https://doi.org/10.31891/2219-9365-2024-79-17
УДК 658

ПАВЛЮК Віталій
Національний університет «Львівська політехніка»
https://orcid.org/0009-0009-3237-8108
vitalii.pavliuk.mknuo.2023@lpnu.ua
НАКОНЕЧНИЙ Адріан
Національний університет «Львівська політехніка»
https://orcid.org/0000-0002-1873-6337
adrian.y.nakonechnyi@lpnu.ua

ІНТЕГРОВАНА АВТОМОБІЛЬНА СИСТЕМА КОМУНІКАЦІЇ ДЛЯ ПОКРАЩЕННЯ БЕЗПЕКИ ТА ЕФЕКТИВНОСТІ ДОРОЖНЬОГО РУХУ

У даній роботі досліджується проблема створення надійних та ефективних комунікаційних протоколів для інтегрованих систем V2X (Vehicle-to-Everything), які сприяють підвищенню безпеки та ефективності дорожнього руху. Актуальність дослідження зумовлена стрімким розвитком транспортної галузі та впровадженням V2X технологій, що забезпечують бездротовий обмін даними між транспортними засобами та інфраструктурою. У ході роботи проаналізовано наявні системи V2X, розглянуто моделі обміну повідомленнями та розроблено комбінований протокол, що поєднує переваги технологій IEEE 802.11p та LTE-V2X. Запропонований підхід дозволяє досягти високої продуктивності, надійності та безпеки в умовах різних сценаріїв використання, забезпечуючи низьку затримку передачі даних та цілісність повідомлень. Особлива увага приділяється розробленню механізмів пріоритетності повідомлень, їхньої цілісності та автентифікації на основі інфраструктури публічних ключів (PKI).

Ключові слова: Vehicle-to-Everything, IEEE 802.11p, LTE-V2X, протокол V2X, V2X комунікація.

PAVLIUK Vitalii, NAKONECHNYI Adrian
Lviv Polytechnic National University

INTEGRATED VEHICLE COMMUNICATION SYSTEM FOR ENHANCING ROAD SAFETY AND EFFICIENCY

Currently, the transportation industry is undergoing significant technical transformations thanks to the introduction of the new Vehicle-to-Everything (V2X) technology. This technology provides direct wireless data exchange between vehicles, road infrastructure and other road users. Systems built according to this technology are able to significantly increase the safety, efficiency and convenience of road traffic, helping to reduce the number of accidents, optimize traffic and support autonomous driving. In view of this, the relevance of the presented research is determined by the need to develop reliable and effective communication protocols for V2X, which are able to meet modern requirements for speed, reliability and security of data transmission.

This paper addresses the development of reliable and efficient communication protocols for integrated V2X (Vehicle-to-Everything) systems, aimed at enhancing road safety and efficiency. The relevance of this research is driven by the rapid development of the transportation sector and the implementation of V2X technologies, which enable wireless data exchange between vehicles and infrastructure. The study analyzes existing V2X systems, examines messaging models, and develops a combined protocol that leverages the advantages of IEEE 802.11p and LTE-V2X technologies. The proposed approach achieves high performance, reliability, and safety under various usage scenarios, ensuring low data transmission latency and message integrity. Special attention is given to the development of mechanisms for message prioritization, integrity, and authentication based on Public Key Infrastructure (PKI).

Kay words: Vehicle-to-Everything, IEEE 802.11p, LTE-V2X, V2X protocol, V2X communication.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

На даний час транспортна галузь зазнає значних технічних перетворень завдяки впровадженню нової технології Vehicle-to-Everything (V2X). Ця технологія забезпечує прямий бездротовий обмін даними між транспортними засобами, дорожньою інфраструктурою та іншими учасниками дорожнього руху. Системи побудовані за даною технологією здатні значно підвищувати безпеку, ефективність та зручність дорожнього руху, сприяючи зменшенню кількості аварій, оптимізації трафіку та підтримці автономного водіння. З огляду на це актуальність представленого дослідження зумовлена необхідністю розроблення надійних і ефективних протоколів комунікації для V2X, які здатні задовольнити сучасні вимоги до швидкості, надійності та безпеки передачі даних.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою дослідження є розроблення протоколу інтегрованої системи V2X комунікації для забезпечення високої продуктивності, надійності та безпеки руху в різних сценаріях використання. Для досягнення поставленої мети в роботі розглядаються наступні питання.

1. Аналіз наявних систем V2X та їхні характеристики.

2. Розгляд основних моделей обміну повідомленнями та протоколів керування доступом до середовища (MAC) у V2X.

3. Розроблення протоколу комунікації для V2X систем на основі вибору протоколу керування доступом до середовища та протоколу транспортного рівня.

4. Реалізація заходів забезпечення цілісності та автентифікації повідомлень у V2X системах.

Таким чином дане дослідження полягає в розробленні комбінованого протоколу комунікації для V2X систем, який би поєднував переваги протоколів IEEE 802.11p та LTE-V2X. Запропонований в роботі підхід дозволяє забезпечити високу швидкість передачі даних, надійність та низьку затримку, що є критичним для застосувань V2X технології. Крім того, в статті розглядається можливість розроблення механізму забезпечення пріоритетів повідомлень та їхньої цілісності й автентифікації за допомогою інфраструктури публічних ключів (PKI).

ОГЛЯД НАЯВНИХ РІШЕНЬ ПОСТАВЛЕНОЇ ЗАДАЧІ

Загальний опис систем V2X

Транспортна галузь зазнає значних перетворень із появою технології зв'язку "Vehicle-to-Everything" (V2X). V2X виходить за рамки традиційних систем, орієнтованих на водія, сприяючи створенню спільного середовища на дорозі завдяки прямому бездротовому обміну даними між транспортними засобами, дорожньою інфраструктурою та навіть пішоходами. Така взаємопов'язана екосистема має великий потенціал революціонізувати транспорт, зробивши його безпечнішим, плавнішим та ефективнішим для всіх [19].

Основні компоненти системи V2X складають.

- Бортові пристрої (on-board units - OBU): встановлені в транспортних засобах і пішоходів, OBU служать центрами комунікації. Вони оснащені радіомодулями, давачами (такими як GPS, камери, радари), антенами та процесорами для полегшення обміну даними [16].
- Придорожні пристрої (roadside units - RSU): розгорнуті вздовж доріг та інфраструктури, RSU збирають та передають інформацію про дорожній рух. Вони діють як ретранслятори інформації в мережі V2X, а також служать як окремі учасники системи [1, 17].
- Центр управління (необов'язковий): керує всією мережею V2X, керує потоком даних, надає послуги (наприклад, оновлення дорожнього руху) та оптимізує продуктивність мережі.

Зв'язок у системах V2X здійснюється [13].

- Протоколами зв'язку V2X, які регулюють взаємодію між OBU та RSU, забезпечуючи безперебійний та надійний обмін даними.
- Обміном даними, який охоплює інформацію в реальному часі, критичну для безпеки та управління дорожнім рухом, включаючи:
  - Положення, швидкість і напрямок руху транспортного засобу
  - Дані датчиків з камер і радарів
  - Стан світлофора
  - Наявність пішоходів

Зазначена схема зв’язку схематично зображена на рис. 1.

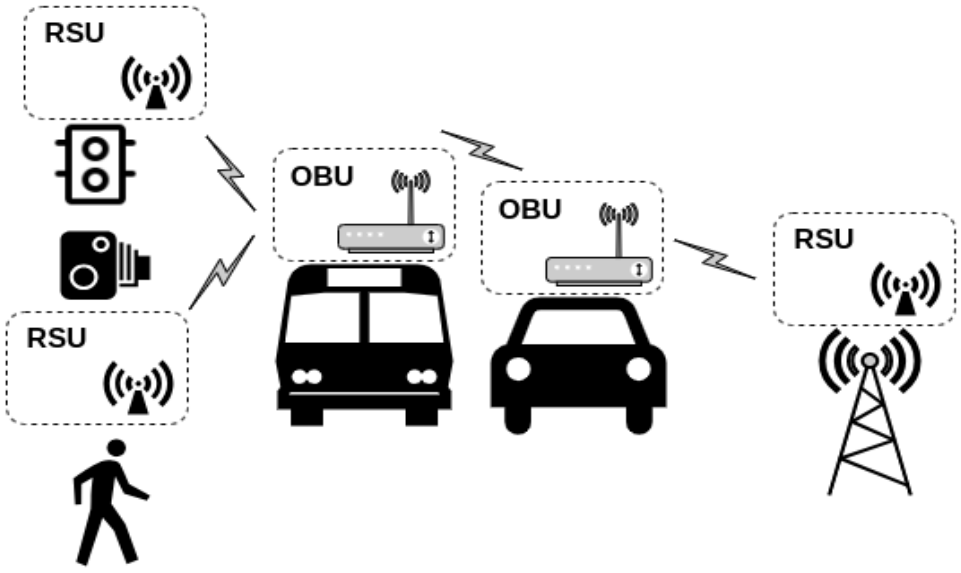

Рис. 1. Структурна схема взаємодії бортових пристроїв (OBU) та придорожніх пристроїв (RSU) у системі V2X

ISSN 2219-9365

V2X дозволяє використовувати широкий спектр застосувань, які змінюють спосіб нашого пересування дорогами [19] і дозволяють реалізувати:

- Запобігання зіткненням: попереджає водіїв про потенційні небезпеки, дозволяючи їм вживати ухильних дій і запобігати аваріям.
- Спільне маневрування: сприяє узгодженим діям, таким як зміна смуги руху та злиття, покращуючи потік руху.
- Оптимізацію світлофорів: транспортні засоби можуть регулювати швидкість залежно від майбутніх світлофорів, зменшуючи затори.
- Безпеку вразливих учасників дорожнього руху: підвищує безпеку пішоходів і велосипедистів за допомогою оповіщень і попереджень у реальному часі.
- Підтримку автоматизованого водіння: надає дані в реальному часі для того, щоб автономні транспортні засоби могли безпечно та ефективно рухатися.

Огляд наявних систем, їх характеристики, переваги та недоліки

Системи типу V2X стають все більш різноманітним і в них використовуються різні протоколи зв'язку та конфігурації інфраструктури. На цей час, найбільш поширеними є наступні системи [4].

- Dedicated Short-Range Communication (DSRC). Дана система використовує стандарт IEEE 802.11p для короткострокового зв'язку (зазвичай до 1000 метрів) між транспортними засобами та інфраструктурою. DSRC широко використовувалася в пілотних проектах, особливо у Сполучених Штатах. Однак її майбутнє залишається невизначеним через появу нових технологій на основі мобільних мереж і наступного покоління з більш широкими можливостями та потенційно нижчими витратами.
- Cellular Vehicle-to-Everything (C-V2X). Система використовує наявні мобільні мережі (LTE) для полегшення зв'язку V2X. Система C-V2X пропонує ширше покриття порівняно з DSRC, охоплюючи райони з обмеженою спеціалізованою інфраструктурою, однак, у C-V2X можливі проблеми з затримкою в перевантажених мобільних мережах, що може вплинути на роботу в режимі реального часу.
- 5G NR V2X. Завдяки використанню технології нового покоління система 5G New Radio (NR), 5G NR V2X обіцяє значні переваги. Вона пропонує надзвичайно малу затримку (що критично важливо для застосунків у режимі реального часу), можливість масового підключення (що підтримує більшу кількість пристроїв) та підвищену надійність. 5G NR V2X має великий потенціал для майбутніх застосунків V2X, особливо для автономних транспортних засобів. Порівняльні характеристики наведених систем наведені в таблиці 1.

Таблиця 1

	DSRC	C-V2X	5G NR V2X
Архітектура	IEEE 802.11p, короткі відстані (до 1 км)	LTE-V2X, Побудована на LTE, підтримка прямих і мережевих режимів	Використання 5G для високошвидкісного зв'язку
Технічні характеристики	Частоти 5.9 ГГц, швидкість до 27 Мбіт/с	Частоти 1.8-2.6 ГГц, висока пропускна здатність	Частоти до 52 ГГц, швидкість до кількох Гбіт/с, наднизька затримка
Переваги	Низька затримка, висока надійність	Великий радіус дії, використання наявної інфраструктури LTE	Висока пропускна здатність, підтримка автономного водіння
Недоліки	Обмежений радіус дії, менша пропускна здатність	Вища затримка, можливі проблеми з перевантаженням мережі	Висока вартість впровадження, значні інвестиції в інфраструктуру

Попри свої переваги, наявні системи V2X мають також і ряд недоліків, які необхідно вирішувати при широкому впровадженні.

- Висока вартість: впровадження та підтримка інфраструктури V2X у великих масштабах може бути дорогою. Тут враховується вартість бортових блоків для транспортних засобів, придорожніх блоків та інфраструктури мережі зв'язку (особливо для DSRC).
- Стандартизація: різні протоколи зв'язку та фрагментовані стандарти між DSRC, C-V2X та 5G NR V2X можуть перешкоджати взаємодії між системами.
- Кібербезпека: системи V2X вразливі до кібератак, що викликає занепокоєння щодо безпеки даних і потенційного маніпулювання. Необхідні надійні заходи кібербезпеки, щоб забезпечити цілісність та правдивість даних V2X.

- Конфіденційність: збір та використання даних V2X викликають занепокоєння щодо конфіденційності, особливо щодо поведінки водія та інформації про місцезнаходження. Для розв'язання цих проблем та підвищення довіри до технології V2X необхідні чіткі правила та механізми контролю з боку користувачів.

З наведеного можна зробити висновки, що технологія V2X має потенціал «революціонізувати» транспорт, роблячи його безпечнішим, плавнішим та ефективнішим. Наявні різні види системи V2X, такі як DSRC, C-V2X та 5G NR V2X, пропонують унікальні характеристики та переваги, однак перед широким впровадженням V2X необхідно розв'язувати ряд ключових задач, або врахувати їх при розробці системи. До них в першу чергу потрібно віднести високу вартість, можливість стандартизації, кібербезпеку та конфіденційність. Для успішного розроблення V2X систем, важливо ретельно вивчити характеристики різних архітектур, використати їх переваги та зосередитися на розв'язанні вказаних задач.

АНАЛІЗ ОСНОВНИХ МОДЕЛЕЙ ТА АЛГОРИТМІВ СИСТЕМИ V2X

Моделі обміну повідомленнями

Системи V2X використовують різні моделі обміну повідомленнями для забезпечення зв'язку та обміну інформацією між різними учасниками дорожнього руху. До основних моделей можна віднести [14].

- Автомобіль-Інфраструктура (Vehicle to Infrastructure - V2I). Модель передбачає обмін повідомленнями між бортовим пристроєм (OBU) у транспортному засобі та придорожнім пристроєм (RSU) або локальним сервером додатків. RSU зазвичай встановлюються вздовж доріг та служать точками доступу до мережі V2X. Вони можуть збирати дані про дорожній рух, передавати попередження про небезпеку та надавати інші послуги
- Автомобіль-Мережа (Vehicle to Network - V2N). Дана модель передбачає зв'язок OBU з віддаленим сервером додатків через мобільну мережу. Віддалені сервери додатків можуть надавати широкий спектр послуг V2X, таких як оновлення дорожнього руху, прогнозування трафіку та послуги з підтримки водіння.
- Автомобіль-Автомобіль (Vehicle to Vehicle - V2V). Така модель забезпечує прямий обмін повідомленнями між OBU в транспортних засобах. V2V може використовуватися для обміну інформацією про місцезнаходження та динаміку транспортних засобів, що може допомогти запобігти зіткненням та покращити потік руху.
- Автомобіль-Пішохід (Vehicle to Pedestrian - V2P). Модель передбачає передачу інформації між OBU в транспортному засобі та User Equipment (UE) у пішоходів, таких як смартфони. V2P може використовуватися для попередження пішоходів про небезпеку, що може допомогти зменшити кількість ДТП з участю пішоходів.

Структурну схему моделей обміну повідомленнями у системах V2X зображено на Рис. 2.

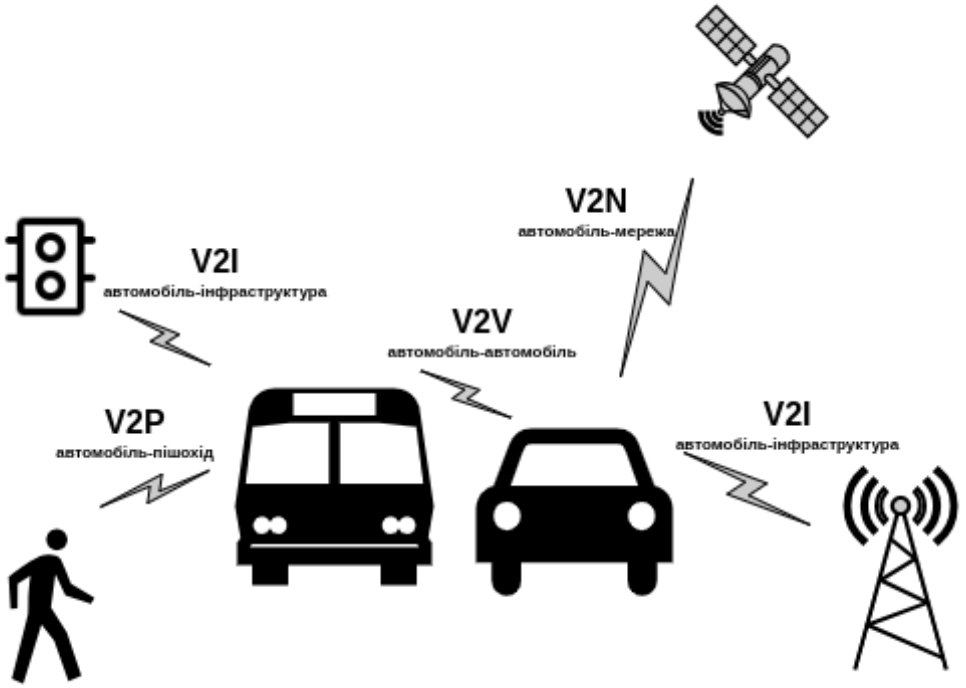

Рис. 2. Структура моделі обміну повідомленнями систем V2X

Протоколи керування доступом до середовища (MAC) у системах V2X

Рівень керування доступом до середовища (MAC) є фундаментальним у всіх протоколах згідно з моделлю OSI, адже саме він визначає правила доступу до фізичного середовища [8]. У контексті V2X систем, MAC протоколи відіграють важливу роль у забезпеченні ефективного та справедливого розподілу обмежених ресурсів бездротового каналу для передачі даних [2]. Одні з найпоширеніших MAC протоколів, що використовуються у V2X системах:

- **IEEE 802.11p**. Протокол був спеціально розроблений для V2X застосувань. Він використовує модифіковану версію алгоритму CSMA/CA з додатковим каналом безпеки для критичних повідомлень про безпеку [12, 5].
  - Переваги.
    - Низька затримка, що робить його ідеальним для застосунків, які потребують швидкого реагування, таких як запобігання зіткненням.
    - Висока надійність, завдяки стійкості до перешкод і механізмів резервування.
  - Недоліки.
    - Обмежений радіус дії, зазвичай до 1000 метрів.
    - Менша пропускна здатність порівняно з LTE-V2X та 5G NR-V2X.
    - Вимагає розгортання спеціалізованої інфраструктури DSRC
- **LTE-V2X.** Даний протокол використовує наявну інфраструктуру стільникової мережі LTE для V2X-зв'язку [10].
  - Переваги.
    - Широкий радіус дії. LTE-V2X може охоплювати більші території, порівняно з протоколом DSRC, завдяки ширшому радіусу дії мережі LTE.
    - Висока пропускна здатність. Протокол LTE-V2X пропонує значно вищу пропускну здатність, що робить його придатним для передачі великих обсягів даних, таких як відео та карти високої роздільної здатності.
  - Недоліки:
    - Більша затримка, порівняно з протоколом DSRC, що може вплинути на чутливі до часу V2X застосунків.
    - Можливі проблеми з перевантаженням мережі, особливо в густонаселених районах.
    - Мала надійність у порівнянні з DSRC, адже може бути вразлива до збоїв у роботі стільникової мережі.
- **5G NR-V2X**. Протокол ґрунтується на принципах LTE-V2X, але пропонує значні покращення у розрізі затримки, пропускної здатності та надійності. Використовує нову технологію стільникового зв’язку 5G [12].
  - Переваги:
    - Має найкращі показники з трьох протоколів по відношенню до затримки, пропускної здатності та надійності.
    - Добре узгоджується з найсучаснішими V2X застосунками.
  - Недоліки:
    - Найдорожчий з трьох протоколів через необхідність розгортання нової інфраструктури 5G.
    - На даний час знаходиться на стадії розроблення і не має широкого доступу.

Таким чином вибір найбільш ефективного протоколу MAC для систем V2X залежить від поставлених початкових задач, конкретного застосування та доступної інфраструктури.

РОЗРОБЛЕННЯ СТЕКУ ТЕХНОЛОГІЙ ДЛЯ ПРОТОКОЛУ КОМУНІКАЦІЙ У СИСТЕМІ V2X

Вибір керування доступом до середовища (MAC)

Вибір протоколу керування доступом до середовища (MAC) є важливим кроком у розробленні протоколу комунікації для V2X систем. З огляду на це доцільно розглянути деякі основні протоколи MAC, кожен з яких має свої переваги та недоліки.

Хоча 5G NR-V2X є ідеальним варіантом для майбутніх V2X застосунків завдяки його оптимізації для таких систем, наразі ця технологія є занадто новою і не має необхідної інфраструктури.

Тому, враховуючи переваги та недоліки протоколів IEEE 802.11p та LTE-V2X, запропоновано використовувати обидва протоколи у зв'язці для розробленого протоколу.

LTE-V2X буде вважатися основним протоколом завдяки його кращим загальним характеристикам передачі даних. Він буде використовуватися для передачі інформаційних повідомлень, таких як: телеметрія автомобіля, зображення та відео з бортових камер, інформація про дорожній рух, тощо.

Щоб адресувати дані із меншою затримкою у передачі повідомлень та вищою надійністю, IEEE 802.11p буде використовуватися як резервний протокол. Також він буде використовуватися для передачі високопріоритетних та екстрених повідомлень, таких як: інформація про потенційне зіткнення, проїзд транспорту екстрених служб, попередження про небезпеку, тощо.

Переваги використання обох протоколів, забезпечує суттєвий позитивний ефект.

Протокол LTE-V2X працює переважно на нижніх рівнях моделі OSI [10, 15], зокрема на фізичному рівні забезпечує передачу та прийом сигналу, включаючи вибір радіочастоти, методи модуляції та контроль потужності сигналу. На канальному рівні керує кадруванням даних, виявленням і виправленням помилок, а також керуванням доступом до середовища (MAC) для спільного використання каналу зв'язку між транспортними засобами. На мережевому рівні (який частково залучений) у деяких сценаріях зв'язку може використовуватися для виконання таких функцій, як адресація та обмін маршрутною інформацією з мережевою інфраструктурою.

Протокол IEEE 802.11p працює головним чином на фізичному та канальному рівнях моделі OSI [10, 15], зокрема на фізичному рівні обробляє фізичну передачу пакетів даних через бездротове середовище, включаючи такі завдання, як модуляція сигналу, керування доступом до середовища та виявлення помилок. На канальному рівні даний протокол відповідає за кадрування даних у пакети, додавання заголовків для маршрутизації та перевірки помилок, а також керування доступом до середовища (MAC) для забезпечення ефективного спільного використання бездротового каналу між пристроями.

Таким чином, протоколи LTE-V2X та IEEE 802.11p закривають нижні рівні моделі OSI розроблюваного протоколу, як показано на Рис. 3.

Рис. 3. Модель OSI пропонованого протоколу із закритими нижніми рівнями

Забезпечення пріоритетності повідомлень

Для гарантування своєчасної доставки критичних повідомлень у V2X-системах додано механізм пріоритетності трафіку. Така операція досягається шляхом використання комбінації протоколів TCP/UDP та додаткового заголовка з пріоритетом повідомлення (PRIO).

Використання TCP/UDP [9]:

- TCP (Transmission Control Protocol). Даний протокол використовується для надійної та впорядкованої передачі даних, що робить його придатним для інформаційних повідомлень, які потребують гарантії доставки, таких як телеметрія та дані про дорожній рух.

- UDP (User Datagram Protocol). Протокол використовується для швидкої передачі даних, що робить його придатним для критичних повідомлень, які потребують низької затримки, таких як попередження про зіткнення та інформація про екстрені служби.

Додатковий заголовок додається до кожного повідомлення V2X, який містить 1-байтове поле пріоритету. Значення пріоритету визначає важливість повідомлення та впливає на його обробку в системі: 0 - найвищий пріоритет, 255 - найнижчий. Пропонується резервувати ¼ пріоритетів під високо пріоритетні повідомлення (пріоритети 0-63) та ¾ під низько пріоритетні повідомлення (пріоритети 64-255). На основі значення пріоритету повідомлення обирається відповідний протокол нижнього рівня (IEEE 802.11p або LTE-V2X).

Високо пріоритетні повідомлення (пріоритети 0-63) передаються через UDP і відправляються по IEEE 802.11p.

Низько пріоритетні повідомлення (пріоритети 64-255) передаються через TCP і відправляються через LTE-V2X.

Таким чином, транспортний рівень моделі OSI для розроблюваного протоколу використовуватиме TCP/UDP із додатковим заголовком пріоритетності повідомлення, як зображено на Рис. 4.

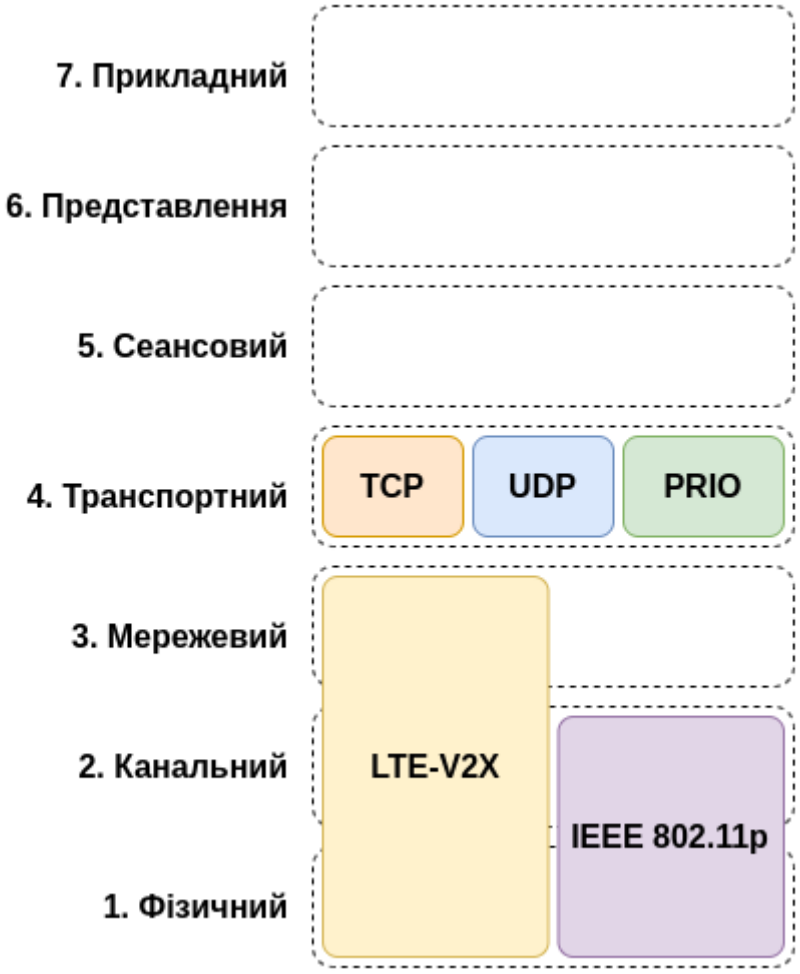

Рис. 4. Поточна модель OSI розроблюваного протоколу із транспортним рівнем

Таким чином, структура формування V2X повідомлення для відправлення із верхніх рівнів виглядатиме, як зображено на Рис. 5. На мові С розроблений код реалізації обгортки повідомлень на транспортному рівні.

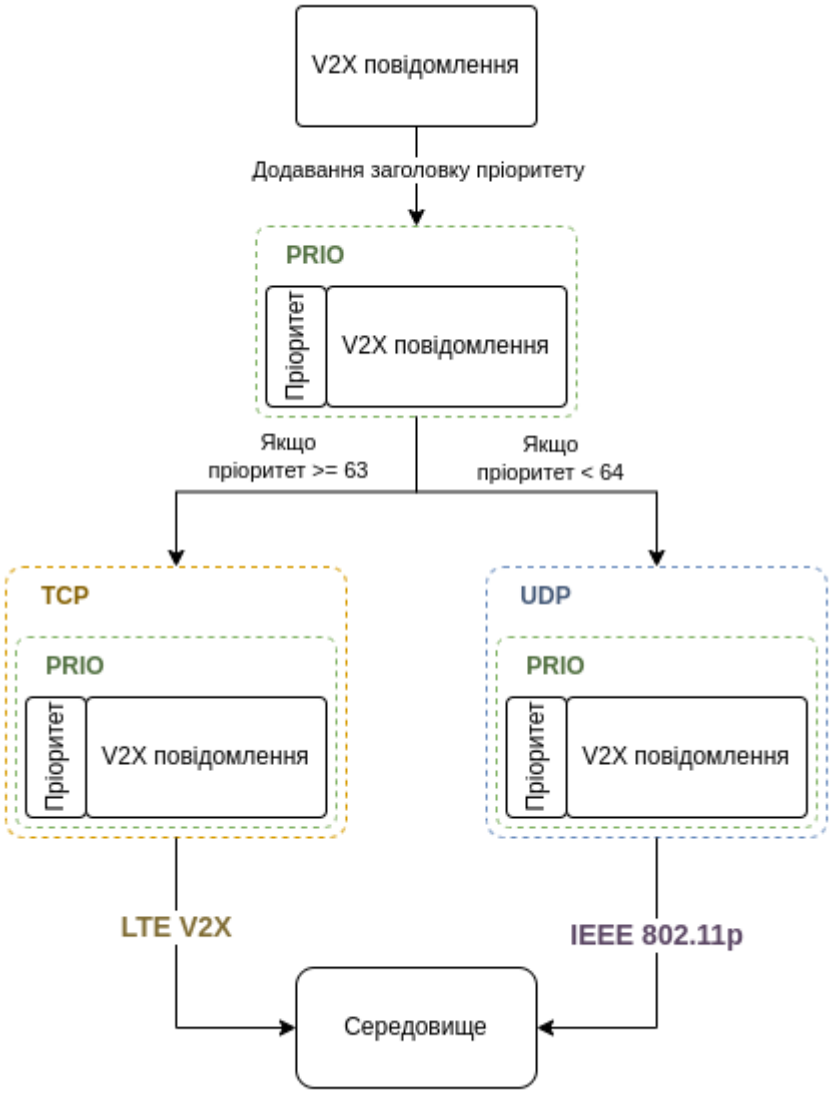

Рис. 5. Структура формування V2X повідомлення для відправлення у фізичне середовище

Забезпечення цілісності та автентифікації

У системах V2X обмін повідомленнями є надзвичайно чутливим, адже вони можуть нести критичну інформацію, що впливає на безпеку дорожнього руху [11]. Тому захист цих повідомлень від модифікації та підробки є дуже важливим.

Для досягнення цієї мети використано інфраструктуру публічних ключів (Public Key Infrastructure, PKI) [6].

Інфраструктура публічних ключів PKI, є основою довіри в цифровій комунікації. Вона керує створенням, розповсюдженням, зберіганням та відкликанням цифрових сертифікатів. Дані сертифікати діють як електронні паспорти, що зв'язують відкритий ключ із певною сутністю (людина, пристрій, веб-сайт) та гарантують його дійсність за допомогою довіреного центру сертифікації. PKI забезпечує безпечне спілкування шляхом перевірки особи учасників та шифрування передачі даних [18].

Відомо, що цифровий підпис представляє криптографічний код, який дозволяє підтвердити автентичність та цілісність повідомлення. Він генерується шляхом застосування приватного криптографічного ключа до хеш-суми повідомлення [3]. Цифровий сертифікат представляє електронний документ, який зв'язує відкритий криптографічний ключ з ідентифікатором власника (наприклад, VIN автомобіля або ID пристрою інфраструктури). Він видається довіреним центром сертифікації (CA) і підписується цифровим підписом CA [7].

Забезпечення цілісності та автентифікації V2X-повідомлень здійснюється наступним чином.

1. Кожен учасник системи V2X (автомобіль, пристрій інфраструктури тощо) повинен мати цифровий сертифікат. Цей сертифікат може бути виданий виробником пристрою або державним органом.

2. Пул довірених центрів сертифікації (Certificate Authority - CA) має бути погоджений між усіма учасниками системи. Це гарантує, що всі сертифікати, що використовуються, є надійними та можуть бути перевірені.

3. V2X-повідомлення підписується цифровим підписом відправника. Цей підпис генерується за допомогою приватного ключа відправника та хеш-суми повідомлення.

4. Отримувач повідомлення перевіряє сертифікат відправника. Дана операція виконується шляхом перевірки цифрового підпису у сертифікаті та ланцюжка довіри (chain of trust), який веде до кореневого CA.

5. Отримувач використовує відкритий ключ відправника, отриманий із сертифіката, для перевірки цифрового підпису повідомлення. Якщо підпис дійсний, це підтверджує, що повідомлення не було модифіковано під час передачі, а також, що відправник дійсно є той, за кого він себе видає.

На Рис. 6 наведений процес формування підпису для V2X повідомлення, а, на Рис. 7 зображено процес перевірки цілісності отриманого повідомлення та перевірка дійсності сертифіката відправника.

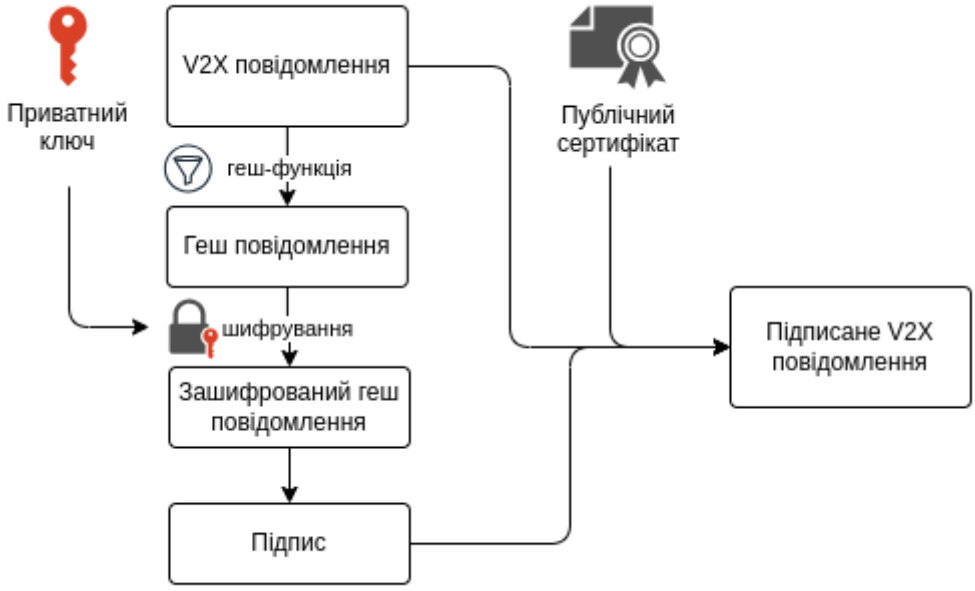

Рис. 6. Схематичне представлення процесу підпису V2X повідомлення цифровим ключем

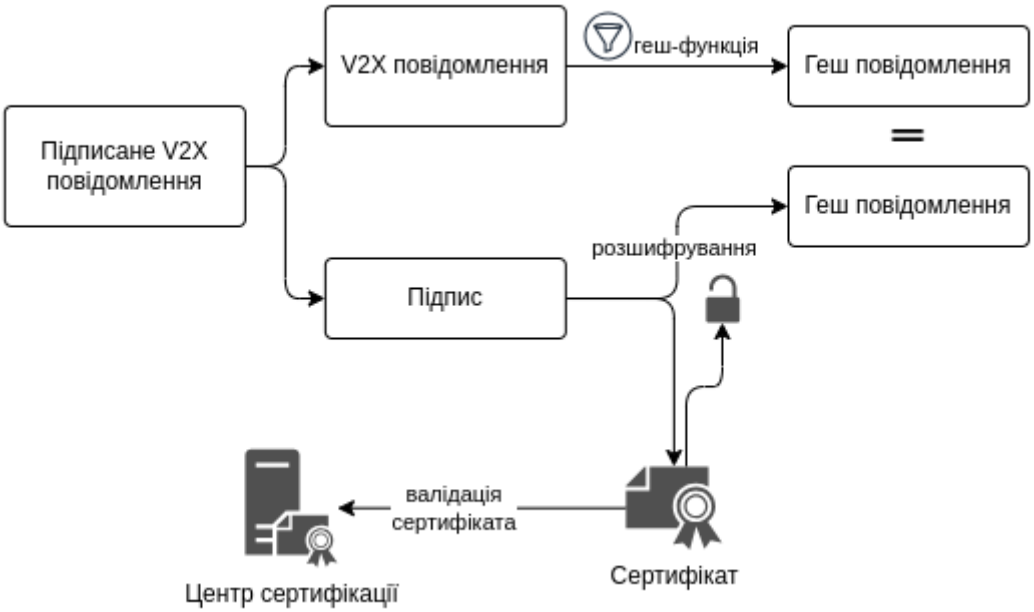

Рис. 7. Схематичне зображення процесу перевірки цілісності отриманого V2X повідомлення та дійсності сертифіката відправника

Остаточний вигляд пропонованого протоколу в моделі OSI наведено на Рис. 8.

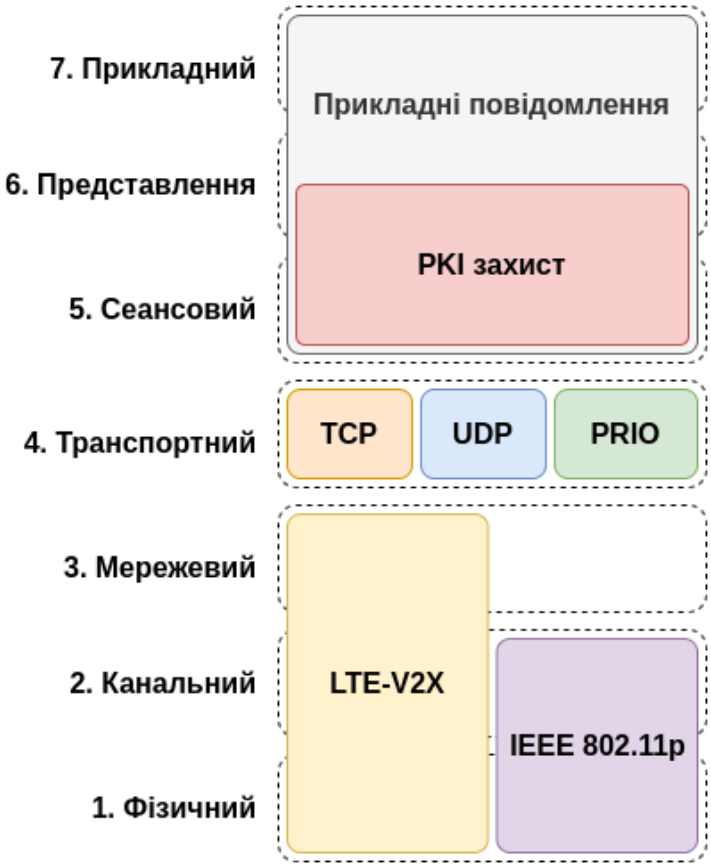

Рис. 8. Модель OSI пропонованого протоколу

Таким чином, можна зробити висновок, що запропоноване поєднання протоколів IEEE 802.11p та LTE-V2X дозволяє на даний час забезпечити високу ефективність та надійність в різних сценаріях, використання комбінації TCP/UDP з додатковим заголовком дозволяє реалізувати пріоритетність своєчасної доставки критичних повідомлень, а використання інфраструктури публічних ключів для цифрового підпису та сертифікації повідомлень, дозволяє запобігти модифікації та підробці.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОПОНОВАНОГО ВИБОРУ ВИКОРИСТАННЯ ДВОХ ПРОТОКОЛІВ ФІЗИЧНОГО РІВНЯ

Наступним важливим етапом є детальне дослідження ефективності вибору двох пропонованих протоколів фізичного рівня, а саме IEEE 802.11p та LTE-V2X. Дане дослідження включає кілька важливих аспектів:

- Аналіз продуктивності. Вивчення продуктивності обраних протоколів у різних умовах трафіку та навантаження на мережу. Дослідження включає вимірювання пропускної здатності, затримок і надійності передачі даних.
- Симуляція та реальні тести. Проведення комп'ютерної симуляції та реальних експериментів для перевірки ефективності протоколів у різних сценаріях, що дозволить оцінити роботу в умовах високої мобільності та динамічного середовища та в загальному доцільність такого вибору.
- Порівняння результатів. Порівняння результатів, отриманих у проведених дослідженнях, з метою визначення найкращого підходу для конкретних випадків використання в системах V2X.

Вимоги до апаратного забезпечення

Для забезпечення ефективної роботи розробленого протоколу необхідно чітко сформулювати вимоги до апаратного забезпечення.

- Вибір радіомодулів. Проведення вибору відповідних радіомодулів для підтримки IEEE 802.11p та LTE-V2X, яке включає оцінку доступних на ринку модулів за такими параметрами, як діапазон частот, пропускна здатність, затримка та енергоефективність.

- Контролери та обчислювальні ресурси. Визначення вимог до контролерів і обчислювальних ресурсів для обробки даних у реальному часі, яке включає вибір процесорів, пам'яті та інших компонентів, що забезпечують швидке і надійне виконання необхідних алгоритмів.

Імплементація пристроїв для проведення досліджень

Наступний крок полягає у проведенні імплементації прототипів пристроїв, які дозволяють проводити експериментальні дослідження.

- Розроблення прототипів. Розроблення прототипів транспортних засобів та інфраструктурних пристроїв, які підтримують обрані протоколи і включають апаратне та програмне забезпечення, необхідне для тестування V2X комунікацій.
- Проведення експериментів. Проведення експериментів з використанням розроблених прототипів у різних умовах дорожнього руху, що дозволяє зібрати дані для подальшого аналізу та вдосконалення протоколу.

Деталізація інфраструктури публічних ключів

З метою забезпечення безпеки V2X комунікацій необхідно деталізувати інфраструктуру публічних ключів (PKI). Для цього необхідно здійснити.

- Визначення процедур. Визначення процедур видачі, зберігання та відкликання цифрових сертифікатів для учасників системи V2X.
- Визначення центрів сертифікації. Визначення процесу створення надійних центрів сертифікації (CA), які відповідають за видачу та управління цифровими сертифікатами.

Таким чином, сформульовані етапи дослідження спрямовані на подальше вдосконалення та підвищення ефективності системи V2X і є ключовими на шляху до створення надійної та ефективної системи комунікації для транспортних засобів.

Запропонований протокол комунікації для V2X систем забезпечує надійний і безпечний обмін даними між транспортними засобами та інфраструктурою, сприяє підвищенню безпеки і ефективності дорожнього руху, а проведення подальших досліджень та впровадження запропонованих рішень дозволять досягти більш високих результатів у цій галузі, що зробить транспортну інфраструктуру більш технологічно розвиненою.

References

1. Ahmed Z., Naz S., Ahmed J. Minimizing transmission delays in vehicular ad hoc networks by optimized. *Wireless Networks*. 2020. Vol. 26, no. 4. P. 2905–2914. URL: https://doi.org/10.1007/s11276-019-02198-x.
2. An Analysis on Contemporary MAC Layer Protocols in Vehicular Networks: / L. Hota et al. *Future Internet*. 2021. Vol. 13, no. 11. P. 287. URL: https://doi.org/10.3390/fi13110287.
3. Andvsilva. Digital Signature with Hash Function – How it works?. *Medium*. 2024. URL: https://andsilvadrcc.medium.com/digital-signature-with-hash-function-how-it-works-f4eed52267f5.
4. Anwar W., Franchi N., Fettweis G. Physical Layer Evaluation of V2X Communications Technologies: 5G NR-V2X,. 2019. URL: https://doi.org/10.1109/vtcfall.2019.8891313.
5. Arena F., Pau G., Severino A. A Review on IEEE 802.11p for Intelligent Transportation Systems. *Journal of Sensor and Actuator Networks*. 2020. Vol. 9, no. 2. P. 22. URL: https://doi.org/10.3390/jsan9020022.
6. Bengtsson J. Steering the Course of Cybersecurity in the Automotive Industry with PKI. *Nexusgroup*. URL: https://www.nexusgroup.com/steering-the-course-of-cybersecurity-in-the-automotive-industry-with-pki/.
7. Content Manager OnDemand for Multiplatforms 10.5.0. *IBM - United States*. URL: https://www.ibm.com/docs/en/cmofm/10.5.0?topic=cryptography-digital-certificates-certificate-authorities (дата звернення: 10.06.2024).
8. Contributors to Wikimedia projects. Medium access control - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Medium_access_control (дата звернення: 10.06.2024).
9. Gorman B. TCP vs UDP: What's the Difference and Which Protocol Is Better?. *TCP vs UDP: What's the Difference and Which Protocol Is Better?*. URL: https://www.avast.com/c-tcp-vs-udp-difference.
10. On the Impact of Multiple Access Interference in LTE-V2X and NR-V2X / A. Rehman et al. *Sensors*. 2023. Vol. 23, no. 10. P. 4901. URL: https://doi.org/10.3390/s23104901.
11. Popović I. V2X - Paving the Superhighway for Tomorrow's Smart Mobility | HTEC | HTEC. *HTEC*. URL: https://htecgroup.com/v2x-paving-the-superhighway-for-tomorrows-smart-mobility/.
12. Review of V2X–IoT Standards and Frameworks for ITS Applications / K. Kiela et al. *Applied Sciences*. 2020. Vol. 10, no. 12. P. 4314. URL: https://doi.org/10.3390/app10124314.
13. Team E. What Is V2X and The Future of Vehicle to Everything Connectivity. *www. emqx. com*. URL: https://www.emqx.com/en/blog/what-is-v2x-and-the-future-of-vehicle-to-everything-connectivity.
14. V2X Communication Technologies and Service Requirements for Connected and / E. Cinque et al. 2020. URL: https://doi.org/10.23919/aeitautomotive50086.2020.9307388.
15. V2X Network Architecture and Standards System / S. Chen et al. *Wireless networks*. 2023. P. 81–116. URL: https://doi.org/10.1007/978-981-19-5130-5_3.
16. Waysion. Unveiling the Power of On-Board Units (OBU) in Modern Vehicles - Waysion. *Waysion*. URL: https://www.waysion.com/blog/on-board-units-obu/.
17. What is a Roadside Unit (RSU)? RSU Meaning | Isarsoft. *Isarsoft | We make every camera count*. URL: https://www.isarsoft.com/knowledge-hub/rsu (дата звернення: 10.06.2024).
18. What is PKI | Public Key Infrastructure | DigiCert. *SSL Digital Certificate Authority | Encryption & Authentication | DigiCert.com*. URL: https://www.digicert.com/what-is-pki (дата звернення: 10.06.2024).
19. What Is Vehicle-to-Everything (V2X)?. *Embedded OS, Support, and Services | BlackBerry QNX*. URL: https://blackberry.qnx.com/en/ultimate-guides/software-defined-vehicle/vehicle-to-everything (дата звернення: 10.06.2024).