МОДЕЛЮВАННЯ ЗАВАДОСТІЙКИХ СИСТЕМ ЗВ'ЯЗКУ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Новицький Віталій Ярославович [1]

Опубліковано	Секція	УДК
30.06.2025	Економіка	35.088.6:[004:007:351.86](477)

DOI: https://doi.org/10.5281/zenodo.17151223

Анотація. У статті досліджено комплексний підхід до моделювання завадостійких систем зв'язку, призначених для обслуговування об'єктів критичної інфраструктури, які відіграють ключову роль у забезпеченні національної безпеки, стабільного функціонування економіки та життєдіяльності суспільства. Зосереджена увага на тому, що сучасні інформаційно-комунікаційні системи в умовах глобальних загроз та гібридних воєн повинні відповідати високим вимогам до надійності, швидкодії, безперервності та захищеності.

У ході дослідження здійснено систематизацію існуючих підходів до моделювання таких систем, із включенням сучасних математичних моделей, інженерних рішень і програмних середовищ. У роботі запропоновано структурований опис ключових параметрів, що впливають на ефективність функціонування завадостійких систем: від вибору моделі каналу зв'язку до використання нейромережевих алгоритмів та засобів квантового шифрування. Розглядаються типові моделі перешкод (AWGN, Rayleigh, Rician), адаптивні методи модуляції (OFDM, FHSS, DSSS), а також інструменти кодування з виправленням помилок (LDPC, Reed-Solomon, Turbo-коди). Досягнення високого рівня завадостійкості є можливим лише за умови інтеграції рішень на різних рівнях архітектури мережі – фізичному, канальному, мережевому та прикладному.

Окремо підкреслюється значення використання сучасних середовищ моделювання, таких як MATLAB/Simulink, NS-3, OMNeT++, OPNET, які дозволяють створювати реалістичні симуляції роботи системи у змінному середовищі. Застосування гібридного моделювання – поєднання аналітичного, дискретного та імітаційного підходів – дає змогу всебічно оцінити продуктивність, адаптивність і стійкість комунікаційних мереж до критичних збоїв. Також розглянуто важливість впровадження механізмів автоматичного резервування, багатоканальної маршрутизації, а також алгоритмів самовідновлення, які є запорукою живучості мережі у разі часткової втрати вузлів або атак типу DoS.

Зазначається, що особливої уваги потребує застосування штучного інтелекту для автоматизованого аналізу трафіку, прогнозування появи завад, адаптивної маршрутизації та швидкого виявлення аномалій. Глибокі нейронні мережі, використані

[1] Науковий співробітник
Український науково-дослідний інститут
спеціальної техніки та судових експертиз
Служби безпеки України
https://orcid.org/0000-0001-7386-1221

в межах моделювання, дозволяють здійснювати самонавчання систем у реальному часі, що значно підвищує ефективність протидії новим загрозам.

Результати дослідження свідчать про необхідність подальшого розвитку цифрових двійників систем зв'язку для об'єктів критичної інфраструктури, що дозволяють здійснювати тестування, прогнозування та оптимізацію ще на етапі проектування. Передбачається, що саме комплексне, інтегроване моделювання за участю інтелектуальних систем, сучасних методів шифрування та гнучких архітектур дозволить забезпечити високий рівень надійності, живучості та безпеки систем зв'язку критичної інфраструктури.

Ключові слова: об'єкти критичної інфраструктури, моделювання систем зв'язку, інформаційно-комунікаційні системи, завадостійкість систем зв'язку, теорія інформації, передача даних, штучний інтелект.

MODELING OF FAILURE-RESISTANT COMMUNICATION SYSTEMS FOR CRITICAL INFRASTRUCTURE

Abstract. The article explores a comprehensive approach to modeling noise-resistant communication systems designed to service critical infrastructure facilities that play a key role in ensuring national security, stable functioning of the economy and the life of society. The focus is on the fact that modern information and communication systems in the context of global threats and hybrid wars must meet high requirements for reliability, speed, continuity and security.

The study systematizes existing approaches to modeling such systems, including modern mathematical models, engineering solutions and software environments. The paper proposes a structured description of key parameters that affect the effectiveness of noise-resistant systems: from the choice of a communication channel model to the use of neural network algorithms and quantum encryption tools. Typical interference models (AWGN, Rayleigh, Rician), adaptive modulation methods (OFDM, FHSS, DSSS), as well as error-correction coding tools (LDPC, Reed-Solomon, Turbo codes) are considered. Achieving a high level of noise immunity is possible only if solutions are integrated at different levels of network architecture – physical, channel, network and application.

The importance of using modern modeling environments, such as MATLAB/Simulink, NS-3, OMNeT++, OPNET, which allow creating realistic simulations of system operation in a changing environment, is emphasized. The use of hybrid modeling – a combination of analytical, discrete and simulation approaches – allows for a comprehensive assessment of the performance, adaptability and resilience of communication networks to critical failures. The importance of implementing automatic backup mechanisms, multi-channel routing, as well as self-healing algorithms, which are the key to network survivability in the event of partial loss of nodes or DoS attacks, is also considered.

It is noted that special attention needs to be paid to the use of artificial intelligence for automated traffic analysis, prediction of interference, adaptive routing and rapid detection of anomalies. Deep neural networks used in the modeling allow for real-time self-learning of systems, which significantly increases the effectiveness of countering new threats.

The results of the study indicate the need for further development of digital twins of communication systems for critical infrastructure facilities, which allow for testing, forecasting and optimization at the design stage. It is assumed that it is complex, integrated modeling with the participation of intelligent systems, modern encryption methods and flexible architectures that will ensure a high level of reliability, survivability and security of critical infrastructure communication systems.

Keywords: critical infrastructure facilities, modeling of communication systems, information and communication systems, noise immunity of communication systems, information theory, data transmission, artificial intelligence.

Вступ

Постановка проблеми. У сучасному світі функціонування критичної інфраструктури держави безпосередньо залежить від надійності інформаційно-комунікаційних систем, що забезпечують управління технологічними процесами, координацію дій у надзвичайних ситуаціях, а також захист життєво важливих об'єктів (енергетика, транспорт, медицина, водопостачання, зв'язок тощо). Завадостійкість комунікаційних систем визначає їх здатність працювати без значних втрат інформації, навіть у складних умовах — при наявності шуму, перешкод, атак зловмисників або фізичних пошкоджень. Одним із найбільш гострих питань є захист від кібератак, які можуть цілеспрямовано знижувати якість або блокувати передачу даних.

Крім того, важливим аспектом є природні фактори, такі як сонячна активність, грозові розряди та радіочастотні перешкоди. Таким чином, враховуючи специфіку роботи критичної інфраструктури, системи зв’язку, що її обслуговують, повинні володіти високою завадостійкістю — здатністю функціонувати в умовах сильних електромагнітних перешкод, пошкодження каналів передачі даних, втрати вузлів мережі, атак типу «відмова в обслуговуванні» (DoS), перехоплення або спотворення сигналу. Крім того, інформація, що передається, повинна зберігати цілісність, конфіденційність та бути доступною в реальному часі.

На даний час, багато країн світу активно працюють над розробкою методів підвищення стійкості систем зв’язку, застосовуючи інноваційні технології та алгоритми захисту. Важливою задачею є не тільки розробка нових методів, а й оптимізація існуючих, удосконалення механізмів кодування, розподілу каналів, адаптації до змінних умов роботи та інтеграції штучного інтелекту [1].

Виходячи з цього, можна стверджувати, що розробка, впровадження та моделювання таких завадостійких систем зв’язку залишається одним із найактуальніших напрямків у галузі інженерії, інформатики та кібербезпеки.

Аналіз останніх досліджень і публікацій. Завадостійкість систем зв’язку для критичної інфраструктури є предметом досліджень багатьох наукових колективів, урядових та оборонних структур. Зокрема, у працях К.Шеннона, Е.Торп розглянуто фундаментальні підходи до теорії інформації та оптимального кодування, які стали базисом для подальших розробок у сфері передачі даних.

Одним із ключових напрямків дослідження є технології корекції помилок, які дозволяють мінімізувати втрати інформації в умовах завад. Використання кодів Ріда-Соломона, турбо-кодів та низькодисперсійних алгоритмів корекції допомагає значно підвищити ефективність передачі даних та забезпечити стійкість сигналу. Крім того, значний прогрес спостерігається у сфері адаптивного резервування ресурсів, де застосовуються технології динамічного розподілу частот для автоматичного вибору менш завантажених каналів, що дозволяє уникати перешкод та покращувати якість зв’язку [2].

Іншою важливою сферою досліджень є використання штучного інтелекту, зокрема машинного навчання та нейромереж. Ці технології забезпечують автоматичний аналіз рівня завад та адаптацію параметрів зв’язку без втручання оператора, що особливо важливо для критичних інфраструктур, де будь-яка затримка у прийнятті рішень може призвести до серйозних наслідків. Паралельно активно досліджується застосування квантових комунікацій як перспективного методу захисту інформації від несанкціонованого перехоплення. Завдяки квантовій криптографії можна забезпечити

абсолютну безпеку каналів зв'язку, що є особливо актуальним для державних та військових комунікацій [3].

Разом з тим, у більшості робіт увага акцентується на вузьких аспектах: фізичному або канальному рівні, не завжди беручи до уваги комплексне моделювання системи в цілому. Саме це й обумовлює потребу в подальших дослідженнях етапів моделювання завадостійких систем зв'язку, адаптованих до умов критичної інфраструктури.

Мета статті – дослідження основних підходів та технологій моделювання завадостійких систем зв'язку, орієнтованих на застосування в умовах критичної інфраструктури.

Результати

Моделювання завадостійких систем зв'язку є критично важливим напрямком для забезпечення безпеки та надійності функціонування об'єктів критичної інфраструктури [4]. Суть моделювання полягає у створенні віртуального середовища, яке імітує роботу системи за різних типів перешкод, включаючи як природні, так і навмисні техногенні впливи. У межах такого моделювання використовуються математичні моделі та симуляційні середовища, що дозволяють оцінити вплив перешкод і перевірити ефективність механізмів їх нейтралізації. Основними складовими таких моделей виступають модель каналу зв'язку (AWGN, Rayleigh fading, Rician fading), модель перешкод (інтерференція, імпульсні завади, атаки типу jamming), алгоритми модуляції та кодування, мережеві топології (дерево, сітка, коміркова структура), протоколи маршрутизації та механізми відновлення зв'язку після збою. Застосування системного підходу до моделювання дозволяє не лише моделювати роботу окремих компонентів, а й аналізувати взаємодію підсистем між собою та з навколишнім середовищем. Це забезпечує комплексну оцінку ефективності системи з точки зору таких метрик, як затримка, пропускна здатність, рівень помилок, коефіцієнт доступності та енергоспоживання.

Для реалізації таких моделей використовуються сучасні інструменти моделювання. MATLAB / Simulink надає широкі можливості для побудови моделей систем зв'язку на фізичному та канальному рівнях. Network Simulator 3 (NS-3) дозволяє імітувати великі мережі з детальним аналізом маршрутизації, протоколів передачі даних та атак. OMNeT++ у поєднанні з INET Framework широко використовується для моделювання IoT-систем, SCADA-мереж, мобільних ad-hoc мереж (MANET), які часто використовуються у сфері критичної інфраструктури. Для промислових цілей ефективними є середовища OPNET і QualNet, які забезпечують високу точність та масштабованість. Окрім інструментів моделювання, значну увагу приділяють стратегіям підвищення завадостійкості.

На фізичному рівні застосовуються технології модуляції з широким спектром (FHSS, DSSS), механізми динамічного вибору частоти та антенні масиви з формуванням напрямку променю (beamforming), які дозволяють адаптувати просторову характеристику передавача і зменшити вплив перешкод. На канальному рівні використовуються коди з виправленням помилок, зокрема Reed-Solomon, Turbo та LDPC-коди, а також методи фрагментації повідомлень із повторною передачею (ARQ, HARQ). Адаптивне управління потужністю дає змогу підтримувати оптимальні умови передачі навіть при змінному середовищі. На мережевому рівні застосовуються механізми самовідновлення маршрутів, із використанням кількох резервних шляхів, а також алгоритми виявлення й ізоляції скомпрометованих або пошкоджених вузлів. Пріоритетний доступ до каналів передачі для критично важливої інформації також є важливою функцією таких систем.

Значну роль у підвищенні завадостійкості відіграє використання штучного інтелекту. Прогнозування рівня завад і навантаження на мережу на основі аналізу

трафіку дозволяє здійснювати адаптивне управління маршрутами. Алгоритми машинного навчання застосовуються для виявлення аномалій сигналу, ознак втручання в передачу даних або ознак кіберзагроз. Використання глибоких нейронних мереж дозволяє автоматично класифікувати типи перешкод, прогнозувати їх розвиток, а також коригувати параметри передачі в режимі реального часу. Такі нейромережеві алгоритми ефективні для оптимізації використання частотних ресурсів, зменшення затримок та підвищення енергетичної ефективності системи.

Окремий напрям забезпечення завадостійкості пов'язаний із криптографічним захистом даних. Сучасні методи шифрування, включаючи гомоморфне шифрування та квантову криптографію, дозволяють суттєво підвищити стійкість системи до атак на канали зв'язку, забезпечуючи не тільки захист від перешкод, але й конфіденційність, цілісність і достовірність переданої інформації. Це особливо актуально для систем критичної інфраструктури, де інформація часто є надважливою і стратегічною.

Особливості об'єктів критичної інфраструктури – таких як енергетичні комплекси, транспортні вузли, медичні установи чи військові об'єкти – вимагають врахування низки специфічних факторів [5]. По-перше, критично важлива вимога — це робота в реальному часі, де допустимі затримки передачі інформації вимірюються мілісекундами. По-друге, системи повинні мати високу надійність і здатність до функціонування навіть у разі часткового виходу з ладу. По-третє, мережі мають бути стійкими до кіберфізичних атак, що вимагає впровадження комплексної кібербезпеки. І, нарешті, важливою є сумісність із існуючими SCADA-системами, що керують об'єктами в режимі реального часу.

Під час моделювання таких систем важливо враховувати можливість відмов окремих сегментів мережі, динамічне переміщення вузлів (особливо в MANET), дію людського фактора (операторів), а також вплив цілеспрямованих атак, зокрема DoS. Застосування гібридного моделювання — поєднання імітаційного, дискретного та аналітичного — дозволяє оцінити ефективність різних конфігурацій у режимі реального часу, а також в умовах обмежених ресурсів, характерних для надзвичайних ситуацій.

Представимо класифікацію основних параметрів моделювання завадостійких систем зв'язку з урахуванням специфіки критичної інфраструктури у вигляді Таблиці 1.

Таблиця 1

Основні параметри моделювання завадостійких систем зв'язку для критичної інфраструктури

Категорія	Параметр	Опис
Модель каналу зв'язку	AWGN, Rayleigh, Rician	Вибір моделі залежить від типу середовища.
Типи завад	Інтерференція, імпульсні завади, jamming	Враховується для тестування стійкості проти перешкод
Методи модуляції	BPSK, QPSK, OFDM, DSSS, FHSS	Вибір залежно від вимог до завадостійкості й пропускної здатності
Кодування	Reed-Solomon, Turbo, LDPC	Для виявлення та виправлення помилок
Топологія мережі	Сітка, дерево, коміркова структура	Впливає на відмовостійкість і ефективність маршрутизації
Протоколи маршрутизації	AODV, OLSR, RPL, DSR	Адаптивна передача даних у нестабільних умовах
Алгоритми відновлення	Multipath routing, rerouting, fault detection	Швидке реагування на збої та пошкодження

Інструменти моделювання	MATLAB/Simulink, NS-3, OMNeT++, OPNET, QualNet	Для створення віртуального середовища тестування систем
Криптографічний захист	AES, гомоморфне шифрування, квантова криптографія	Забезпечують конфіденційність і захист від кібератак
Штучний інтелект / ML	Прогнозування перешкод, класифікація аномалій, адаптивна маршрутизація	Підвищують адаптивність і ефективність у динамічних умовах
Масиви антен	Beamforming, MIMO	Покращення якості сигналу й зменшення впливу завад
Якість обслуговування (QoS)	Затримка, пропускна здатність, рівень BER, доступність	Основні метрики для оцінки ефективності моделі системи
Сумісність	Інтеграція з SCADA, IoT, MANET	Важлива для взаємодії з інфраструктурою
Надійність системи	Час безвідмовної роботи, стійкість до збоїв	Ключові параметри для систем критичного значення
Тип атаки / загроз	DoS, Spoofing, Physical layer attacks	Враховуються під час моделювання кіберфізичних загроз

Аналіз і узагальнення наведених у таблиці параметрів дозволяє сформувати цілісне уявлення про основні вимоги до моделювання завадостійких систем зв'язку, орієнтованих на забезпечення надійної роботи критичної інфраструктури. Зокрема, особливу увагу слід приділяти параметрам, що визначають здатність системи функціонувати в умовах інтенсивних завад, кібератак та відмов окремих компонентів.

Врахування різноманітних моделей каналу зв'язку (AWGN, Rayleigh, Rician) у поєднанні з сучасними методами кодування (Turbo, LDPC), модуляції (OFDM, DSSS), адаптивного маршрутизаційного протоколу й засобів відновлення дозволяє адекватно відтворити умови експлуатації системи у віртуальному середовищі. Для об'єктів критичної інфраструктури, таких як енергетичні або транспортні системи, ключовими є параметри затримки, надійності, стійкості до втрат зв'язку та швидкості відновлення після збоїв.

Крім технічних характеристик, важливо інтегрувати в моделі інструменти штучного інтелекту, що забезпечують адаптивність у реальному часі, а також криптографічні механізми захисту інформації, зокрема у випадках перехоплення або спотворення сигналу. Таким чином, побудова моделі, що базується на комплексному урахуванні наведених параметрів, відповідає ключовим принципам розробки безпечних, надійних і завадостійких комунікаційних систем для критично важливих об'єктів.

Зазначимо, що сучасні підходи до моделювання завадостійких систем зв'язку демонструють потужний синтез інженерних рішень, математичного апарату та штучного інтелекту. Вони дозволяють створювати надійні, адаптивні й стійкі до зовнішніх загроз комунікаційні мережі, здатні ефективно забезпечувати зв'язок навіть у найбільш критичних умовах.

Висновки

У статті розглянуто сучасні підходи до моделювання завадостійких систем зв'язку з урахуванням специфіки критичної інфраструктури. Моделювання завадостійких систем зв'язку для критичної інфраструктури є складним і багатогранним процесом, що вимагає комплексного підходу. Використання адаптивних алгоритмів, нейромережевих

методів та передових криптографічних технологій значно підвищує надійність систем зв'язку. Зроблено акцент на системному підході, що охоплює всі рівні архітектури зв'язку — від фізичного до прикладного.

Встановлено, що ефективне функціонування таких систем можливе лише за умов поєднання новітніх технологій (Multiple Input – Multiple Output, AI, багаторівневе кодування), правильного вибору топології мережі, використання адаптивних алгоритмів маршрутизації та впровадження моделей захисту від цілеспрямованих атак.

Подальші дослідження повинні бути спрямовані на розробку цифрових двійників комунікаційних систем для об'єктів критичної інфраструктури. А також на інтеграцію моделей зв'язку з кіберзахистом та удосконалення алгоритмів самовідновлення після аварій.

Передбачається, що комплексне моделювання дозволить не лише прогнозувати поведінку системи у разі надзвичайних подій, але й оптимізувати її структуру ще на етапі проєктування, що є пріоритетним для забезпечення стійкості, безпеки та безперервності функціонування систем зв'язку для критичної інфраструктури.

Література:

1. Bulygin Yu. I., Tkacheva V.A, Lutkova E.M. Elements of risk-oriented approach in industrial safety and labor protection management systems of enterprises. 6 Eastern European Magazine Naukowe (East European Scientific Journal), №11 (51), 2019. pp. 35-40.

2. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83-93.

3. Кібербезпека енергетики, науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України: матеріали, 27 травня 2022 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2022. 128 с.

4. Павук І. В., Кобилкін, Д. С. Особливості формування концепції управління проєктними ризиками на об'єктах критичної інфраструктури. Інновінг сучасних трендів в менеджменті безпеки: тези доповідей Всеукр. наук.-практ. конф. (м. Львів, 26 травня 2023 року.). Львів : Астропринт, 2023. С. 47-49.

5. Шведов В., Рудик Ю., Куць В. Урахування воєнних ризиків втрат якості електропостачання об'єктів критичної інфраструктури. Управління якістю в освіті та промисловості: досвід, проблеми та перспективи: тези доповідей VI Міжнар. наук.-практ. конф., (16–17 листопада) 2023 року. Режим доступу: https://science.lpnu.ua/qm-2023/proceedings (англ.); https://science.lpnu.ua/uk/qm-2023/tezy-dopovidey (укр.), С.296-298.