

ОПТИМІЗАЦІЯ МОБІЛЬНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

¹ Вінницький національний технічний університет

Анотація

Доповідь присвячена дослідженню підходів до оптимізації мобільності та підвищення безпеки телекомунікаційних мереж транспортних систем на основі методів штучного інтелекту. Розглянуто архітектуру, сервіси та особливості функціонування мереж транспортних засобів типу VANET як складової інтелектуальних транспортних систем (ITS). Проаналізовано основні вимоги до таких мереж, зокрема мінімальну затримку передавання даних, високу надійність, масштабованість і стійкість до загроз безпеці. Обґрунтовано доцільність застосування методів глибокого навчання (DNN, CNN, RNN, DBN) для формування довіри, виявлення аномалій і прогнозування поведінки вузлів у мережах VANET. Запропоновано архітектурний підхід до інтеграції моделей штучного інтелекту у механізми управління мобільністю та безпекою. Отримані результати свідчать про перспективність інтеграції інтелектуальних алгоритмів у телекомунікаційні мережі транспортних систем для побудови надійних і безпечних комунікацій у «розумних містах».

Ключові слова: штучний інтелект, глибоке навчання, VANET, інтелектуальна транспортна система, оптимізація мобільності, довіра в мережах, безпека телекомунікацій, V2X-комунікації.

Abstract

The article is devoted to the study of approaches to optimizing mobility and enhancing the security of telecommunication networks in transportation systems based on artificial intelligence methods. The architecture, services, and operational features of vehicular ad hoc networks (VANETs) as a component of intelligent transportation systems (ITS) are considered. The main requirements for such networks are analyzed, including minimal data transmission delay, high reliability, scalability, and resilience to security threats. The feasibility of applying deep learning methods (DNN, CNN, RNN, DBN) is substantiated for trust management, anomaly detection, and behavior prediction of nodes in VANETs. An architectural approach to integrating artificial intelligence models into mobility and security management mechanisms is proposed. The obtained results demonstrate the potential of integrating intelligent algorithms into telecommunication networks of transportation systems to establish reliable and secure communications in smart cities.

Keywords: artificial intelligence, deep learning, VANET, intelligent transportation system, mobility optimization, network trust, telecommunication security, V2X communications.

Вступ

Стрімкий розвиток урбанізації та зростання кількості транспортних засобів призводить до перевантаження дорожньої інфраструктури, виникнення заторів та підвищення ризику дорожньо-транспортних пригод. Ці чинники негативно впливають на ефективність транспортних потоків і безпеку руху, особливо у великих мегаполісах та за несприятливих погодних умов. Для подолання зазначених проблем активно впроваджуються інтелектуальні транспортні системи (Intelligent Transportation Systems, ITS), які поєднують сенсорні технології, бездротові комунікації та методи штучного інтелекту для моніторингу, аналізу та управління дорожнім рухом у реальному часі [1].

В основі ITS лежать мережі VANET (Vehicular Ad-hoc Networks) — різновид мобільних самоорганізованих мереж (MANET), що забезпечують динамічний обмін даними між транспортними засобами (V2V), інфраструктурою (V2I), пішоходами (V2P) та іншими елементами (V2X). Такі мережі підтримують як сервіси безпеки (попередження про аварії, екстрене гальмування, моніторинг дорожніх умов), так і інформаційно-навігаційні сервіси. Однак висока мобільність

вузлів, динамічна топологія та жорсткі вимоги до затримки передачі даних створюють суттєві виклики для забезпечення стабільності та безпеки комунікацій у VANET.

Традиційні методи управління трафіком та довірою у таких мережах виявляються малоефективними за умов швидкої зміни середовища. У цьому контексті методи глибинного навчання та штучного інтелекту відкривають нові можливості для оптимізації мобільності телекомунікаційних мереж, прогнозування поведінки вузлів, виявлення аномалій і загроз, а також динамічного маршрутизаційного управління. Застосування згорткових (CNN), рекурентних (RNN, LSTM) та глибинних нейронних мереж (DNN, DBN) дозволяє підвищити точність класифікації, адаптивність та ефективність систем управління довірою в мережах ITS [2].

Таким чином, актуальність дослідження зумовлена потребою у створенні інтелектуальних підходів до оптимізації мобільності та безпеки телекомунікаційних мереж у сучасних транспортних системах. Використання методів штучного інтелекту сприятиме підвищенню надійності комунікацій, ефективності управління транспортними потоками та розвитку інфраструктури «розумних міст».

Результати дослідження

У результаті проведеного дослідження проаналізовано архітектуру, сервіси та засоби забезпечення безпеки у мережах транспортних засобів (VANET) як складовій інтелектуальних транспортних систем (ITS). Було визначено ключові структурні компоненти VANET — бортові вузли (OBU), прикладні модулі (AU) та дорожні інфраструктурні вузли (RSU), які забезпечують реалізацію комунікаційних сценаріїв типу V2V, V2I, V2P та V2X. Досліджено середовище обміну даними у V2X, що включає як короткодіапазонні технології DSRC, так і стільникові рішення C-V2X на базі LTE та 5G [3].

Встановлено, що основними вимогами до VANET є мінімальна затримка передавання (менше 100 мс), висока надійність, масштабованість та захищеність комунікацій. Розроблено узагальнену модель безпечної взаємодії транспортних вузлів, яка поєднує криптографічні механізми автентифікації з адаптивними схемами довіри, що дозволяє виявляти як зовнішні, так і внутрішні загрози мережевій безпеці.

Проведено порівняльний аналіз характеристик VANET і MANET, у результаті якого встановлено, що мережі VANET відрізняються високою мобільністю вузлів, частими змінами топології, відсутністю енергетичних обмежень та обмеженою траєкторією руху. Ці особливості визначають необхідність розроблення спеціалізованих алгоритмів маршрутизації та довіри, здатних до самоналаштування в реальному часі [4].

На основі огляду сучасних досліджень визначено доцільність використання методів глибинного навчання (Deep Learning) у задачах формування довіри та виявлення аномалій у VANET. Запропоновано архітектурний підхід, який інтегрує глибинні нейронні мережі (DNN, CNN, RNN, DBN) для динамічної оцінки довіри між вузлами. Експериментальне моделювання у середовищі міської мобільності (SUMO) із застосуванням даних OpenStreetMap показало, що моделі на основі DNN забезпечують підвищення точності класифікації довірених вузлів до 96–98%, зменшення кількості хибних попереджень до 3–5%, а час реакції системи не перевищує 80 мс при середній щільності транспортних вузлів [5].

Отримані результати підтверджують ефективність інтеграції методів глибинного навчання у механізми управління довірою та безпеки VANET. Застосування таких моделей дозволяє покращити стійкість мережі до атак типу «Sybil» та «Black Hole», а також забезпечити стабільність і достовірність передавання критично важливих повідомлень у режимі реального часу [1, 2].

Таким чином, результати дослідження демонструють перспективність поєднання інтелектуальних алгоритмів обробки даних з адаптивними схемами довіри в архітектурі VANET для побудови надійних і безпечних інтелектуальних транспортних систем майбутнього.

Висновки

У результаті проведеного дослідження встановлено, що мережі VANET є фундаментальною складовою інтелектуальних транспортних систем, забезпечуючи високошвидкісний та надійний обмін даними між транспортними засобами, дорожньою інфраструктурою та іншими учасниками руху через комунікаційні моделі V2X (V2V, V2I, V2P, V2N, V2G). Ключові компоненти

архітектури VANET — OBU, AU та RSU — формують основу для реалізації як сервісів безпеки (попередження про ДТП, екстрене гальмування, оповіщення про наближення спецтранспорту), так і інформаційно-навігаційних та розважальних сервісів.

Доведено, що традиційні алгоритми маршрутизації, запозичені з MANET, є малоефективними в умовах високої мобільності вузлів, динамічної топології та обмежень часу затримки, що зумовлює потребу у використанні спеціалізованих підходів до оптимізації комунікацій у VANET.

Застосування методів глибокого навчання (DNN, DBN, RNN, CNN, DMN) відкриває можливість для побудови адаптивних систем управління довірою, виявлення аномальної поведінки вузлів та прогнозування мережевих подій у реальному часі. Такі методи підвищують точність класифікації, знижують ризики внутрішніх атак і забезпечують стабільність передавання критично важливих повідомлень.

Отримані результати підтверджують, що використання штучного інтелекту та глибокого навчання є перспективним напрямом для оптимізації мобільності та безпеки телекомунікаційних мереж у транспортних системах нового покоління. Подальші дослідження доцільно спрямувати на розроблення інтегрованих AI-моделей для динамічного маршрутизаційного управління та прогнозування стану мережі VANET в умовах інтенсивного трафіку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cheong, C., Song, Y., Cao, Y., Zhang, Y., Cai, B., Ni, Q.: Multidimensional trust evidence fusion and path-backtracking mechanism for trust management in vanets. IEEE Internet Things J. 11 (2024). <https://doi.org/10.1109/JIOT.2024.3363755>

2. Ullah, F., Salam, A., Amin, F., Khan, I.A., Ahmed, J., Zaib, S.A., Choi, G.S.: Deep trust: a novel framework for dynamic trust and reputation management in the internet of things (IoT)- based networks. IEEE Access 12, 87407–87419 (2024). <https://doi.org/10.1109/ACCESS.2024.3409273>

3. Васильківський, М. В., Грабчак, Н. В., Бриль, Д. Р., & Олійник, А. О. (2025). Сценарії застосування технологій 6G-IoT в інфокомунікаційних мережах нового покоління. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО, (60), 358-368. <https://doi.org/10.36910/6775-2524-0560-2025-60-38>

4. Оптимізація інтелектуальних телекомунікаційних мереж [Текст] / М. В. Васильківський, А. В. Прикмета, А. Олійник, Д. В. Нікітович // Вісник Хмельницького національного університету. Серія «Технічні науки». – 2023. – № 1. (317). – С. 33–41.

5. Васильківський М. Інтелектуальний радіоінтерфейс з підтримкою штучного інтелекту [Текст] / М. В. Васильківський, Г. Варганюк, О. Болдирева // Вісник Хмельницького національного університету. Серія «Технічні науки». – 2023. – № 1. (317). – С. 26–32.

Васильківський Микола Володимирович — кандидат технічних наук, доцент, доцент кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: mvasylkivskyi@gmail.com

Будаш Михайло Володимирович — аспірант групи 172-22а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: mika@budash.dp.ua

Вікулов Микола Миколайович — студент групи TSM-24м, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: nikolayvikylov12356@gmail.com

Vasylkivskyi Mykola V. — candidate of technical sciences, associate professor, associate professor of the Department of Information Communication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: mvasylkivskyi@gmail.com

Budash Mykhailo V. — graduate student of group 172-22a, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: mika@budash.dp.ua

Vikulov Mykola M. - student of group TSN-24m, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: nikolayvikylov12356@gmail.com