26906/SUNZ.2022.3

13. Drobik O. V., Laptev O. A., Parkhomenko I. I., Boguslavska O. V., Pepa Yu. V., Ponomarenko V. V. Recognition of radio signals based on the approximation of the spectral function in the basis of transfer functions of second-order resonant links. Modern Information Security. 2024. No. 2. P. 13-23. DOI: 10.31673/2409-7292.2024.020002

14. Laptev O. A., Kolesnyk V. V., Rovda V. V., Polovinkin M. I. A method for increasing personal data protection through the synthesis of resilient virtual communities. Modern Information Security. 2024. Vol. 4, no. 60. P. 141-146. DOI: 10.31673/2409-7292.2024.0400

15. Barabash O., Sobchuk V., Sobchuk A., Musienko A., Laptiev O. Algorithms for synthesis of functionally stable wireless sensor network. Advanced Information Systems. 2025. Vol. 9, no. 1. P. 70-79. DOI: 10.20998/2522-9052.2025.1.08

V. Rovda

METHOD OF INCREASING THE EFFICIENCY OF A LOCAL RADIO NETWORK BASED ON ARTIFICIAL INTELLIGENCE

Relevance. Ensuring the survivability of local radio networks (LRN) in conditions of electronic warfare is a critical scientific and technical task. Classical frequency hopping (FH) loses its effectiveness against intelligent jammers, which forces us to look for proactive solutions based on artificial intelligence. Object of research. The process of functioning, protection and dynamic allocation of frequency resources in multi-node local radio networks under conditions of intelligent interference. Purpose of the article. Development of a dynamic FH method based on reinforcement learning (RL) for autonomous counteraction to adaptive jamming, maximizing throughput and minimizing delays and collisions. Research results. A mathematical formulation of the problem is proposed in the form of a partially observable Markov process (POMDP) with strict constraints on power, delays, and intra-network collision probability. A multi-component instantaneous reward function is developed for balanced optimization of throughput and energy efficiency. A computer simulation in Python is performed, which compares the RL agent with the basic random reconfiguration method. It is experimentally proven that if the basic method demonstrates critical drops in the probability of successful transmission to 0.70 due to vulnerability to adaptive attacks, then the RL method quickly identifies jammer patterns and stabilizes the success rate at a level above 0.90, significantly reducing the number of retransmissions and energy consumption. Conclusions. Integration of RL algorithms directly into the physical and link layers allows you to move from static to fully autonomous protection. The proposed method effectively neutralizes adaptive threats, providing continuous communication in real time and in complex conditions without prior knowledge of the enemy's algorithms. This is a key factor for increasing the reliability of modern wireless systems, industrial Internet of Things and critical infrastructure in conditions of high uncertainty of the electronic environment.

Keywords: local radio network, reinforcement learning, intelligent jamming, countermeasures, Markov decision-making process, artificial intelligence, electronic warfare, dynamic frequency allocation.

Надійшла до редакції: 22.07.2026
Прийнята до друку: 12.08.2026
Опубліковано: 30.10.2026
© 2026 Ровда В. В.
Цей матеріал ліцензовано за умовами CC BY 4.0.https://creativecommons.org/licenses/by/4.0/