Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

Павлюченко Владислав Андрійович

УДК 654.026

ДИСЕРТАЦІЯ
АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІОТ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ РУХУ У SMART-МІСТІ

171 Електроніка
Електроніка та телекомунікації

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____/Павлюченко В.А.

Науковий керівник Макаренко Володимир Васильович, кандидат технічних наук, доцент

Київ – 2024

АНОТАЦІЯ

Павлюченко В.А. Аналіз можливості використання технологій IoT для підвищення безпеки руху у smart-місті. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 171 "Електроніка". – Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", МОН України, Київ, 2024.

В дисертаційній роботі вперше отримано наступні наукові результати:

1. Вперше проведено моделювання та аналіз розповсюдження енергії поля сигналу від дорожніх станцій DSRC у складних умовах міської забудови.

2. Вперше запропоновано використовувати дорожні станції DSRC в якості повторювачів сигналу на складних ділянках руху.

3. Виконано моделювання та аналіз розповсюдження енергії поля від різних типів RFID-міток, що використовуються у транспортній мережі міста.

4. Вперше запропоновано використовувати безшовне Wi-Fi покриття для підвищення безпеки руху транспортної мережі міста.

5. Виконано моделювання та аналіз розповсюдження рівня сигналу для створення безшовного покриття від точок доступу Wi-Fi для транспортних засобів та пішоходів.

6. Проведено дослідження можливості використання безшовної мережі Wi-Fi для попередження водіїв та пішоходів при руху транспортних засобів.

Дисертаційна робота присвячена аналізу можливості використання технологій IoT для підвищення безпеки руху у сучасному місті.

Дисертаційне дослідження представлене у чотирьох розділах, у яких наведені та обґрунтовані основні результати роботи.

У вступі обґрунтовано актуальність дисертаційної роботи, сформульовано мету та задачі дослідження, наведено методи дослідження, представлена

інформація про наукову новизну, а також практичне значення отриманих результатів.

Перший розділ присвячено огляду останніх публікацій в яких проводилися дослідження використання технологій IoT у транспортній мережі міста. Розглянуто наукові роботи по використанню безпроводових технологій у транспортній системі, розглянуто характеристики безпроводових технологій, на основі яких було зроблено висновки про доцільність використання у дослідженні технологій IoT, а саме: DSRC, Wi-Fi та RFID в якості допоміжних технологій у ідентифікації транспортних засобів, дорожніх знаків та пішоходів.

У другому розділі проведено дослідження залежності інтенсивності поля сигналу сформованого активними та пасивними мітками системи радіочастотної ідентифікації (RFID) від умов розповсюдження сигналу. Проведено аналіз розповсюдження енергії поля від активних та пасивних RFID-міток. Визначено, що використання пасивних RFID-міток для інформування водіїв недостатньо для доріг, що мають дві та більше смуг руху в одну сторону. Такі мітки буде доцільно використовувати для доріг з однією смугою руху в одному напрямку або для доріг з двома смугами руху в одному напрямку за умови встановлення міток на дорожні знаки з обох боків дороги. Встановлено, що використання активних RFID-міток дає змогу інформувати транспортні засоби на дорогах, які мають більше ніж 2 смуги руху в одному напрямку. Для доріг з однією та двома смугами руху в одному напрямку буде достатньо інтеграції однієї активної RFID-мітки на дорожній знак. Для доріг з трьома та чотирма смугами руху в одному напрямку необхідно інтегрувати активні RFID-мітки з двох боків дороги для забезпечення надійного зв’язку. Для аналізу розподілення енергії поля у навколишньому середовищі використані програмні продукти Altair WinProp та Altair WallMan. Порівняння результатів моделювання і розрахунків енергії поля за формулою Фрііса показали високий ступінь збіжності результатів. Це свідчить про коректність результатів моделювання розповсюдження поля у складних умовах забудови міста. Використання характеристик радіочастотних міток, як пасивних так і активних, що випускаються промисловістю для застосування в системах контролю руху

транспорту, дозволило отримати результати що добре корелюються з результатами досліджень опублікованими іншими авторами.

Аналіз розповсюдження сигналів від RFID-міток на багато смугових дорогах, при різній конфігурації розташування транспортних засобів на дорозі, дозволив сформулювати вимоги до характеристик та місць розташування радіочастотних міток для реалізації надійного зв’язку з транспортними засобами в умовах щільного трафіку. Отримані результати можна використати при проектуванні автоматизованої транспортної мережі смарт-міста.

У третьому розділі проведений аналіз розповсюдження сигналів пристроїв DSRC в умовах складної міської забудови при різній конфігурації вулиць і взаємному розташуванні транспортних засобів. З’ясовані межі впевненого обміну інформацією між транспортними засобами в умовах щільної міської забудови з великою кількістю будівель та складною конфігурацією вулиць. Проведено дослідження залежності інтенсивності поля сигналу, сформованого дорожніми станціями DSRC та бортовими пристроями транспортних засобів, від умов розповсюдження сигналу та взаємного положення станцій та транспортних засобів. Досліджено вплив місця розташування дорожньої станції на розповсюдження сигналу у міських умовах.

Проведений аналіз можливостей системи DSRC для своєчасного попередження водіїв транспортних засобів про можливість зіткнення в умовах щільної міської забудови. Встановлено, що в умовах обмеженої видимості пристроїв DSRC, встановлених на транспортних засобах, недостатньо для забезпечення своєчасного інформування водіїв. Для усунення цього недоліку запропоновано встановлювати дорожні станції DSRC у зонах обмеженої видимості у якості повторювачів сигналів транспортних засобів. Це дає змогу на прямих ділянках збільшити відстань впевненого зв'язку і дозволить завчасно отримати повідомлення про небезпеку, що особливо важливо в умовах мокрого або покритого льодом дорожнього полотна. Дослідження показали, що використання дорожніх станцій для ретрансляції сигналів призводить до збільшення відстані

впевненого прийому сигналів від двох до десяти разів в залежності від характеру забудови.

Результати отримані за допомогою імітаційного моделювання у програмному середовищі Altair WinProp. Отримані результати можна використати при проектуванні мережі DSRC розумного міста в умовах високого рівня завад.

У четвертому розділі проведено дослідження розповсюдження рівня сигналу від точок доступу Wi-Fi. В результаті проведеного дослідження встановлено, що незважаючи на те що технологія Wi-Fi забезпечує меншу швидкість з'єднання між пристроями, ніж технологія DSRC, при організації безшовного Wi-Fi покриття можна компенсувати цю ваду даної технології завдяки тому, що пристроям Wi-Fi не треба щоразу встановлювати з'єднання з точкою доступу, поки вони знаходяться в зоні дії безшовного покриття. Таким чином технологію Wi-Fi можна використовувати для оповіщення про місцезнаходження транспортних засобів та пішоходів на небезпечних ділянках руху.

Аналіз розповсюдження сигналу від точок доступу Wi-Fi здійснювався у програмному середовищі Altair WinProp. Проведена експериментальна перевірка якості каналу передачі даних шляхом тестування втрат пакетів та пропускної здатності при різних рівнях сигналу в умовах щільної забудови у місті Києві. Дослідження проведені за допомогою Wi-Fi маршрутизатора "Mikrotik" та ноутбука з Wi-Fi модулем.

Знайдено граничний рівень сигналу сформованого точкою доступу Wi-Fi, при якому кількість втрат пакетів буде припустимою, для побудови "безшовного" покриття для транспортної мережі.

За результатами моделювання та експериментальних досліджень встановлено, що для побудови "безшовної" мережі необхідно створити зону з рівнем сигналу не меншим за -70 дБм для Wi-Fi 2.4 ГГц стандарту 802.11n. Такий рівень сигналу забезпечують чотири точки доступу Wi-Fi з потужністю передавача +20 дБм, встановлених на відстані 50 м одна від одної. Така побудова мережі Wi-Fi забезпечить надійним зв'язком учасників дорожнього руху на відстані до 50 м від перехрестя.

Практичне значення одержаних в дисертаційній роботі результатів полягає в тому, що отримані результати можуть бути використані для проектування безпроводової транспортної мережі безпечного міста. Проведене дослідження та моделювання по розповсюдженню енергії поля сигналу від точок доступу Wi-Fi можна використовувати для проектування "безшовного" Wi-Fi покриття для організації безпечного руху пішоходів та транспортних засобів у smart-місті. Результати отримані при дослідженні розповсюдження енергії поля від активних та пасивних RFID-міток можна використати при проектуванні системи оповіщення про дорожні знаки. Отримані результати містять інформацію про вибір правильного місце розташування, потужність передавача та необхідну кількість міток при побудові системи.

Ключові слова: IoT, транспортна мережа, безпроводові технології, технологія DSRC, технологія Wi-Fi, безшовне покриття, smart-місто, розповсюдження сигналу, антенна, рівень сигналу, технологія RFID, активна RFID-мітка, пасивна RFID-мітка, RFID-зчитувач, точка доступу Wi-Fi, дорожні станції, бортові пристрої, чутливість приймача, потужність.

SUMMARY

Pavliuchenko V.A. Analysis of the possibilities of using IoT technologies to increase traffic safety in a smart city. – Qualifying scientific work on the rights of the manuscript.

The dissertation on competition of a scientific degree of the doctor of philosophy on a specialty 171 "Electronics". – National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky", Ministry of Education and Science of Ukraine, Kyiv, 2024.

The following scientific results were first obtained in the dissertation:

1. For the first time, the modeling and analysis of the energy propagation of the signal field from DSRC road stations in complex urban conditions were carried out.

2. For the first time, it was proposed to use DSRC road stations as signal repeaters in complex traffic areas.

3. The modeling and analysis of field energy propagation from different types of RFID tags used in the city's transport network were performed.

4. For the first time, it is proposed to use seamless Wi-Fi coverage for the city's transportation network.

5. The modeling and analysis of signal strength propagation to create a "seamless" coverage from Wi-Fi access points for vehicles and pedestrians were performed.

6. The minimum signal level for creating high-quality "seamless" coverage from Wi-Fi access points has been found.

The dissertation research is presented in four chapters, in which the main results of the work are presented and substantiated.

The introduction substantiates the relevance of the dissertation, formulates the purpose and objectives of the study, presents the research methods, and provides information on the scientific novelty and practical significance of the results.

The first chapter is devoted to a review of recent publications that have studied the use of IoT technologies in the city's transport network. The scientific works on the use of wireless technologies in the transport system had been considered, and the characteristics

of wireless technologies had been analyzed, on the basis of which conclusions were drawn about the feasibility of using IoT technologies in the study, namely: DSRC, Wi-Fi, and RFID as auxiliary technologies for identifying vehicles, road signs, and pedestrians.

In the second section, we study the dependence of the intensity of the signal field formed by active and passive tags of the radio frequency identification (RFID) system on the conditions of signal propagation. The analysis of the field energy propagation from active and passive RFID tags has been carried out. It is determined that the use of passive RFID tags to inform drivers is not sufficient for roads with two or more lanes in one direction. Such tags would be appropriate for roads with one lane in one direction or for roads with two lanes in one direction, provided that the tags are installed on road signs on both sides of the road. It has been established that the use of active RFID tags makes it possible to inform vehicles on roads with more than 2 lanes in one direction. For roads with one and two lanes in the same direction, the integration of one active RFID tag per road sign will be sufficient. For roads with three and four lanes in one direction, it is necessary to integrate active RFID tags on both sides of the road to ensure reliable communication. The Altair WinProp and Altair WallMan software products were used to analyze the field energy distribution in the environment. Comparison of the modeling results and field energy calculations using the Friis formula showed a high degree of convergence. This indicates the correctness of the results of modeling the field propagation in complex urban conditions. The use of the characteristics of radio frequency tags, both passive and active, produced by the industry for use in traffic control systems, allowed us to obtain results that correlate well with the results of studies published by other authors.

The analysis of the propagation of signals from RFID tags on multi-lane roads, with different configurations of vehicles on the road, made it possible to formulate requirements for the characteristics and locations of radio frequency tags to realize reliable communication with vehicles in dense traffic. The obtained results can be used in the design of an automated transport network of a smart city.

In the third section, we analyze the propagation of DSRC device signals in a complex urban environment with different street configurations and relative positions of

vehicles. The limits of confident information exchange between vehicles in dense urban areas with a large number of buildings and a complex street configuration are determined. The dependence of the intensity of the signal field formed by DSRC road stations and vehicle on-board devices on the signal propagation conditions and the relative position of the stations and vehicles was studied. The influence of the location of the road station on signal propagation in urban areas is investigated.

An analysis of the capabilities of the DSRC system for timely warning of vehicle drivers about the possibility of a collision in dense urban areas is carried out. It was found that in conditions of limited visibility, DSRC devices installed on vehicles are not sufficient to provide timely information to drivers. To address this shortcoming, it is proposed to install DSRC road stations in areas of limited visibility as vehicle signal repeaters. This will increase the distance of confident communication on straight sections and allow for early warning of danger, which is especially important in wet or icy road conditions. Studies have shown that the use of road stations for signal relaying leads to an increase in the distance of reliable signal reception from two to ten times, depending on the nature of the building.

The results were obtained using simulation modeling in the Altair WinProp software environment. The results obtained can be used in the design of a smart city DSRC network in conditions of high interference.

Section 4 investigates the signal propagation from Wi-Fi access points. As a result of the study, it was found that even though Wi-Fi technology provides a slower connection speed between devices than DSRC technology when organizing seamless Wi-Fi coverage, this disadvantage of this technology can be compensated since Wi-Fi devices do not need to establish a connection with the access point every time they are within the coverage area of seamless coverage. Thus, Wi-Fi technology can be used to alert vehicles and pedestrians to the location of dangerous traffic areas.

The analysis of signal propagation from Wi-Fi access points was carried out in the Altair WinProp software environment. The quality of the data transmission channel was experimentally verified by testing packet loss and throughput at different signal levels in

dense urban areas in Kyiv. The research was conducted using a Mikrotik Wi-Fi router and a laptop with a Wi-Fi module.

The maximum signal level generated by the Wi-Fi access point, at which the number of packet losses will be acceptable, was found to build a "seamless" coverage for the transport network.

Based on the results of modeling and experimental studies, it was found that to build a "seamless" network, it is necessary to create a zone with a signal strength not less than -70 dBm for Wi-Fi 2.4 Ghz 802.11n standard. This signal level is provided by four Wi-Fi access points with a transmitter power of +20 dBm, installed at a distance of 50 meters from each other. This construction of the Wi-Fi network will provide reliable communication for road users at a distance of up to 50 m from the intersection.

The practical significance of the results obtained in this thesis is that the findings can be used to design a wireless transport network for a safe city. The conducted research and modeling on the propagation of signal field energy from Wi-Fi access points can be used to design a "seamless" Wi-Fi coverage for the organization of safe pedestrian and vehicle traffic in a smart city. The results obtained from the study of field energy propagation from active and passive RFID tags can be used to design a traffic sign warning system. The results contain information on choosing the right location, transmitter power, and the required number of tags when building a system.

Keywords: IoT, transport network, wireless technology, DSRC technology, Wi-Fi technology, RFID technology seamless network, smart-city, propagation of the signal, antenna, receiver sensitivity, signal strength, active RFID-tag, passive RFID-tag, RFID-reader, Wi-Fi access point, RSU, OBU, power.

Список публікацій здобувача

1. Павлюченко В. А., Макаренко В.В. Використання дорожніх станцій DSRC для підвищення безпеки руху в умовах міської забудови. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. 2022. Випуск 4 (135). С. 63-68. DOI: 10.32782/1995-0519.2022.4.8. ISSN 1995-0519, (фахове видання категорії Б).

2. Павлюченко В.А., Макаренко В.В. Вибір конфігурації та розташування міток RFID для підвищення безпеки руху транспортної мережі міста. *Вісник Кременчуцького національного університету імені Михайла Остроградського.* 2023. Випуск 2 (139). С. 162-168. DOI: 10.32782/1995-0519.2023.2.20. ISSN 1995-0519, (фахове видання категорії Б).

3. Павлюченко В.А, Макаренко В.В. Аналіз можливості застосування технології Wi-Fi у транспортній мережі для підвищення безпеки руху транспорту та пішоходів. *Технології та інжиніринг.* 2023. Випуск №4 (15). С.20-29. DOI: 10.30857/2786-5371.2023.4.3. ISSN 2786-538X, (фахове видання категорії Б).

4. Павлюченко В.А., Макаренко В.В. Підвищення безпеки руху з використанням дорожніх станцій DSRC. *V міжнародна науково-практична конференція "SCIENCE AND INNOVATION OF MODERN WORLD". Cognum Publishing House.* (м. Лондон, 25-27 січня 2023р.) Лондон. 2023. С. 179-184, (матеріали конференції). ISBN: 978-92-9472-194-5. URL: https://sci-conf.com.ua/v-mizhnarodna-naukovo-praktichna-konferentsiyascience-and-innovation-of-modern-world-25-27-01-2023-london-velikobritaniya-arhiv/.

5. Павлюченко В.А., Макаренко В.В. Вибір місцезнаходження та конфігурації RFID міток транспортної мережі. *XI міжнародна науково-практична конференція "Scientific progress: innovations, achievements and prospects. MPDC Publishing.* (м. Мюнхен, 23-25 липня 2023р.) Мюнхен. 2023. С. 94-99, (матеріали конференції). ISBN: 978-3-954753-04-8. URL: https://sci-conf.com.ua/xi-mizhnarodna-naukovo-praktichnakonferentsiya-scientific-progress-innovations-achievements-and-prospects-23-25-07-2023-myunhen-nimechchina-arhiv/.

6. Павлюченко В.А., Макаренко В.В. Використання технології Wi-Fi для контролю транспорту у розумному місті. *І міжнародна науково-практична конференція "Current challenges of science and education". MPDC Publishing.* (м. Берлін, 18-20 вересня 2023) Берлін. 2023, (матеріали конференції). ISBN: 978-3-954753-05-5. URL: https://sciconf.com.ua/i-mizhnarodna-naukovo-praktichna-konferentsiya-current-challengesof-science-and-education-18-20-09-2023-berlin-nimechchina-arhiv/.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ЕТЗ	–	еталонний транспортний засіб;
ІТС	–	інтелектуальна транспортна система
ЛТЗ	–	легковий транспортний засіб
СМ	–	стаціонарна мітка
ТЗ	–	транспортний засіб
AES	–	Advanced Encryption Standard;
AODV	–	Ad hoc On-Demand Distance Vector;
ASCII	–	American Standard Code for Information Interchange
BLE	–	Bluetooth Low Energy
CPPA	–	Conditional Privacy-Preserving Authentication
DACOP	–	Dynamic Authentication with Conditional Privacy-preservation
DSDV	–	Destination Sequenced Distance Vector
DSRC	–	Dedicated Short Range Communication
DSSS	–	Direct-Sequence Spread Spectrum
eSBR	–	enhanced Street Broadcast Reduction
GPS	–	Global Positioning System
HTTP	–	HyperText Transfer Protocol
IoT	–	Internet of Things
IPSEC	–	Internet Protocol Security
ITS	–	Intellectual Transport Systems
LMM	–	LSSVM Multiple Model
LPWAN	–	Low Power Wide Area Network
LSSVM	–	Least Square Support Vector Machine
LTE	–	Long-Term Evolution
MGWS	–	Multiple Gigabit Wireless Systems
MIMO	–	Multiple-Input Multiple-Output

MU-MIMO	–	Multi-User Multiple-Input Multiple-Output technology
NFC	–	Near Field Communication
NGTP	–	Next-Generation Telematics Protocol
NS-2	–	Network Simulator 2
OBU	–	Onboard Unit
OFDM	–	Orthogonal frequency-division multiplexing
OFDMA	–	Orthogonal Frequency Division Multiple Access
OSI	–	The Open Systems Interconnection model
PKI	–	Public Key infrastructure
QAM	–	Quadrature Amplitude Modulation
QAS	–	Q Ary Search
RFID	–	Radio Frequency Identification
RSS	–	Received Signal Strength
RSU	–	Roadside Unit
SMTP	–	Simple Mail Transfer Protocol
SUMO	–	Simulation of Urban Mobility
TCP	–	Transmission Control Protocol
TKIP	–	Temporal Key Integrity Protocol
UDP	–	User Datagram Protocol
V2I	–	Vehicle-to-Infrastructure
V2V	–	Vehicle-to-Vehicle
VSN	–	Visual Sensor Network
VTL	–	Virtual Traffic Lights
WAP	–	Wireless Application Protocol
WAVE	–	Wireless Access in Vehicular Environment
WEP	–	Wired Equivalent Privacy
Wi-Fi	–	Wireless Fidelity
WPA	–	WiFi Protected Access
WSMP	–	WAVE Short-Message Protocol.

ВСТУП

Обґрунтування вибору теми дослідження. Щоденне збільшення кількості транспортних засобів призвело до збільшення кількості заторів та виникнення більшого числа дорожньо-транспортних пригод. Основними причинами аварійних випадків є неуважність водіїв, обмежений огляд дороги, несподівана поява пішохода на дорозі, погані погодні умови, що перешкоджають видимості транспортних засобів та пішоходів. Через ці чинники, виникла необхідність у встановленні додаткового контролю за транспортною мережею міста та інтегрування технологій інтернету речей (IoT) у об’єкти транспортної мережі, задля зменшення кількості аварійних випадків на дорогах міста. До систем IoT входить велика кількість безпроводових технологій, проте не всі з них можна використовувати у транспортній мережі, оскільки до технології, що буде працювати в міських умовах і від якої буде залежати безпека людей, висуваються особливі – посилені вимоги.

В результаті проведеного аналізу наукових праць по інтеграції технології IoT у транспортну мережу міста зроблено висновок, що технології концепції IoT здатні зменшити ризик виникнення аварій у "сліпих кутах" та зонах з обмеженою видимістю. Значний внесок у наукові дослідження по інтеграції технологій IoT у транспортну мережу міста зробили такі вчені, як Саншай Яксирангкун, Кулит На Накорн, Кутида Ройвибуншай, Криштоф Малецки, Камил Копашик, Хуа Квін, Вейхонг Чен, Веймін Чен, Ни Ли, Минг Женг, Янг Пенг та інш. Дослідження у сфері IoT наразі є пріоритетними та дуже перспективними, оскільки все більше країн світу намагаються зробити smart-міста, тим самим підвищити безпеку пересування транспортних засобів та пішоходів. Тому виникає необхідність у проведені аналізу можливості використання технологій концепції IoT у smart-місті, зокрема розповсюдження рівня електромагнітного сигналу у складних умовах міської забудови.

В результаті проведеного аналізу наукових робіт, які стосуються технології RFID, що використовується на транспортній мережі, було виявлено, що існуючі

дослідження були проведені без врахування різних типів RFID-міток. Зокрема не було проведено досліджень по розповсюдженню рівня сигналу в умовах міської забудови та в умовах щільного потоку транспорту. В рамках наукової роботи запропоновано використовувати дорожні станції DSRC у якості повторювачів сигналу для збільшення відстані на якій можлива взаємодія бортових пристроїв та дорожніх станцій DSRC. Модулі технології DSRC не інтегровані у сучасні пристрої пішоходів, тому пішоходи будуть невидимими для пристроїв DSRC, що встановлені на транспортних засобах та вздовж доріг. Модулі технології Wi-Fi інтегровані у сучасні пристрої пішоходів. Завдяки технології Wi-Fi можна інтегрувати пристрої пішоходів у транспортну мережу. Технологія Wi-Fi поступається технології DSRC у швидкості з'єднання пристроїв, дальності дії та завадостійкості, проте її можна використовувати на обмежених ділянках руху для упередження зіткнень.

Отримані результати моделювання та проведеного аналізу наукових досліджень можуть бути використані для проектування безпроводової транспортної мережі безпечного міста.

Мета і задачі дослідження. *Метою дисертаційної роботи* є дослідження, моделювання та аналіз використання технологій IoT для підвищення безпеки руху автомобілів та пішоходів в транспортної мережі міста.

Об'єкт дослідження – безпроводові технології систем IoT, що використовуються при побудові транспортної мережі міста.

Предмет дослідження – пристрої систем IoT та розповсюдження сигналу від цих пристроїв в умовах щільної міської забудови.

Для досягнення поставленої мети необхідно було вирішити такі завдання:

1. Провести аналіз сучасних публікацій в яких проводились дослідження використання технологій IoT у транспортній мережі міста.

2. Провести моделювання розповсюдження енергії поля сигналів пристроїв IoT в залежності від інфраструктури міста з обмеженими умовами видимості для транспортних засобів.

3. Дослідити розповсюдження енергії поля від активних RFID міток на багатосмугових дорогах.

4. Дослідити розповсюдження енергії поля від пасивних RFID міток на багатосмугових дорогах.

5. Виконати аналіз розповсюдження енергії поля від пасивних та активних RFID-міток та зробити висновки щодо їх використання на багато смугових дорогах.

6. Дослідити розповсюдження енергії поля від бортових пристроїв системи DSRC.

7. Дослідити розповсюдження енергії поля від дорожніх станцій системи DSRC.

8. Виконати аналіз розповсюдження енергії поля від бортових та дорожніх пристроїв та зробити висновки щодо їх використання у місцях з обмеженою видимістю транспортних засобів.

9. Провести аналіз можливості використання технології Wi-Fi при побудові транспортної мережі міста.

10. Провести моделювання розповсюдження енергії поля точок доступу Wi-Fi на перехрестях для подальшого дослідження можливості використання технології Wi-Fi для підвищення безпеки пішоходів.

11. Провести аналіз розповсюдження енергії поля точок доступу Wi-Fi в міських умовах.

12. З’ясувати якість каналу зв’язку шляхом перевірки кількості доставлених пакетів між точкою доступу і пристроєм Wi-Fi при заданому рівні сигналу.

13. Навести приклади перспективного застосування результатів моделювання та досліджень для підвищеня безпеки на дорогах smart-міста.

Методи дослідження. Для виконання поставленої мети і вирішення поставлених завдань було використано метод аналізу розповсюдження рівня сигналу від бортових пристроїв DSRC, дорожніх станцій DSRC, активних та пасивних RFID-міток та від точок доступу Wi-Fi шляхом імітаційного моделювання.

Для проведення аналізу розповсюдження енергії поля від активних і пасивних RFID-міток, а також від бортових та дорожніх пристроїв DSRC використовувалося моделювання у програмному середовищі Altair WinProp. Моделювання міської забудови проведено у програмному середовищі Altair WallMan.

Наукова новизна одержаних результатів полягає в проведеному аналізі застосування технологій концепції IoT у транспортній мережі smart-міста.

1. Вперше проведено моделювання та аналіз розповсюдження енергії поля сигналу від дорожніх станцій DSRC у складних умовах міської забудови.

2. Вперше запропоновано використовувати дорожні станції DSRC в якості повторювачів сигналу на складних ділянках руху.

3. Виконано моделювання та аналіз розповсюдження енергії поля від різних типів RFID-міток, що використовуються у транспортній мережі міста.

4. Вперше запропоновано використовувати безшовне Wi-Fi покриття для підвищення безпеки руху транспортної мережі міста.

5. Виконано моделювання та аналіз розповсюдження рівня сигналу для створення безшовного покриття від точок доступу Wi-Fi для транспортних засобів та пішоходів.

6. Проведено дослідження можливості використання безшовної мережі Wi-Fi для попередження водіїв та пішоходів при руху транспортних засобів.

Особистий внесок здобувача. Результати досліджень, що наведені у дисертаційній роботі та винесені на захист, були отримані особисто автором або ж за його активної участі та були опубліковані у спеціалізованих фахових виданнях України.

В рамках наукової роботи [1], що була опублікована в співавторстві у фаховому виданні України, здобувачем особисто було виконано наступне: моделювання розподілу інтенсивності поля передавача дорожньої станції DSRC, моделювання розподілу інтенсивності поля передавача бортового пристрою DSRC проведено аналіз можливостей системи DSRC для своєчасного попередження

водіїв транспортних засобів про можливість зіткнення в умовах щільної міської забудови.

В рамках наукової роботи [2], що була опублікована в співавторстві у фаховому виданні України, здобувачем особисто було виконано моделювання розповсюдження енергії поля сигналу від пасивних та активних RFID-міток та проведено аналіз їх використання на транспортній мережі міста.

В рамках наукової роботи [3], опублікованій у співавторстві, здобувачем особисто виконано аналіз можливості застосування технології Wi-Fi при побудові транспортної мережі smart-міста, проведено моделювання та аналіз рівня сигналу від точок доступу Wi-Fi в рамках міської забудови, запропоновано використання "безшовного" покриття Wi-Fi для транспортної мережі.

Практичне значення одержаних результатів:

Отримані результати можуть бути використані для проектування безпроводової системи контролю транспортної мережі безпечного міста. Проведені дослідження та моделювання по розповсюдженню енергії поля сигналу від точок доступу Wi-Fi можна використовувати для проектування "безшовного" Wi-Fi покриття для організації безпечного руху пішоходів та транспортних засобів у smart-місті. Результати отримані при дослідженні розповсюдження енергії поля від активних та пасивних RFID-міток можна використати при проектуванні системи оповіщення про дорожні знаки. Отримані результати містять інформацію про вибір правильного місця розташування, потужність передавача та необхідну кількість міток при побудові системи.

Зв'язок роботи з науковими програмами, планами, темами.

Робота виконувалася на кафедрі Акустичних та Мультимедійних Електронних систем Національного Технічного Університету України "Київський політехнічний інститут імені Ігоря Сікорського" у рамках НДР "Особливості формування електромагнітної обстановки у приміщеннях обладнаних технічними засобами з безпроводовим інтерфейсом" (№ держреєстрації 0119U102796).

Апробація результатів дисертації. Матеріали дисертаційних досліджень обговорювалися на міжнародних конференціях:

- V міжнародна науково-практична конференція "SCIENCE AND INNOVATION OF MODERN WORLD", м. Лондон, 23-25 липня 2023 р.
- XI міжнародна науково-практична конференція "Scientific progress: innovations, achievements and prospects", м. Мюнхен, 15-17.04.2023 р.
- I міжнародна науково-практична конференція "Current challenges of science and education", м. Берлін, 18-20 вересня 2023 р.

Публікації. Основні результати дисертаційної роботи представлені у 6 публікаціях наукових робіт, у тому числі в 3 статтях у наукових фахових виданнях України, які включені до міжнародних науко метричних баз; 3 тези доповіді у збірниках матеріалів конференцій.

Структура та обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 55 найменувань. Робота містить 102 рисунків та 5 таблиць. Загальний обсяг дисертаційної роботи становить 140 сторінок.

1 ОГЛЯД ТА АНАЛІЗ НАУКОВИХ ПРАЦЬ ПО ІНТЕГРАЦІЇ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ІОТ У ТРАНСПОРТНУ МЕРЕЖУ

1.1 Структура IoT

Інтернет речей (Internet of Things, скорочено IoT) – це глобальна мережа підключених до Інтернету речей пристроїв, оснащених датчиками та засобами передавання сигналів. Ці цифрові пристрої можуть за допомогою датчиків збирати інформацію про стан навколишнього середовища, про стан людей, сільськогосподарських земель та рослин, про стан пристроїв та різноманітних механізмів і вступати у взаємодію з іншими пристроями, обмінюватися даними з метою віддаленого моніторингу за станом об’єктів, аналізу зібраних даних і прийняття на їх основі рішень. Прикладом можуть бути гаражні двері, кавоварки, телевізори, мобільні телефони, відеокамери, датчики світла та температури тощо.

Термін "Інтернет речей" запропонував у 1999 році засновник дослідницького центру AutoID Center в Массачусетському технологічному інституті Кевін Ештон. Він висловив припущення, що згодом у кожної з речей реального фізичного світу в IoT буде цифровий двійник, її віртуальне представлення.

IoT з технологічної точки зору – це, по суті, мережа мереж, що складаються з унікально ідентифікованих об’єктів (по факту "речей"), які можуть взаємодіяти між собою через IP-підключення без втручання людини [4].

Завдяки обміну інформацією між пристроями IoT стало можливим відстежувати, контролювати та моніторити об’єкти, на яких ці пристрої встановлено. На основі IoT з’явилися технології "Розумного будинку", "Smart міста" та "Smart складів".

Архітектура ІОТ наведена на рис. 1.1.

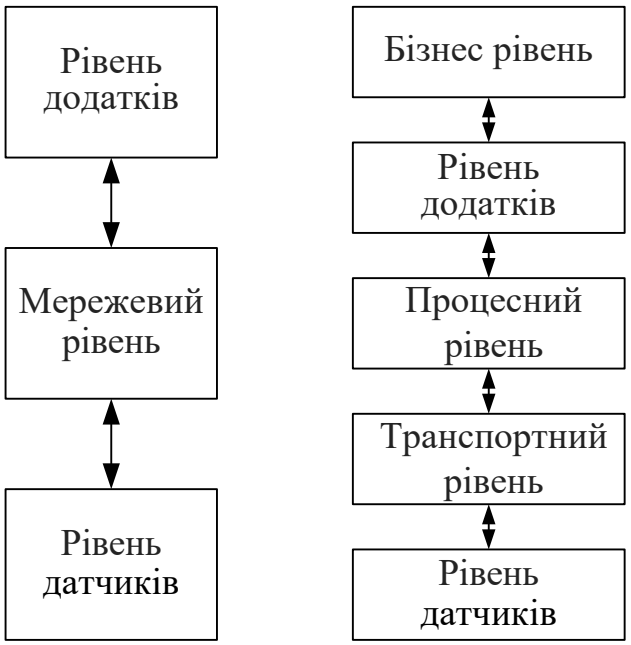


Рисунок 1.1 – Трирівнева (а) та п'ятирівнева (б) моделі архітектури IoT

У трирівневій моделі прийняті наступні позначення:

1. Рівень сприйняття (рівень датчиків) – це фізичний рівень, який має сенсори для зондування та збору інформації про навколишнє середовище. Він вимірює деякі фізичні параметри та взаємодіє з іншими розумними об'єктами в навколишньому середовищі. Цей рівень виконує три завдання:

- перше завдання – ідентифікація об'єктів (пристроїв);
- друге – збір інформації з об'єктів;
- третє завдання – передача інформації на мережевий/транспортний рівні для безпечної передавання на рівень обробки.

2. Мережевий рівень відповідає за підключення до інших розумних речей, мережевих пристроїв і серверів. Його функції також використовуються для передавання та обробки даних з датчиків.

3. Рівень додатків відповідає за надання користувачеві специфічних послуг. Цей рівень використовується для розробки та розгортання додатків Інтернету речей з використанням різних технологій Інтернету речей. До таких додатків Інтернету речей відносяться "розумний дім", "розумні будівлі", "розумні міста", "розумна

охорона здоров'я", "розумне сільське господарство", автомобільна і виробнича промисловість та багато інших. Для користувачів це один з важливих рівнів, оскільки він виступає інтерфейсом між ними та системою IoT, яка контролює і відстежує різні аспекти застосування. Він також може бути використаний для прогнозування майбутніх подій за допомогою аналізу даних [5].

Трирівнева архітектура визначає основну ідею Інтернету речей, але її недостатньо, оскільки дослідження часто зосереджуються на більш тонких аспектах IoT. Тому в літературі пропонується багато інших багаторівневих архітектур. Однією з них є п'ятирівнева архітектура, яка додатково включає обробку та бізнес-рівень. П'ять рівнів – це сприйняття, транспорт, обробка, застосування та бізнес-рівень (рис. 1.1). Роль рівнів сприйняття і застосування така ж, як і в архітектурі з трьома рівнями. Окреслимо функції решти трьох рівнів:

Транспортний рівень діє як інтерфейс між рівнем сприйняття та рівнем додатків. Транспортний рівень має два завдання: мережеве та транспортне. У мережевому завданні різні розумні речі та пристрої підключаються до мережевих пристроїв з відповідними функціями управління, контролем доступу та механізмом автентифікації. У транспортному завданні, зібрані дані з датчиків та інших пристроїв передаються на рівень обробки. Середовище передавання може бути дротовим або бездротовим, наприклад, Bluetooth, Wireless Fidelity (Wi-Fi), RFID, Near Field Communication (NFC), стільниковий зв'язок тощо. Цей рівень також дуже чутливий до атак, особливо в обмежених мережах.

Процесний рівень також відомий як проміжний рівень. Він зберігає, аналізує та обробляє величезні обсяги даних, які надходять з транспортного рівня. Він може керувати та надавати різноманітні послуги нижчим рівням. Він використовує багато технологій, таких як бази даних, хмарні обчислення і модулі обробки великих даних. Також тут видаляється нерелевантна інформація, а релевантна інформація обробляється і зберігається за допомогою таких технологій, як хмарні обчислення, повсюдні обчислення та аналітика даних. Цей рівень зберігає, аналізує та обробляє дані, отримані з транспортного рівня. Основною метою цього рівня є автоматизація процесу прийняття рішень шляхом передавання команд фізичним

пристроям на рівні сприйняття для виконання дій, що впливають на загальний стан середовища, в якому розгорнуті пристрої.

Бізнес-рівень керує всією системою IoT. Цей рівень відповідає за управління і контроль додатків, бізнес-моделей і моделей прибутку для системи Інтернету речей, наприклад, за допомогою блок-схем, граф-моделей і інформаційної панелі. Дані, отримані з прикладного рівня, далі обробляються на цьому рівні. Цей рівень визначає бізнес-стратегії, майбутні дії і стратегічно контролює загальну функціональність платформи IoT. Цей рівень також відповідає за конфіденційність користувача [6].

В IoT використовуються такі технології:

- Ethernet;
- WiFi, DSRC;
- стільникові технології;
- LPWAN (Low Power Wide Area Network);
- BLE (Bluetooth Low Energy);
- ZigBee;
- NFC;
- RFID та інші.

VSN-системи (Vehicular Sensor Networks), що входять до системи IoT, забезпечують підключення безпроводових пристроїв до транспортних засобів для збору даних про координати, швидкість і напрям руху для підвищення безпеки рху на дорогах. Сучасні транспортні засоби оснащені різноманітними сенсорними пристроями, такими як Bluetooth, GPS (Global Positioning System) та вбудовані мікро-комп'ютери, завдяки цьому транспортні засоби можуть проводити обмін даними з іншими транспортними засобами або з придорожньою інфраструктурою, використовуючи протоколи зв’язку, такі як HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), WAP (Wireless Application Protocol) та NGTP (Next-Generation Telematics Protocol). В результаті були розроблені технології

дистанційного вимкнення двигуна та дистанційна діагностика транспортного засобу, системи запобігання зіткненням та сповіщення про дорожні знаки, тощо [7].

1.2 Порівняння технологій IoT для побудови транспортної мережі

Транспортна система міста дуже мобільна та потребує надійного з'єднання між пристроями системи для уникнення аварійних випадків на дорогах, тому вимоги до безпроводової технології, що буде використовуватися у транспортній системі дуже жорсткі. Безпроводова технологія для транспорту, що буде інтегрована у smart-місто має відповідати наступним вимогам:

- швидке з'єднання пристроїв між собою;
- великий радіус дії (зона покриття);
- висока завадостійкість;
- здатність підтримувати велику кількість пристроїв в системі.

У табл.1.1 наведено основні технології IoT та їх характеристики для проведення порівняння та аналізу можливості використання у транспортній мережі міста.

Таблиця 1.1 – Порівняльна характеристика технологій концепції IoT [6]

IoT технологія	Стандарт	Споживання енергії	Тип мережі	Швидкість передавання даних	Дальність дії	Частотний спектр
Bluetooth (BLE)	IEEE 802.15.1	10 мВт	PAN	1 Мбіт/с	до 50 м	2.4 ГГц
ZigBee	IEEE 802.15.4	Дуже низьке	PAN	250 кбіт/с	до 100 м	2.4 ГГц
6LoWPAN	IEEE 802.15.4	Дуже низьке	PAN	250 кбіт/с	10…100 м	2.4 ГГц
Wi-Fi	IEEE 802.11	Високе	LAN	100…250 Мбіт/с	більше 100 м	2.4 ГГц / 5 ГГц

Продовження табл. 1.1.

IoT технологія	Стандарт	Споживання енергії	Тип мережі	Швидкість передавання даних	Дальність дії	Частотний спектр
LoRa / LoRaWAN	IEEE 802.15g	Високе	LPWAN	27 кбіт/с	більше 10 км	470…510 МГц (Китай) 865…925 ГГц
WiMAX	IEEE 802.16	Високе	MAN	70 Мбіт/с	50 км	2…11 ГГц
GSM/GPRS	ETSI	Дуже високе	WAN	50 біт/с	більше 35 км	850 МГц / 1.9 ГГц
LTE	3GPP	Дуже високе	WAN	0.1…1 Гбіт/с	28 км/10 км	700…2600 МГц
LTE-M	3GPP	Помірне	LPWAN	1 Мбіт/с	великий	різночастотний
NB-IoT	3GPP	помірне	LPWAN	250 кбіт/с	20 км	різночастотний
Z-Wave	Z-Wave Alliance	Дуже низьке	PAN	100 кбіт/с	30 м	908.42 МГц
RFID	ISO 14443, ISO 18000-6	Дуже низьке		53 кбіт/с	до 100 м (активні мітки)	125, 134…135 кГц/13.56 МГц/865…868 МГц/2.4 ГГц
DSRC	IEEE 802.11p	Високе	LAN	27 Мбіт/с	до 1 км	5.850… 5.925 ГГц

З табл. 1.1 випливає, що для побудови транспортної мережі краще використовувати технології сімейства IEEE 802.11 та RFID. IEEE 802.11 – це набір специфікацій фізичного рівня (PHY) і керування доступом до середовища (MAC) для реалізації безпроводових локальних мереж у діапазонах 2.4; 3.6; 5 і 60 ГГц. Вони підтримуються Комітетом зі стандартів IEEE 802LAN з 1997 року. IEEE 802.11p або DSRC (Dedicated Short Range Communication) – одна з останніх затверджених поправок до стандарту IEEE 802.11, цей стандарт також має назву WAVE (Wireless Access in Vehicular Environment). В рамках стандарту 802.11p було проведено вдосконалення до останньої версії 802.11, які стосуються підтримки додатків інтелектуальних транспортних систем (ITS).

Стандарт IEEE 802.11p дозволяє використання діапазону 5,9 ГГц (5.850… 5.925 ГГц) з інтервалом між каналами 20 МГц, 10 МГц і 5 МГц і встановлює вимоги для використання цього діапазону в Європі і США. Стандарт IEEE 802.11p використовує механізми, передбачені стандартом IEEE 802.11 для роботи з безпроводовою технологією DSRC, заснованою на стандарті IEEE 802.11a для роботи в діапазоні 5,9 ГГц в США або 5,8 ГГц в Японії та Європі. Технологія DSRC забезпечує обмін даними між транспортними засобами (V2V) та між транспортними засобами і придорожньою інфраструктурою (V2I) в радіусі 1 км зі швидкістю передавання даних від 3 Мбіт/с до 27 Мбіт/с і швидкістю транспортного засобу до 260 км/год.

Технологія DSRC працює на 9 каналах, кожен з яких має смугу частот, як показано на рис 1.2. CH172-5.860 ГГц і CH184-5.920 ГГц - це канали, призначені для забезпечення безпеки. Перший з них вирішує серйозні рішення з безпеки передач даних, тоді як другий відіграє захисну роль від перевантаження інших каналів. Канал CH178-5.890 ГГц є контрольним каналом, який відповідає за управління передачею та встановлення з'єднання. Шість інших службових каналів призначені для двоспрямованого зв'язку між різними типами пристроїв. Насправді, це чотири канали, але пара каналів 174, 176 і канали 180, 182 можуть бути об'єднані разом, щоб сформувати один канал 20 МГц, канал 175 і 181 відповідно. 5 МГц на початку діапазону 5.85 використовується як захисна смуга (GB) [8]. Список каналів DSRC та виділені частотні діапазони наведено у табл. 1.2.

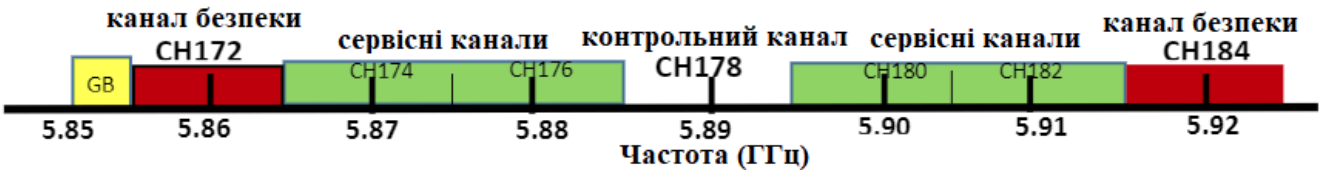


Рисунок 1.2 – Частотні канали DSRC

Таблиця 1.2 – Список каналів DSRC та виділені частоти [9]

Номер каналу	Призначення каналу	Виділені частотні діапазони, МГц
170	Зарезервований	5850…5855
172	Сервісний канал (публічна безпека)	5855…5865
174	Сервісний канал	5865…5875
175	Сервісний канал	5865…5885
176	Сервісний канал	5875…5885
178	Контрольний канал	5885…5895
180	Сервісний канал	5895…5905
181	Сервісний канал	5895…5915
182	Сервісний канал	5905…5915
184	Сервісний канал (публічна безпека)	5915…5925

Стандарти IEEE 802.11p та IEEE 1609.x разом називаються стандартами бездротового доступу в автомобільних середовищах WAVE (Wireless Access in Vehicular Environments). Архітектура WAVE підтримує два стеки протоколів, як показано на рис. 1.3.

Стандарт WAVE не визначає сеансовий, представницький або прикладний рівні, на відміну від стандартної моделі OSI (The Open Systems Interconnection model). До стандарту WAVE входять два елементи, яких немає в моделі OSI: ресурсний менеджер та блок сервісів безпеки (рис. 1.12). Стандарт WAVE підтримує 2 стеки: традиційний інтернет-протокол шостої версії (IPv6) і власний протокол WSMP (WAVE Short-Message Protocol).

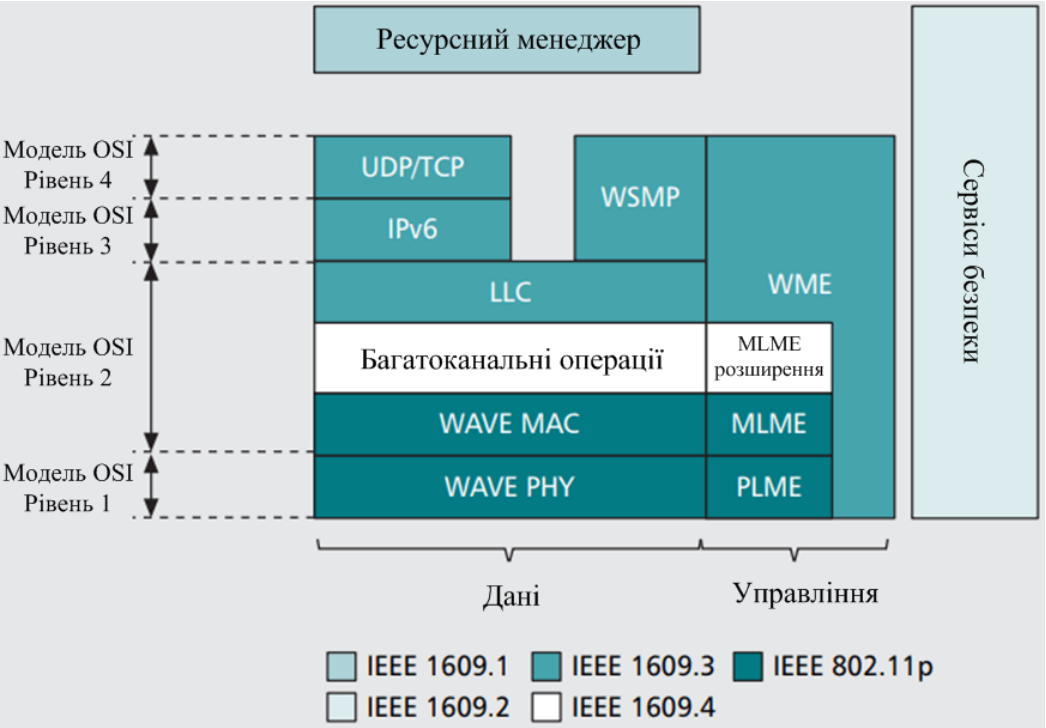


Рисунок 1.3 – Комунікаційний стек WAVE

Причина наявності двох стеків протоколів полягає в тому, щоб забезпечити чутливі до часу комунікації з високим пріоритетом, такі як TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). WSMP дозволяє додаткам транспортної мережі надсилати короткі повідомлення і безпосередньо керувати параметрами радіо ресурсу, щоб максимізувати ймовірність того, що всі залучені сторони отримають повідомлення вчасно. Протоколу WSMP недостатньо для підтримки інтернет-додатків, саме тому необхідне залучення стеку з IPv6 [10].

Основна перевага технології DSRC – це можливість об’єднання всіх пристроїв системи в єдину мережу. Згідно з принципом роботи технології DSRC, кожен транспортний засіб, на якому встановлено DSRC пристрій, передає інформацію про своє місцезнаходження (координати), а також швидкість пересування і напрямок руху 10 разів на секунду кожному транспортному засобу, що знаходиться в радіусі дії пристрою. Інші транспортні засоби, після отримання цих даних проводять оцінку будь-якого потенційного ризику зіткнення з іншим транспортним засобом, спираючись на потік даних, що постійно оновлюється.

Отримані повідомлення розшифровуються в різні функціональні програми, кожна з яких визначається за допомогою зручної ініціалізації. До цих програм належать:

- допомога при русі на перехрестях;
- допомога при повороті ліворуч;
- кооперативні попереджувальні повідомлення;
- децентралізовані екологічні повідомлення;
- базові повідомлення безпеки.

На рис. 1.4 наведено приклад взаємодії пристроїв у системі DSRC.

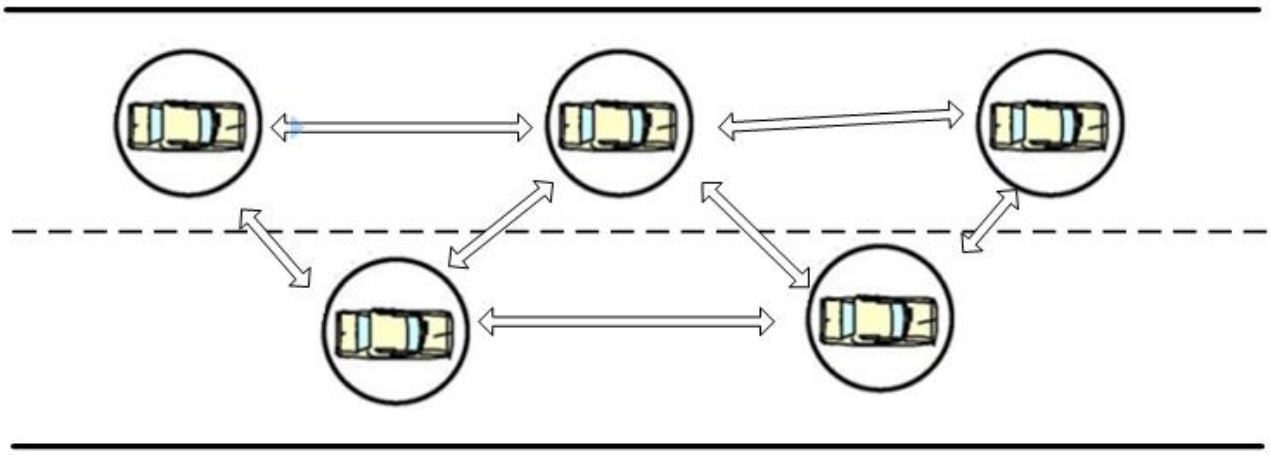


Рисунок 1.4 – Приклад взаємодії пристроїв у системі DSRC

В рамках дослідження [11] проведено порівняльний аналіз технологій LTE (Long-Term Evolution) та DSRC у транспортній мережі міста. На рис. 1.5 наведено графік залежності відсотку втрачених пакетів при передавання даних від швидкості руху транспортного засобу для технологій DSRC та LTE.

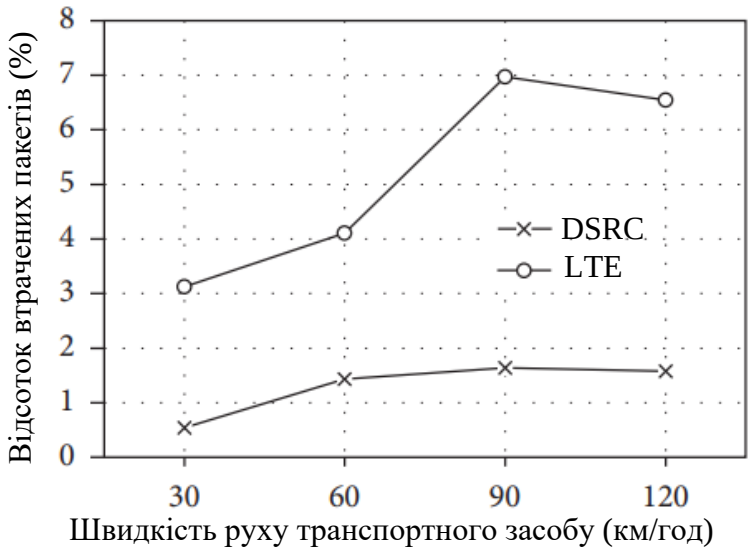


Рисунок 1.5 – Графік залежності відсотку втрачених пакетів від швидкості руху транспортного засобу

На рис. 1.6 наведено графік залежності пропускної здатності каналу передавання даних від швидкості руху транспортного засобу.

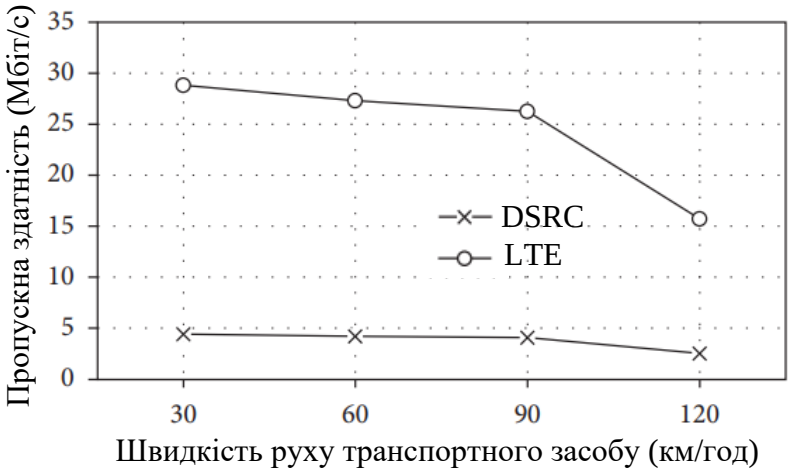


Рисунок 1.6 – Графік залежності пропускної здатності каналу передавання даних від швидкості руху транспортного засобу

На рис. 1.7 наведено графік залежності середньої затримки при передаванні пакетів даних від швидкості руху транспортного засобу.

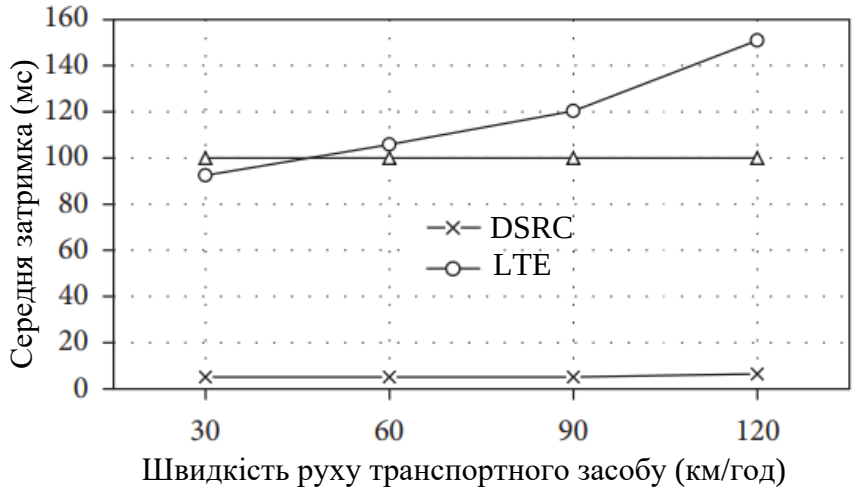


Рисунок 1.7 – Графік залежності середньої затримки при передаванні пакетів даних від швидкості руху транспортного засобу

Як випливає з рис. 1.6 технологія LTE має кращі показники пропускної здатності каналу, проте технологія DSRC має менший відсоток втрачених пакетів при збільшенні руху транспортного засобу (рис. 1.5) та менші показники затримки у передаванні пакетів (рис. 1.7) при збільшенні руху транспортного засобу. Можна зробити висновок, що технологію DSRC краще використовувати при побудові системи для упередження зіткнень транспортних засобів та систем безпеки транспортної мережі міста.

Системи, що використовують технологію DSRC, забезпечують надійний зв'язок для транспортних засобів, але мають доволі дорогі пристрої. Також цю технологію буде доволі важко інтегрувати у транспортну систему, оскільки під дорожні пристрої потрібно буде провести окрему кабельну систему. Звісно, можна використовувати оптичну або Ethernet мережу від придорожніх камер, проте місце встановлення дорожніх пристроїв DSRC не завжди буде співпадати з місцем встановлення придорожніх камер. Ще одним недоліком даної технології є низька відмово стійкість. Якщо не буде встановлено DSRC пристрою на транспортному засобі, або у разі виходу зі строю пристрою на одному з транспортних засобів, він стає невидимим для інших транспортних засобів, що може привезти до виникнення аварійного випадку.

Технологія RFID (Radio Frequency Identification), або радіочастотна ідентифікація, позбавлена деяких недоліків технології DSRC. Для пристроїв RFID не треба проводити окрему кабельну систему, що спрощує її інтеграцію у транспортну систему міста. Радіочастотна ідентифікація працює за принципом ідентифікації об'єктів шляхом обробки радіосигналів, де за допомогою транспондера (зчитувача) зчитуються дані з RFID-міток. Системи RFID складаються з: транспондера, мітки та системи обробки даних. Всередині міток міститься електронна інформація у вигляді коду, за допомогою якого проводиться ідентифікація об’єкту. RFID-мітки бувають двох типів:

- пасивні (живляться від електромагнітного поля, що випромінює транспондер);
- активні (мають вбудовану акумуляторну батарею).

Принцип роботи технології RFID з пасивними мітками полягає в наступному: антена транспондера створює електромагнітні хвилі, які активують пасивну RFID-мітку. Живлення, що формується в результаті дії електромагнітних хвиль, достатньо для активації передавача антени, що передає дані від пасивної мітки до транспондера. Мітка відправляє свої дані транспондера, який здійснює демодуляцію отриманого сигналу, розшифровує його і передає системі обробки даних для подальшого аналізу. Принцип роботи технології RFID з пасивною міткою наведено на рис. 1.8. Принцип роботи технології RFID з активною міткою відрізняється тим, що транспондер не створює електромагнітного поля, оскільки активна мітка має вбудоване джерело живлення.

RFID-мітки мають різні робочі частотні діапазони. Порівняльна характеристика RFID-міток по різним діапазонам частот наведена у табл. 1.3.

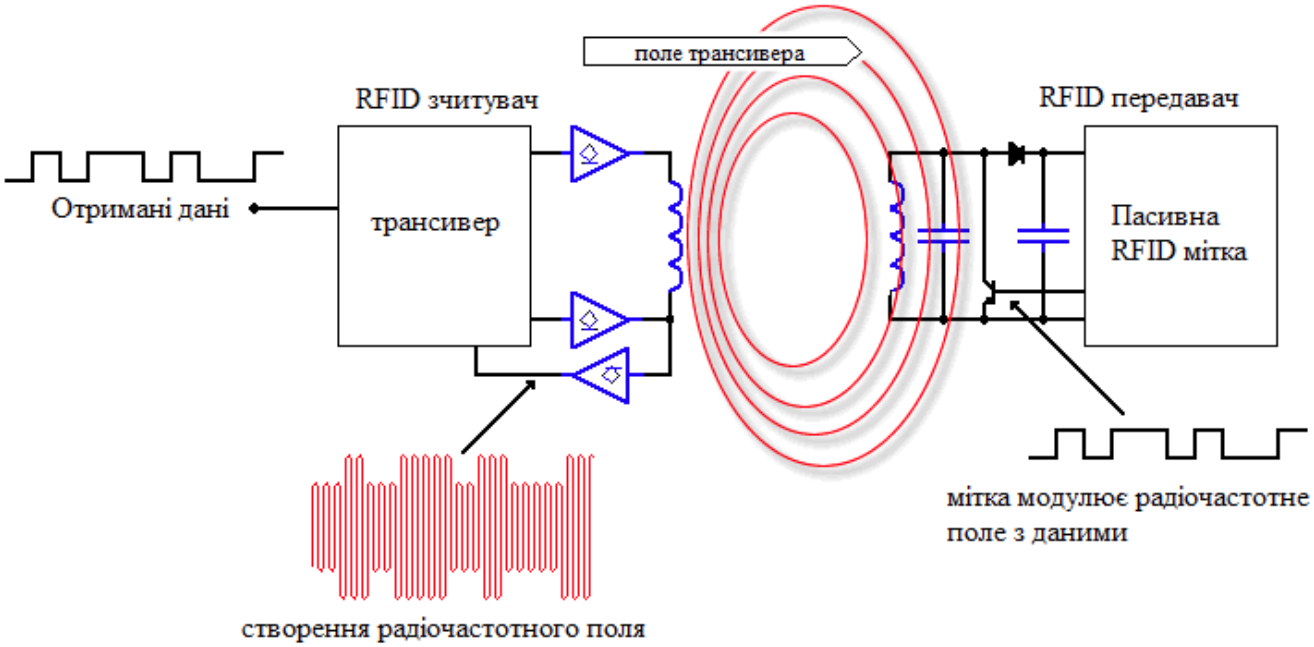


Рисунок 1.8 – Принцип роботи технології RFID

Таблиця 1.3 – Порівняльна характеристика частотних діапазонів RFID-міток [12]

Частоти	Низькочастотні (НЧ)	Високочастотні (ВЧ)	Надвисокочастотні (НВЧ)	Мікрохвильові (МЧ)
	125, 134…135 кГц	13.56 МГц	902…908 МГц (США), 865…868 МГц (Європа), 908.5…914 МГц (Корея)	2.4 ГГц
Радіус дії	до 1 м	до 1.5 м	3..8 м	до 10 м
Швидкість передавання даних	~ 1 кбіт/с	до 25 кбіт/с	до 30 кбіт/с	до 100 кбіт/с
Принцип дії	Індуктивний зв’язок		Електромагнітний зв’язок (зворотне розсіювання)	
Живлення	Пасивне		Пасивне та активне	
Розмір мітки	Великий	Середній	Маленький	Маленький
Стандарти ISO	14223, 11784/5, 18000-2	15693, 14443, 18000-3	10374, 18000-6	10374, 18000- 4, 18000- 5
EPC стандарти	–	Class 1, Gen 1 (HF)	Class 0 (Gen 1), Class 1 (Gen 1), UHF Class 2 (Gen 2)	–

Як випливає з табл. 1.3, краще використовувати мітки з надвисокочастотного та мікрохвильового частотних діапазонів для побудови системи ідентифікації

транспортних засобів, оскільки мітки саме цих діапазонів мають відносно велику дальність дії.

Технологія RFID в основному застосовується для контролю переміщення, контролю доступу для регулювання безпеки та обліку товару або предметів. Застосування технології RFID у транспортній мережі буде обмеженим, оскільки швидкість обміну інформацією між транспондером і міткою буде поступатися технологіям сімейства 802.11, проте її можна використовувати для ідентифікації транспортних засобів та дорожніх знаків.

Технологія RFID, використовуючи пасивні мітки, забезпечує зв'язок лише в обмеженій зоні, тому RFID-мітки, що інтегровані у дорожню інфраструктуру, можуть надавати інформацію у визначених зонах, і за допомогою цього можна дуже точно ідентифікувати місцезнаходження транспортного засобу. Електромагнітні пасивні RFID-мітки не потребують джерела живлення, мають високу стійкість до пилу та перешкод і дуже малий розмір. RFID-мітки дуже дешеві, тому їх можна встановлювати у великій кількості, задля підвищення завадостійкості системи. Таким чином, RFID-мітки позбавлені недоліків, що пов'язані з вартістю пристроїв і рівнем обслуговування технології DSRC.

Задля підвищення безпеки руху транспортних засобів можна інтегрувати системи DSRC та RFID у транспортну мережу, проте пішоходи залишаються "невидимими" для цих систем. Модуль технології DSRC не інтегрований у сучасні смартфони, що є в наявності у кожного пішохода, а інтегровані модулі Bluetooth та NFC мають невелику дальність дії. З усіх існуючих технологій, що інтегровані у сучасні смартфони, технологія Wi-Fi задовольняє більшість вимог до технології, що може бути інтегрована у транспортну мережу міста.

Технологія Wi-Fi належить до стандарту IEEE 802.11. Порівняльна таблиця стандартів технології Wi-Fi наведена у табл. 1.4.

Таблиця 1.4 – Порівняльна таблиця стандартів Wi-Fi

Стандарти	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad	802.11ah	802.11ax
Робочі частоти, ГГц	5	2.4	2.4	2.4 / 5	2.4 / 5	60	0,9	2.4 / 5
Максимальна пропускна здатність, Мбіт/с	54	11	54	до 600	до 1300	до 6700	347	до 10000

1. Стандарт 802.11a був одним з перших стандартів, випущених під назвою 802.11 у 1999 році. Пристрої цього стандарту працюють на частоті 5 ГГц. Щоб досягти більшої швидкості, у стандарті застосовано технологію ортогонального частотного мультиплексування або OFDM (Orthogonal frequency-division multiplexing) – це метод цифрової модуляції, який використовується для кодування даних на декількох частотах. Завдяки цьому пристрої цього стандарту можуть досягти максимальної пропускної здатності у 54 Мбіт/с.

2. Стандарт 802.11b використовує метод прямої послідовності для розширення спектру або DSSS (Direct-Sequence Spread Spectrum) – це метод модуляції, який використовується для зменшення перешкод сигналу в діапазоні 2.4 ГГц, завдяки цьому сигнал від пристроїв краще проникає крізь перешкоди, забезпечуючи більшу зону покриття WiFi. Проте, в діапазоні 2.4 ГГц багато завад у каналі передавання даних, що спричинені пристроями, які працюють на тій самій частоті (мікрохвильові печі, бездротові телефони, електроприлади та Bluetooth-пристрої). Максимальна пропускна здатність пристроїв стандарту 802.11b – до 11 Мбіт/с.

3. Стандарт 802.11g має максимальну пропускну здатність мережі до 54 Мбіт/с і працює в діапазоні 2.4 ГГц. Стандарт 802.11g є зворотно сумісним з пристроями стандарту 802.11b.

4. Стандарт 802.11n використовує технологію MIMO (Multiple-Input Multiple-Output). Продукти MIMO використовують декілька антен для отримання більшої

кількості даних з одного пристрою за один раз, що призводить до збільшення пропускної здатності каналу. Пристрої стандарту 802.11n можуть працювати одразу на двох радіочастотах – 2.4 ГГц та 5 ГГц. Використання обох частот робить стандарт 802.11n сумісним з пристроями 802.11a/b/g. Пропускна здатність – до 600 Мбіт/с. Пристрої цього стандарту мають теоретичний радіус дії у 70 м.

5. Стандарт 802.11ac. Пристрої стандарту 802.11ac мають пропускну здатність у 1300 Мбіт/с у частоті 5 ГГц та до 450 Мбіт/с на частоті 2,4 ГГц. У цьому стандарті застосовано технологію Downlink Multi-User MIMO. Завдяки цьому стало можливим передавати інформацію на кілька пристроїв одночасно, підвищуючи швидкість передавання даних і зменшуючи затримки. Пристрої стандарту 802.11ac сумісні з пристроями 802.11a/b/g/n.

6. Стандарт 802.11ad розроблений для забезпечення швидкісної безпроводової системи або MGWS (Multiple Gigabit Wireless Systems). Пристрої цього стандарту мають високу пропускну здатність – до 6.7 Гбіт/с. Робоча частота стандарту – 60 ГГц, через що радіус дії даного стандарту не перевищував відстань у 9 м.

7. Стандарт 802.11ah спрямований на використання неліцензованих частотних діапазонів нижче 1 ГГц. Метою створення цього стандарту було знизити енергоспоживання і створити бездротові мережі розширеного радіусу дії. Пристрої цього стандарту працюють у діапазоні 900 МГц. Теоретичний радіус дії пристроїв цього стандарту – 543 м у приміщенні, пропускна здатність каналу передавання даних – до 347 Мбіт/с.

8. Стандарт 802.11ax працює з технологіями OFDMA (Orthogonal Frequency Division Multiple Access), MU-MIMO (Multi-User Multiple-Input Multiple-Output technology) та 1024-QAM (Quadrature Amplitude Modulation). Теоретична максимальна пропускна здатність – до 10 Гбіт/с. Пристрої цього стандарту працюють в діапазонах 2,4 і 5 ГГц, завдяки цьому пристрої стандарту 802.11ax сумісні з пристроями стандартів 802.11a/b/g/n/ac.

Згідно характеристик підстандартів IEEE 802.11, для побудови транспортної мережі необхідно використовувати пристрої стандартів 802.11ac.

Пристрої стандарту мають оптимальні параметри пропускної здатності каналу та дальності дії, можуть працювати у двох різних діапазонах (2.4 ГГц та 5 ГГц) та на відміну від стандарту 802.11ax, усі сучасні смартфони мають Wi-Fi модулі, що підтримують цей стандарт зв’язку.

1.3 Безпека передавання даних в IoT

Системи RFID, як і інші бездротові технології, несуть ряд ризиків для безпеки та конфіденційності користувачів – як споживачів, так і виробників. Конфіденційність – це багатовимірне питання, що включає в себе багато аспектів, таких як політика, безпека і правоохоронні органи. Ідеальна секретність – це лише математична концепція; в реальності завжди буде присутній людський фактор, який важко піддається кількісній оцінці в будь-якій математичній формулі. Таким чином, практично неможливо мати ідеально захищену систему. RFID система може піддатися наступним видам атак:

1. Глушіння сигналу. Це означає навмисну спробу порушити безпроводовий інтерфейс між зчитувачем і міткою, і тим самим атакувати цілісність або доступність зв'язку. Цього можна досягти за допомогою потужних передавачів на великій відстані, а також за допомогою більш пасивних засобів, таких як екранування.

2. Прослуховування сигналу. Прослуховування відбувається, коли зловмисник перехоплює дані за допомогою сумісного зчитувача, в той час, коли мітка зчитується авторизованим RFID-зчитувачем. Оскільки більшість RFID-систем використовують відкритий текстовий зв'язок, через обмежений обсяг пам'яті мітки або її вартість, підслуховування є простим, але ефективним засобом для зловмисника отримати інформацію про зібрані дані мітки.

3. Повторна атака. У разі повторної атаки зловмисник повторює ту саму послідовність автентифікації, що була надана уповноваженою особою. Атака повторення може бути здійснена за допомогою клону легітимної мітки або шляхом повторної відправки прослуханого сигналу з комп'ютера, який оснащений

відповідною картою та антеною. Для того, щоб здійснити атаку, зловмиснику необхідно отримати певну інформацію, яка надсилається міткою під час звичайної комунікації [13].

4. Спуфінг. У спуфінг-атаці зловмисник маскується під легітимного користувача системи. Зловмисник може видавати себе за авторизованого користувача служби іменування об'єктів або користувача бази даних. Якщо зловмисник може успішно отримати доступ до системи з підробленими обліковими даними, він може робити з даними RIFD все, що завгодно, наприклад, відповідати на недійсні запити, змінювати ідентифікатор RFID, відмовляти в нормальному обслуговуванні або навіть писати шкідливий код в системі.

З цього можна зробити висновок, що RFID система слабо захищена і є ризик злому системи. Тому краще використовувати дану технологію у випадках, коли не треба отримувати від користувача персональних даних. Наприклад дану технологію можна використовувати для додаткового інформування водіїв про дорожні знаки та зміну маршруту руху.

Перший протокол безпеки для версії стандартів WiFi мав назву WEP (Wired Equivalent Privacy) і був включений в стандарт IEEE 802.11. Протокол забезпечує шифрування даних і контроль доступу за допомогою автентифікації. Стандартний 64-бітний ключ WEP – це фактично 40-бітний відкритий ключ у поєднанні з 24-бітовим "вектором ініціалізації" (IV), тоді як 128-бітний ключ базується на 104-бітному відкритому ключі. Довжина ключів, що використовуються в WEP, досить мала, тому значення ключа можна легко знайти методом підбору.

На зміну WEP прийшли дві технології безпеки, відомі як WPA і WPA2. WPA (Wi-Fi Protected Access). Протокол WPA був розроблений для сумісності з обладнанням Wi-Fi, яке забезпечувало достатні можливості для підтримки WEP. Для WPA не існує офіційно затвердженого стандарту IEEE; він знаходиться між стандартом 802.11 для WEP і стандартом 802.11i, який визначає WPA2. WPA підтримує два режими роботи.

Перший – це режим попереднього спільного ключа (WPA-PSK), коли обидві сторони зв'язку повинні знати один і той самий ключ. Спільний ключ надається

адміністратором і повинен бути змінений, як на точці доступу, так і у клієнта. Якщо ключ точки доступу змінено асинхронно, то пристрої, що були під'єднані раніше не зможуть підключитися, що призведе до необхідності звернення до служби підтримки для виправлення ситуації. Це призводить до того, що, як і у випадку з WEP та більшістю протоколів на основі попередньо наданих ключів, від IPSEC (Internet Protocol Security) до PIN-кодів банківських карток, цей ключ не часто змінюється. Ключі можуть надаватися у вигляді шістдесяти чотирьох шістнадцяткових цифр або у вигляді парольної фрази від восьми до шістдесяти трьох символів ASCII (American Standard Code for Information Interchange).

Версія ASCII доповнюється відповідним чином, і обидва варіанти перетворюються на 256-бітний ключ. Протокол WPA також вразливий до атак методом підбору, особливо, якщо обрано слабкий базовий ключ [14].

Протокол WPA2 відноситься до стандарту IEEE 802.11i, включаючи протокол TKIP (Temporal Key Integrity Protocol) та блочний шифр AES (Advanced Encryption Standard). Протокол TKIP забезпечує шифрування кожного пакету, а також перевірку цілісності повідомлень та механізм повторного шифрування. Протокол WPA2 вважається повністю безпечним.

Пристрої системи DSRC використовують протоколи безпеки стандарту IEEE 1609.2, згідно цього стандарту кожен транспортний засіб під час реєстрації отримує багато сертифікатів псевдонімів з парами ключів і використовує їх для підписання повідомлень. Науковці Рая та Юбо запропонували схему захищеного автомобільного зв'язку з використанням сертифікатів на основі PKI (Public Key infrastructure). Згідно цього методу, кожен транспортний засіб попередньо завантажується великою кількістю анонімних пар відкритих/закритих ключів і відповідних сертифікатів відкритих ключів.

Для посилення безпеки кожна пара відкритих/закритих ключів оновлюється з коротким терміном дії, при цьому використовується псевдо ідентифікатор у кожному сертифікаті відкритого ключа. Цей метод вимагає більшого обсягу пам'яті і, як наслідок, додаткових витрат на перевірку, коли сертифікат відкритого ключа потрібно перевіряти для кожного повідомлення. Крім того, складно знайти

справжню ідентифікацію транспортного засобу, оскільки при отриманні фальшивого повідомлення орган влади повинен виконати вичерпний пошук всіх збережених сертифікатів.

Щоб усунути недоліки схеми Райя та Юбо, було запропоновано нову схему CPPA (Conditional Privacy-Preserving Authentication) з використанням анонімних сертифікатів. Згідно цієї схеми транспортний засіб отримує тимчасовий анонімний сертифікат, коли він проїжджає повз придорожній пристрій DSRC. Для забезпечення умов конфіденційності кожен транспортний засіб повинен часто запитувати новий анонімний сертифікат у придорожнього пристрою, оскільки зловмиснику може бути легше відстежити транспортний засіб, якщо його сертифікат використовується протягом тривалого часу.

Однак, підтримувати часту взаємодію з придорожніми пристроями неефективно. Тому схема CPPA не може задовольнити вимогу ефективності каналу в мережах V2X. В рамках дослідження [15] було представлено новий метод автентифікації з умовним збереженням конфіденційності на основі ідентифікатора DACOP (dynamic authentication with conditional privacy-preservation) для мереж V2X, що базується на матричній криптографії. DACOP забезпечує швидкий динамічний алгоритм для анонімної автентифікації V2X-повідомлень, який особливо ефективний для сценаріїв V2V-зв'язку. Метод автентифікації DACOP підвищує рівень безпеки і конфіденційності для комунікацій V2X в інтелектуальних транспортних системах. В рамках дослідження експериментально доведено, що DACOP суттєво зменшує час обробки автентифікації, а отже, суттєво зменшує втрати повідомлень порівняно зі стандартом IEEE1609.2. Таким чином, запропонований метод є ефективним рішенням для швидкої та анонімної автентифікації повідомлень для мереж V2X з підвищеним рівнем безпеки.

1.4 Аналіз використання технології RFID у транспортній мережі міста

Завдяки дорожнім знакам водії отримують нормативну, попереджувальну та вказівну інформацію. Водії транспортних засобів повинні реагувати на динамічну візуальну інформацію (інші транспортні засоби, пішоходи та сигнали світлофора), а також статичну візуальну інформацію (дорожні знаки), і відповідно до отриманої інформації маневрувати транспортним засобом. Однак, дорожні знаки та інша статична візуальна інформація частіше ігнорується під час маневру, ніж динамічна візуальна інформація. У випадку, якщо водій не побачить дорожнього знаку – це може призвести до виникнення аварійного випадку. Очікується, що ефективним рішенням цієї проблеми стануть бортові системи, які здатні відображати знаки на екрані в транспортному засобі.

В рамках наукової роботи [16] було побудовано систему для зчитування даних з дорожніх знаків за допомогою сигналів, що зберігаються в RFID-мітках, які розміщені на дорожньому покритті. За допомогою бортового RFID-зчитувача, який встановлено на транспортному засобі відбувається зчитування даних з дорожніх міток. Отримані дані обробляються бортовим комп'ютером і передаються на бортовий екран у вигляді знаків із дублюванням голосовим повідомленням. Схему з планом дослідження наведено на рис. 1.9.

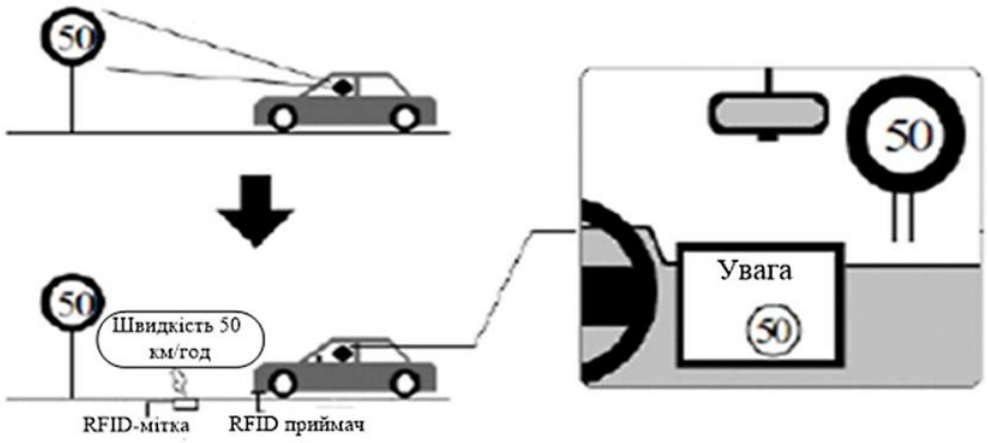


Рисунок 1.9 – Схема плану дослідження зчитування RFID-міток з дорожнього полотна

Якщо інформація відображається на основі даних, збережених лише в одній мітці на смузі, неможливо визначити напрямок руху транспортного засобу. Як наслідок, у випадку, коли транспортний засіб використовує смугу зустрічного руху, щоб об'їхати інший транспортний засіб або об'їхати перешкоду, або коли транспортний засіб рухається прямою нерозділеною дорогою, збираються дані, що зберігаються в мітках на дорожньому покритті смуги зустрічного руху. У отриманні даних з міток дороги зустрічного руху немає необхідності. Тому в цьому дослідженні для перевірки розпізнавання знаків визначено 3 мітки:

- мітка 0 (попередня мітка);
- мітка 1 (стартова мітка);
- мітка 2 (кінцева мітка).

Усі три мітки розташовані послідовно на смузі руху. Схематичне розташування міток на дорозі наведено на рис. 1.10.

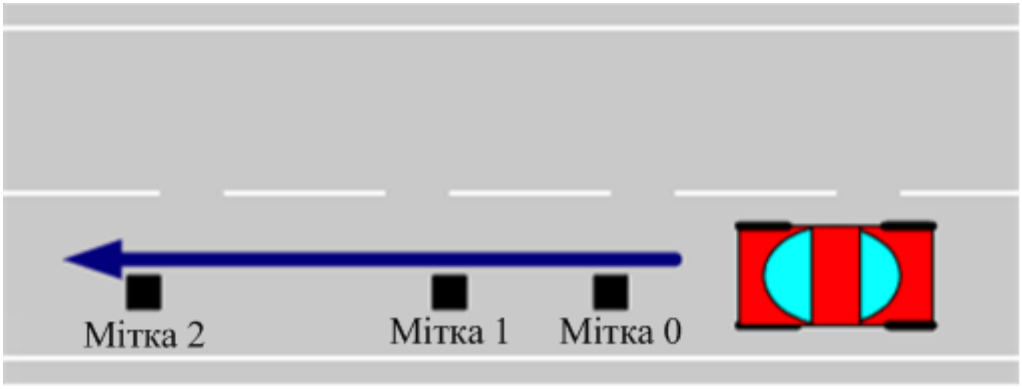


Рисунок 1.10 – Схематичне розташування міток на дорозі

Мітка-0 забезпечує наявність знаку перед смугою руху і виконує роль перевірки напрямку руху транспортного засобу та розпізнаних даних. Дані відображаються за умови, що вони отримані від мітки-0, а потім від мітки-1. Коли дані отримані від мітки-2, відображення даних припиняється. Мітка-1 та мітка-2 позначають початок і кінець ділянки відповідно. Такий підхід робить систему придатною для вузьких нерозділених доріг з двостороннім рухом.

Тип мітки (0, 1 або 2) зберігається в першій цифрі RFID-мітки, за якою слідує ідентифікатор дорожнього знаку, як наведено на рис. 1.11. Числові дані, такі як обмеження швидкості та обмеження ваги, зберігаються у наступних цифрах, якщо такі є. Дані дорожніх знаків зберігаються у 32-бітних блоках. Мітка, що використовувалася в дослідженні, може вмістити максимум 64 дорожні знаки на одну мітку. Однак у тесті в кожній мітці зберігалися дані максимум про чотири дорожні знаки, щоб скоротити час, необхідний для зчитування даних.

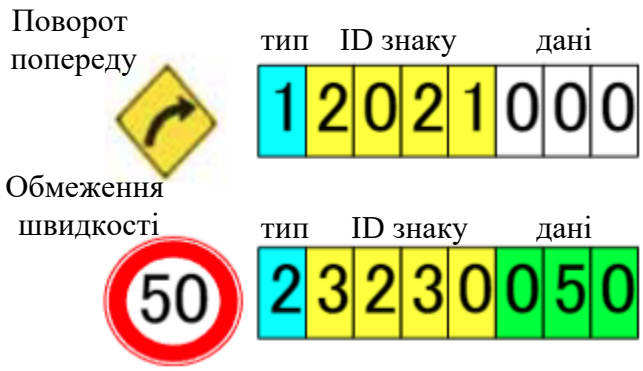


Рисунок 1.11 – Формат зберігання даних у мітці

В результаті польових і лабораторних випробувань в рамках цього дослідження система бортових знаків з використанням RFID-міток в якості цифрових дорожніх знаків була визнана високоефективною, а зображення і голосові дані, що передаються в транспортному засобі, виявилися легкими для сприйняття. В рамках дослідження встановлені мітки були захищені акриловими пластинами та були прикріплені безпосередньо до дорожнього покриття. Немає даних, чи можливе зчитування міток при інтегруванні в асфальтне покриття, оскільки збільшиться загасання сигналу. Також в рамках цієї наукової роботи не розглянуто побудову даної системи на основі активних RFID-міток.

В рамках дослідження [17] було запропоновано 2 додатки для зчитування дорожніх RFID-міток:

- Traffic Sign Manager (менеджер дорожніх знаків) – для управління RFID-мітками;

- Traffic Sign Reader (зчитувач дорожніх знаків) – для управління RFID-зчитувачем.

Архітектура системи розпізнавання дорожніх знаків наведено на рис. 1.12.

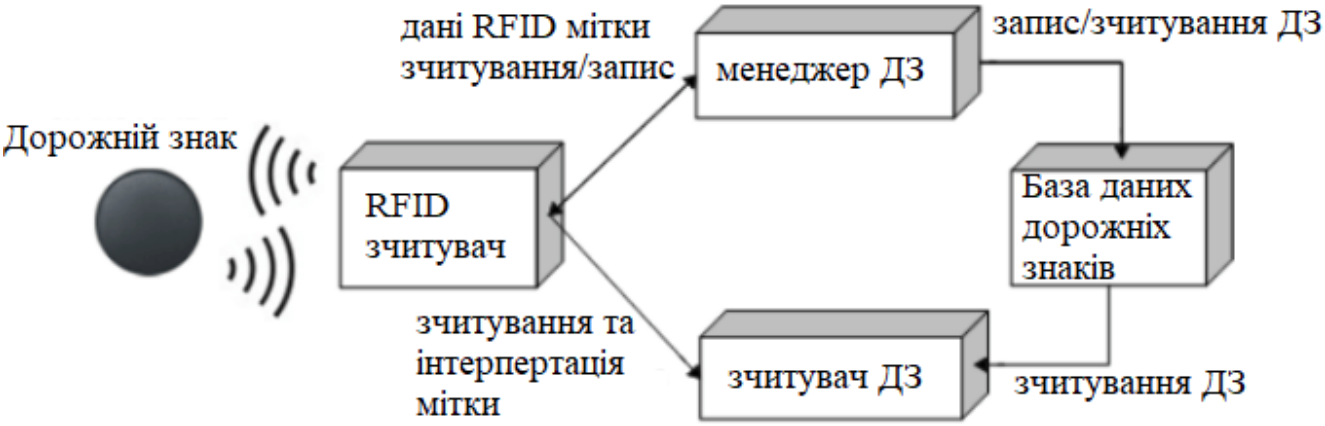


Рисунок 1.12 – Архітектура системи розпізнавання дорожніх знаків

Менеджер дорожніх знаків – дозволяє додавати нові знаки, видаляти існуючі та змінювати пов'язані з ними метадані. Інтерфейс програми "менеджер дорожніх знаків" наведено на рис. 1.13.

Рисунок 1.13 – Інтерфейс програми "менеджер дорожніх знаків"

Зчитувач дорожніх знаків – завданням цієї програми є виявлення міток, розташованих в зоні дії зчитувача, зчитування збережених даних та їх відповідна інтерпретація. Інтерфейс програми для зчитування дорожніх знаків наведено на рис. 1.14.

Рисунок 1.14 – Інтерфейс програми "зчитувач дорожніх знаків"

Програма пропонує додаткові функції:

1. Групування знаків (за категоріями: заборонні, обов'язкові, попереджувальні, інформаційні). Це вводить певну конвенцію, яка дозволяє користувачеві швидко перевірити категорію, яку він шукає, замість того, щоб шукати певний знак у всьому робочому просторі програми. Також є можливість вибрати кількість відображуваних знаків категорії і шукати знаки обраного типу, якщо їх більше, ніж вказано в налаштуваннях.

2. Вмикати (вимикати) звук – у разі зчитування знаку, який ще не відображався, вмикається (або не вмикається) звукове сповіщення. Це має на меті підвищити безпеку та комфорт користування додатком і зменшити необхідність підтримувати зоровий контакт з пристроєм, на якому запущено додаток.

Категоризація дорожніх знаків – відображення лише знаків із заданого користувачем набору. На вибір є три попередньо визначені набори: легковий, вантажний, інший. Завдяки цьому на екрані відображаються лише знаки з обраної

колекції. Це дозволяє оптимізувати розмір необхідного робочого простору та мінімізувати кількість непотрібної для користувача інформації.

У рамках цієї статті було представлено 2 різні додатки для обробки RFID-міток для дорожніх знаків, проте немає інформації стосовно роботи системи RFID при завантаженому дорожньому трафіку.

В рамках дослідження [18] було розглянуто IoT-систему для покращення локалізації транспортних засобів на основі технологій RFID, GPS та DSRC. GPS з підтримкою RFID (RF-GPS) підвищує точність координат транспортних засобів з GPS системами завдяки використанню "еталонних" транспортних засобів на дорозі. На відміну від традиційної системи GPS, яка використовує фіксовану точку відліку, у системі RF-GPS транспортний засіб з GPS тимчасово стає рухомою точкою відліку. На рис. 1.12 наведено принцип роботи даної системи.

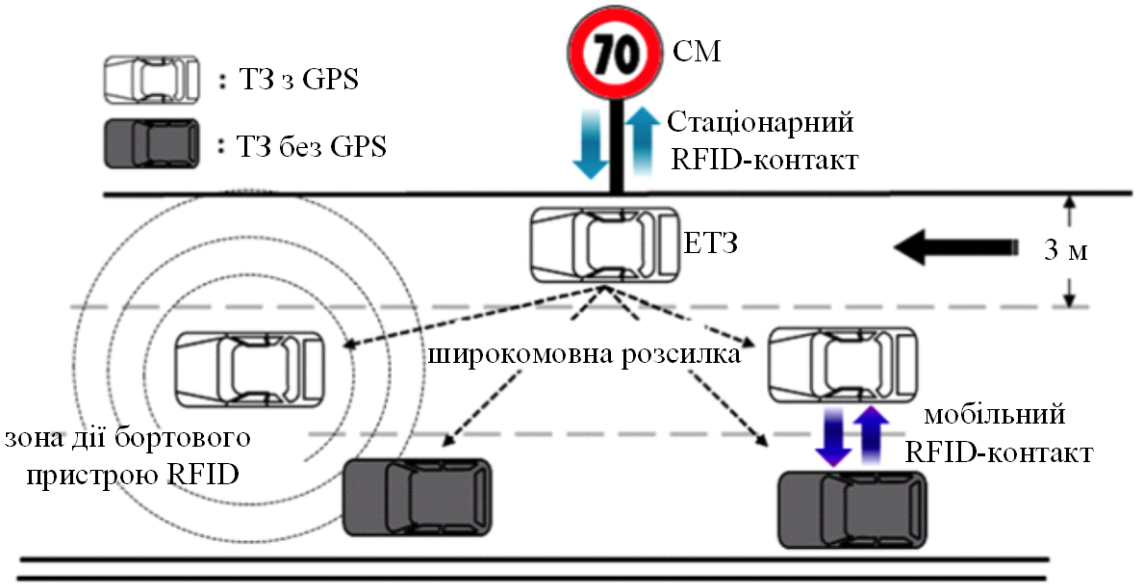


Рисунок 1.15 – Принцип роботи системи локалізації транспортних засобів на основі технологій RFID, GPS та DSRC

Принцип роботи системи локалізації транспортних засобів на основі технологій RFID, GPS та DSRC:

1. Проїжджаючи повз стаціонарну RFID-мітку, транспортний засіб отримує координати від даної мітки та обчислює значення похибки GPS, використовуючи

свої власні координати GPS. Після цього транспортний засіб передає значення помилки GPS (координати різниці) сусідам, щоб допомогти їм скоригувати свої GPS-координати.

2. Стаціонарний RFID-контакт. Стаціонарні RFID-мітки, які зберігають в пам'яті координати абсцис, встановлюються на придорожніх пристроях. Коли транспортний засіб без GPS-системи (ТЗ без GPS на рис. 1.15) потрапляє в радіус дії стаціонарної мітки (СМ на рис. 1.15), мобільний RFID-зчитувач на транспортному засобі отримує координати від СМ за допомогою RFID-зв'язку. Через малий радіус дії радіочастотного зв'язку, тільки ті транспортні засоби, які рухаються по смузі, найближчій до роздільника (або до узбіччя), можуть зчитувати координати від СМ. Якщо транспортний засіб має систему GPS, то він обчислює координати різниці шляхом віднімання власних координат GPS, від координат, які були отримані від СМ. Після цього транспортний засіб стає "еталонним" транспортним засобом (ЕТЗ на рис. 1.15). Автомобіль без GPS не може бути "еталонним", оскільки він не має GPS-координат.

3. Широкомовна розсилка (broadcasting). "Еталонний" транспортний засіб ЕТЗ передає координати різниці сусідам за допомогою технології DSRC (802.11p). Оскільки транспортні засоби в радіусі дії радіозв'язку, з великою ймовірністю мають однакову похибку GPS, сусідній автомобіль з GPS може обчислити свої точні координати, використовуючи отримані координати різниці. Цей транспортний засіб не повторює передачу координат різниці, а також не пересилає їх сусіднім транспортним засобам. Якщо "еталонний" транспортний засіб отримує інформацію від іншого "еталонного" транспортного засобу, він не передає координати різниці протягом короткого інтервалу часу, навіть якщо він отримує координати від стаціонарної RFID-мітки. В рамках наукової статті даний механізм обробки даних називається "обмеженням трансляції". Автомобілі без GPS (ТЗ без GPS) в межах діапазону не можуть обчислювати точні координати, оскільки вони не мають власних GPS-координат.

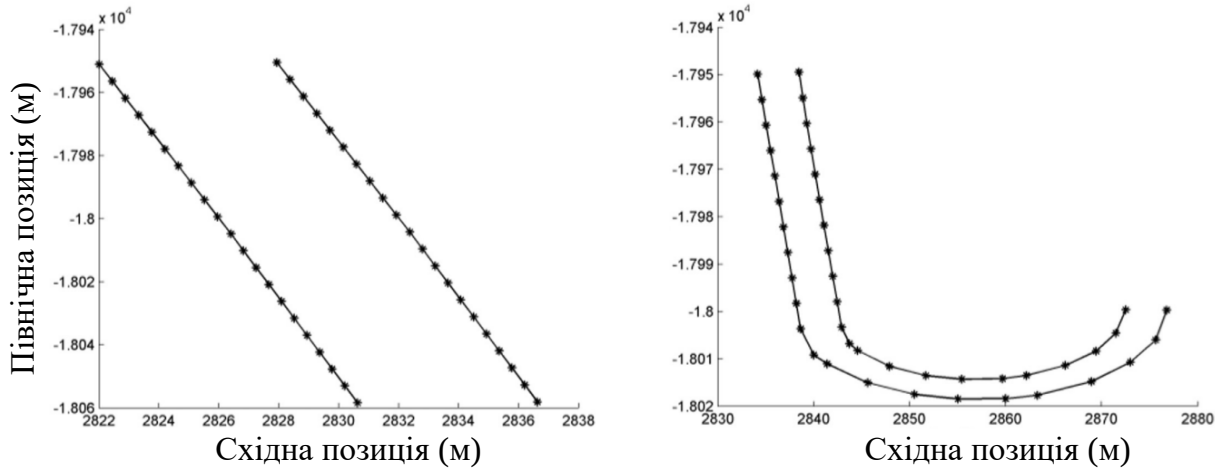
4. Мобільний RFID-контакт. Коли транспортний засіб без GPS (ТЗ без GPS) проїжджає повз транспортний засіб з GPS (ТЗ з GPS), ТЗ без GPS зчитує

ідентифікатор ТЗ з GPS, через мобільний RFID-контакт і мобільний RFID-зчитувач на ТЗ без GPS отримує доступ до мобільної RFID-мітки на ТЗ з GPS. Для подальших розрахунків ТЗ без GPS записує контактну інформацію мобільної RFID-мітки, наприклад, ідентифікатор транспортного засобу і час контакту, а потім обидва транспортні засоби встановлюють однорангове з'єднання через технологію 802.11p.

Результати симуляцій в рамках дослідження [18] на базі QualNet показали продуктивність запропонованої RF-GPS системи. Проте, як і в науковій роботі [16] дослідження проводилося лише за допомогою пасивних RFID міток, саме тому, дальність дій стаціонарної мітки була обмежена лише однією смугою руху.

Результати перевірки роботи технології RFID та GPS на логістичних підприємствах [19] показали, що завдяки системі RFID-GPS можна значно спростити ідентифікацію транспортного засобу і відслідковування маршруту його руху.

Для відслідковування переміщення транспортних засобів у тунелях було запропоновано в роботі [20] інтегрувати технологію RFID у транспортні засоби. Для досягнення визначення координат транспортного засобу запропоновано два алгоритму. Розроблено алгоритм LSSVM (Least Square Support Vector Machine) для отримання відстані між RFID-міткою та зчитувачем на основі сили прийнятого сигналу (RSS – Received Signal Strength), а також алгоритм LMM (LSSVM Multiple Model) для реалізації глобального об’єднання пристроїв. Алгоритм LMM призначений для об'єднання декількох джерел спостереження з різною частотою дискретизації для досягнення кращої продуктивності. Для проведення тестування протоколів LSSVM та LMM було побудовано схему з місцем розташування RFID міток вздовж тунелю На рис. 1.16 наведена схема розташування RFID-міток вздовж прямого тунелю (а) та тунелю з кривизною (б).



а) *б)*

Рисунок 1.16 – Схема розташування RFID-міток вздовж прямого тунелю (а) та тунелю з кривизною (б)

На рис. 1.17 наведено результат тестування визначення місцезнаходження автомобілю у тунелі за допомогою протоколу LMM.

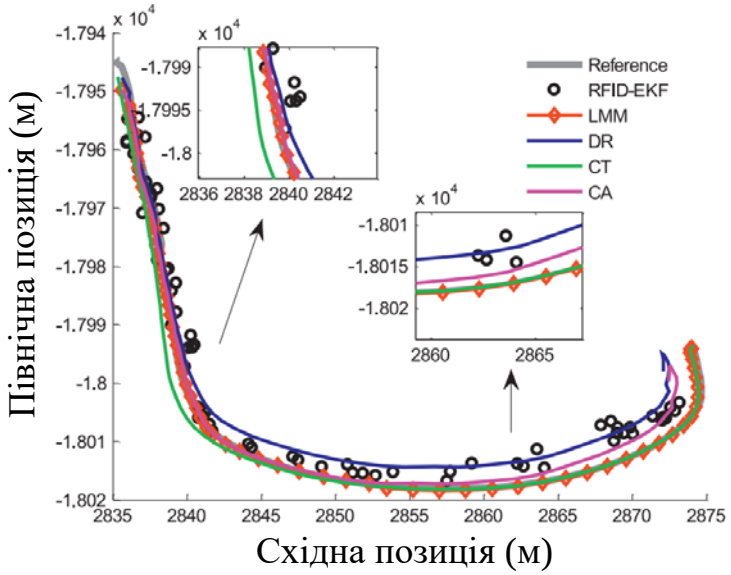


Рисунок 1.17 – Результат тестування визначення місцезнаходження автомобілю у тунелі за допомогою протоколу LMM

Як випливає з рис. 1.17, практичним шляхом доведена ефективність протоколу LMM, проте в рамках дослідження [20] не було перевірено роботу RFID-

міток при щільному потоці транспортних засобів та для більше ніж двох полос руху в один бік.

В рамках статті [21] представлено підхід до локалізації та навігації на основі RFID-міток для автоматизованого керованого транспортного засобу. Підхід базується на антенній решітці Дольфа-Чебишева. Антенна решітка Дольфа-Чебишева використовується для ефективного усунення помилок відбиття у вертикальному напрямку. В рамках статті не було проведено аналізу розповсюдження сигналу від різних типів RFID-міток та в умовах інтенсивного трафіку на дорозі.

У дослідженні [22] продемонстровано ідентифікацію об’єкту з RFID-зчитувачем на основі мультілатерації. Мультілатерація – це процес, який визначає місцезнаходження цілі на основі оцінки відстаней від декількох опорних точок в яких встановлено RFID-мітки. У запропонованій системі локалізації на основі RFID позиція об’єкту зі зчитувачем визначається на основі оцінки відстаней між кількома мітками і зчитувачем з використанням значень рівня сигналу, зібраних зчитувачем RFID, що встановлений на об’єкті, що пересувається. Кожна оцінена відстань представлена колом навколо фіксованої асоційованої мітки. Перетин різних кіл забезпечує спільну точку або зону покриття прийнятих сигналів, як показано на рис. 1.18.

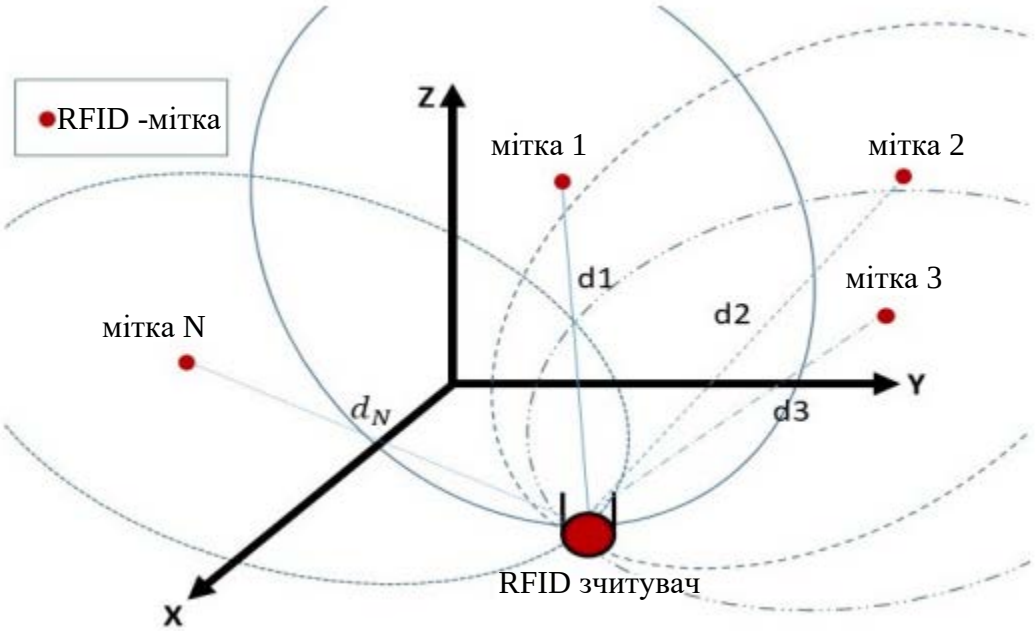


Рисунок 1.18 – Визначення місцезнаходження об’єкту на основі методу мультілатерації

У роботі [23] розглянуто протоколи захисту системи від колізій. На рис. 1.19 наведені можливі варіанти колізій у системі RFID.

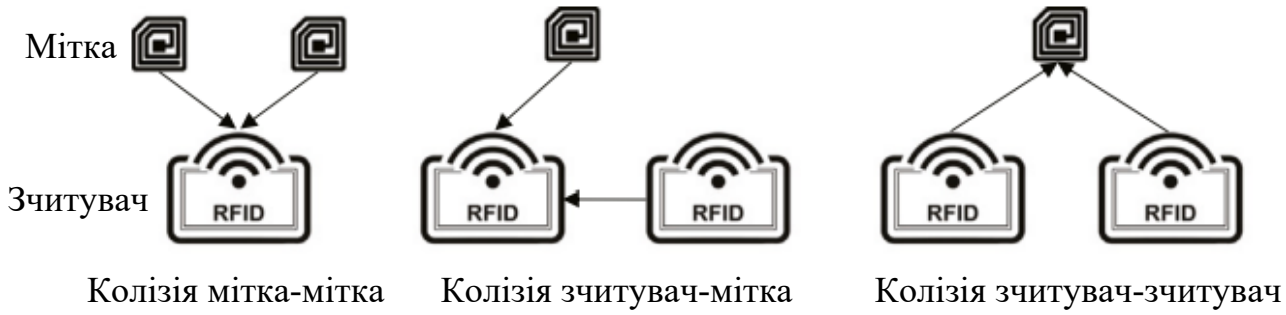


Рисунок 1.19 – Варіанти можливих колізій у системі RFID

Варіанти можливих колізій у системі RFID:

1. Колізія мітка-мітка (виникає, коли один зчитувач намагається зчитати дані одразу з декількох міток).

2. Колізія зчитувач-мітка (виникає, коли декілька зчитувачів намагаються зчитати дані з однієї мітки. В цьому випадку запит на зчитування від одного зчитувача заважає сигналу-відповіді від мітки).

3. Колізія зчитувач-зчитувач (виникає, коли декілька зчитувачів намагаються зчитати дані з однієї мітки. В цьому випадку сигнали від зчитувачів заважають один одному при їх прийомі на мітці).

Для зменшення колізій між тегами створено алгоритми на основі "Aloha" та алгоритми на основі "дерев". Основна ідея алгоритмів на основі ALOHA полягає в тому, що тег чекає протягом випадкового періоду часу, а потім повторно передає дані, коли виявлено колізії тегів. Алгоритм використовує політику розбиття кадру, за допомогою якої зчитувач може ефективно використовувати статистику каналу для визначення оптимального розміру кадру для усунення колізій. Оскільки алгоритми на основі ALOHA випадковим чином планують передачу даних, деякі

теги не можуть бути ідентифіковані протягом тривалого часу, що призводить до проблем зчитування мобільних міток.

Для вирішення цієї проблеми розроблено алгоритми на основі дерев. Принцип роботи деревовидних алгоритмів полягає в рекурсивному розбитті тегів на менші підмножини до тих пір, поки в кожній підмножині не залишиться тільки один або нуль тегів. QAS (Q Ary Search) – це алгоритм квадратичного пошуку, який зменшує цикл колізій за рахунок використання механізму бітового кодування ідентифікатора мітки.

В рамках дослідження [23] також експериментально перевірено, що вірогідність зчитування RFID-мітки при швидкості руху транспортного засобу близько 10 км/год складає майже 100%, і падає до 85% при швидкості транспортного засобу близько 60 км/год. Графік залежності відсотку зчитування мітки від швидкості транспортного засобу наведено на рис. 1.20.

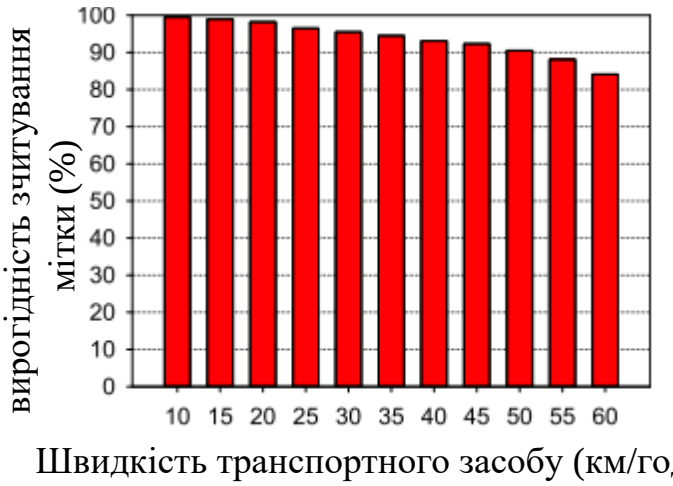


Рисунок 1.20 – Графік залежності відсотку зчитування мітки від швидкості транспортного засобу

У роботі [24] представлено концептуальну модель упередження зіткнень транспортних засобів на основі технології RFID (рис. 1.21). Згідно цієї моделі, кожен транспортний засіб має RFID-зчитувач, який закріплено в його задній частині, та RFID-мітку з унікальним ідентифікатором, яка прикріплена в передній частині транспортного засобу. Також всередині кожного транспортного засобу

розташований блок "Particle Electron" який з’єднується з хмарними сервісами ("хмара" на рис. 1.21) та з пристроєм сповіщення водія про небезпеку.

В разі, якщо RFID-зчитувач, що встановлений на транспортному засобі №1 (1 на рис. 1.21) зможе ідентифікувати RFID-мітку, що встановлена на транспортному засобі №2 (2 на рис. 1.21), це означає, що дистанція між транспортними засобами скоротилася до небезпечної і транспортний засіб №2 отримає оповіщення про небезпеку зіткнення. У разі виникнення повторного випадку скорочення дистанції між транспортними засобами, автомобільний номер транспортного засобу №2 буде відправлено до контролюючих органів, які в свою чергу зможуть застосувати дисциплінарні стягнення до власника транспортного засобу.

Недоліками даної моделі є використання технології RFID, оскільки ідентифікація транспортних засобів буде проходити на дуже короткій відстані і унеможливить використання даної моделі на широкосмугових ділянках руху, оскільки транспортні засоби з сусідніх смуг руху будуть також потрапляти у зону дії зчитувача.

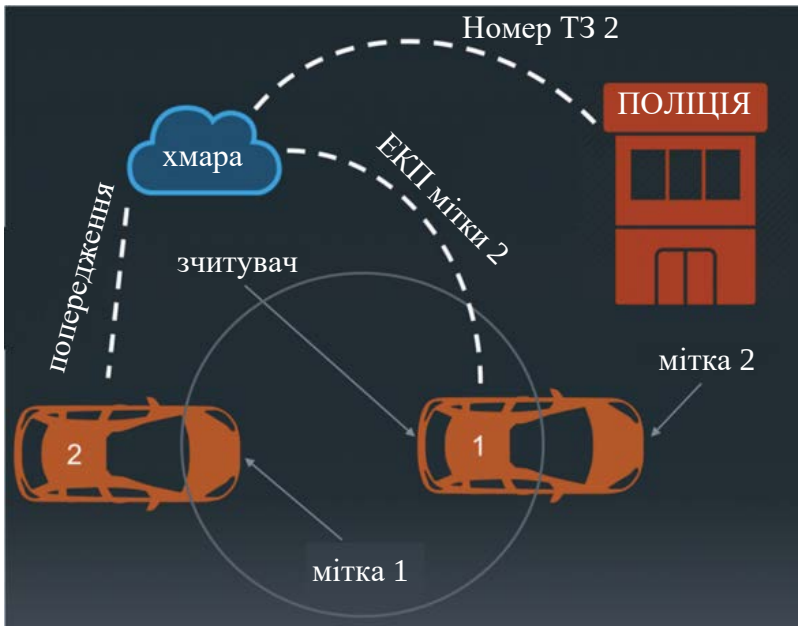


Рисунок 1.21 – Концептуальна модель упередження зіткнень транспортних засобів на основі технології RFID

1.5 Аналіз використання технології DSRC при побудові транспортної мережі міста

Згідно з принципом роботи системи DSRC, кожен транспортний засіб, що обладнаний пристроєм DSRC, надсилає в ефір броадкаст-повідомлення, в якому міститься інформація про його координати, швидкість та напрямок руху. Завдяки цьому можна повідомляти транспортні засоби, що знаходяться поза зоною видимості водія [25]. Приклад наведено на рис. 1.22.

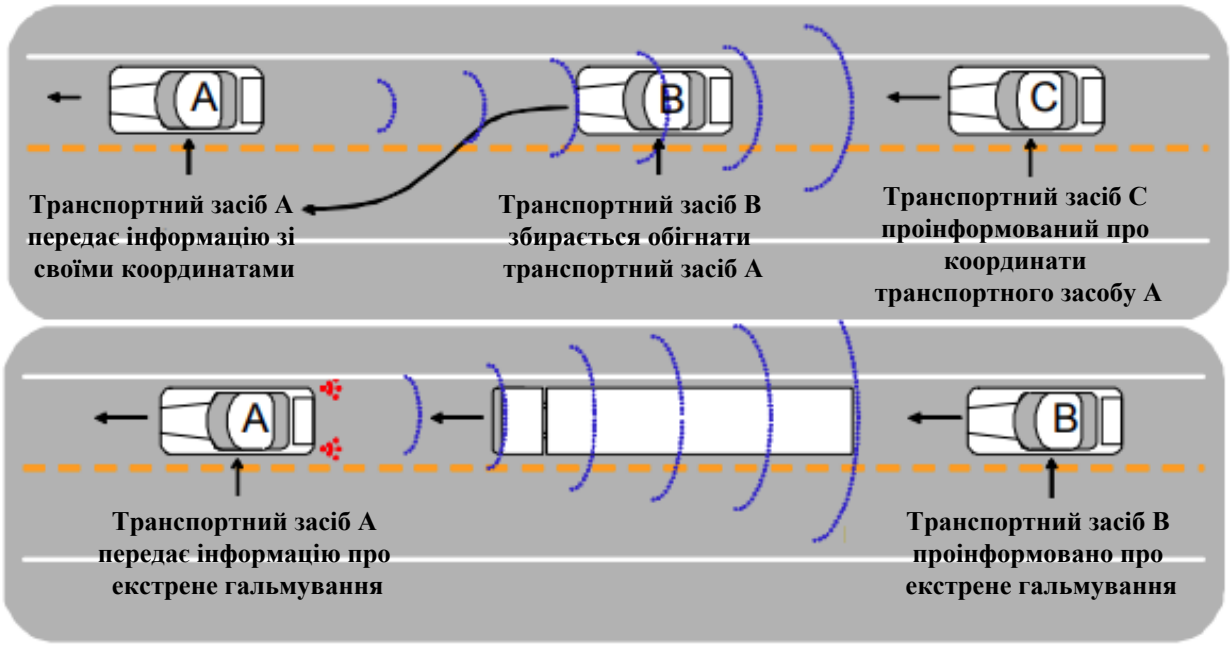


Рисунок 1.22 – Приклад роботи системи DSRC для упередження зіткнень

Через особливості роботи системи DSRC, де кожен пристрій надсилає велику кількість пакетів, які містять інформацію про свій транспортний засіб а також про сусідні транспортні засоби, система DSRC може бути перевантажена купою дублюючої і непотрібної інформації. Автори роботи [26] винайшли вдосконалену схему зменшення вуличного мовлення (enhanced Street Broadcast Reduction (eSBR)), призначену для уникнення проблеми перевантаження системи в реальних міських сценаріях. На рис. 1.23 наведена мапа міста з транспортними засобами, на яких встановлено пристрої DSRC для пояснення принципу роботи eSBR.

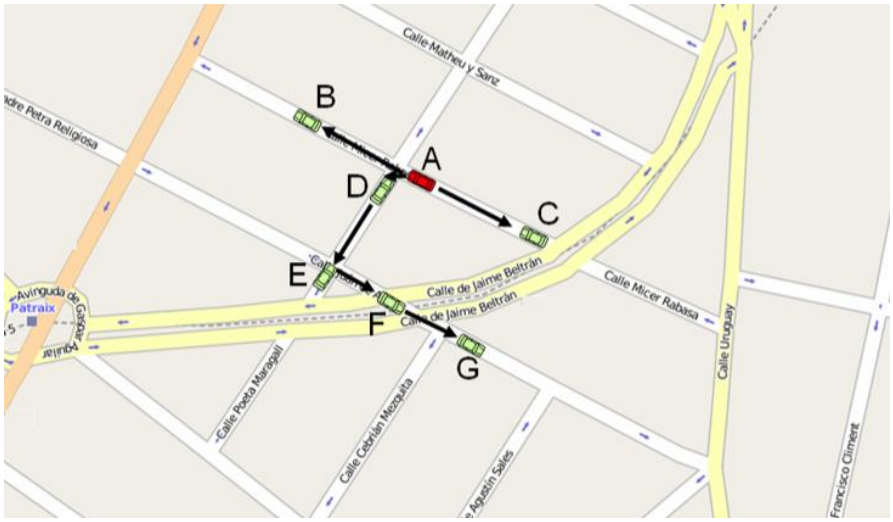


Рисунок 1.23 – Мапа міста з транспортними засобами, на яких встановлено пристрої DSRC для пояснення принципу роботи eSBR

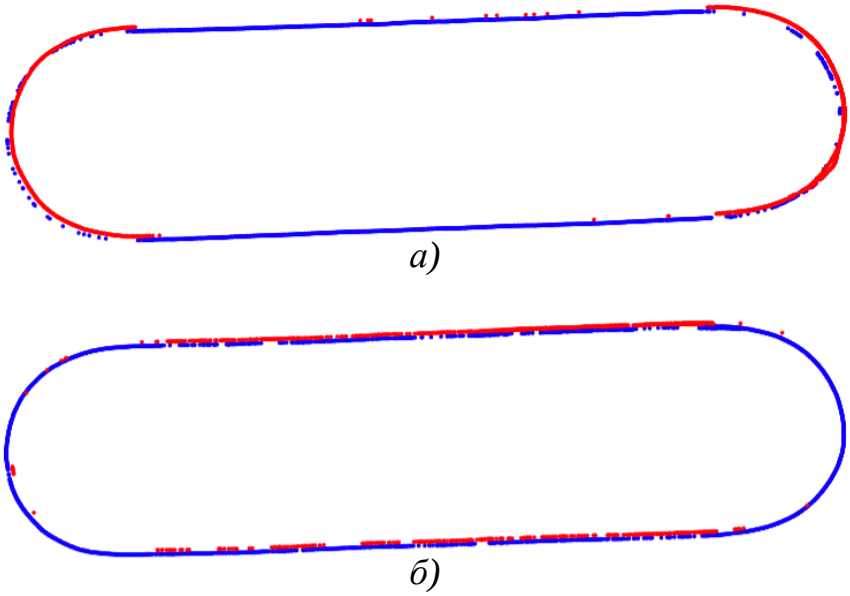
Коли транспортний засіб A передає попереджувальне повідомлення, його отримують лише сусідні транспортні засоби B, C та D, оскільки будівлі заважають поширенню радіосигналу. У цій ситуації, якщо використовується схема на основі відстані або місцезнаходження, транспортні засоби B, C і D будуть ретранслювати повідомлення тільки в тому випадку, якщо відстані досить великі (тобто відстань більше порогу відстані D), або їх додаткові зони покриття досить широкі. Отже, якщо припустити, що тільки транспортний засіб C відповідає цій умові, попереджувальне повідомлення все одно не може бути поширене на решту транспортних засобів (тобто E, F і G).

Згідно схеми eSBR транспортний засіб D буде ретранслювати попереджувальне повідомлення, оскільки він знаходиться на іншій вулиці, ніж транспортний засіб A. Таким чином, попереджувальне повідомлення надійде до всіх транспортних засобів, представлених у схемі, лише за чотири переходи. У сучасних інтелектуальних транспортних системах (ITC) транспортні засоби оснащені бортовими системами GPS, що містять інтегровані карти вулиць. Таким чином, інформація про місцезнаходження та вулиці може бути легко використана

eSBR для полегшення розповсюдження попереджувальних повідомлень. Якщо додаткова зона покриття достатньо широка, транспортні засоби ретранслюють отримане попереджувальне повідомлення.

Однак, якщо додаткова зона покриття дуже мала, транспортні засоби ретранслюють попереджувальні повідомлення, тільки якщо вони перебувають на іншій дорозі. Схеми відстані та місцезнаходження можуть бути дуже обмеженими, особливо коли будівлі заважають поширенню радіосигналу. Без eSBR попереджувальні повідомлення не надійдуть до транспортних засобів E, F та G через наявність будівель.

В роботі [27] було проведено тестування роботи технології DSRC на вантажному транспортному засобі при різних варіаціях встановлення антен: зовнішнє (встановлення антени на збоку корпусу вантажівки) та внутрішнє (встановлення антени всередині вантажівки). На рис. 1.24 представлено результат тестування завадостійкості обладнання на треку. Синій колір на рис.1.24 означає успішно передані дані, червоний колір вказує на втрати в каналі передавання даних.



а)

б)

Рисунок 1.24 – Тестування завадостійкості обладнання DSRC на треку і встановленою антеною ззовні (а) та всередині (б) вантажівки

Як випливає з рис. 1.24, антена, що встановлена всередині вантажівки має кращі показники передавання даних на ділянці дороги з кривизною. Антена, що

встановлена ззовні має кращі показники передавання даних на прямих ділянках руху.

На рис. 1.25 наведені залежності пропускної здатності системи DSRC на одиницю площі в залежності від щільності транспортних засобів, обладнаних DSRC обладнанням (OBU – Onboard Unit) для різної щільності RSU (RSU – Roadside Unit).

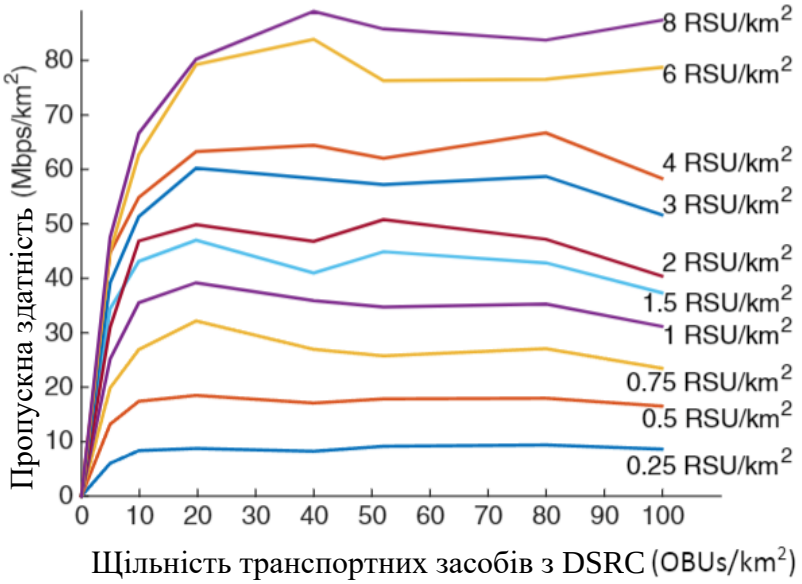


Рисунок 1.25 – Залежності пропускної здатності системи DSRC на одиницю площі в залежності від щільності транспортних засобів

З рис. 1.25 випливає, що пропускна здатність лінійно зростає при збільшенні кількості транспортних засобів, коли щільність OBU низька, а потім залишається близькою до свого максимуму для всіх щільностей OBU вище порогового значення. Пропускна здатність на км^2 завжди зростає з додаванням RSU для всіх рівнів навантаження та для всіх досліджуваних щільностей OBU. Новий RSU може, як збільшити покриття і охопити транспортні засоби, які раніше були відключені, так і забезпечити коротші і, відповідно, більш пропускні канали зв’язку з транспортними засобами, які вже були підключені. Проте через збільшення кількості пристроїв можуть виникати колізії у каналі передавання даних. Автори роботи [28] провели дослідження пропускної здатності каналу передавання даних

в залежності від щільності дорожніх пристроїв DSRC (RSU) з використанням протоколу Request-to-Send та Clear-to-Send (RTS/CTS). Результат тестування наведені на рис. 1.26.

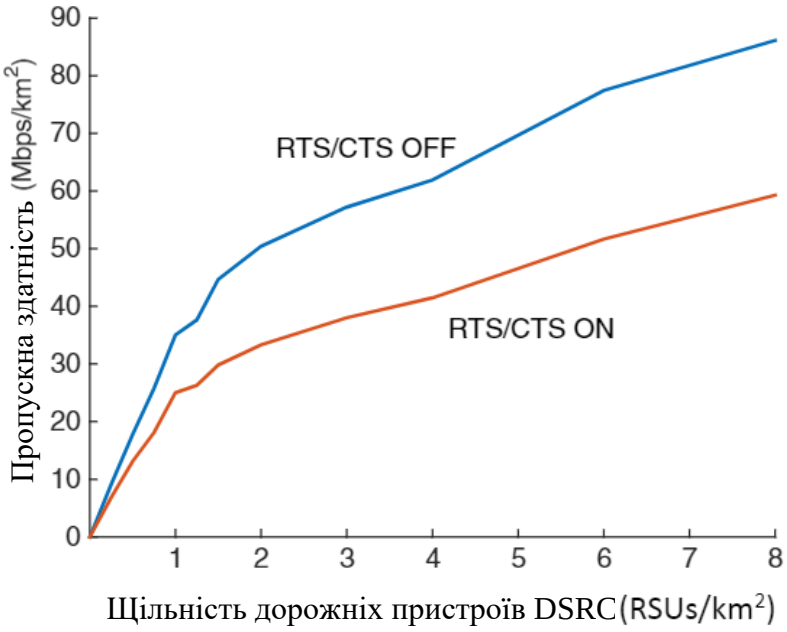


Рисунок 1.26 – Залежності пропускної здатності каналу передавання даних від щільності дорожніх пристроїв DSRC

Як випливає з рис. 1.26 використання протоколу RTS/CTS значно знижує пропускну здатність в каналі передавання даних, проте дозволяє уникати колізій в каналі передавання даних.

Пристрої DSRC мають високі показники рівня сигналу на великій відстані мають високу чутливість приймача, що дозволяє підтримувати зв'язок на великій відстані. У роботі [29] було експериментальним шляхом перевірено рівень сигналу, що надходить від обладнання DSRC при збільшенні відстані між пристроями. Графік залежності рівня сигналу від відстані між пристроями DSRC наведено на рис. 1.27.

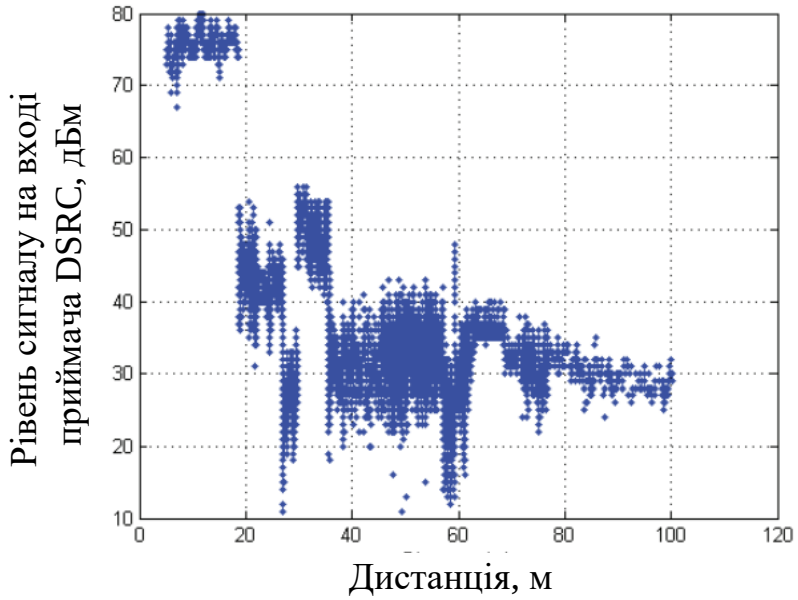


Рисунок 1.27 – Графік залежності рівня сигналу на вході приймача DSRC від відстані між пристроями DSRC

З рис. 1.27 випливає, що значення рівня сигналу (RSSI) на відстані менше двадцяти метрів є меншими (близько 70…80 дБм) порівняно зі значеннями RSSI, отриманими на відстані від 20 до 100 метрів. У більшості випадків рівень сигналу знаходиться на позначці 25…45 дБм, але на графіках можна помітити і винятки. Це може бути пов'язано з наявністю перешкод та інших завад, що були створені пристроями інших безпроводових локальних мереж, що працювали в зоні дослідження.

Найбільшою проблемою для роботи технології DSRC у місті, є завади у вигляді будівель. В рамках досліджень [30] та [31] було представлено недорогу в обчислювальному плані модель загасання сигналу стандарту IEEE 802.11p/DSRC в міських умовах. Представлена у дослідженні модель, дозволяє точно оцінити ослаблення сигналу безпроводової технології між перешкодами, такими як будівлі. З проведених досліджень по загасанню сигналу DSRC можна зробити висновок, що технологія DSRC має середні показники проходження сигналу крізь перешкоди, тому треба розглядати варіанти по збільшенню кількості пристроїв системи для вирішення проблеми загасання сигналу.

На основі технології DSRC було створено алгоритм віртуального світлофору або VTL (Virtual Traffic Lights) [32], [33]. VTL – це алгоритм, який дозволяє транспортним засобам самостійно визначати пріоритети на дорожніх перехрестях за відсутності стаціонарної інфраструктури (тобто звичайних світлофорів). Для розробки ефективної системи VTL зв'язок між транспортними засобами є вирішальним фактором і може бути забезпечений або за допомогою стільникової інфраструктури та технології DSRC. На рис. 1.28 наведено приклад роботи алгоритму VTL на нерегульованому перехресті.

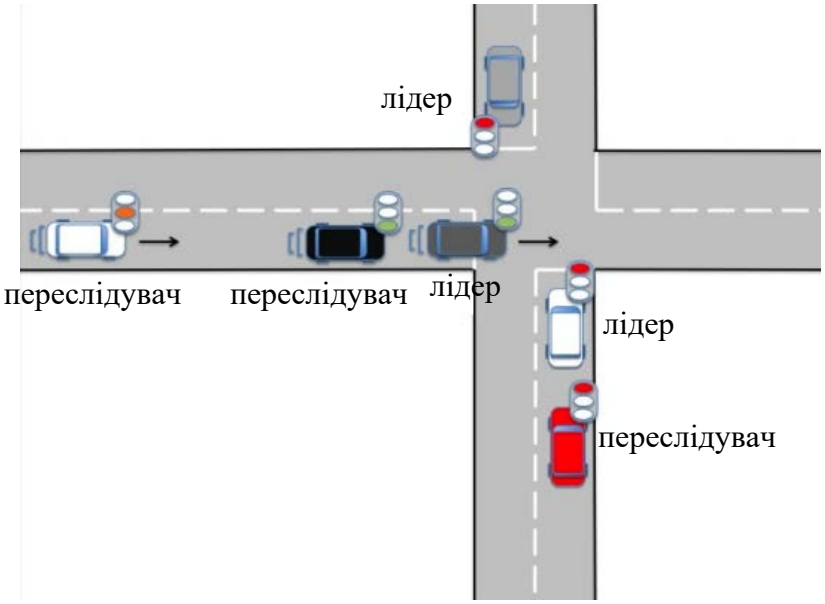


Рисунок 1.28 – Приклад роботи алгоритму VTL на нерегульованому перехесті

Згідно з алгоритмом VTL, транспортні засоби на одній дорозі утворюють кластер і обирають лідером кластера той, який знаходиться ближче до перехрестя. Лідер групи, який знаходиться далі від перехрестя, обирається лідером перехрестя, який буде відповідати за визначення пріоритетів і передачу сигналів світлофора. Як тільки лідер перехрестя залишає перехрестя, він визначає нового лідера перехрестя.

В рамках роботи [33] було представлено блок-схему алгоритму VTL, яку наведено на рис. 1.29.

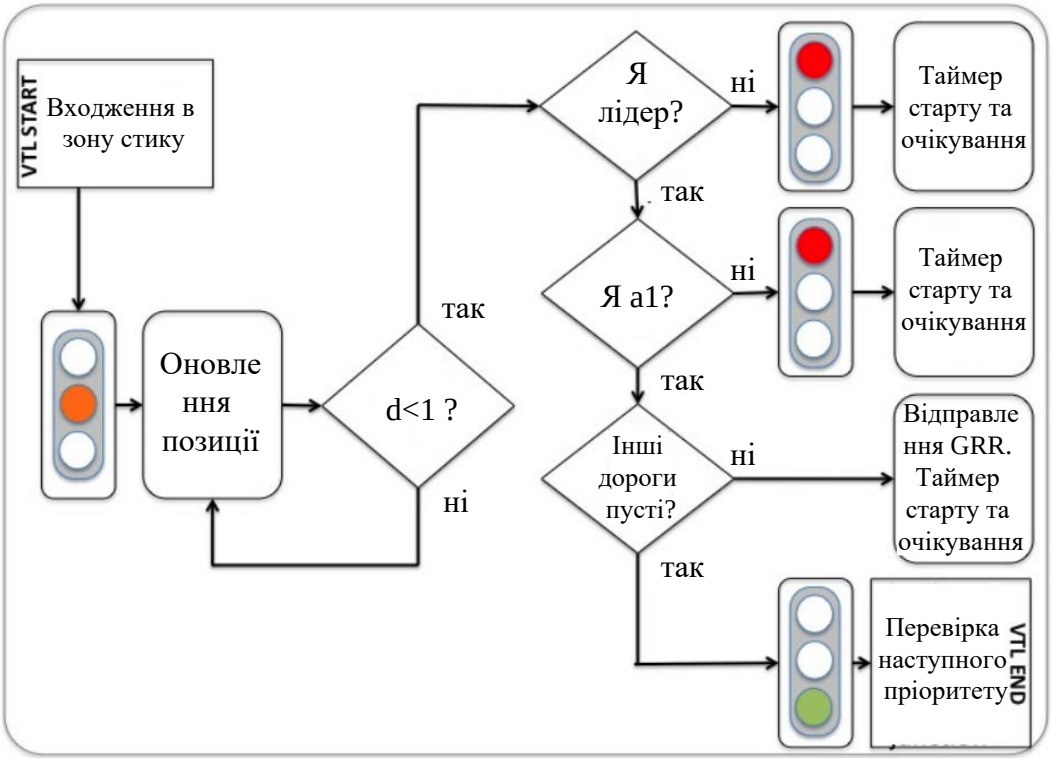


Рисунок 1.29 – Блок-схема алгоритму VTL

Як випливає з рис. 1.29, завдяки алгоритму VTL можна позбутися дорожньої інфраструктури у вигляді світлофорів та дорожніх знаків, проте ця схема несе великі ризики, оскільки у разі виникнення проблем з DSRC обладнанням на одному з транспортних засобів, він стає невидимим для інших транспортних засобів і тому зростає ризик виникнення дорожньо-транспортної пригоди.

1.6 Аналіз можливості використання технології Wi-Fi при побудові smart-міста

Використання технології Wi-Fi дозволяє інтегрувати пристрої пішоходів у транспортну IoT-систему міста. Проте в місцях великого скупчення людей та транспортних засобів можуть виникати проблеми з перевантаженістю Wi-Fi мережі і браком пропускної здатності. У роботах [34-36] розглянуто варіанти по зменшенню навантаження на Wi-Fi мережу шляхом розвантаження її за допомогою технологій стільникового зв’язку. Завдяки розвантаженню Wi-Fi мережі

стільниковими технологіями, можна буде уникнути втрат пакетів та великих затримок в каналі передавання даних.

Технологія Wi-Fi входить до стандартів 802.11, як і DSRC. В рамках дослідження [37] було проведено моделювання та тестування технологій DSRC та Wi-Fi Direct в рамках міста Бандунг, Індонезія за допомогою симуляторів NS-2 (Network Simulator 2) та симулятора трафіку SUMO (Simulation of Urban Mobility), щоб проаналізувати продуктивність протоколів маршрутизації AODV (Ad hoc On-Demand Distance Vector) і DSDV (Destination Sequenced Distance Vector) для цих технологій. На рис. 1.30 наведено графіки залежності пропускної здатності каналів передавання даних від кількості транспортних засобів на дорозі.

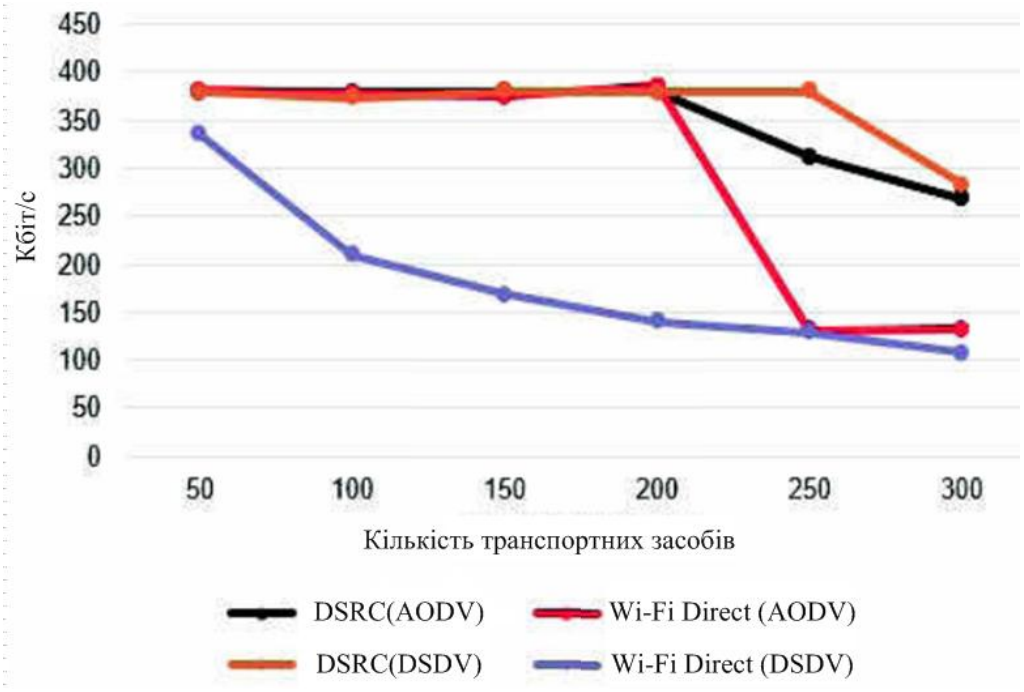


Рисунок 1.30 – Залежності пропускної здатності каналів передавання даних від кількості транспортних засобів на дорозі

Як випливає з рис. 1.30, середня пропускна здатність більша для протоколу AODV у Wi-Fi Direct, ніж у DSRC, коли кількість транспортних засобів досягає 200. Однак при збільшенні кількості транспортних засобів до 300, показники пропускної здатності для AODV Wi-Fi Direct погіршуються. Відзначено, що робочий діапазон Wi-Fi Direct коротший, ніж у DSRC, що може призвести до

збільшення кількості стрибків у маршруті передачі даних. Зміна кількості стрибків спричинена швидкою зміною топології мережі. Через велику кількість змін, що відбуваються в мережі, виникає більша затримка, що призводить до зниження пропускної здатності каналу передавання даних.

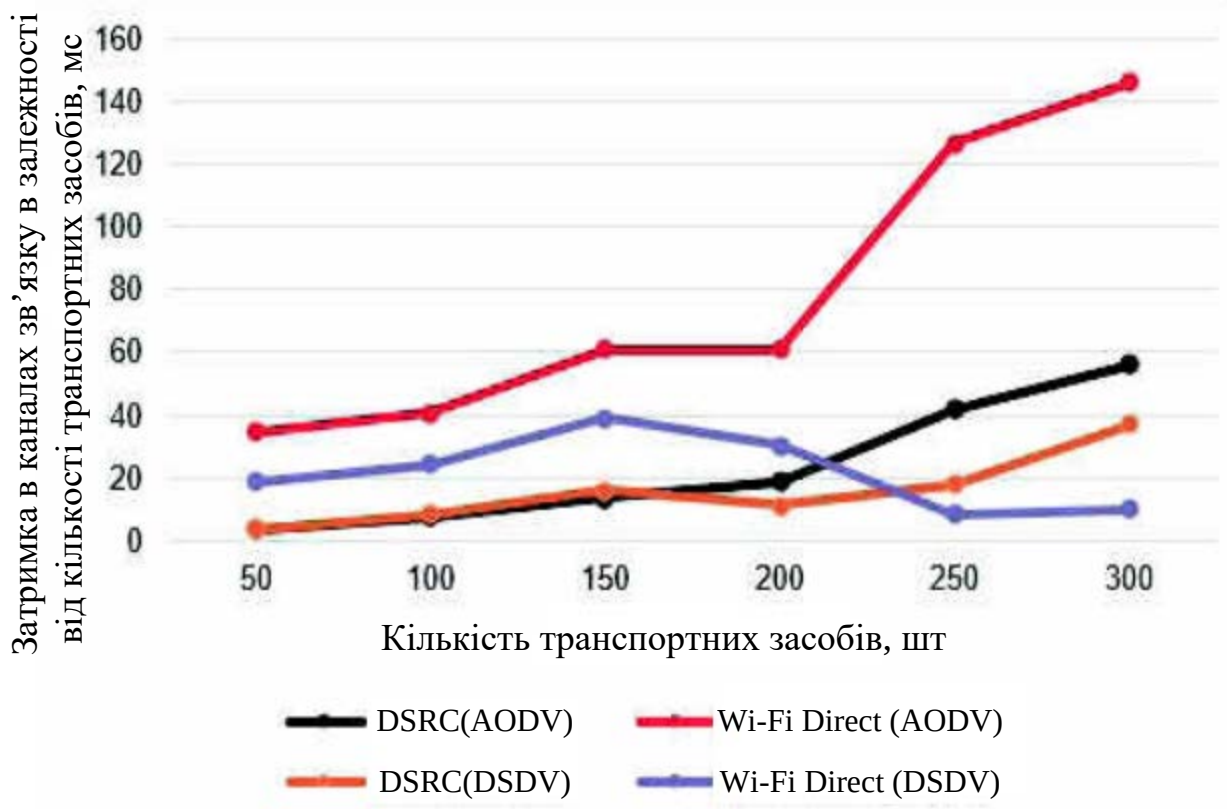


Рисунок 1.31 – Затримки в каналі передавання даних при кількості транспортних засобів

Як випливає з рис. 1.31, затримка у мережі DSRC для обох протоколів маршрутизації зростає зі збільшенням кількості транспортних засобів. Те саме стосується і технології Wi-Fi Direct, за винятком сценарію з використанням протоколу маршрутизації DSDV. Тут затримка зменшилася за рахунок рівня втрат пакетів, який досяг 98,5%, де майже всі передані пакети не досягли місця призначення, навіть незважаючи на кількаразову ретрансляцію. Зазначено, що збільшення кількості транспортних засобів призведе до збільшення кількості даних, що передаються в мережі, де буде існувати ймовірність колізій.

На рис. 1.32 показано, що протоколи маршрутизації AODV та DSDV в стандартах DSRC і Wi-Fi Direct мають однакову пропускну здатність у діапазоні від 10 км/год до 80 км/год, що становить 120,39 кбіт/с.

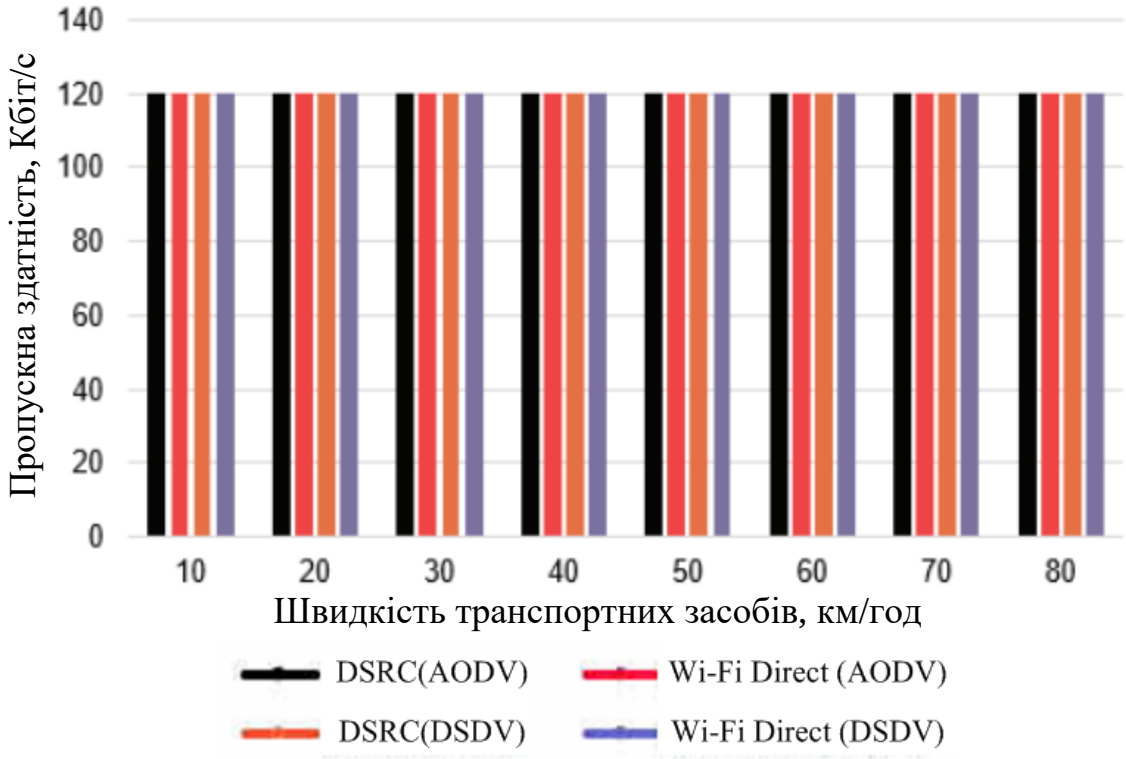


Рисунок 1.32 – Графіки залежності пропускної здатності каналів зв'язку від швидкості транспортного засобу

На рис. 1.33 наведено графік залежності відсотку втрачених пакетів від швидкості транспортного засобу. Як випливає з рис. 1.33, відсоток втрат пакетів для технологій DSRC та Wi-Fi Direct з використанням протоколу маршрутизації AODV майже однаковий і становить 0% для швидкості до 70 км/год. При швидкості транспортного засобу 80 км/год показник кількості втрачених пакетів для Wi-Fi Direct з використанням протоколів маршрутизації AODV і DSDV, виріс до 0,14%. Звідси можна зробити висновок, що показники втрачених пакетів при використанні AODV кращі, ніж при використанні DSDV. Це пов'язано з особливостями DSDV, який періодично оновлює свою таблицю маршрутизації, що призводить до збільшення навантаження на мережу та втрату пакетів. В цьому випадку, можна зробити висновок, що показник втрати пакетів в DSRC менший, в

порівнянні з Wi-Fi Direct. Крім того, якщо топологія мережі не змінюється, коефіцієнт втрати пакетів для обох стандартів буде мінімальним.

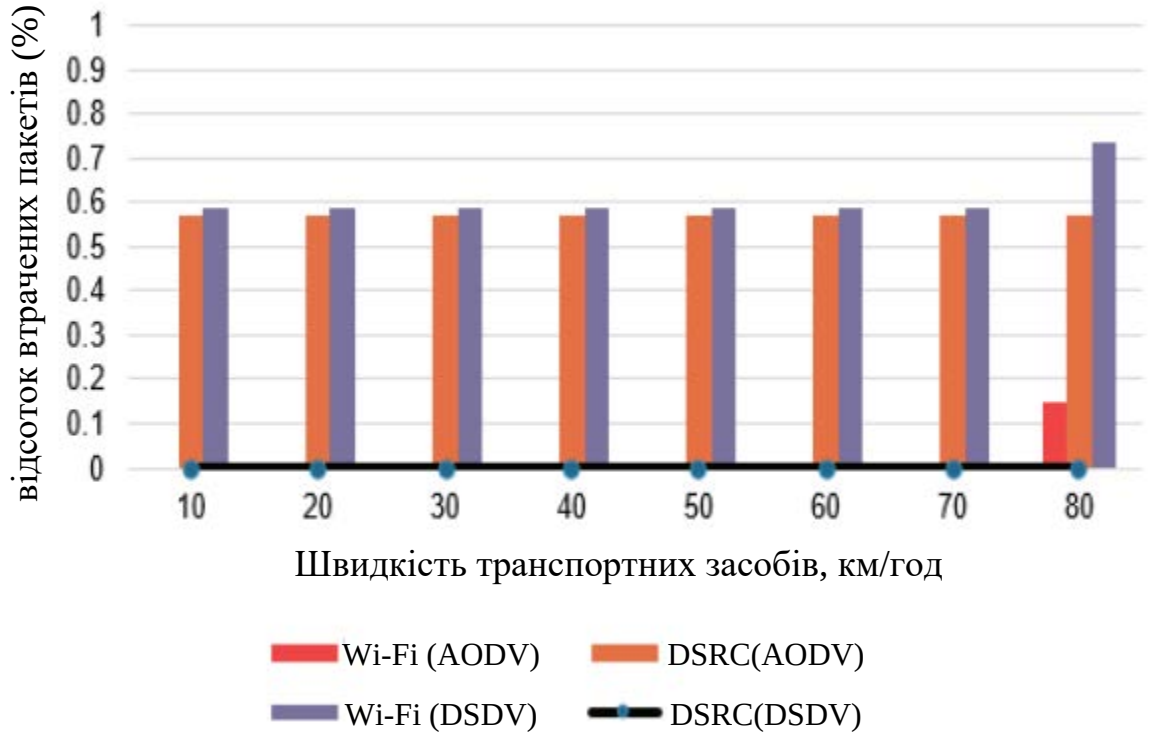


Рисунок 1.33 – Графіки залежності відсотку втрачених пакетів в каналах зв'язку від швидкості транспортного засобу

В рамках дослідження [37] доведено, що при швидкості руху транспортних засобів до 70 км/год немає суттєвого впливу на пропускну здатність та затримки передавання пакетів технологій Wi-Fi та DSRC. Отже технологія Wi-Fi може використовуватися у міських умовах, де швидкість транспортних засобів не перевищує 70 км/год.

У роботі [38] проведено тестування роботи технології Wi-Fi на транспортній мережі. В рамках тестування було встановлено 2 ноутбуки з Wi-Fi модулями на 2 транспортних засоби. Водії потрапляють у зону дії Wi-Fi сигналу на відстані у 91 м один між одним. На кожному етапі тестування водії їдуть з однаковою швидкістю (20 миль/год, 30 миль/год, і т.д.) на зустріч один одному. Схема тестування роботи технології Wi-Fi на транспортній мережі наведено на рис. 1.34.

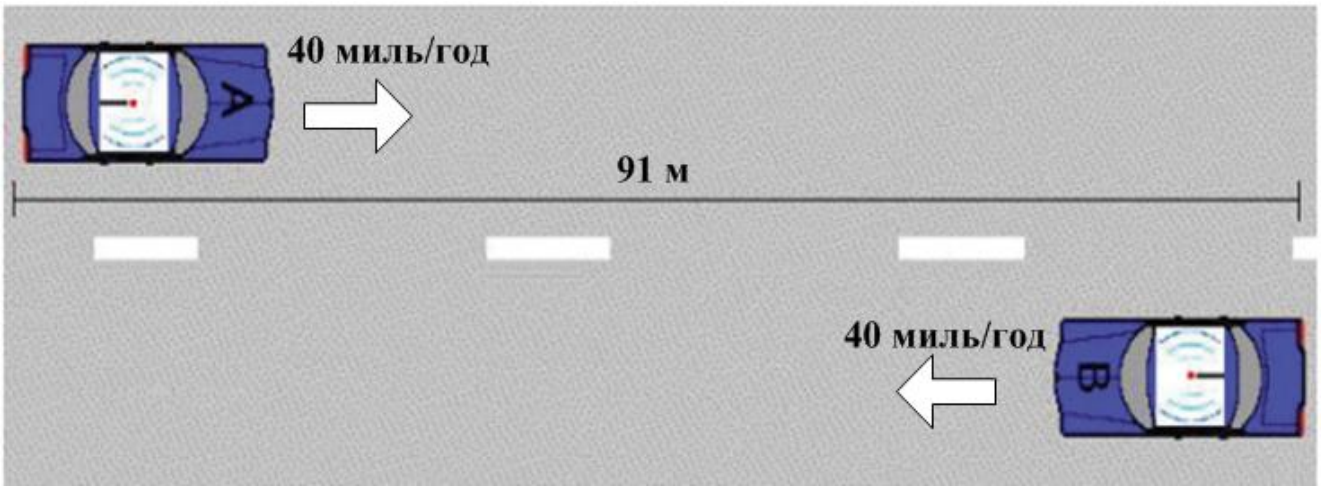


Рисунок 1.34 – Схема тестування роботи технології Wi-Fi на транспортній мережі

Графік на рис. 1.35 показує результати сумарної кількості переданих даних між двома рухомими транспортними засобами. Результати, показані на графіку, є сумою всіх даних, переданих за один сеанс зв'язку між двома транспортними засобами на певній швидкості (наприклад, на швидкості 20 миль/год показана сума у 15.1 МБ). Результати тестування показали, що навіть при максимальній швидкості 60 миль/год можна передати до 0,3 МБ даних. Експерименти показують, що максимальний обсяг переданих даних становив 15,08 МБ на швидкості 20 миль/год.

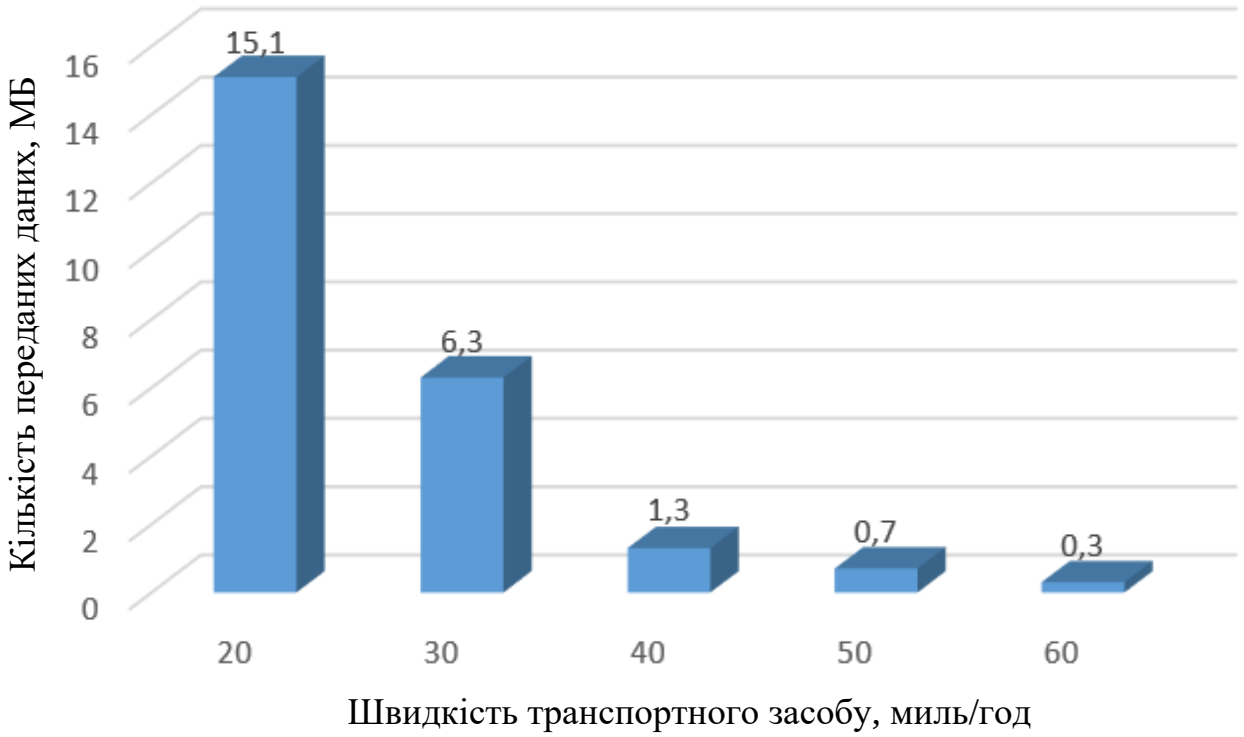


Рисунок 1.35 – Залежність сумарної кількісті переданих даних в каналі зв'язку Wi-Fi від швидкості руху транспортного засобу

Графік на рис. 1.36 показує результати експерименту з точки зору швидкості передавання даних. Швидкість передавання даних показана на різних обмеженнях швидкості транспортних засобів. Результати, що показані на графіку, є середнім значенням швидкості передавання даних за один сеанс зв'язку між двома транспортними засобами на певній швидкості (наприклад, на швидкості 30 миль/год показано середнє значення у 5.6 Мбіт/с).

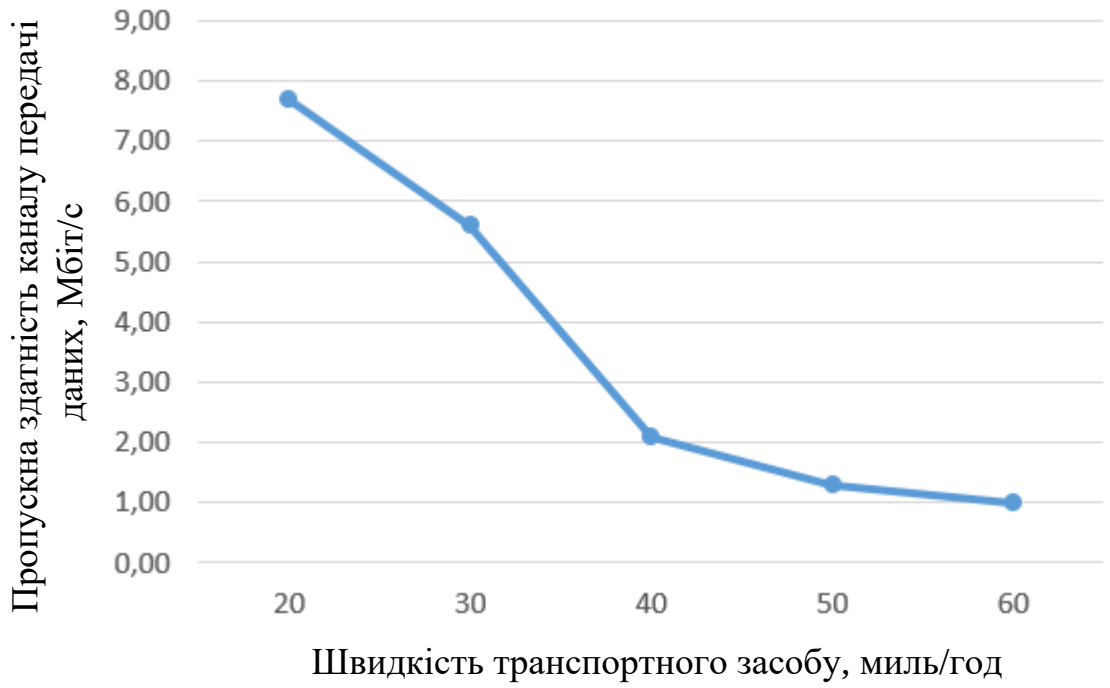


Рисунок 1.36 – Графік залежності швидкості передавання даних від швидкості транспортного засобу

Максимальна швидкість передавання даних становить 7.7 Мбіт/с при швидкості транспортних засобів у 20 миль/год. При максимальній швидкості транспортних засобів у 60 миль/год отримано 1 Мбіт/с. Цієї швидкості передавання даних буде достатньо для передавання даних, у яких містяться координати, напрямок руху та швидкість транспортного засобу.

В рамках дослідження [39] було проведено моделювання технологій DSRC та Wi-Fi у програмному середовищі NS-2.35 для двох сценаріїв: на шосе, та у міських умовах. На рис. 1.37 наведено результати сумарних коефіцієнтів доставки пакетів для всіх пристроїв сценарію.

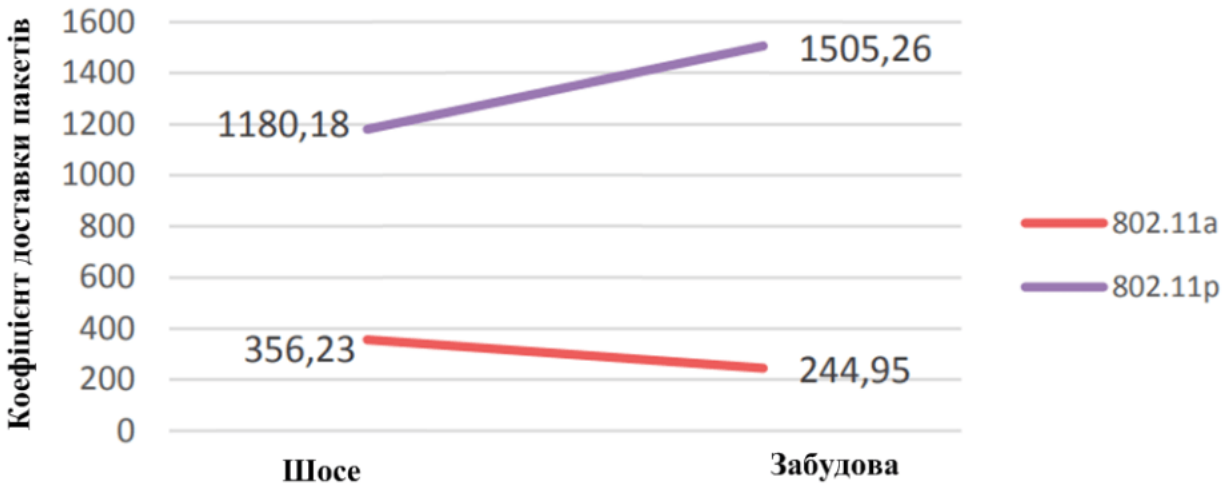


Рисунок 1.37 – Коефіцієнт доставки пакетів технологій DSRC (802.11p) та Wi-Fi для сценаріїв "шосе" та "забудова"

Як випливає з рис. 1.38, технологія DSRC має кращі показники коефіцієнтів доставлених пакетів. Також, можна зробити висновки, що технологія DSRC має кращий результат для сценарію "забудова". Технологія Wi-Fi, навпаки, має кращі результати у сценарію "шосе".

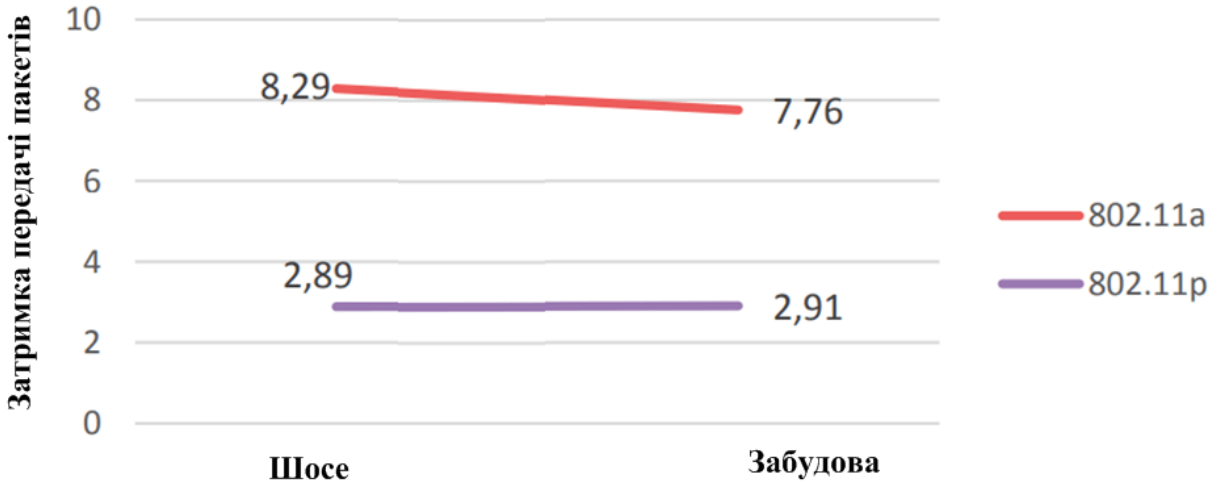


Рисунок 1.38 – Затримка передавання пакетів технологій DSRC (802.11p) та Wi-Fi для сценаріїв "шосе" та "забудова"

Як випливає з рис. 1.38, затримка у передавання пакетів майже не змінилася для обох сценаріїв та обох технологій, проте можна зробити висновок, що технологія DSRC має нижчі показники затримок у каналі передавання даних. На

рис. 1.39 представлено результати пропускної здатності каналів передавання даних для обох сценаріїв.

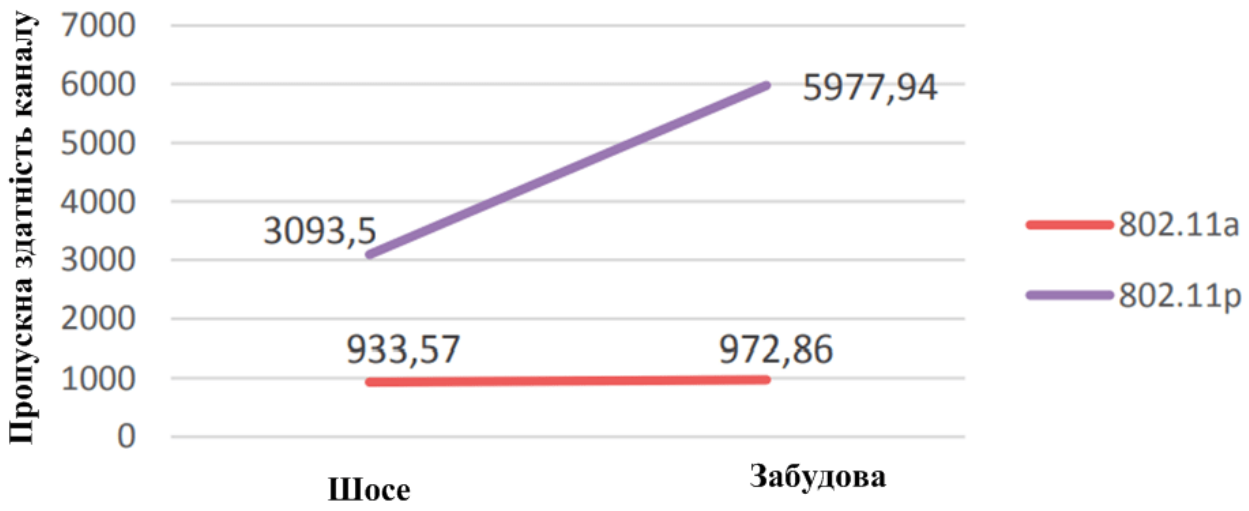


Рисунок 1.39 – Пропускна здатність каналу передавання даних технологій DSRC (802.11p) та Wi-Fi для сценаріїв "шосе" та "забудова"

Як випливає з рис. 1.39, пропускна здатність майже не змінилася для технології Wi-Fi у обох сценаріях, проте для технології DSRC показники різних сценаріїв відрізняються майже у 2 рази.

У роботі [40] висвітлено, що технологію Wi-Fi можна використовувати для встановлення місцезнаходження об’єктів. Для цього генерується радіолокаційна карта приміщення чи зони. В даному дослідженні було використано смартфон з Wi-Fi модулем у якості пристрою для виявлення місцезнаходження. На рис. 1.40 наведено радіолокаційну мапу з покриттям зони тестування. Радіолокаційна мапа генерується на основі рівня сигналу, визначеного через місцезнаходження Wi-Fi передавача (смартфону з Wi-Fi модулем). Зелена частина мапи має високий рівень сигналу, отже, точність визначення місцезнаходження буде вищою. Жовта частина потребує додаткового збору даних, червона зона – це місця, де немає сигналу для збору даних про місцезнаходження.

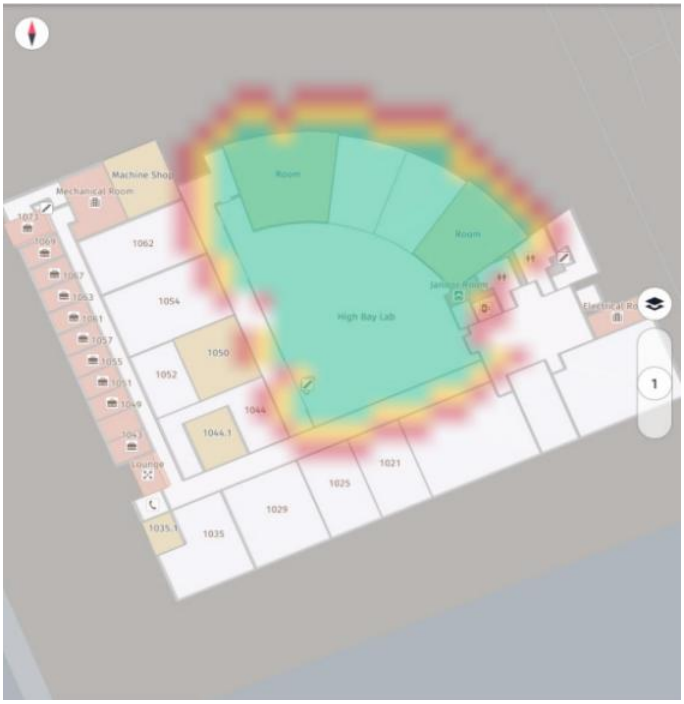


Рисунок 1.40 – Радіолокаційна мапа з покриттям зони тестування

Після створення радіолокаційної мапи можна проводити вистежування об’єкту з Wi-Fi модулем, як показано на рис. 1.41.

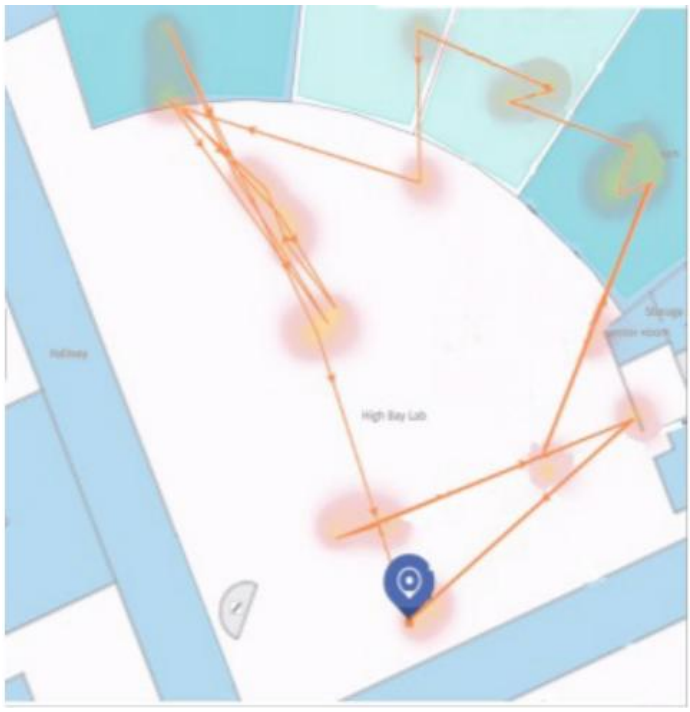


Рисунок 1.41 – Вистежування місцезнаходження об'єкту за допомогою технології Wi-Fi

В рамках дослідження [41] також було перевірено практичним шляхом, що технологія Wi-Fi може доволі точно передавати дані про місцезнаходження об’єкту. Результати перевірки цього дослідження наведено на рис. 1.42.

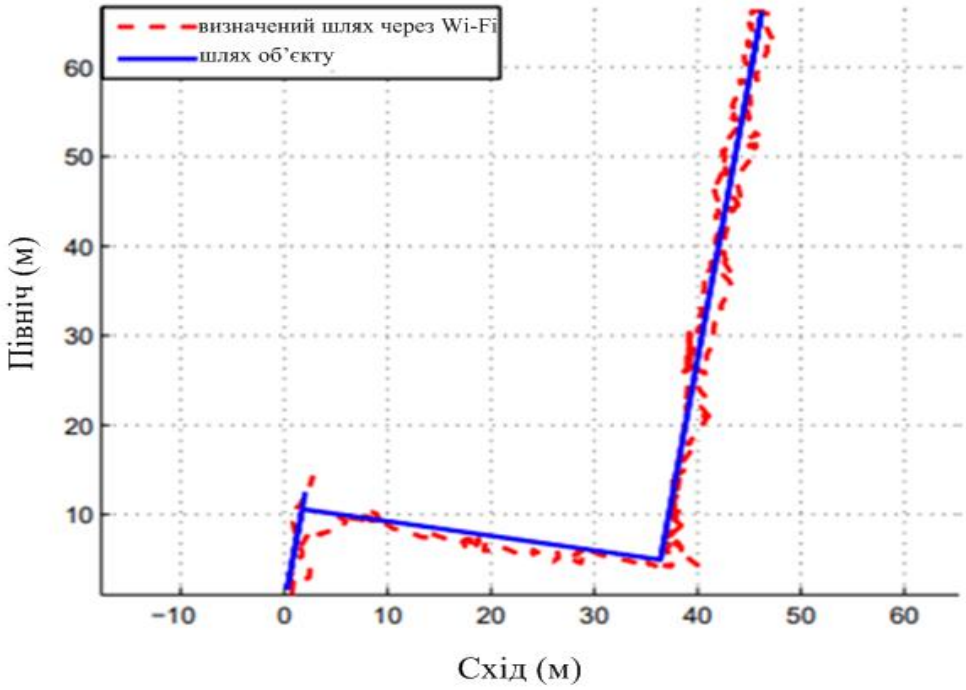


Рисунок 1.42 – Визначення шляху об’єкту за допомогою технології Wi-Fi

Висновки до розділу 1

В результаті проведено аналізу виявлено, що для побудови транспортної мережі краще використовувати технології сімейства IEEE 802.11 та RFID.

Системи, що використовують технологію DSRC, забезпечують надійний зв'язок для транспортних засобів, але мають доволі дорогі пристрої. Також цю технологію буде доволі важко інтегрувати у транспортну систему, оскільки під дорожні пристрої потрібно буде провести окрему кабельну систему. Звісно, можна використовувати оптичну або Ethernet мережу від придорожніх камер, проте місце встановлення дорожніх пристроїв DSRC не завжди буде співпадати з місцем встановлення придорожніх камер.

Технологія RFID, використовуючи пасивні мітки, забезпечує зв'язок лише в обмеженій зоні, тому RFID-мітки, що інтегровані у дорожню інфраструктуру, можуть надавати інформацію у визначених зонах, і за допомогою цього можна дуже точно ідентифікувати місцезнаходження транспортного засобу. Електромагнітні пасивні RFID-мітки не потребують джерела живлення, мають високу стійкість до пилу та перешкод і дуже малий розмір. RFID-мітки дуже дешеві, тому їх можна встановлювати у великій кількості, задля підвищення завадостійкості системи. Таким чином, RFID-мітки позбавлені недоліків, що пов'язані з вартістю пристроїв і рівнем обслуговування технології DSRC.

Задля підвищення безпеки руху транспортних засобів можна інтегрувати системи DSRC та RFID у транспортну мережу, проте пішоходи залишаються "невидимими" для цих систем. Модуль технології DSRC не інтегрований у сучасні смартфони, що є в наявності у кожного пішохода, а інтегровані модулі Bluetooth та NFC мають невелику дальність дії. З усіх існуючих технологій, що інтегровані у сучасні смартфони, технологія Wi-Fi задовольняє більшість вимог до технології, що може бути інтегрована у транспортну мережу міста.

2 ВИБІР КОНФІГУРАЦІЇ ТА РОЗТАШУВАННЯ МІТОК RFID ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ РУХУ ТРАНСПОРТНОЇ МЕРЕЖІ МІСТА

2.1 Актуальність проведення дослідження технології RFID у smart-місті

Безпеку руху у smart-місті можна значно підвищити шляхом своєчасного інформування водія про стан на дорогах, наявність пішоходів та небезпечні ситуації. Використання системи радіочастотної ідентифікації у транспортній мережі міста дозволяє:

- отримувати водіям інформацію про зміну швидкісного режиму на дорозі;
- наявність небезпечних ділянок руху;
- про появу пішоходів на дорозі та інше.

Особливо важливе таке інформування в умовах щільного трафіку, коли дорожні знаки або пішоходи можуть бути закриті іншими транспортними засобами. Світова тенденція на використання транспортних засобів з автопілотами теж вимагає розвинутої інфраструктури інформування транспортних засобів.

Кількість транспортних засобів на дорогах загального використання невпинно зростає що призводить до зростання кількості дорожньо-транспортних пригод. До основних причин цього явища можна віднести нехтування правилами дорожнього руху і недостатня інформованість водія про наявність загрози зіткнення на дорозі. Інформованість водіїв можна значно покращити при використанні сучасних технологій.

Використання технологій DSRC і RFID (Radio Frequency Identification) дозволяє підвищити безпеку руху за рахунок забезпечення контролю місцезнаходження і взаємного розташування як учасників дорожнього руху, так і з дорожньою інфраструктури. Крім того в системі здійснюється ідентифікація учасників руху.

Однією з вагомих переваг технології RFID є здатність отримувати зчитувачем інформацію від багатьох міток одночасно, використовуючи технологію

антиколізій. Крім того, при використанні систем RFID відсутні необхідність прямої видимості між мітками та зчитувачами а також можливість зв’язку на відстані до декількох десятків метрів. Ці особливості дають можливість використовувати RFID-технологію в транспортних мережах smart-міста.

При використанні можливостей технологій RFID та DSRC забезпечується висока швидкість обміну даними між учасниками дорожнього руху і мала затримка передавання даних, що дозволяє будувати системи працюючі на упередження зіткнення між різними об'єктами на дорогах.

Для безпечного руху транспортного засобу водію необхідно контролювати велику кількість об’єктів транспортної інфраструктури, таких як інші транспортні засоби, пішоходи, дорожні знаки та світлофори, які входять до дорожньої інфраструктури, ями на дорозі, та рухатися у правильному швидкісному режимі. В такому динамічному ритмі дуже легко не помітити дорожній знак або інший важливий об’єкт транспортної інфраструктури.

В дослідженнях з інтеграції RFID міток у дорожнє покриття [16, 17] та у дорожні знаки [18] розглянуті питання забезпечення додаткового інформування водія про зміну швидкісного режиму чи головної дороги. В роботі [23] розглянуті питання використання технології RFID для ідентифікації транспортних засобів на дорогах. В роботі [19] розглянуті питання використання технології RFID для логістичних цілей та виявлення позиціювання транспортного засобу на дорозі [20]. Інтегрування технології радіочастотної ідентифікації у промислових системах "інтелектуального складу" або "інтелектуального виробництва" [21] дозволяє автоматизувати виробничі процеси і значно підвищити продуктивність праці.

Використання технології RFID при створенні системи розумного міста [7, 24] виявило декілька вад даної технології. Дослідження показали, що транспортні системи, що створені для упередження виникнення аварії, працюють з великою затримкою через обробку іншими додатками. Тому для побудови систем, що призначені для упередження зіткнення, краще використовувати технологію DSRC, що забезпечує значно меншу затримку і більшу швидкість передавання інформації.

Хоча технологія RFID має більшу затримку ніж технологія DSRC, однак її можна використовувати для додаткового інформування водія про дорожні знаки чи наближення до небезпечної ділянки шляху, що сприятиме зменшенню аварій на складних ділянках шляхів. Дослідження ефективності використання технології радіочастотної ідентифікації, що проводились різними авторами з використанням пасивних RFID-міток, не враховували різні варіанти розташування міток в дорожній інфраструктурі через що неможливо зробити повноцінні висновки про можливість застосування даної технології у смарт-місті.

2.2 Вибір обладнання для проведення моделювання розповсюдження енергії поля RFID-міток

Пристрої RFID різного призначення використовують декілька частотних діапазонів. Тому перед проведенням дослідження по використанню технології RFID у транспортній мережі міста, необхідно коректно обрати частотний діапазон у якому будуть працювати мітки. Порівняльний аналіз характеристик RFID-міток наведений у табл. 2.1.

Таблиця 2.1 – Порівняльний аналіз характеристик RFID-міток

Тип мітки	Діапазон частот	Тип живлення	Радіус дії
Низькочастотні	30…300 кГц	пасивні	до 10 см
Високочастотні	3…30 МГц	пасивні	до 1 м
Ультрависокочастотні	300…3000 МГц	пасивні, активні	до 100 м

RFID-мітки, що встановлюються у транспортній інфраструктурі, мають відповідати декільком вимогам: великий радіус дії, стійкість до електромагнітних завад та надійна робота в жорстких умовах експлуатації в широкому діапазоні температур та вологості. Виходячи з даних табл. 2.1 використанні у транспортній мережі міста необхідно обирати ультрависокочастотні та мікрохвильові RFID-мітки оскільки вони забезпечують великий радіус дії.

Для налізу розповсюдження сигналу від пасивної RFID-мітки було обрано мітку з ультрависокочастотного діапазону OPP130 [42]. Мітка призначена для встановлення на металеві поверхні. Характеристики пасивної RFID-мітки OPP130:

- діапазон робочих частот 865…868 МГц;
- потужність передавача -30,7 дБм;
- максимальна дальність зв'язку 28 м;
- збереження даних не менше 50 років;
- ступень захисту IP68;
- діапазон робочих температур -30…+100 °C;
- габаритні розміри 130×42×10,5 мм.

Пасивна RFID-мітка має невеликі габарити, що дозволяє з легкістю встановити її на металевий дорожній знак. Завдяки широкому діапазону робочих температур та ступеню захисту IP68 мітку можна буде використовувати у важких умовах експлуатації. Зовнішній вигляд пасивної RFID-мітки наведено на рис. 2.1.

Рисунок 2.1 – Зовнішній вигляд пасивної RFID-мітки

В якості зчитувача інформації від пасивної RFID-мітки було обрано пристрій "Impinj R700 RAIN" [43]. Зовнішній вигляд зчитувача пасивних RFID-міток наведено на рис. 2.2. Основні характеристики зчитувача "Impinj R700 RAIN":

- діапазон робочих частот 865…928 МГц;
- максимальна чутливість приймача -93 дБм;
- максимальна потужність передавача +33 дБм.

Рисунок 2.2 – Зовнішній вигляд зчитувача "Impinj R700 RAIN"

В якості активної RFID-мітки було обрано мітку SAAT T508 [44]. Зовнішній вигляд активної RFID-мітки наведено на рис. 2.3. Основні характеристики мітки SAAT T508:

- діапазон робочих частот 2,4…2.8 ГГц;
- потужність передавача -6 дБм;
- термін безперервної роботи без заміни батареї не менше 3 років;
- діапазон робочих температур -40…+60 °С;
- габаритні розміри 80×42×9 мм.

Рисунок 2.3 – Зовнішній вигляд активної RFID-мітки SAAT T508

В якості зчитувача інформації від активної RFID-мітки було обрано RFID-зчитувач SAAT-F527A [45].

Основні характеристики RFID-зчитувача SAAT-F527A:

- діапазон робочих частот 2.4…2.48 ГГц;
- максимальна дальність зчитування ~80 м;
- чутливість приймача ~ -92дБм ;
- діапазон робочих температур -40…+60 °С;

Зовнішній вигляд зчитувача активних RFID-міток наведено на рис. 2.4.

Рисунок 2.4 – Зовнішній вигляд зчитувача активних RFID-міток SAAT-F527A

2.3 Аналіз розповсюдження сигналу від RFID-міток

Моделювання розповсюдження енергії поля від пристроїв RFID проводилось в програмі Altair WinProp. На рис. 2.5 наведена схема розташування легкового транспортного засобу (блакитного кольору), на якому встановлено зчитувач "Impinj R700 RAIN" та стовпа з дорожнім знаком, на якому встановлено RFID-мітку. Дослідження проводилось у найбільш складному випадку розташування транспортних засобів. Між легковим транспортним засобом (далі – ЛТЗ) та стовпом з розташованою на ньому міткою знаходяться вантажівки (помаранчевого

кольору) на дорозі з чотирма смугами руху. На ЛТЗ встановлений RFID-зчитувач "Impinj R700 RAIN".

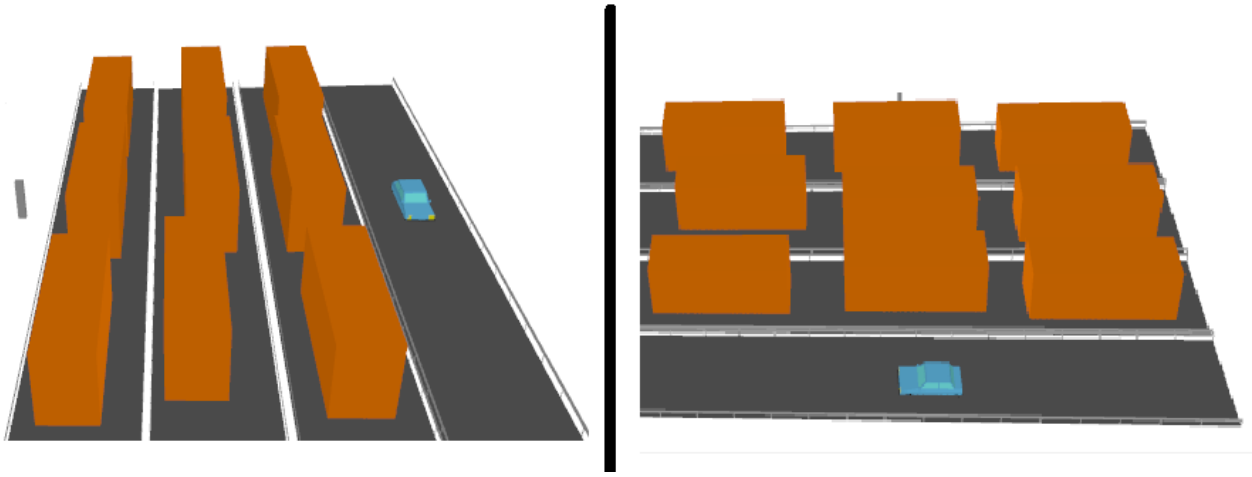


Рисунок 2.5 – Схема розташування транспортних засобів для проведення дослідження у найскладнішому випадку роботи системи RFID

Проведено перевірку коректності розрахунку енергії поля програмою Altair Winprop за допомогою формули Фріїса:

$$P_{in}(d) = P_t \cdot G_r \cdot G_t \cdot (\frac{\lambda}{4 \cdot \pi \cdot d})^2 \quad (1)$$

де $P_{in}(d)$ – потужність прийнятого сигналу, P_t – потужність передавача [Вт], G_t – коефіцієнт підсилення передавальної антени, G_r – коефіцієнт підсилення приймальної антени, λ – довжина хвилі, d – дистанція у метрах [11].

Для перевірки коректності моделювання енергії поля програмою Altair Winprop було обрано активну мітку SAAT T508. Потужність передавача мітки дорівнює -6 дБм, що відповідає значенню $2{,}51 \cdot 10^{-4}$ Вт. Перевірку проведено для дистанції у 60 м без перешкод. Згідно формули Фріїса потужність сигналу на відстані 60 м від мітки буде дорівнювати:

$$P_{in}(d) = 2.51 \cdot 10^{-4} (\frac{3 \cdot 10^8}{4 \cdot 3.14 \cdot 60 \cdot 2.8 \cdot 10^9})^2 = 5.074 \cdot 10^{-12} \text{ Вт} = -83 \text{ дБм} \quad (2)$$

Згідно розрахунків, потужність сигналу на відстані 60 м від мітки при переведенні у величину дБм буде дорівнювати -83 дБм. Результат моделювання енергії поля наведено на рис. 2.6.

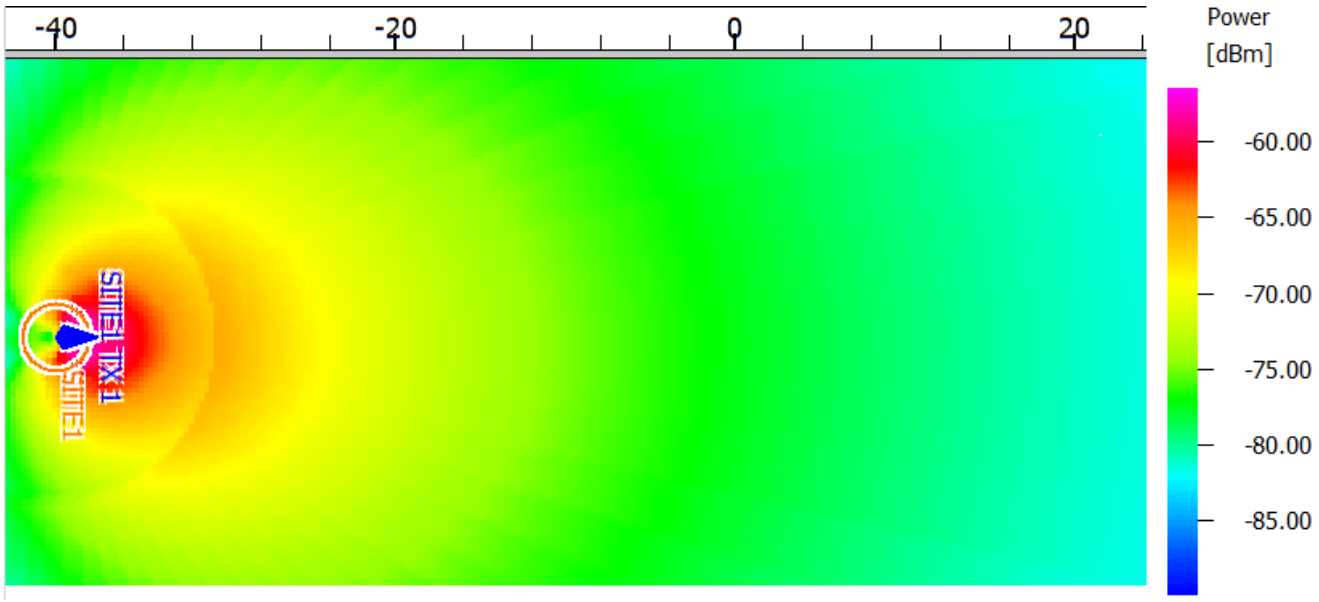


Рисунок 2.6 – Розповсюдження енергії поля від активної мітки SAAT T508

Як випливає з рис. 2.6 енергія поля на відстані 60 м від мітки знаходиться на рівні -83 дБм, отже можна зробити висновки, що програма робить коректні розрахунки енергії поля сигналу.

Результат моделювання розповсюдження енергії поля сигналу від пасивної RFID-мітки OPP130 наведений на рис. 2.7.

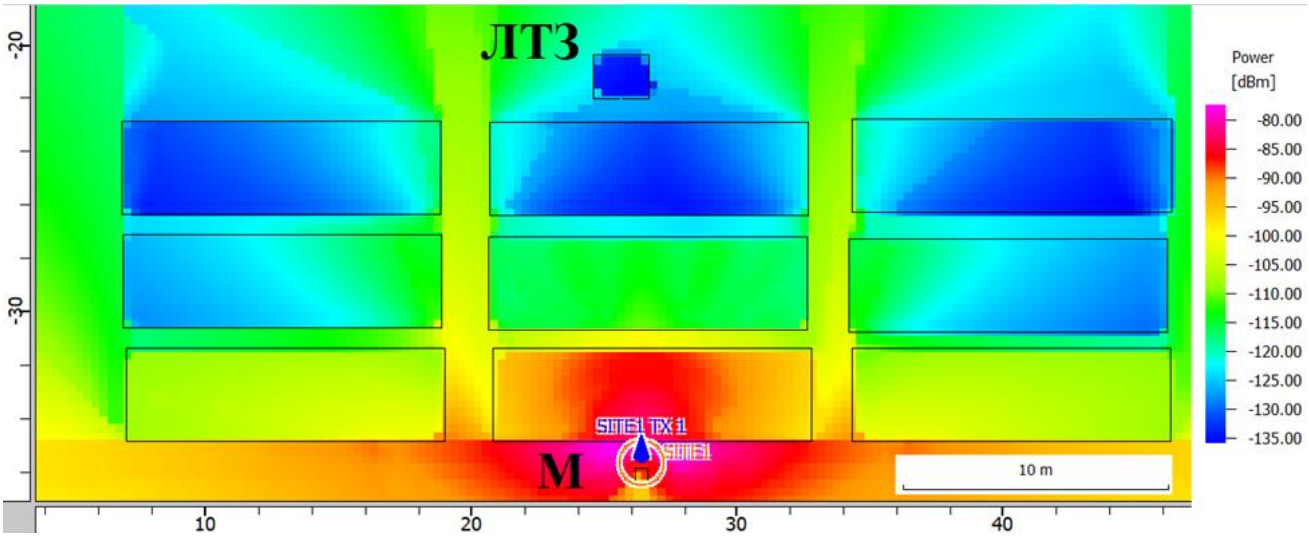


Рисунок 2.7 – Розповсюдження енергії поля сигналу пасивної мітки OPP130

Згідно результатів моделювання енергія поля сигналу від RFID-мітки OPP130 (точка М на рис. 2.7)) в місці розташування ЛТЗ дорівнює -135 дБм. Максимальна чутливість приймача "Impinj R700 RAIN", що встановлений на легковому транспортному засобі дорівнює -92 дБм. Отже такого рівня сигналу замало для того щоб легковий транспортний засіб отримав інформацію надіслану від RFID-мітки, яка інтегрована у дорожній знак.

Для перевірки розповсюдження енергії поля вздовж усіх смуг руху встановлено додаткову RFID-мітку OPP130 на стовпі з іншого боку дороги. Для проведення дослідження в ускладнених умовах ЛТЗ було переміщено у другу смугу, а між міткою та легковим транспортним засобом було розміщено вантажівку. Розповсюдження енергії поля сигналу від RFID-міток OPP130 при встановленні їх з двох боків 4-х смугової дороги наведено на рис. 2.8.

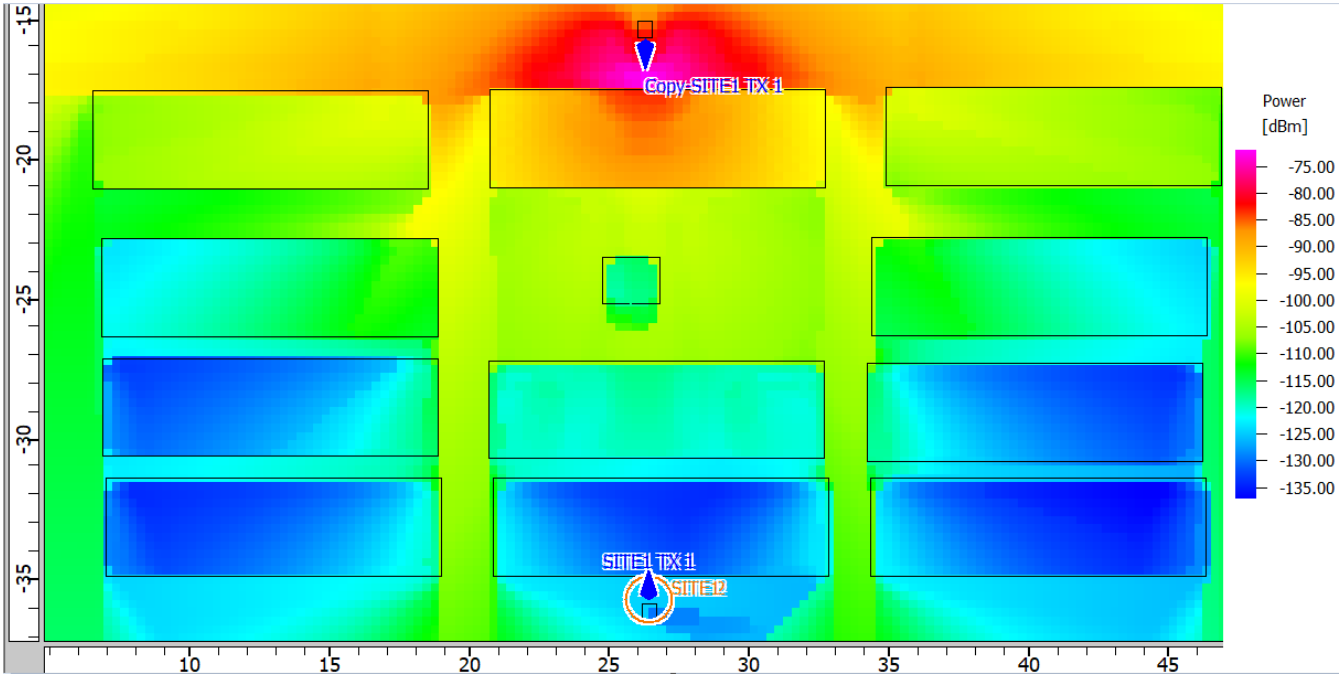


Рисунок 2.8 – Розподіл інтенсивності поля сигналу двох пасивних RFID-міток OPP130 при їх встановленні з обох боків дороги

При такому розташуванні міток і взаємному розташуванні транспортних засобів рівень сигналу прийнятого ЛТЗ від міток дорівнює -100 дБм, що недостатньо для прийому сигналів міток зчитувачем "Impinj R700 RAIN".

Результати дослідження з використанням пасивних RFID-міток дають змогу зробити висновок, що їх використання для інформування водіїв на дорогах з трьома і більше смугами руху недоцільно. Пасивні RFID-мітки при встановленні на дорожні знаки доцільно використовувати лише на дорогах з однією або з двома смугами руху при розташуванні міток з обох боків дороги.

При інтеграції пасивних RFID-міток в асфальтне покриття, доведеться встановлювати по одній мітці у кожну смугу руху. Таке розташування міток недоцільно використовувати на дорогах з інтенсивним рухом бо при ремонті дорожнього покритті доведеться кожного разу встановлювати нові мітки.

Найкращим варіантом інтеграції пасивних RFID-міток у транспортну мережу буде їх встановлення на підвісних світлофорах або інформаційних екранах, що знаходяться над смугами руху. В такому випадку буде достатньо двох пасивних RFID-міток OPP130 для покриття чотирьох смуг руху.

Оскільки енергії поля від пасивної RFID-мітки недостатньо для забезпечення стабільного покриття дороги з чотирма смугами, необхідно провести аналогічні дослідження з використанням активних міток, що мають більшу потужність передавача, і зможуть забезпечити більшу зону покриття.

Розповсюдження енергії поля сигналу активної RFID-мітки SAAT T508 наведено на рис. 2.9.

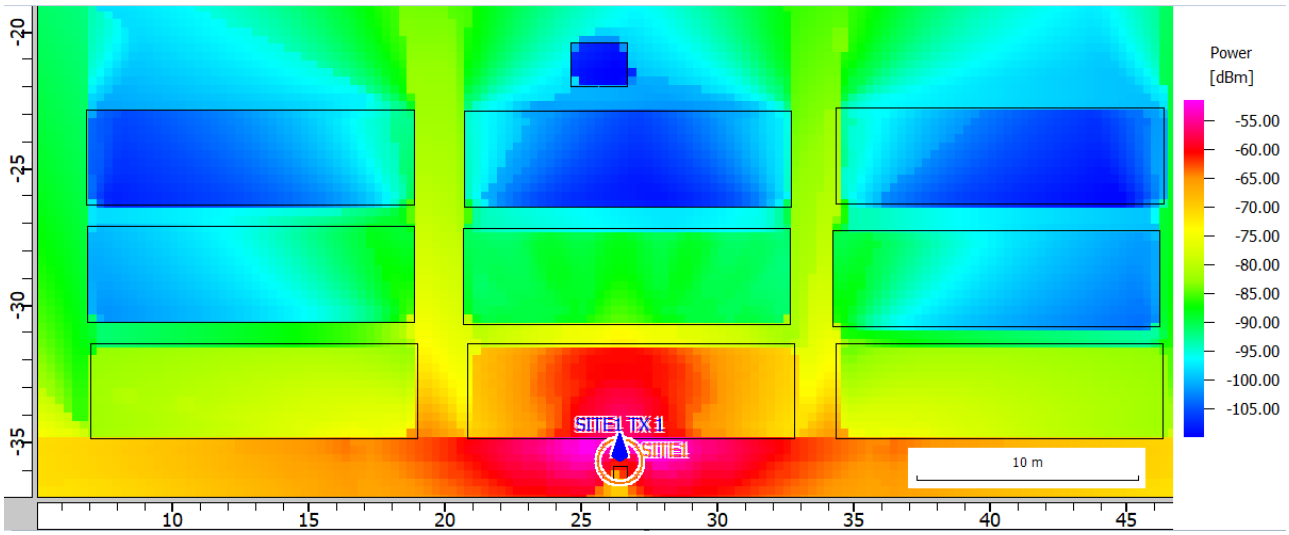


Рисунок 2.9 – Розповсюдження енергії поля сигналу від активної RFID-мітки SAAT T508

Як випливає з рис. 2.9 енергія поля сигналу від активної мітки SAAT T508 в місці розташування ЛТЗ дорівнює -100 дБм. Рівень сигналу, отриманий від мітки SAAT T508 менший за максимальну чутливість приймача зчитувача SAAT-F527A, через що ЛТЗ не зможе отримати інформацію від активної мітки SAAT T508, що встановлена на стовпі.

Для перевірки розповсюдження енергії поля вздовж усіх смуг руху встановлено ще одну мітку SAAT T508 на стовпі з іншого боку дороги, так само, як це було зроблено для пасивної мітки OPP130, замінюючи місцями ЛТЗ з вантажівкою, щоб ЛТЗ не був у зоні прямої видимості з RFID-мітками.

Розповсюдження енергії поля сигналу від активних RFID-міток SAAT T508 при встановленні їх з двох боків 4-х смугової дороги наведено на рис. 2.10.

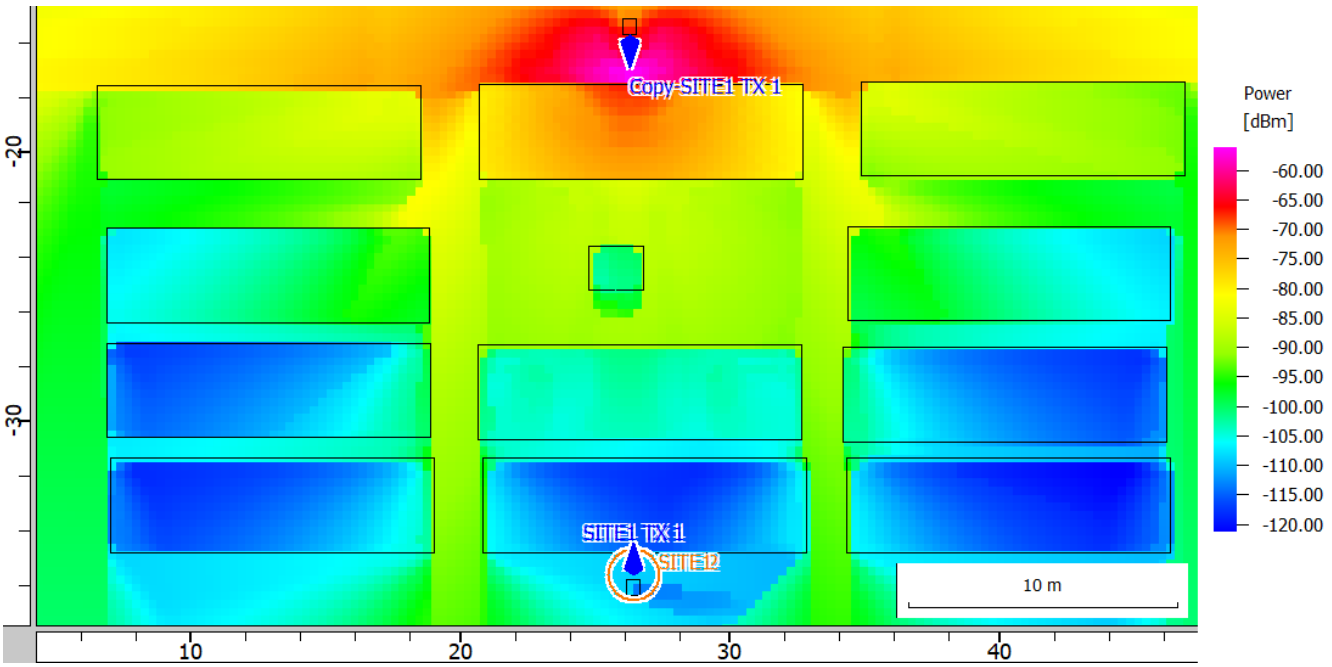


Рисунок 2.10 – Розподіл інтенсивності поля сигналу активної RFID-мітки SAAT T508 при встановленні міток з обох боків дороги

Як випливає з рис. 2.10, після встановлення додаткової активної RFID-мітки SAAT T508 рівень сигналу в області знаходження ЛТЗ збільшилася до -83 дБм, що дає змогу ЛТЗ отримати і обробити сигнал від мітки встановленої край дороги.

Після проведення дослідження з використанням активних RFID-міток можна зробити висновок, що при інтеграції цих міток на дорожні знаки з обох боків дороги можна забезпечити енергію поля, якої буде достатньо для отримання інформації від міток навіть в умовах щільного трафіку.

Недоліком використання даних міток є те, що вони мають активне джерело живлення яке розряджається і потребує періодичної заміни. Але оскільки термін безперервної роботи розглянутої мітки складає 3 роки без заміни джерела живлення, то це не викликає значних витрат на підтримку такої дорожньої інфраструктури. До того ж такі мітки автоматично формують сигнал про низький заряд батареї живлення, що дозволяє своєчасно здійснювати її заміну. Тому, їх доцільно застосовувати на багатосмугових дорогах в умовах щільної забудови.

Висновки до розділу 2

В результаті аналізу розповсюдження енергії поля від RFID-міток було визначено, що використання пасивних RFID-міток для інформування водіїв недостатньо для доріг, що мають дві та більше смуг руху в один бік. Такі мітки доцільно використовувати для доріг з однією смугою руху в одному напрямку або для доріг з двома смугами руху в одному напрямку за умови встановлення міток на дорожні знаки з обох боків дороги.

Встановлено, що використання активних RFID-міток дає змогу інформувати транспортні засоби на дорогах, які мають більше ніж 2 смуги руху в одному напрямку. Для доріг з однією та двома смугами руху в одному напрямку буде достатньо інтеграції однієї активної RFID-мітки на дорожній знак. Для доріг з трьома та чотирма смугами руху в одному напрямку необхідно інтегрувати активні RFID-мітки з двох боків дороги для забезпечення надійного зв’язку.

При кількості смуг більше чотирьох в одному напрямку доцільно використовувати додаткові активні мітки на підвісних дорожніх знаках або світлофорах.

3 ВИКОРИСТАННЯ ДОРОЖНІХ СТАНЦІЙ DSRC ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ РУХУ В УМОВАХ МІСЬКОЇ ЗАБУДОВИ

3.1 Актуальність проведення дослідження технології DSRC у smart-місті

Наразі перед людством постала дуже серйозна проблема, пов’язана зі зростанням кількості аварій на автомагістралях та дорогах загального користування. Неуважність водіїв, нехтування правилами дорожнього руху, вплив деяких лікарських засобів, що погіршують реакцію лише збільшують кількість аварійних ситуацій на дорогах. Використання безпроводових технологій зв'язку між транспортними засобами та пішоходами, дозволяє значно знизити ризики дорожньо-транспортних пригод.

У 1999 році FCC (федеральна комісія зв’язку Сполучених Штатів Америки) виділила діапазон частот від 5850 МГц до 5925 МГц спеціально для технології безпроводових мереж малого радіусу дії (Dedicated Short Range Communication – DSRC). Технологія DSRC є частиною системи зв’язку WAVE (Wireless Access for Vehicular Environment). Фізичний рівень та канальний рівні моделі OSI системи DSRC визначені в сімействі стандартів IEEE 802.11 і IEEE 1609.x.. Основною перевагою технології DSRC є швидке з’єднання між пристроями та мала затримка передавання пакетів, що досягається завдяки використанню протоколу WSMP (Wave Short Message Protocol) на транспортному рівні моделі OSI. Ці особливості технології DSRC дозволяють побудувати безпроводову систему попередження водіїв та пішоходів про можливу небезпеку, що в свою чергу дозволить зменшити кількість дорожньо-транспортних пригод.

Використання технології DSRC для встановлення зв'язку між дорожньою інфраструктурою, пішоходами та транспортними засобами, дозволяє суттєво зменшити вірогідність виникнення дорожньо-транспортних пригод та дозволяє посилити контроль функціонування транспортної мережі міста.

Важливою умовою для використання технології DSRC є забезпечення мережі надійним зв’язком на великій відстані, оскільки об’єктами системи виступають

високошвидкісні транспортні засоби. Через низький рівень сигналу може виникнути затримка у ідентифікації об’єкту системи, що у свою чергу може призвести до виникнення аварійної ситуації. В той же час, дорожні станції в системі DSRC, які призначені для автоматизованого контролю транспортних засобів на пунктах пропуску безоплатного проїзду та до парко місць, можуть бути використані для підвищення безпеки руху у зонах з обмеженою видимістю. Такі зони в умовах щільної забудови завжди існують у містах і є зонами підвищеної небезпеки руху.

Пристрої стандарту IEEE 802.11p забезпечують дальність зв'язку до 1000 м, при швидкості транспортних засобів до 200 км/год та за відсутності завад у каналі передавання даних. Перешкоди у вигляді будівель не тільки заважають водієві бачити інші транспортні засоби, але й перешкоджають поширенню сигналу від пристроїв DSRC. Отже, зв'язок між транспортними засобами при наявності забудови між ними може бути відсутнім. Оскільки сліпий кут є одним з критичних місць, де легко можуть статися аварії, пристрої DSRC допоможуть сповістити водія про небезпеку.

Під сліпим кутом мається на увазі відсутність прямого бачення транспортних засобів через перешкоду у вигляді будівлі. В рамках роботи [46] було проведено дослідження технології DSRC у "сліпому куті". Дослідження проводилось з двома транспортними засобами, обладнаних пристроями DSRC, що рухалися назустріч з однаковою швидкістю і знаходились на однаковій відстані від перехрестя. Аналіз проводився для різних умов – з щільною забудовою та з малою щільністю забудови. На рис. 3.1 наведено схему проведення тестування технології DSRC у "сліпому куті".

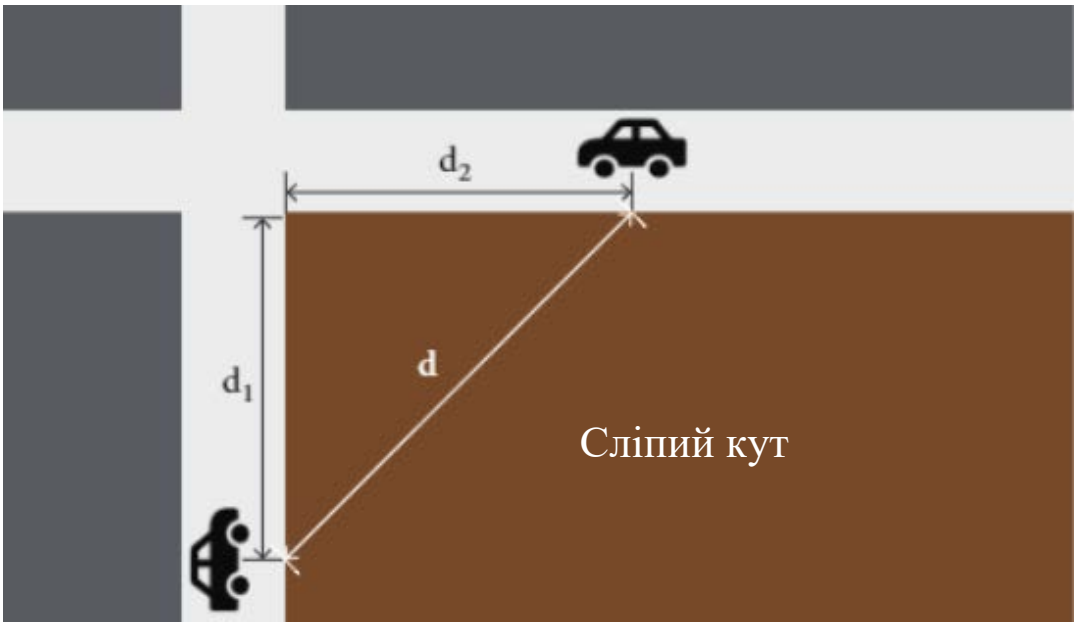
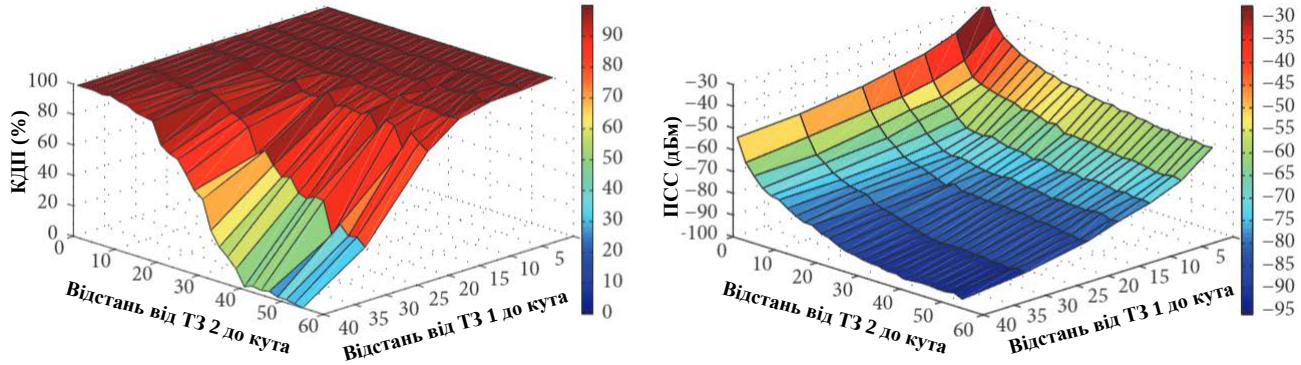


Рисунок 3.1 – Схема для проведення дослідження технології DSRC у "сліпому куті"

На рис.3.2 наведено результат тестування технології DSRC у "сліпому куті" при забудові з малою щільністю забудови.



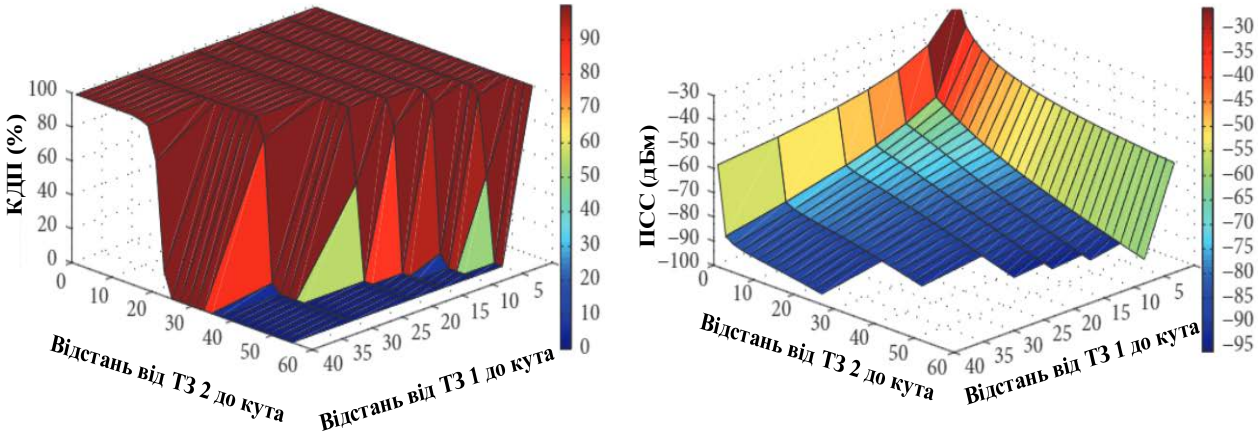
а) *б)*

Рисунок 3.2 – Результат тестування технології DSRC у "сліпому куті" при забудові з молою щільністю

Як випливає з рис. 3.2 пристрої DSRC мають високі показники коефіцієнту доставлених пакетів (КДП на рис. 3.2) та рівня сигналу (РС на рис. 3.2) тільки коли знаходяться на відстані до 30 метрів від перехрестя. Після досягнення відстані у 30

м від перехрестя обома транспортними засобами, спостерігається суттєве зменшення рівня сигналу та відсотку доставлених пакетів.

На рис. 3.3 наведено результат тестування технології DSRC у "сліпому куті" при щільній забудові.



а) *б)*

Рисунок 3.3 – Результат тестування технології DSRC у "сліпому куті" при щільній забудові

Як випливає з рис. 3.3, показники рівня сигналу та відсотку доставлених пакетів суттєво зменшуються після досягнення відстані у 5 метрів від перехрестя обома транспортними засобами. З цього можна зробити висновок, що при щільній забудові розповсюдження сигналу від пристроїв DSRC суттєво зменшується і система DSRC потребує встановлення додаткового обладнання.

Вплив міської забудови на розповсюдження енергії сигналу від пристроїв DSRC є дуже вагомим. Проведені дослідження відбиття хвиль сигналу від будівель та проходження сигналу крізь будівлі [47, 48, 49] показали, що сигнал може розповсюджуватись на дальні відстані завдяки явищам дифракції та відбиття, проте немає проведених досліджень розповсюдження енергії сигналу від пристроїв DSRC у гірших умовах зв’язку.

3.2 Вибір обладнання DSRC для проведення моделювання розповсюдження енергії поля

Для аналізу характеристик поля сигналів в системі DSRC необхідно враховувати параметри вже існуючого обладнання для побудови такої системи. Для моделювання було обрано модуль OBU-301U компанії "Unex" [50]. Зовнішній вигляд безпроводового модуля DSRC наведено на рис. 3.4.

Основні характеристики бортового модуля DSRC OBU-301U:

- діапазон робочих частот 5,850…5,925 ГГц;
- канали: 172, 174, 176, 178, 180, 182, 184;
- швидкість передачі даних: 3, 4.5, 6, 9, 12, 18, 24, 27 МБ/с для 10 МГц;
- потужність передавача 20 дБм;
- чутливість приймача -92 дБм;
- діапазон робочих температур -40…+85 °С;
- габаритні розміри: 103 × 95 × 31 мм.

Рисунок 3.4 – Зовнішній вигляд безпроводового модуля DSRC OBU-301U

В якості дорожньої станції DSRC, встановленої у дорожній інфраструктурі, була обрана станція RIS-9160 австрійської компанії "Kapsch" [51]. Зовнішній вигляд дорожньої станції DSRC наведено на рис. 3.5.

Основні характеристики дорожньої станції DSRC RIS-9160:

- діапазон робочих частот 5,850…5,925 ГГц;
- канали 172, 174, 176, 178, 180, 182, 184;
- потужність передавача 21 дБм;
- чутливість приймача -95 дБм;
- швидкість передачі даних 6 Мбайт/с;
- діапазон робочих температур -40…+85 °С;
- габаритні розміри 290 × 200 × 78 мм.

Рисунок 3.5 – Зовнішній вигляд дорожньої станції DSRC RIS-9160

3.3 Аналіз розповсюдження сигналу пристроїв DSRC

Моделювання розповсюдження енергії поля в умовах міста в системі DSRC проводилось в програмі Altair WinProp.

У моделі на рис. 3.6 транспортні засоби розташовані у найбільш складному випадку взаємного розташування автомобілів та будинків.

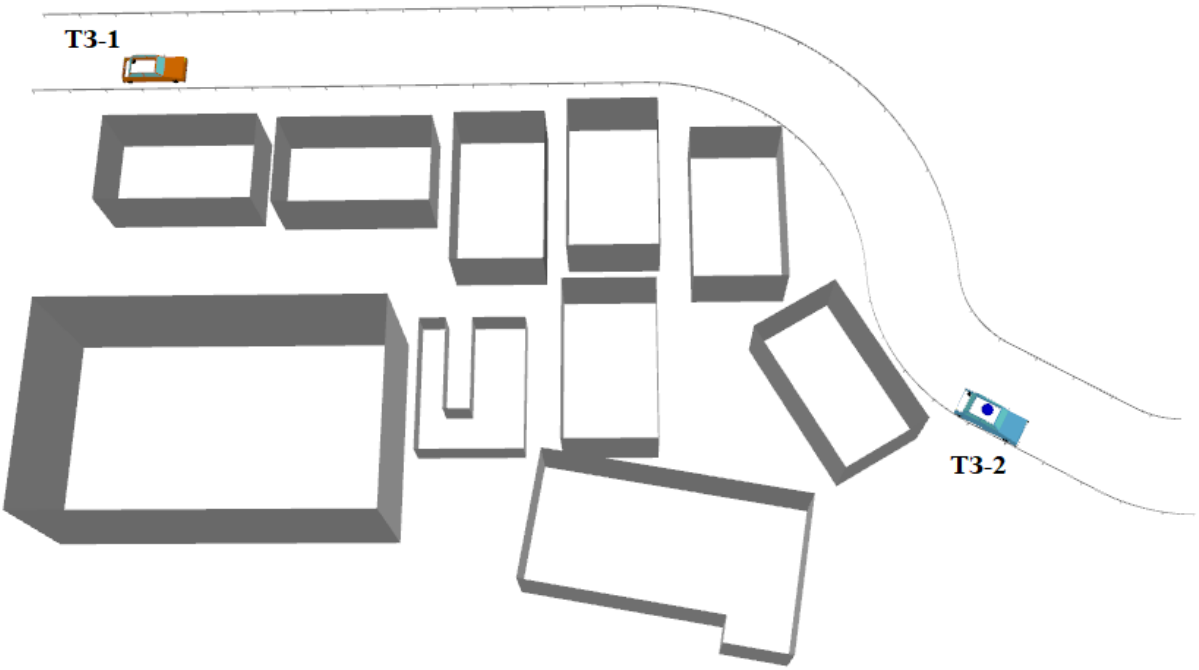


Рисунок 3.6 – Розташування транспортних засобів для найбільш складного випадку взаємного розташування цих об'єктів

Транспортні засоби знаходяться поза зоною прямої видимості. Між ними розташована велика кількість різних об'єктів міської забудови. Транспортний засіб 1 (далі ТЗ-1) здійснює рух у напрямку транспортного засобу 2 (далі ТЗ-2), що стоїть припаркований на дорозі загального користування. Обидва транспортні засоби оснащені пристроями DSRC OBU-301U. При моделюванні матеріалом будівель обрано бетон, щоб перевірити зону впевненого прийому сигналу при обміні даними в системі DSRC для випадку найбільшого загасання сигналу. Розподіл потужності поля, що випромінює модуль ТЗ-2 наведено на рис. 3.7.

Згідно результатів моделювання рівень сигналу в точці розташування ТЗ-1 дорівнює -110 дБм. А оскільки чутливість приймача модуля DSRC складає -92 дБм, то ТЗ-1 не отримає інформацію про місцезнаходження ТЗ-2. Для прикладу, що розглядається, відстань між транспортними засобами становить 80 м.

Для того щоб з’ясувати на якій максимальній відстані модуль, встановлений на ТЗ-1, зможе прийняти і обробити сигнал, отриманий від модуля ТЗ-2, включено режим з двома градаціями потужності сигналу – більше та менше -92 дБм. Цей

рівень відповідає чутливості приймачів модулів OBU-301U. Розподіл інтенсивності поля сигналу при двох градаціях потужності наведено на рис. 3.8.

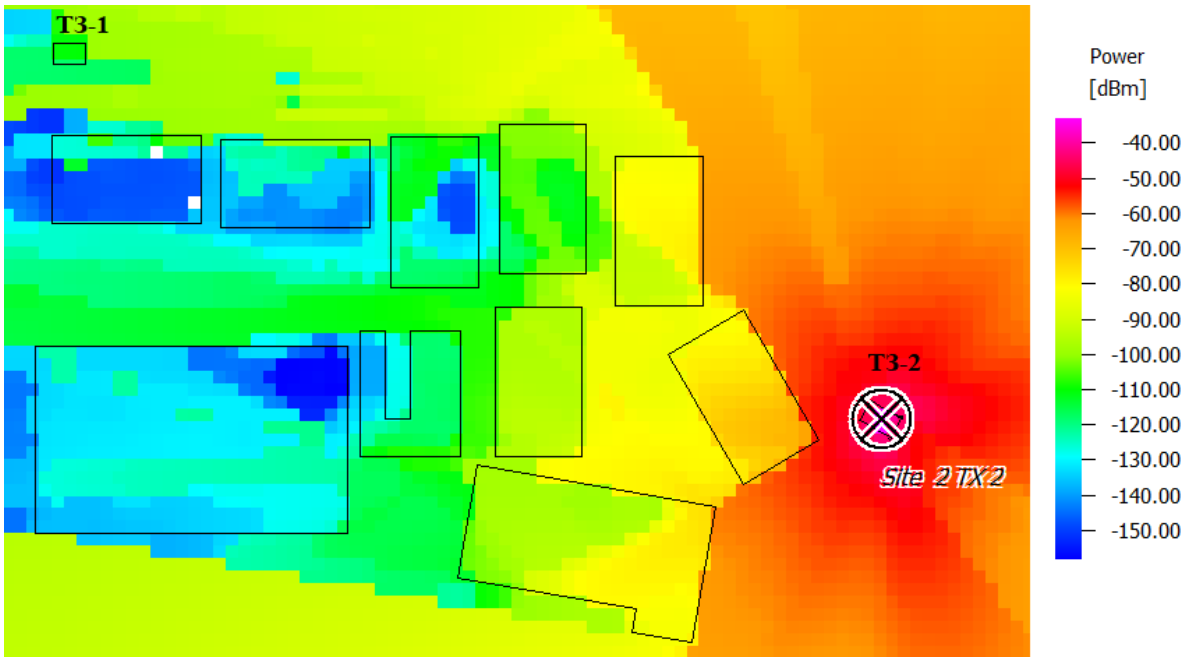


Рисунок 3.7 – Розподіл інтенсивності поля сигналу при двох градаціях потужності

Рисунок 3.8 – Розподіл інтенсивності поля модуля OBU-301U при двох градаціях потужності

З результатів моделювання випливає, що ТЗ-1 не потрапляє у зону з рівнем сигналу більшим ніж -92 дБм. Максимальна відстань на якій ТЗ-1 може ідентифікувати ТЗ-2 становить 60 м (точка А на рис. 3.8). Використавши формулу розрахунку гальмівного шляху можна знайти відстань на якій ТЗ-1 зможе завершити свій гальмівний шлях після отримання координат від ТЗ-2:

$$S = \frac{V^2}{250 \cdot K} \tag{1}$$

де V – швидкість автомобіля, K – коефіцієнт зчеплення коліс з асфальтом (0.8 при умові сухого асфальту, 0.4 при умові вологого асфальту, 0.1 при умові голольоду).

Якщо ТЗ-1 рухається зі швидкістю 60 км/год, його гальмівний шлях становитиме:

$$S = \frac{V^2}{250 \cdot K} = \frac{60^2}{250 \cdot 0.8} = 18\,\text{м} \tag{2}$$

За умови сухого асфальту та миттєвої реакції водія на повідомлення від системи DSRC про небезпеку зіткнення, вдасться уникнути аварії з ТЗ-2. Проте, за умови наявності льоду на асфальті, гальмівний шлях збільшиться і буде дорівнювати:

$$S_2 = \frac{V^2}{250 \cdot K} = \frac{60^2}{250 \cdot 0.1} = 144\,\text{м} \tag{3}$$

За умови льодового покриття на асфальті, ТЗ-1 не зможе завчасно отримати повідомлення про небезпеку, тому необхідне збільшення рівня сигналу DSRC в умовах щільної міської забудови. Для збільшення рівня сигналу на ділянках з обмеженою видимістю пропонується встановлювати дорожні станції DSRC на цих ділянках таким чином, щоб забезпечите максимальну зону покриття у небезпечних, з точки зору ДТП, місцях.

При встановленні дорожньої станції DSRC на стику ділянок з обмеженою видимістю отримано розподіл енергії поля, випромінюваного її передавачем, що наведений на рис. 3.9.

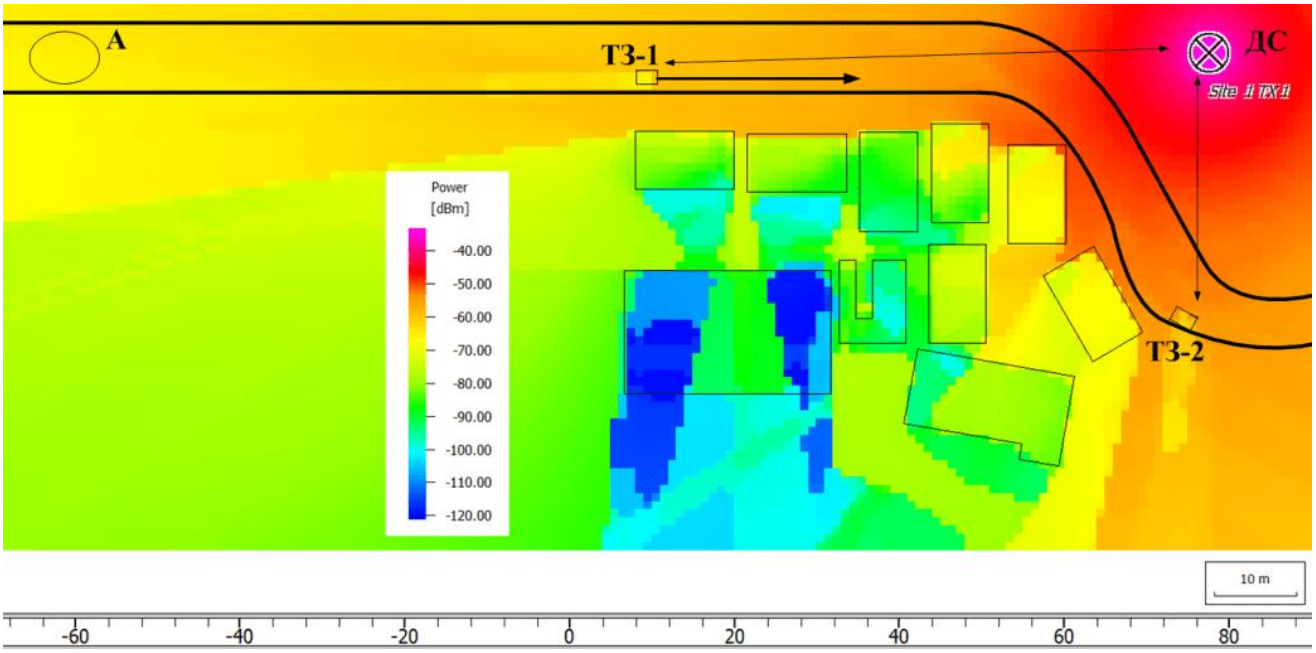


Рисунок 3.9 – Розподіл інтенсивності поля, випромінюваного передавачем дорожньої станції DSRC

Як слідує з рис. 3.9, зона покриття після встановлення дорожньої станції DSRC (ДС) суттєво збільшилась, що дозволяє збільшити час для прийняття рішення водієм у декілька разів.

За принципом роботи системи DSRC, ТЗ-2 відправляє повідомлення про своє місце знаходження усім іншим пристроям, що потрапляють у зону покриття сигналу модуля DSRC. В зону дії модуля ТЗ-2 потрапляє лише дорожня станція DSRC, яка ретранслює повідомлення від ТЗ-2 і відправляє його координати всім транспортним засобам, що потрапляють у її зону дії. Дорожня станція встановлена у зоні прямої видимості модулів, тому рівень сигналу від її модуля для обох транспортних засобів складає не менше ніж -66 дБм. Такий рівень сигналу дозволяє ТЗ-1 своєчасно отримати повідомлення про місцезнаходження ТЗ-2 і уникнути зіткнення навіть при наявності ожеледиці.

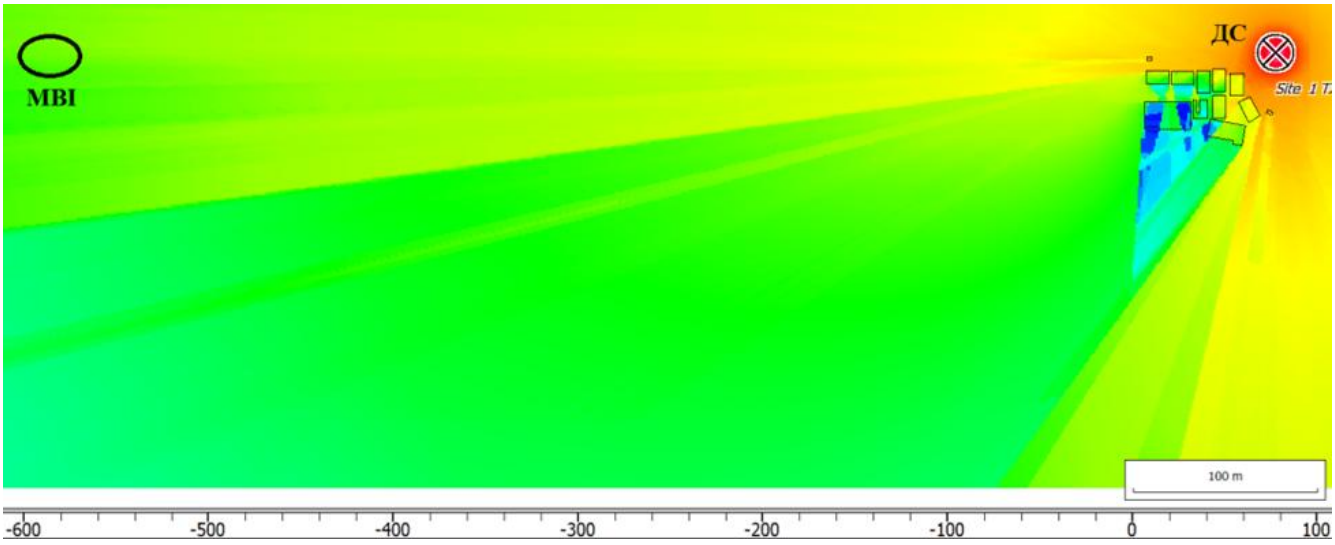


Рисунок 3.10 – Розподіл енергії поля, випромінюваного передавачем дорожньої станції DSRC

Як випливає з рис. 3.10, максимальна відстань інформування водіїв у випадку відсутності завад становить близько 700 м. У дослідженні не було враховано завади у вигляді дерев, машин, людей та інших об’єктів дорожньої інфраструктури. При врахування усіх видів завад розподіл енергії поля буде іншим, що призведе зменшення максимальної відстані виявлення іншого транспортного засобу. Встановлення дорожніх станцій в умовах обмеженої видимості збільшує максимальну відстань інформування, що надає змогу зупинити свій транспортний засіб завчасно без виникнення аварійної ситуації.

Висновки до розділу 3

Проведений аналіз можливостей системи DSRC для своєчасного попередження водіїв транспортних засобів про можливість зіткнення в умовах щільної міської забудови показав, що в умовах обмеженої видимості пристроїв DSRC, встановлених на транспортних засобах, недостатньо для забезпечення своєчасного інформування водіїв.

Для усунення цього недоліку запропоновано встановлювати дорожні станції DSRC у зонах обмеженої видимості у якості повторювачів (ретрансляторів)

сигналів транспортних засобів. Це дає змогу на відрізках з прямою видимістю збільшити відстань впевненого зв'язку у декілька разів, що в свою чергу дозволить завчасно отримати повідомлення про небезпеку. Своєчасне попередження про наявність інших транспортних засобів на дорогах особливо важливо в умовах мокрого або покритого льодом дорожнього полотна.

4 ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ WI-FI ПРИ ПОБУДОВІ ТРАНСПОРТНОЇ МЕРЕЖІ SMART-МІСТА

4.1 Актуальність проведення дослідження технології Wi-Fi у smart-місті

Технології Інтернету речей стрімко розвиваються та займають передові позиції при побудові нових інтелектуальних систем безпеки. "Розумні будинки" та "розумна техніка" дозволяють уникати пожеж, завчасно попереджають про небезпеку та захищають будинок від шахраїв. Однак наразі існує дуже багато аварій на дорогах, в яких страждають як водії так і пішоходи. Більшість дорожньо-транспортних пригод можна було б уникнути, якщо б пішохід або водій були завчасно попереджені про можливу небезпеку зіткнення. Пристрої DSRC можуть створювати mesh-мережу з пристроїв, що встановлені в транспортних засобах та дорожній інфраструктурі, і своєчасно інформувати водіїв про небезпеку зіткнення. Однак пішоходи невидимі для такої мережі DSRC, а отже небезпека аварій від зіткнення з пішоходами (особливо у темні години) залишається високою. Оскільки наразі у 99% пішоходів є смартфон з Wi-Fi модулем доцільно розглянути можливість застосування технології Wi-Fi для попередження пішоходів і водіїв транспортних засобів про можливість зіткнення.

Навіть при наявності пішохідного переходу, перехід через дорогу не завжди є безпечним, оскільки пішоходи дуже часто потрапляють до "сліпих зон" транспортних засобів. Транспортні засоби, що запарковані дуже близько до пішохідних переходів з порушенням правил дорожнього руху, дуже часто стають причинами раптової появи пішохода в зоні видимості інших учасників дорожнього руху, через що може статися аварія. Задля безпечного пересування транспортного засобу та переходу дороги пішоходом необхідно, щоб всі учасники дорожнього руху мали інформацію про місцезнаходження один одного.

У дослідженні [37] показано, що при швидкості руху транспортних засобів до 80 км/год немає суттєвого впливу на затримки передавання пакетів пристроями

Wi-Fi та DSRC. Отже технологія Wi-Fi може використовуватися у міських умовах, де швидкість транспортних засобів не повинна перевищувати 80 км/год.

У роботі [38] показано, що при швидкості близько 80 км/год швидкість передавання даних по мережі Wi-Fi падає до 1 Мбіт/с. Проте цієї швидкості буде цілком достатньо для обміну даними у транспортній мережі. При використанні технології Wi-Fi можна виявляти місцезнаходження об'єктів. Здійснюючи моніторинг рівня сигналу від пристроїв Wi-Fi [40, 41], можна виявляти координати пішоходів та транспортних засобів без залучення GPS сервісів.

У роботі [39] показано, що технологія Wi-Fi програє технології DSRC у швидкості з'єднання пристроїв та у затримці передавання пакетів даних, проте має більшу пропускну здатність, що можна використати як значну перевагу у місцях скупчення людей, особливо на пішохідних переходах.

Проведений аналіз наукових статей по розвантаженню Wi-Fi мереж через стільниковий зв'язок у роботах [34, 35, 36] показав, що Wi-Fi мережу можна розвантажити у складних випадках в місцях великого скупчення людей. У роботі [52] запропоновано метод об'єднання технології Wi-Fi та WiMax, що дає змогу утворити одну спільну комбіновану мережу. В рамках дослідження [53] представлено гібридну систему DSRC/Wi-Fi та експериментально оцінено її продуктивність. В [54] було показано, що покриття однієї точки доступу буде достатньо для забезпечення неперервним зв'язком протягом 10 с транспортний засіб, що рухається зі швидкістю 180 км/год. Однак на границях зон покриття з'являється проблема з великими втратами пакетів через послаблений сигнал від точки доступу. Поки транспортний засіб з'єднається з іншою точкою він подолає велику відстань, через що на деякий час зникне з видимості інших пристроїв транспортної системи, що може привезти до виникнення аварійної ситуації.

Для подолання цього недоліку пропонується організувати "безшовне" покриття для забезпечення надійного зв'язку вздовж доріг між пристроями Wi-Fi, встановленими на транспортних засобах, та пристроями пішоходів. "Безшовна" мережа Wi-Fi дозволить уникнути втрат часу при перемиканні між точками доступу Wi-Fi і зменшить ризики зіткнення на дорогах. При побудові безшовного

покриття на дорогах та тротуарах необхідно розрахувати максимальну відстань між точками доступу Wi-Fi та мінімальний рівень сигналу, при якому якість каналу передавання даних буде достатньою для надійного зв’язку.

Згідно з принципом організації безшовного Wi-Fi, точки доступу з’єднуються мережевим кабелем до контролера, через який відбувається керування безпроводовою безшовною мережею. На рис. 4.1 наведено приклад організації безшовного зв’язку Wi-Fi.

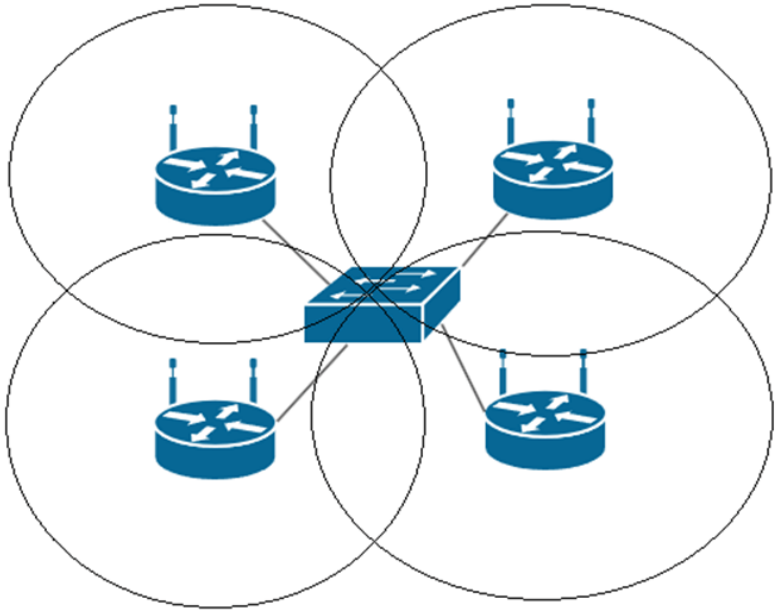


Рисунок 4.1 – Приклад організації безшовного зв’язку Wi-Fi

Час з’єднання пристроїв Wi-Fi з точкою доступу складає приблизно 2 с. Отже, коли транспортний засіб виїжджає з зони дії Wi-Fi точки йому потрібно приблизно 2 с для організації зв’язку з наступною точкою доступу. При швидкості 50 км/год за 2 с транспортний засіб встигне проїхати приблизно 28 м без надання інформації про своє місцезнаходження, напрямок та швидкість руху, що може привести до виникнення аварійної ситуації. Для усунення цієї проблеми пропонується організувати безшовне покриття Wi-Fi вздовж дороги. При безшовному покритті переключення між точками доступу відбувається приблизно за 50 мс, що дає змогу не втрачати зв’язок між пристроєм пішохода/транспортного засобу та точкою

доступу. Приклад організації безшовного зв’язку Wi-Fi вздовж дороги наведено на рис. 4.2.

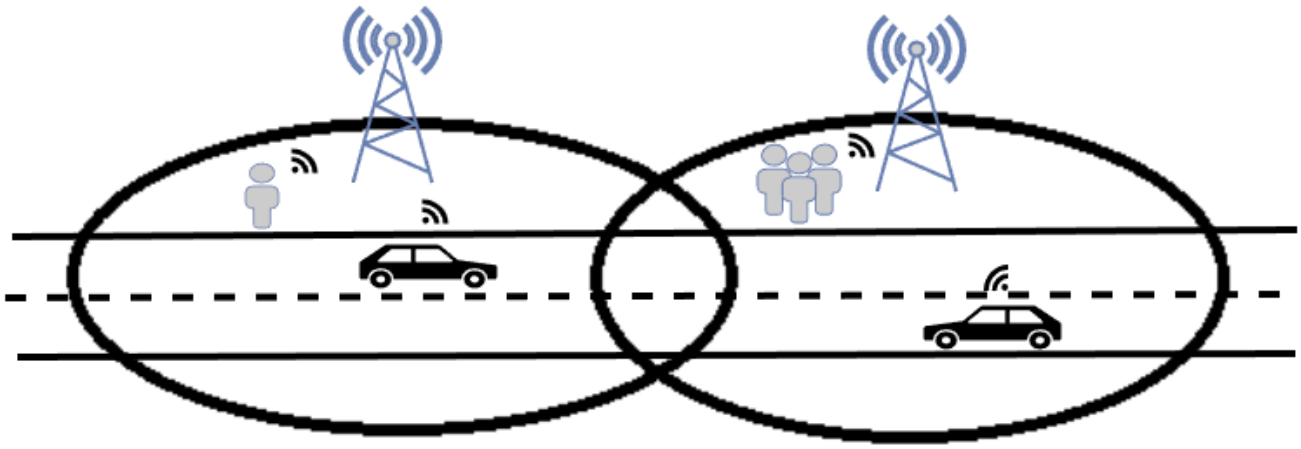


Рисунок 4.2 – Приклад організації безшовного зв’язку Wi-Fi вздовж дороги

Як випливає з рис. 4.2 транспортні засоби, що рухаються по дорозі та пішоходи, що йдуть вздовж дороги, не будуть виходити з зони покриття точок доступу Wi-Fi. Згідно з принципом роботи безшовного Wi-Fi, якщо пристрій буде знаходитись у зоні перетину покриття від декількох точок, то підключення буде здійснюватися до точки доступу з найвищим півнем сигналу [3].

Однією з проблем при побудові безшовного покриття є розрахунок максимальної відстані між точками доступу та розрахунок рівня сигналу для забезпечення зв'язку без втрат та затримок при передачі пакетів даних.

4.2 Тестування безшовної мережі Wi-Fi

Для визначення максимальної відстані між точками доступу для організації безшовної мережі Wi-Fi проведено експериментальне дослідження. Для тестування мережі було задіяно 2 Wi-Fi маршрутизатора “Mikrotik HAP AC^2”, що з’єднані між собою витаю парою (UTP-кабелем). Схема для проведення тестування безшовного зв’язку Wi-Fi зображено на рис. 4.2.

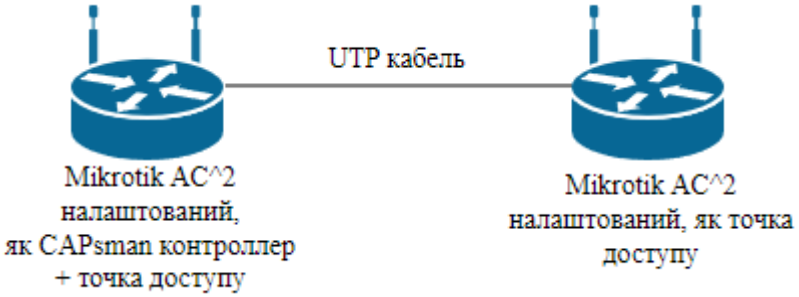


Рисунок 4.2 – Схема для проведення тестування безшовного зв’язку

Один з маршрутизаторів налаштовано в режимі контролера “CAPSman” та точки доступу. Другий маршрутизатор налаштовано у режимі точки доступу. Налаштування обладнання проводилося за допомогою ноутбуку та програмного середовища “WinBox”. Версія прошивки маршрутизаторів – RouterOS 7.11.2.

Характеристики маршрутизатора “Mikrotik HAP AC^2” [55]:

- живлення 12..30 В;
- вихідна потужність модуля Wi-Fi: при частотах 2400…2483.5 МГц – 20 дБм; при частотах 5150…5250 МГц – 23 дБм; при частотах 5250…5350 МГц – 20 дБм; при частотах 5470…5725 МГц – 27 дБм;
- стандарти Wi-Fi: ac, b, g, n.

4.2.1 Налаштування контролера безшовної мережі CAPSman

Порядок налаштування безшовного Wi-Fi “CAPsman”:

1. Першочергово проведено налаштування безпеки Wi-Fi мережі. Налаштовано профіль безпеки із встановленням шифрування та паролю. Інтерфейс налаштування профілю безпеки зі вказаними параметрами наведено на рис. 4.3.

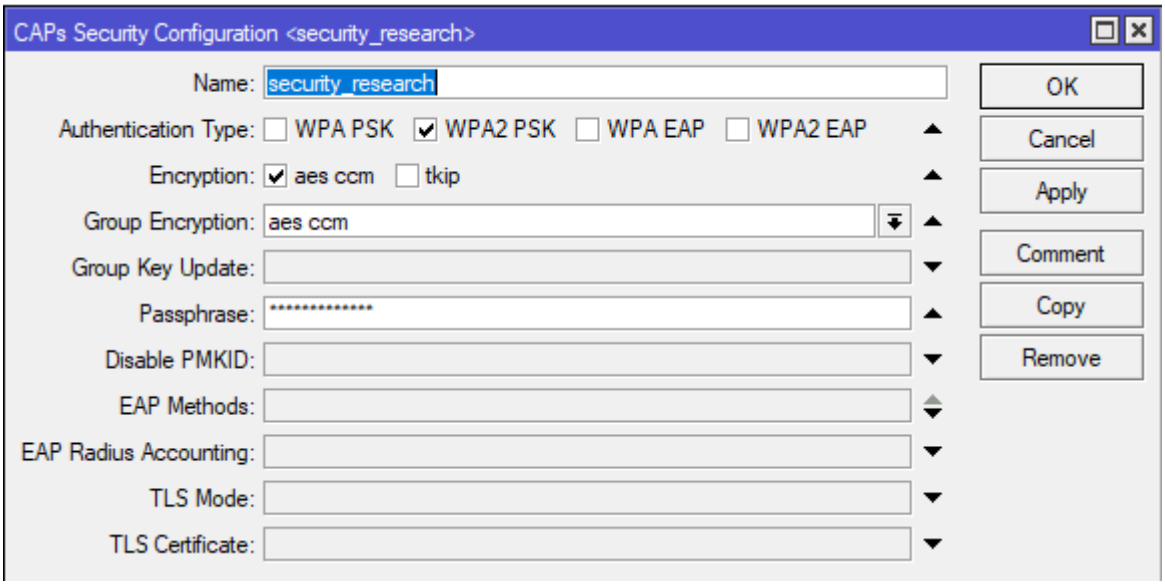


Рисунок 4.3 – Інтерфейс налаштування профілю безпеки мереж Wi-Fi

2. Проведено аналіз завантаженості частотних каналів у навколишньому середовищі для визначення частоти для проведення тестування та налаштування каналів “CAPsman” контролера. Частотний аналіз проведено командою “interface wireless frequency monitor” через термінал маршрутизатору “Mikrotik HAP AC^2”. Результат проведеного частотного аналізу задіяних та вільних каналів для Wi-Fi у діапазоні частот 5 ГГц наведено на рис. 4.4.

```
[admin@Controller] > interface wireless frequency-monitor
number: 1
Columns: FREQ, USE, NF
FREQ     USE   NF
5180MHz  2.6%  -106
5200MHz  0.3%  -107
5220MHz  0.2%  -106
5240MHz  0.1%  -106
5260MHz  0%    -106
5280MHz  0%    -106
5300MHz  0%    -106
5320MHz  0%    -106
5500MHz  0%    -103
5520MHz  0%    -104
5540MHz  0%    -104
5560MHz  0%    -103
5580MHz  0%    -104
5600MHz  0%    -104
5620MHz  2.6%  -103
5640MHz  0%    -104
5660MHz  0%    -103
5680MHz  0%    -103
5700MHz  0%    -103
```

Рисунок 4.4 – Аналіз задіяних та вільних каналів Wi-Fi у діапазоні частот 5 ГГц

Як випливає з рис. 4.4, не навантаженим залишається діапазон частот 5240…5600 ГГц та 5640…5700 ГГц. Для проведення тестування було обрано частоту 5280 ГГц.

Аналогічно проведено аналіз вільних каналів навколишнього середовища для діапазону частот 2,4 ГГц Wi-Fi. Результат аналізу у діапазоні 2,4 ГГц наведено на рис. 4.5.

```
[admin@Controller] > interface wireless frequency-monitor
number: 0
Columns: FREQ, USE, NF
FREQ     USE    NF
2412MHz  8.3%   -97
2417MHz  0.9%   -98
2422MHz  0.2%   -98
2427MHz  1.9%   -98
2432MHz  1.5%   -98
2437MHz  2%     -99
2442MHz  16.4%  -99
2447MHz  1.2%   -99
2452MHz  1.4%   -99
2457MHz  4.1%   -100
2462MHz  1.8%   -100
2467MHz  0%     -100
2472MHz  0.7%   -101
```

Рисунок 4.5 – Аналіз наявності вільних каналаів Wi-Fi у діапазоні частот 2.4 ГГц

3. Проведено налаштування каналів “CAPs Channel” та “datapath”. Для каналу “CAPs Channel” 5 ГГц було обрано назву – "research_5". Було обрано частоту – 5280 ГГц, враховуючи частотний аналіз, який наведено на рис. 4.4. Обрана ширина каналу – 20 МГц. Стандартом Wi-Fi 5 ГГц було обрано 802.11ac. На рис. 4.6 наведено web-інтерфейс налаштування "CAPs Channel" для діапазону 5 ГГц із вказаними параметрами.

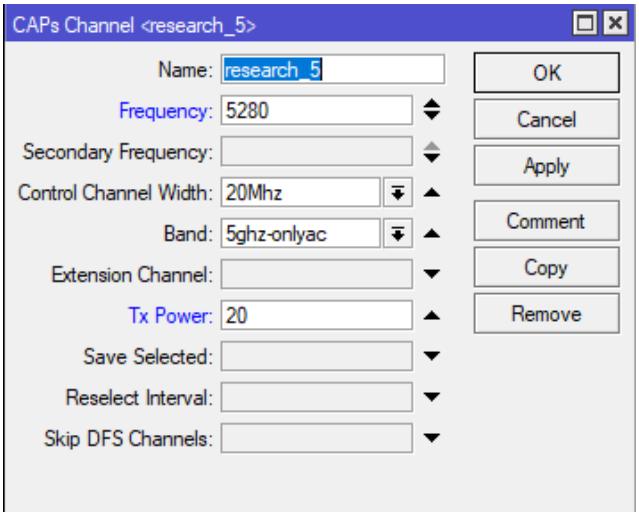


Рисунок 4.6 – Web-інтерфейс налаштування "CAPs Channel" для діапазона 5 ГГц

Аналогічно мережі Wi-Fi 5 ГГц було проведено налаштування для Wi-Fi мережі 2.4 ГГц. Для каналу “CAPs Channel” було обрано назву – "research_2.4". Було обрано частоту – 2462 ГГц. Обрана ширина каналу – 20 МГц. Стандарт Wi-Fi – 2.4 ГГц (802.11n). На рис. 4.7 наведено web-інтерфейс налаштування "CAPs Channel" для 2.4 ГГц Wi-Fi.

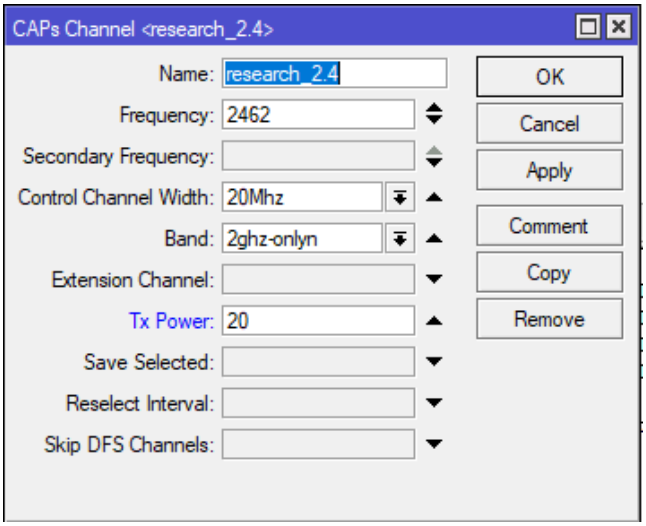


Рисунок 4.7 – Web-інтерфейс налаштування "CAPs Channel" для 2.4 ГГц Wi-Fi

Для конфігурації “datapath” обрано ім’я "datapath1" і у полі Bridge обрано "bridge". Web-інтерфейс налаштування "datapath" наведено на рис. 4.8.

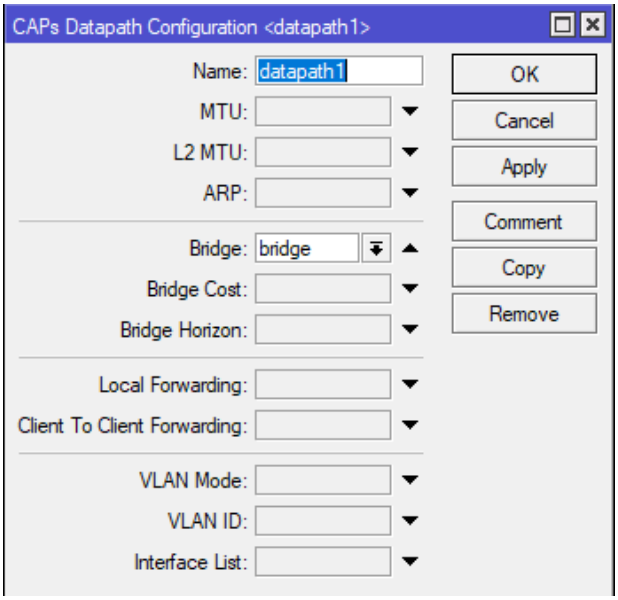


Рисунок 4.8 – Web-інтерфейс налаштування "datapath"

4. Проведено налаштування назв Wi-Fi мереж у вкладці "CAPs Configuration". Обрано режимом інтерфейсу точка доступу AP (Access Point). Обрано назву Wi-Fi мережі – "Research_2.4". Web-інтерфейс налаштування "CAPs Configuration" для частоти 2.4 ГГц наведено на рис. 4.9.

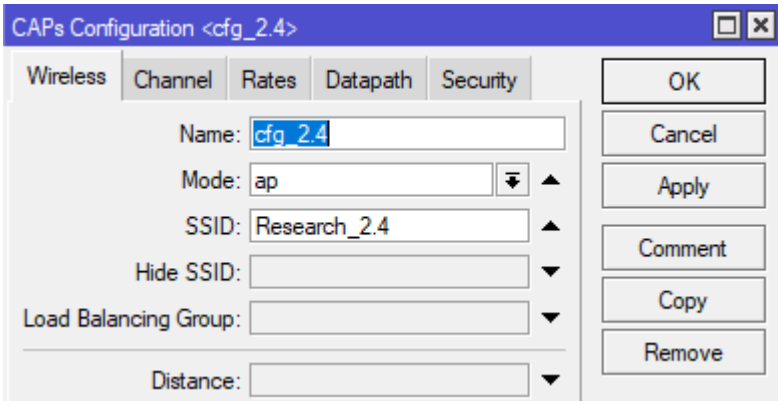


Рисунок 4.9 – Web-інтерфейс налаштування "CAPs Configuration" для Wi-Fi мережі 2.4 ГГц

Проведено налаштування також і для частоти 5 ГГц Wi-Fi. Обрано назву мережі Wi-Fi – "Research_5". Інтерфейс налаштування "CAPs Configuration" для частоти 5 ГГц наведено на рис. 4.10.

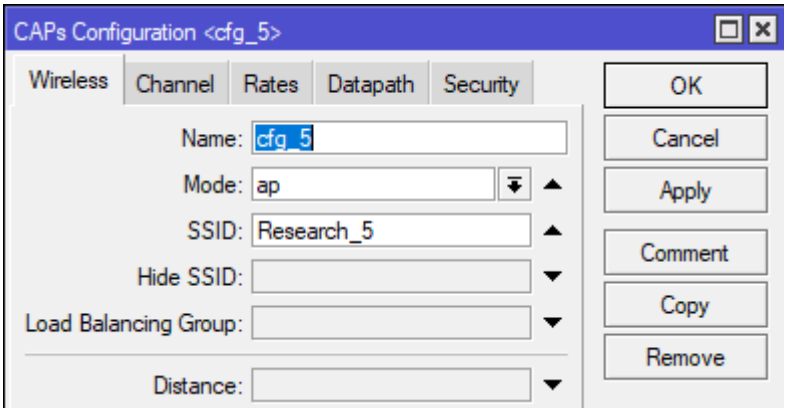


Рисунок 4.10 – Web-інтерфейс налаштування "CAPs Configuration" для мережі Wi-Fi 5 ГГц

5. Проведено налаштування параметрів розгортання безпроводової мережі у інтерфейсі "CAPs Provisioning" для 2.4 ГГц Wi-Fi. Обрано режим – "gn", оскільки дослідження для діапазону 2.4 ГГц проводиться при роботі обладнання у стандарті 802.11n. Інші налаштування: "Action" – "create dysnamic enabled", Master configuration – "cfg_2.4", Name format – cap. Web-інтерфейс налаштування "CAPs Provisioning" для частоти 2.4 ГГц з вказаними налаштуваннями зображено на рис. 4.11.

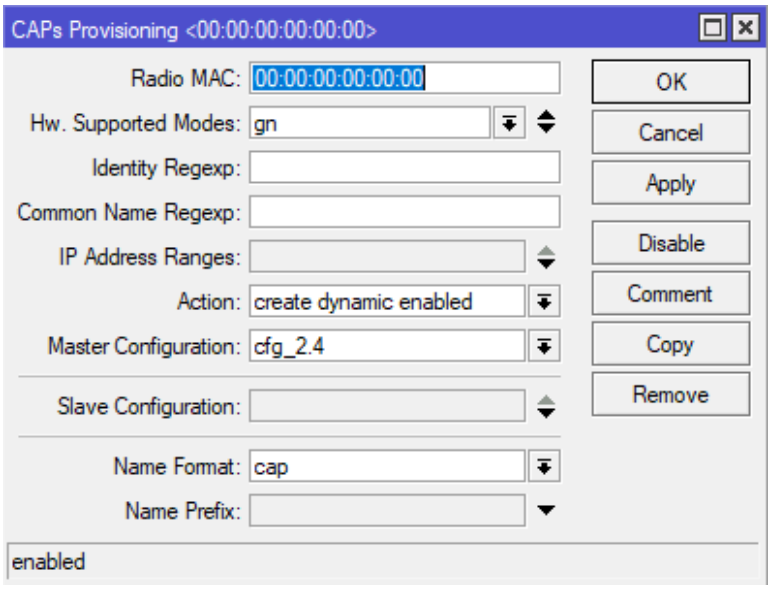


Рисунок 4.11 – Web-інтерфейс налаштування "CAPs Provisioning" для частоти 2.4 ГГц

Також проведено налаштування параметрів розгортання безпроводової мережі у інтерфейсі "CAPs Provisioning" для 5 ГГц Wi-Fi. Web-інтерфейс налаштування "CAPs Provisioning" для частоти 5 ГГц з вказаними налаштуваннями зображено на рис. 4.12.

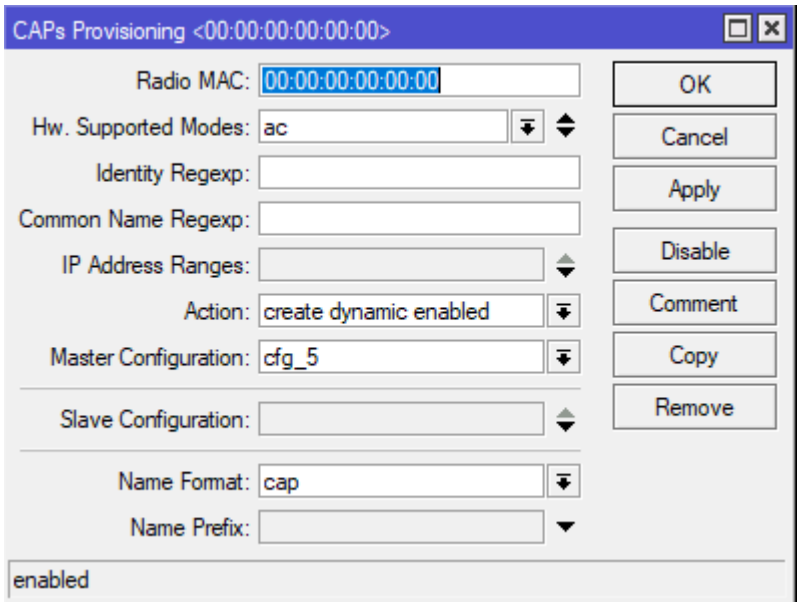


Рисунок 4.12 – Web-інтерфейс налаштування "CAPs Provisioning" для частоти 5 ГГц

6. Проведено налаштування правил мережевого екрану (Firewall). Firewall налаштовано з наступними правилами: Chain – input, Source Address Type – "local", "Destination address type" – local, Action – "accept". Web-інтерфейси налаштування вкладок Firewall: "General", "Extra" та "Action" наведено на рис. 4.13, 4.14 та 4.15 відповідно.

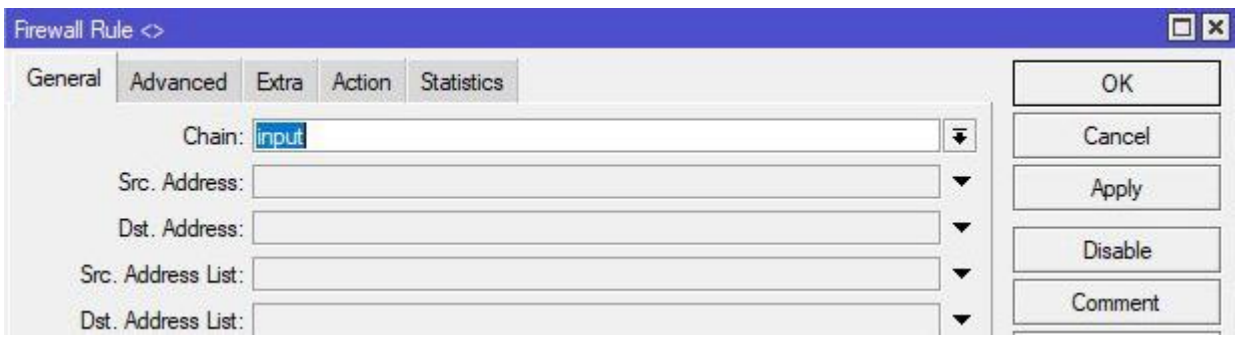


Рисунок 4.13 – Налаштування вкладки "General" правил Firewall

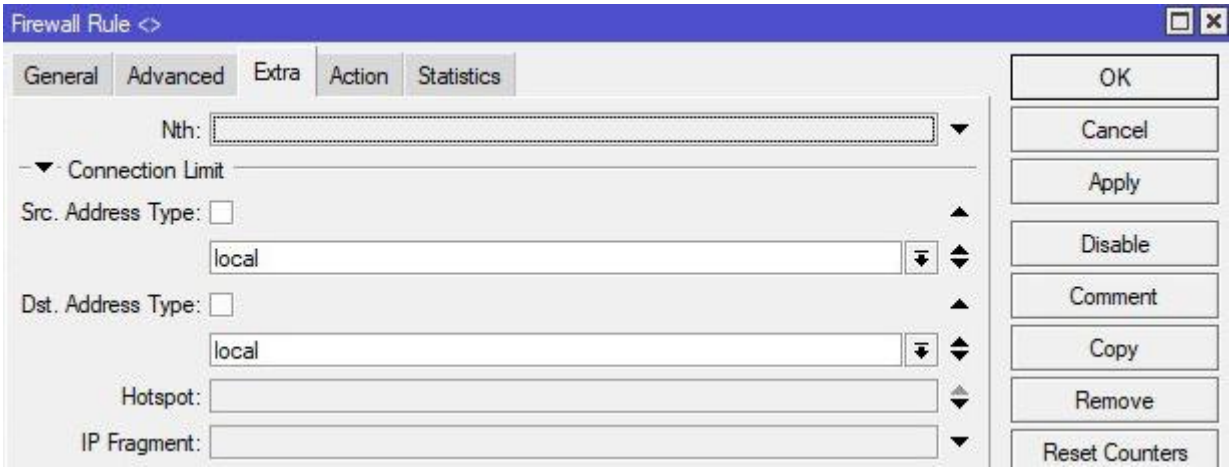


Рисунок 4.14 – Налаштування вкладки "Extra" правила Firewall

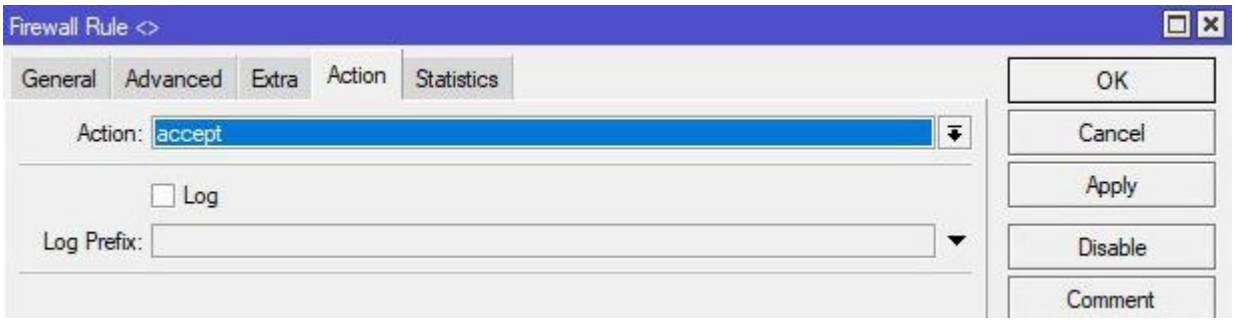


Рисунок 4.15 – Налаштування вкладки "Action" правила Firewall

Після налаштування правила Firewall йому було надано перший пріоритет у загальному списку правил Firewall. Якщо не підняти пріоритет даному правилу в загальному списку, воно може бути заблоковано одним з правил, що йдуть в прошивці RouterOS 7.11.2. Список Firewall правил зображено на рис. 4.16.

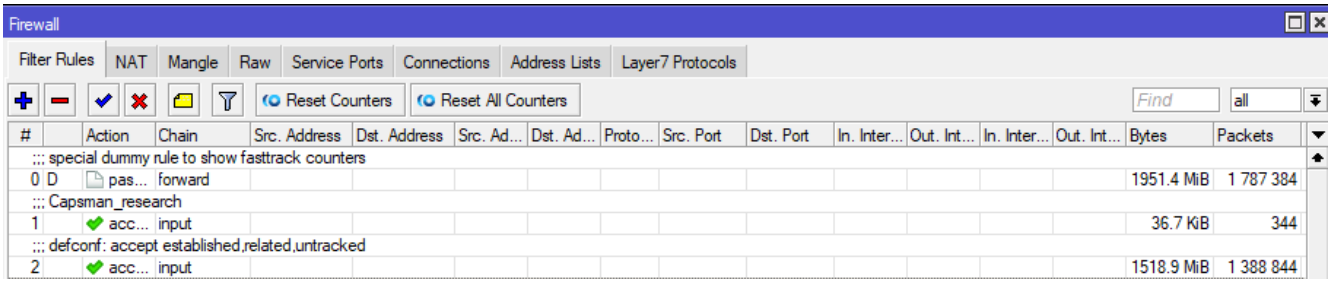


Рисунок 4.16 – Список Firewall правил контроллеру

За для уникнення випадків некоректного підключення до контролеру, відключено WAN порт (ether1) у вкладці "CAPs Manager Interfaces". Web-інтерфейс "CAPs Manager Interfaces" наведено на рис. 4.17.

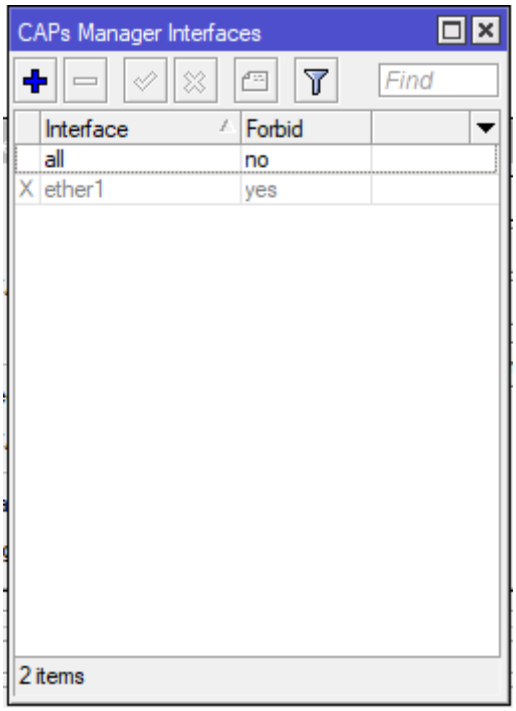


Рисунок 4.17 – Web-інтерфейс "CAPs Manager Interfaces"

7. Після налаштування маршрутизатору "Mikrotik hap AC^2" в якості контролеру “CAPsman”, було додано інтерфейси Wi-Fi мереж до контролеру CAPsman у web-інтерфейсі “CAP”, як зображено на рис. 4.18.

Налаштування “CAPsman” контролеру проведено успішно, оскільки безпроводові інтерфейси перейшли під контроль контролеру “CAPsman”, як зображено на рис. 4.19 та рис. 4.20.

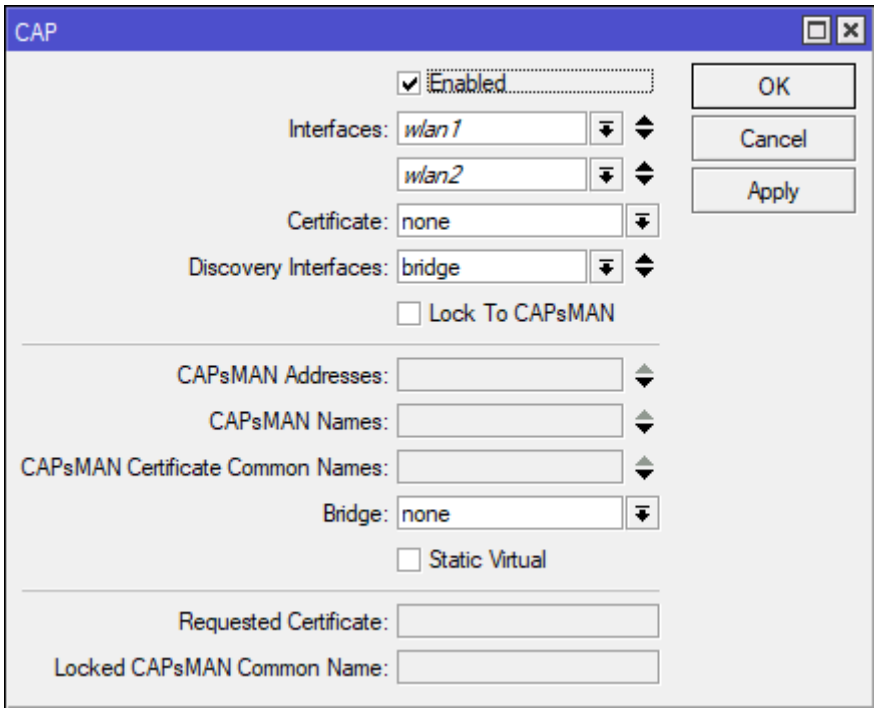


Рисунок 4.18 – Налаштування у web-інтерфейсі “CAP”

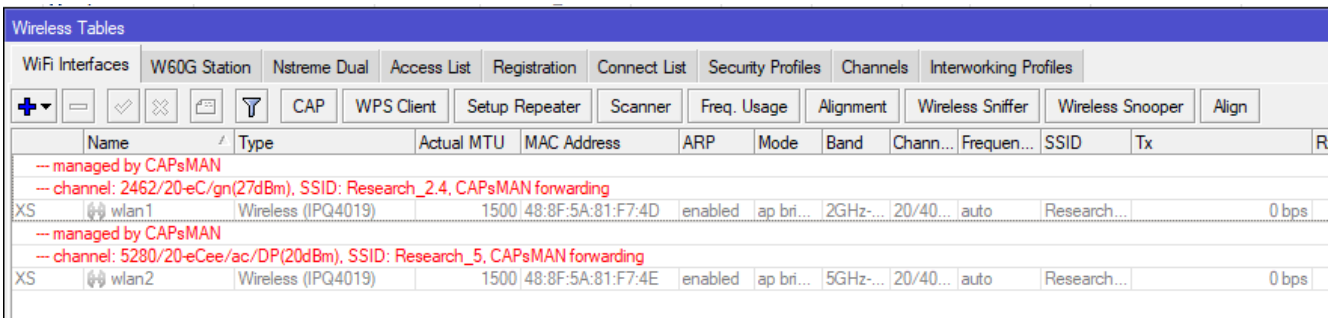


Рисунок 4.19 – Web-інтерфейс таблиці безпроводових мереж "Wireless tables"

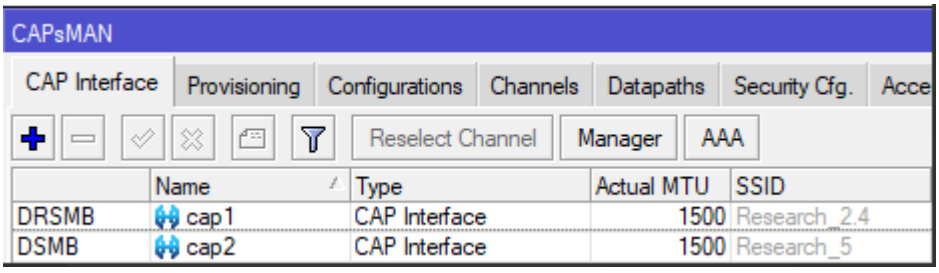


Рисунок 4.20 – Web-інтерфейс контролеру "CAPsman"

4.2.2 Налаштування точки доступу Wi-Fi Capsman

Для налаштування маршрутизатору "Mikrotik hap AC^2" в режимі точки доступу було під’єднано ноутбук кабелем вита пара до LAN порту ether2 та за допомогою програмного забезпечення WinBox отримано доступ до налаштування маршрутизатора. Налаштування маршрутизатору в режимі точки доступу “CAPsman” проведено у Web-інтерфейсі швидкого налаштування "Quick Set". Обрано швидке налаштування "CAP", щоб налаштувати точку в режимі точки доступу “CAPsman”. Отримання IP-адреси для точки (Address Acquision) обрано по DHCP (Automatic). Усі LAN інтерфейси (ether2…ether5) об’єднано в “LAN-bridge”. Web-інтерфейс налаштування маршрутизатору в режимі точки доступу “CAPsman” через "Quick Set" наведено на рис. 4.21.

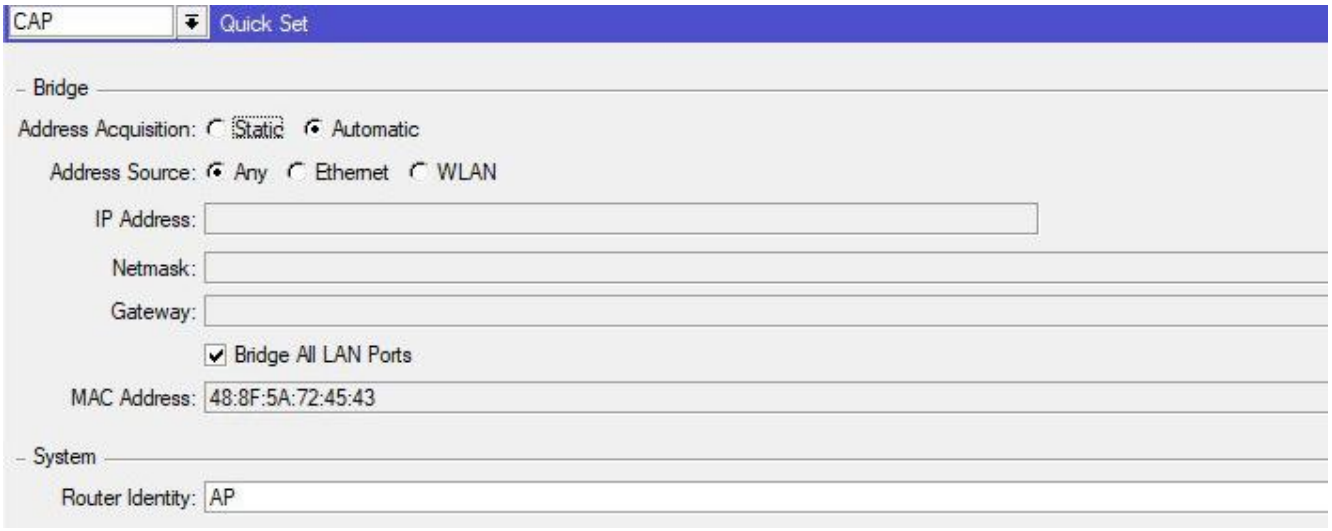


Рисунок 4.21 – Web-інтерфейс налаштування маршрутизатору "Mikrotik hap AC^2" в режимі точки доступу CAPsman через "Quick Set"

Після налаштування маршрутизатору "Mikrotik hap AC^2" в режимі точки доступу CAPsman через інтерфейс швидкого налаштування "QuickSet", було додано інтерфейси Wi-Fi мереж до контролеру CAPsman у web-інтерфейсі “CAP”, як зображено на рис. 4.22.

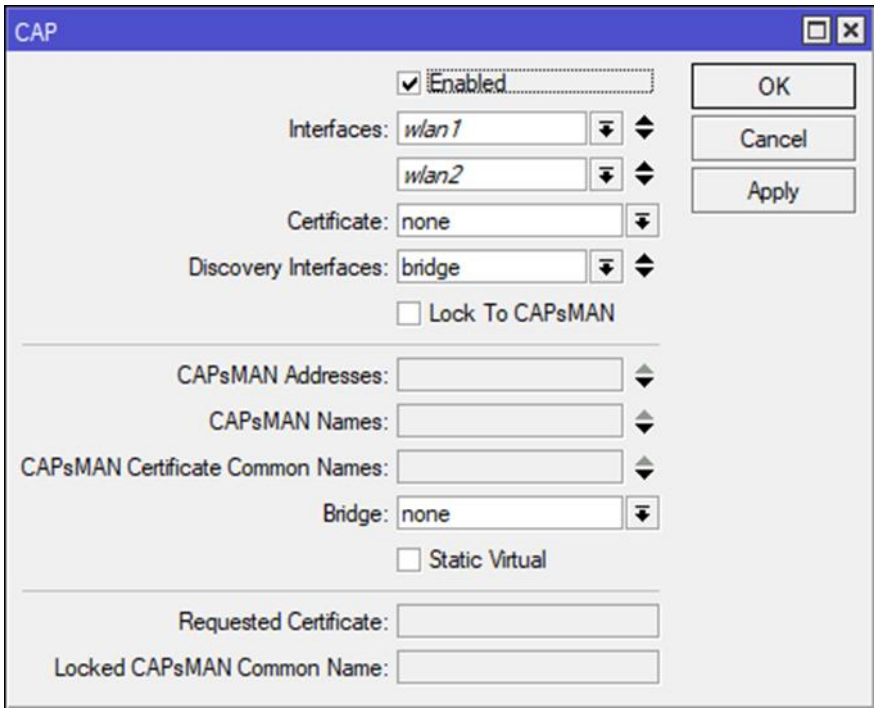


Рисунок 4.22 – Налаштування у web-інтерфейсі “CAP”

Налаштовано правила Firewall для точки доступу “CAPsman”, аналогічно, як і для контролеру “CAPsman” (рис. 4.13, 4.14, 4.15).

Налаштування точки доступу для “CAPsman” контролеру проведено успішно, оскільки безпроводові інтерфейси перейшли під контроль контролеру “CAPsman”, як зображено на рис. 4.23.

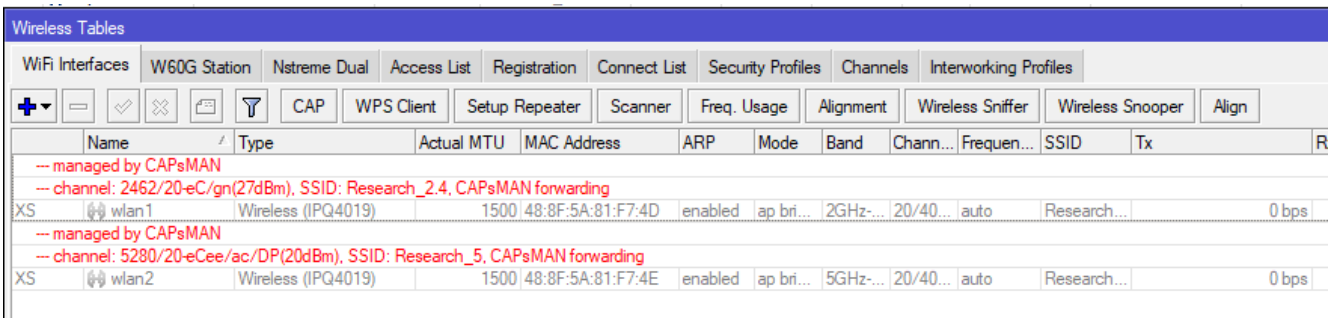


Рисунок 4.23 – Web-інтерфейс "Wireless tables" точки доступу “CAPsman”

Після налаштування маршрутизатору в режимі точки доступу “CAPsman”, було виконано з’єднання контролеру “CAPsman” і точки доступу “CAPsman” кабелем вита пара. Налаштування проведено успішно, оскільки у Web-інтерфейсі

контролеру “CAPsman” з’явилися безпроводові інтерфейси точки доступу “CAPsman” разом з існуючими інтерфейсами “CAPsman” від контролеру, як зображено на рис. 4.24.

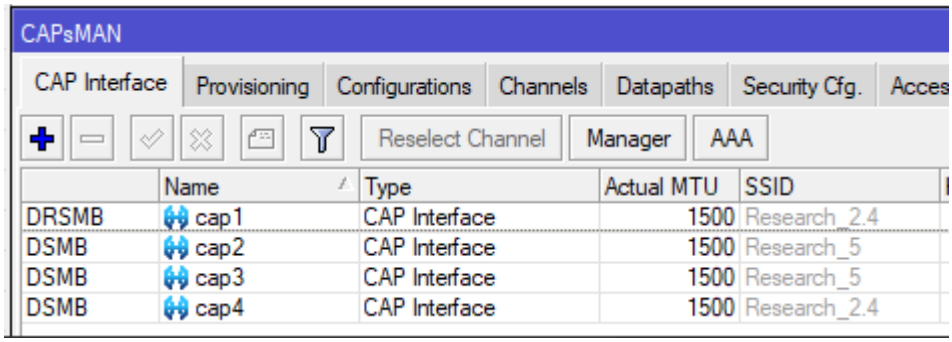


Рисунок 4.24 – Web-інтерфейс контролеру "CAPsman"

4.3 Тестування безшовного Wi-Fi для пошуку оптимального налаштування обладнання для транспортної мережі

За допомогою двох маршрутизаторів Mikrotik HAP AC^2 побудовано локальну мережу з “безшовним” зв’язком Wi-Fi з рівнем сигналу на перетині полів в діапазоні -83…-86 дБм для Wi-Fi 802.11ac. Схему локальної безшовної мережі Wi-Fi 5 ГГц стандарту 802.11ac наведено на рис. 4.25.

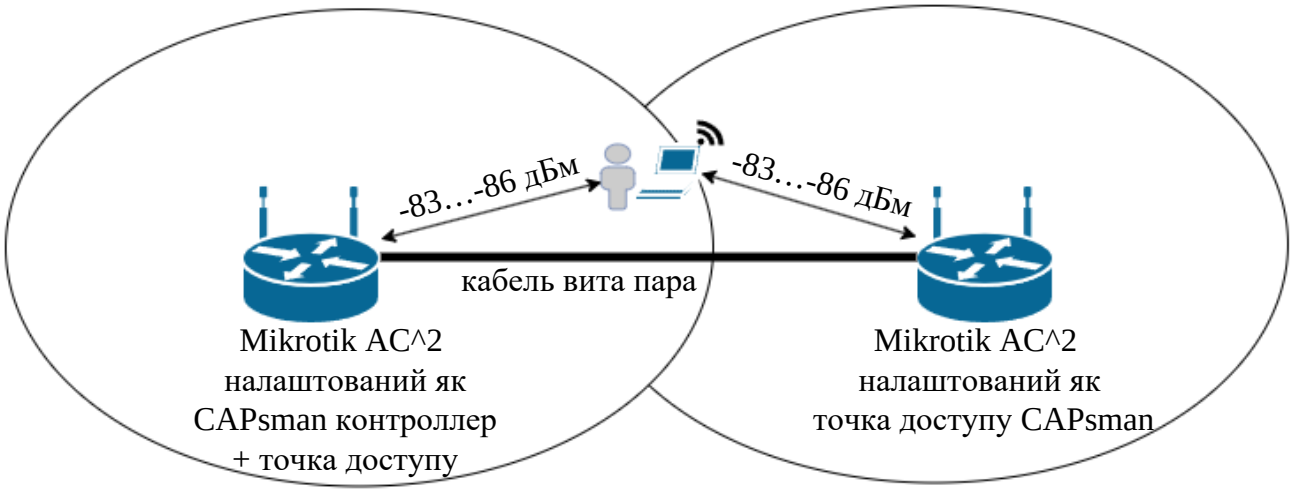


Рисунок 4.25 – Схема локальної безшовної мережі Wi-Fi 5 ГГц стандарту 802.11ac

За допомогою ноутбуку з Wi-Fi модулем проведено тестування втрат в каналі передавання даних при рівні сигналу -83…-86 дБм від маршрутизатору Mikrotik HAP AC^2. Виявлено, що при перетині двох полів на рівні -83…-86 дБм присутні втрати в каналі передачі даних. Для виявлення рівня сигналу, при якому буде належна якість каналу передачі даних, відключено маршрутизатор, який було налаштовано в режимі точки доступу CAPsman. Схему для тестування втрат в каналі передачі даних та пропускної здатності мережі при рівнях сигналу -83…-86 дБм від маршрутизаторів Mikrotik HAP AC^2 наведено на рис. 4.26.

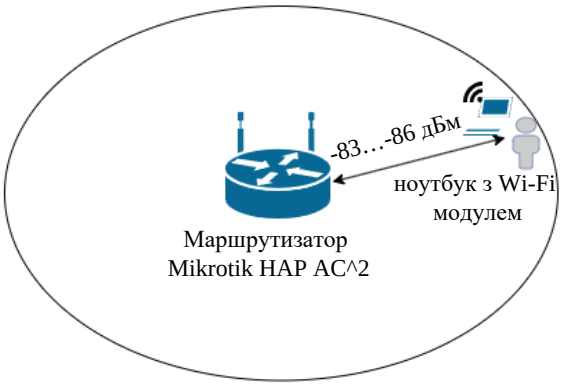


Рисунок 4.26 – Схема тестування якості передачі даних по Wi-Fi в залежності від рівня сигналу

Спостереження за зміною рівня сигналу проводилося через Web-інтерфейс маршрутизатору Mikrotik HAP AC^2. Результати перевірки втрат пакетів в каналі передачі даних при рівні сигналу в діапазоні -83…-86 дБм наведені на рис. 4.27.

SSID	MAC Address	EAP Identity	Tx Rate	Rx Rate	Tx Signal	Rx Signal
Research_5	20:2B:20:65:C6:E1					-86

SSID	MAC Address	EAP Identity	Tx Rate	Rx Rate	Tx Signal	Rx Signal
Research_5	20:2B:20:65:C6:E1					-83

```
--- 192.168.1.1 ping statistics ---
100 packets transmitted, 91 received, 9% packet loss, time 19947ms
rtt min/avg/max/mdev = 43.744/308.644/2223.374/471.882 ms, pipe 10
```

Рисунок 4.27 – Результат перевірки втрат пакетів в каналі передавання даних Wi-Fi 802.11ac 5 ГГц при рівні сигналу в діапазоні -83…-86 дБм

Як випливає з рис. 4.27, при коливанні рівня сигналу Wi-Fi 802.11ac 5 ГГц в діапазоні -83…-86 дБм, наявність втрат в каналі передавання даних становить у найгіршому випадку 9%, а середня затримка доставки пакетів дорівнює близько 308 мс, що є показником поганої якості зв'язку. Тестування втрат і затримок в каналі передавання даних проводилося командою ping від ноутбуку з Wi-Fi модулем до маршрутизатора Mikrotik HAP AC^2. Розмір пакета даних при пінгу становить – 64 біт.

При рівні сигналу Wi-Fi 802.11ac 5 ГГц в діапазоні -83…-86 дБм, пропускна здатність каналу передавання даних становить близько 11 Мбіт/с і іноді опускається до 0 Мбіт/с через розрив з'єднання. Результат тестування пропускної здатності Wi-Fi 802.11ac 5 ГГц при рівні сигналу -83…-86 дБм наведено на рис. 4.28. Перевірка пропускної здатності каналу проводилася за допомогою утиліти iperf3 в 1 потік. В якості сервера виступав персональний комп'ютер, що знаходиться в одній локальній мережі з ноутбуком через який проводилося тестування якості каналу.

```
ubuntu@research:~$ iperf3 -c 192.168.1.250 -t 60
Connecting to host 192.168.1.250, port 5201
[  5] local 192.168.1.252 port 36184 connected to 192.168.1.250 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  1.43 MBytes  12.0 Mbits/sec    0    115 KBytes
[  5]   1.00-2.00   sec  1.30 MBytes  10.9 Mbits/sec    0    171 KBytes
[  5]   2.00-3.00   sec  1.30 MBytes  10.9 Mbits/sec    0    219 KBytes
[  5]   3.00-4.00   sec  1.68 MBytes  14.1 Mbits/sec    0    280 KBytes
[  5]   4.00-5.00   sec  1.30 MBytes  10.9 Mbits/sec    0    334 KBytes
[  5]   5.00-6.00   sec  1.55 MBytes  13.0 Mbits/sec    0    390 KBytes
[  5]   6.00-7.00   sec  0.00 Bytes  0.00 bits/sec    0    397 KBytes
[  5]   7.00-8.00   sec  0.00 Bytes  0.00 bits/sec    0    397 KBytes
[  5]   8.00-9.00   sec  0.00 Bytes  0.00 bits/sec    0    397 KBytes
[  5]   9.00-10.00  sec   827 KBytes  6.78 Mbits/sec    0    397 KBytes
[  5]  10.00-11.00  sec  1018 KBytes  8.35 Mbits/sec    0    485 KBytes
[  5]  11.00-12.00  sec  1.24 MBytes  10.4 Mbits/sec    0    872 KBytes
```

Рисунок 4.28 – Результат тестування пропускної здатності Wi-Fi 802.11ac 5 ГГц при рівні сигналу -83…-86 дБм

Шляхом зменшення відстані між тестовим ноутбуком та маршрутизатором Mikrotik HAP AC^2 було збільшено рівень сигналу між цими пристроями та

виявлено, що при рівні сигналу Wi-Fi 802.11ac 5 ГГц в діапазоні -78…-80 дБм зберігається належна якість передавання даних в каналі, без втрат пакетів. Результат перевірки каналу передавання даних при рівні сигналу -78…-80 дБм наведено на рис. 4.29.

SSID	MAC Address	EAP Identity	Tx Rate	Rx Rate	Tx Signal	Rx Signal
Research_5	20:2B:20:65:C6:E1					-78

SSID	MAC Address	EAP Identity	Tx Rate	Rx Rate	Tx Signal	Rx Signal
Research_5	20:2B:20:65:C6:E1					-80

```
--- 192.168.1.1 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 19907ms
rtt min/avg/max/mdev = 1.835/28.580/320.282/64.201 ms, pipe 2
```

Рисунок 4.29 – Результат перевірки втрат пакетів в каналі передавання даних Wi-Fi 802.11ac 5 ГГц при рівні сигналу в діапазоні -78…-80 дБм

При тестуванні пропускної здатності Wi-Fi 802.11ac 5 ГГц при рівні сигналу -78…-80 дБм отримано близько 40 Мбіт/с, що є задовільним показником пропускної здатності. Результат тестування пропускної здатності Wi-Fi 802.11ac 5 ГГц при рівні сигналу -78…-80 дБм наведено на рис. 4.30.

```
ubuntu@research:~$ iperf3 -c 192.168.1.250 -t 60
Connecting to host 192.168.1.250, port 5201
[  5] local 192.168.1.252 port 36792 connected to 192.168.1.250 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  5.56 MBytes  46.7 Mbits/sec    0    304 KBytes
[  5]   1.00-2.00   sec  5.41 MBytes  45.3 Mbits/sec    0    527 KBytes
[  5]   2.00-3.00   sec  6.04 MBytes  50.7 Mbits/sec    0    708 KBytes
[  5]   3.00-4.00   sec  3.75 MBytes  31.4 Mbits/sec    0    856 KBytes
[  5]   4.00-5.00   sec  6.25 MBytes  52.4 Mbits/sec    0    856 KBytes
[  5]   5.00-6.00   sec  5.00 MBytes  42.0 Mbits/sec    0    926 KBytes
[  5]   6.00-7.00   sec  6.25 MBytes  52.4 Mbits/sec    0    993 KBytes
[  5]   7.00-8.00   sec  5.00 MBytes  41.9 Mbits/sec    0   1.04 MBytes
[  5]   8.00-9.00   sec  5.00 MBytes  41.9 Mbits/sec    0   1.04 MBytes
[  5]   9.00-10.00  sec  7.50 MBytes  62.9 Mbits/sec    0   1.04 MBytes
[  5]  10.00-11.00  sec  5.00 MBytes  41.9 Mbits/sec    0   1.04 MBytes
[  5]  11.00-12.00  sec  3.75 MBytes  31.4 Mbits/sec    0   1.04 MBytes
[  5]  12.00-13.00  sec  5.00 MBytes  42.0 Mbits/sec    0   1.10 MBytes
[  5]  13.00-14.00  sec  2.50 MBytes  21.0 Mbits/sec    0   1.10 MBytes
[  5]  14.00-15.00  sec  6.25 MBytes  52.5 Mbits/sec    0   1.54 MBytes
```

Рисунок 4.30 – Результат тестування пропускної здатності Wi-Fi 802.11ac 5 ГГц при рівні сигналу -78…-80 дБм

Аналогічні тестування проведено для Wi-Fi 802.11n 2.4 ГГц. Виявлено, що при рівні сигналу Wi-Fi 802.11n 2.4 ГГц в діапазоні -70…-76 дБм наявність втрат в каналі передавання даних становить близько 8%, а середня затримка доставки пакетів дорівнює близько 231 мс, що є показником поганої якості зв'язку. Результат перевірки втрат пакетів в каналі передавання даних Wi-Fi 802.11n 2.4 ГГц при рівні сигналу в діапазоні -70…-76 дБм наведено на рис. 4.31.

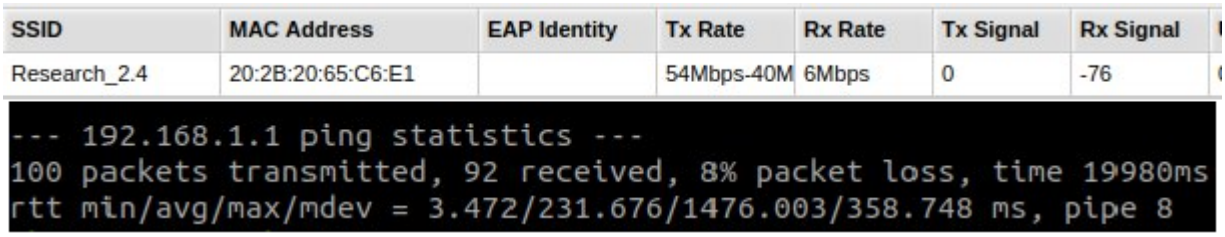


Рисунок 4.31 – Результат перевірки втрат пакетів в каналі передавання даних Wi-Fi 802.11n 2.4 ГГц при рівні сигналу в діапазоні -70…-76 дБм

Виявлено, що при рівні сигналу в діапазоні -65…-70 дБм зберігається належна якість передавання даних в каналі, без втрат пакетів. Результат перевірки каналу передавання даних при рівні сигналу -65…-70 дБм наведено на рис. 4.32.

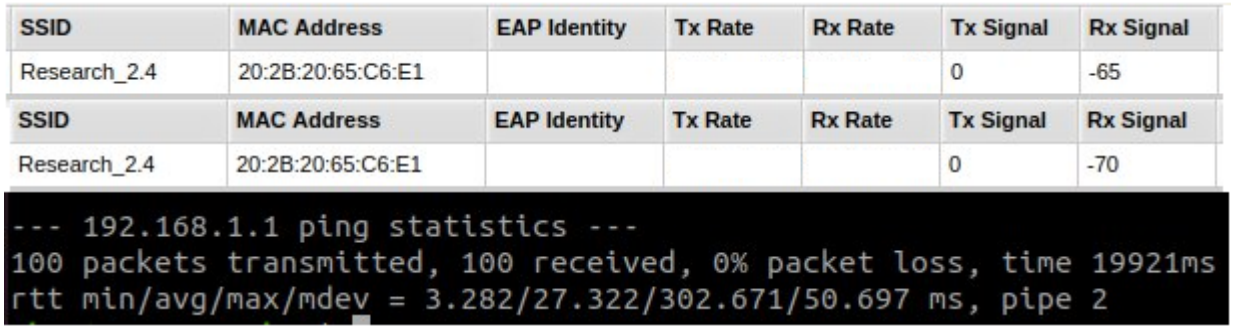


Рисунок 4.32 – Результат перевірки втрат пакетів в каналі передавання даних Wi-Fi 802.11n 2.4 ГГц при рівні сигналу в діапазоні -65…-70 дБм

При тестуванні пропускної здатності Wi-Fi 802.11n 2.4 ГГц при рівні сигналу -65…-70 дБм отримано близько 42 Мбіт/с, що є задовільним показником

пропускної здатності. Результат тестування пропускної здатності Wi-Fi 802.11n 2.4 ГГц при рівні сигналу -65…-70 дБм наведено на рис. 4.33.

```
ubuntu@research:~$ iperf3 -c 192.168.1.250 -t 60
Connecting to host 192.168.1.250, port 5201
[  5] local 192.168.1.252 port 44198 connected to 192.168.1.250 port 520
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  2.84 MBytes  23.8 Mbits/sec    0    136 KBytes
[  5]   1.00-2.00   sec  5.10 MBytes  42.7 Mbits/sec    0    361 KBytes
[  5]   2.00-3.00   sec  6.84 MBytes  57.3 Mbits/sec    0    636 KBytes
[  5]   3.00-4.00   sec  5.00 MBytes  41.9 Mbits/sec    0    778 KBytes
[  5]   4.00-5.00   sec  5.00 MBytes  42.0 Mbits/sec   12    337 KBytes
[  5]   5.00-6.00   sec  5.00 MBytes  41.9 Mbits/sec    0    757 KBytes
[  5]   6.00-7.00   sec  5.00 MBytes  42.0 Mbits/sec    0    834 KBytes
[  5]   7.00-8.00   sec  6.25 MBytes  52.4 Mbits/sec    0    887 KBytes
[  5]   8.00-9.00   sec  5.00 MBytes  41.9 Mbits/sec    9    458 KBytes
[  5]   9.00-10.00  sec  5.00 MBytes  42.0 Mbits/sec    0    496 KBytes
[  5]  10.00-11.00  sec  5.00 MBytes  41.9 Mbits/sec    2    373 KBytes
[  5]  11.00-12.00  sec  5.00 MBytes  42.0 Mbits/sec    0    403 KBytes
```

Рисунок 4.33 – Результат тестування пропускної здатності Wi-Fi 802.11n 2.4 ГГц при рівні сигналу -65…-70 дБм

З отриманих результатів тестування можна зробити висновок, що для забезпечення надійного каналу передачі даних без втрат необхідно, щоб в точках перетину полів рівень сигналу не нижче -80 дБм для уникнення роз’єднання пристроїв з точками доступу Wi-Fi 5 ГГц стандарту 802.11ac та не менше за -70 дБм для Wi-Fi 2.4 ГГц стандарту 802.11n.

Для проведення моделювання розповсюдження сигналу було використано характеристики маршрутизатору “Mikrotik HAP AC^2” з підтримкою стандарту 802.11ac:

- антени з круговою діаграмою спрямованості;
- максимальна вихідна потужність передавача +20 дБм;
- чутливість приймача -90 дБм;
- робочі діапазони частот 2.4 та 5 ГГц.

Моделювання розповсюдження сигналу для транспортної мережі проводилося в програмному середовищі Altair WinProp, створення міської інфраструктури проводилося в програмі Altair Wallman.

В якості об’єкту моделювання міської інфраструктури було обрано ділянку руху транспортних засобів на перехресті. Змодельована ділянка руху транспортної системи для тестування розповсюдження сигналу від точок доступу Wi-Fi наведена на рис. 4.34.

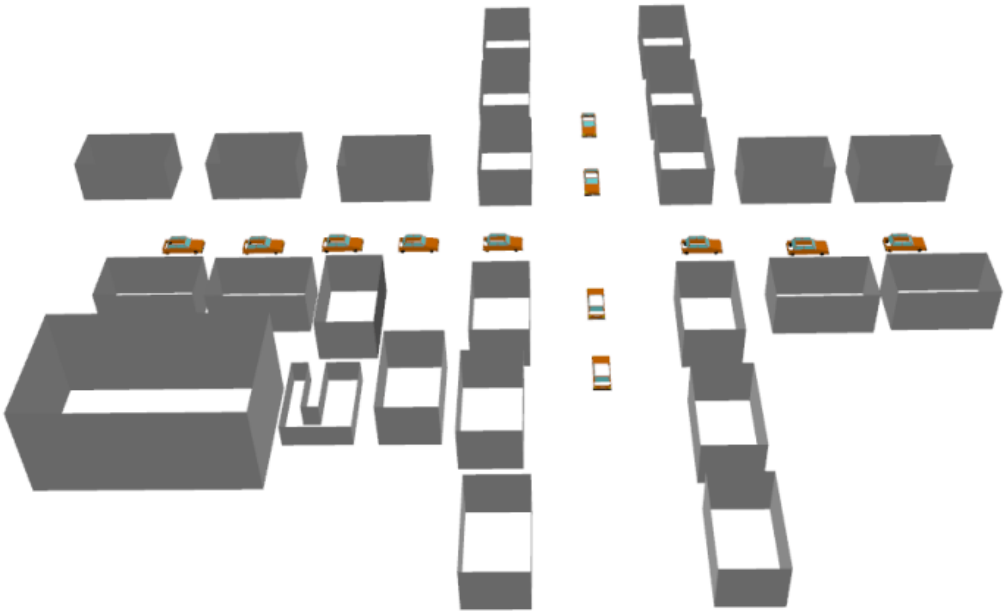


Рисунок 4.34 – Змодельована ділянка руху транспортної системи для тестування розповсюдження сигналу від точок доступу Wi-Fi

Враховуючи вихідну потужність передавача точок доступу, відстань між ними при якій на перетині зон дії рівень сигналу не менше за -80 дБм, буде дорівнювати приблизно 120 м. Ця відстань отримана шляхом моделювання розповсюдження сигналів від точок доступу на перехресті у програмному середовищі “Altair WinProp”. Розповсюдження рівня сигналу від точок доступу Wi-Fi 5 ГГц стандарту 802.11ac на перехресті наведено на рис. 4.35.

Для організації надійного зв’язку і забезпечення високого рівня сигналу встановлено 4 точки доступу таким чином, щоб зона перетину електромагнітних полів проходила поза межами розташування будинків, тобто посередині вулиць.

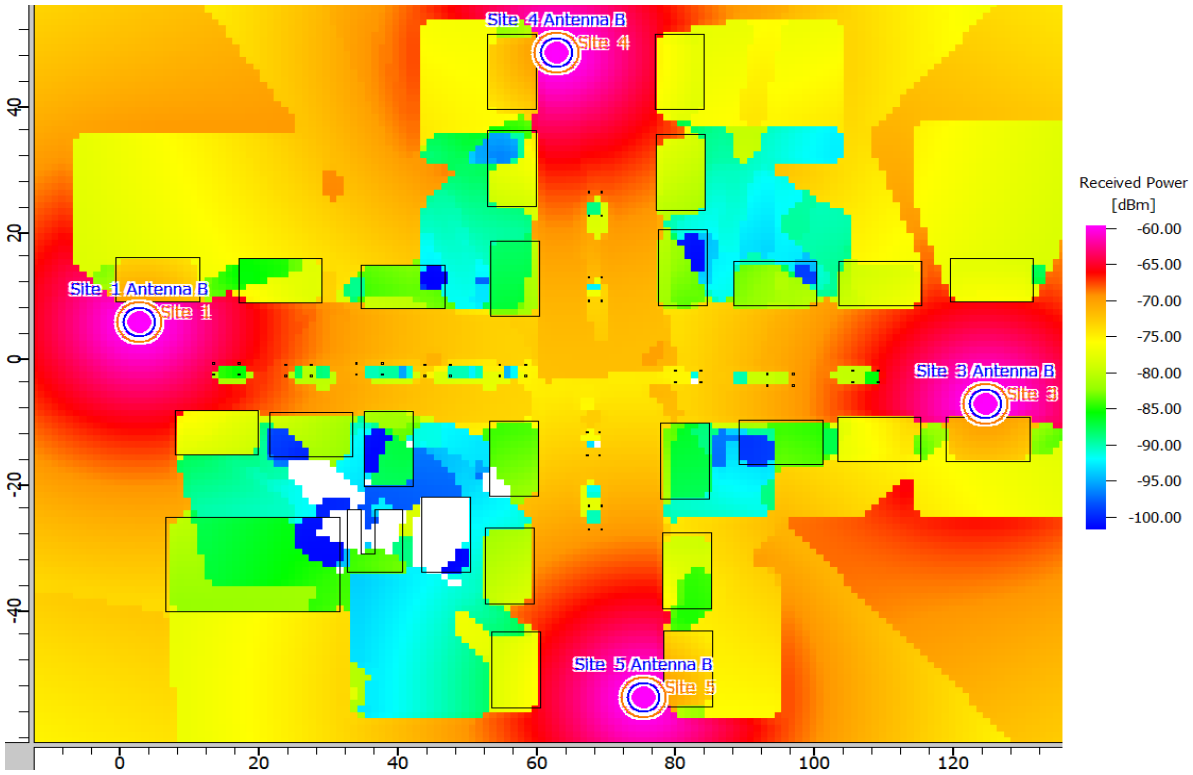


Рисунок 4.35 – Розповсюдження рівня сигналу Wi-Fi від точок доступу Wi-Fi 5 ГГц стандарту 802.11ac вздовж доріг на перехресті

Як випливає з рис. 4.35, вздовж доріг, що перетинаються на перехресті, організовано безшовний Wi-Fi зв’язок з рівнем сигналу не менше ніж -80 дБм. На перехресті, у місці, де перетинаються зони дії усіх точок доступу рівень сигналу знаходиться на рівні -73…-78 дБм.

Розповсюдження рівня сигналу Wi-Fi 802.11n 2.4 ГГц від точок доступу Wi-Fi вздовж доріг на перехресті наведено на рис. 4.36.

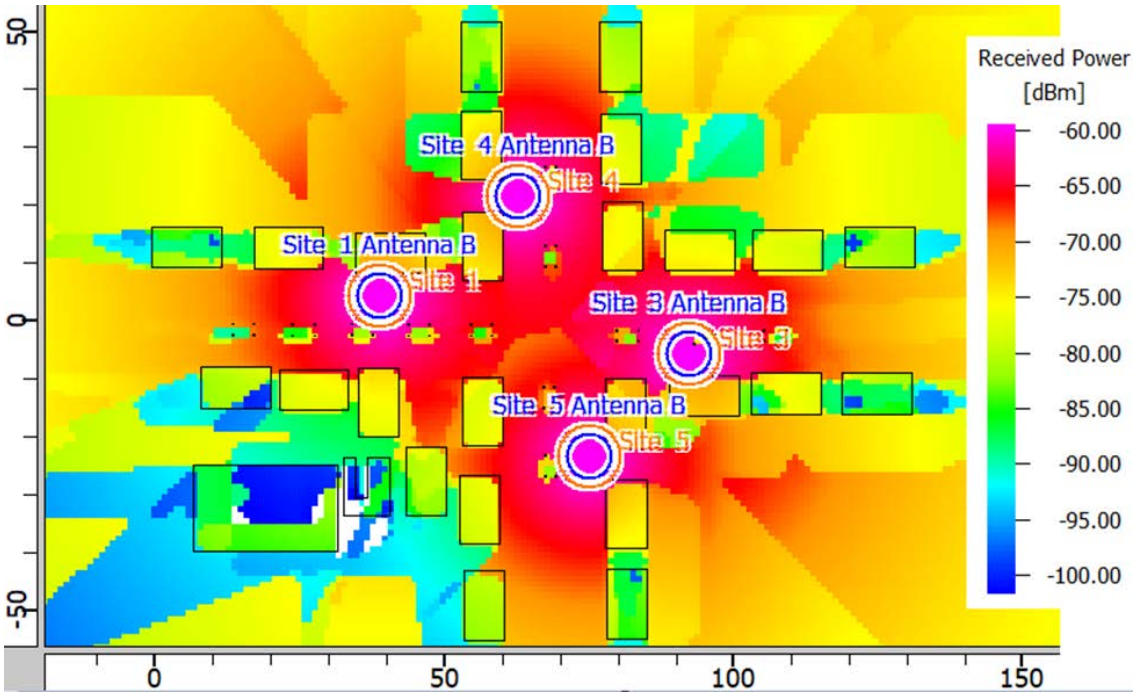


Рисунок 4.36 – Розповсюдження рівня сигналу Wi-Fi 802.11n 2.4 ГГц від точок доступу Wi-Fi вздовж доріг на перехресті

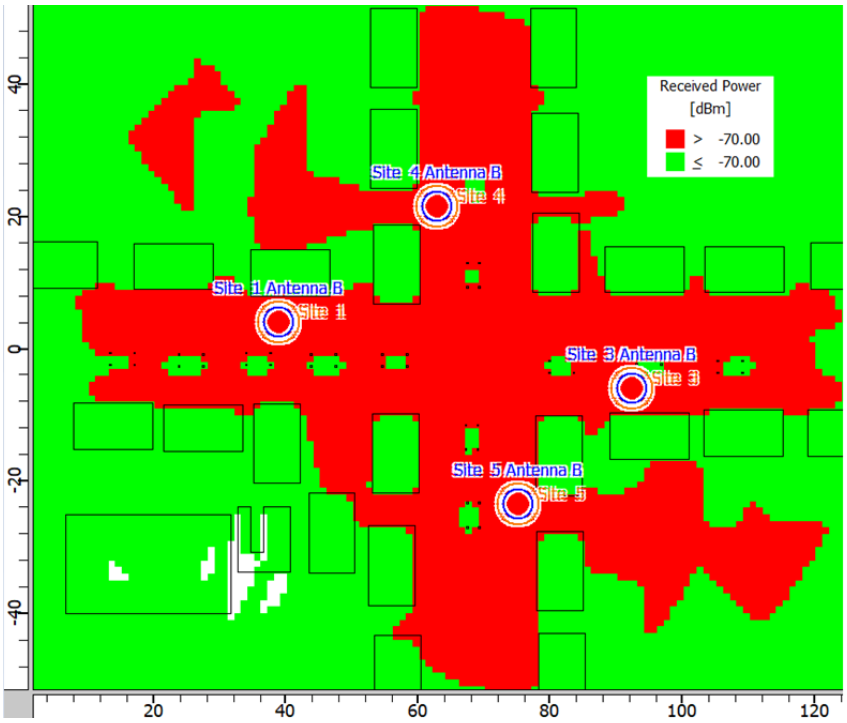


Рисунок 4.37 – Розповсюдження рівня сигналу Wi-Fi 802.11n 2.4 ГГц від точок доступу Wi-Fi вздовж доріг на перехресті з градацією -70 дБм

Як випливає з рис. 4.36 та рис. 4.37, рівень сигналу на перехресті та вздовж дороги знаходиться на рівні не менше за -70 дБм. Цього рівня сигналу цілком достатньо для того, щоб пристрої, що встановлені на транспортних засобах, що пересуваються по дорозі та пішоходи, які знаходяться на тротуарі були забезпечені безперервним зв'язком з точками доступу Wi-Fi.

Рівень сигналу більший за -70 дБм забезпечується на відстані до 50 м від перехрестя на будь якому напрямку для мережі Wi-Fi 2.4 ГГц стандарту 802.11n та на відстані 120 м від перехрестя для мережі Wi-Fi 5 ГГц стандарту 802.11ac. З цього можна зробити висновок, що чотирьох точок доступу Wi-Fi 2.4 ГГц стандарту 802.11n, з потужністю передавача +20 дБм, що встановлені на відстані близько 50 м одна від одної буде достатньо для того, щоб забезпечити надійним зв'язком учасників дорожнього руху на відстані до 50 м від перехрестя.

Було проведено практичну перевірку якості безшовного зв'язку Wi-Fi. Встановлено 2 маршрутизатора "Mikrotik HAP AC^2" на висоті 3м. У зоні розповсюдження сигналу від маршрутизаторів не було завад у вигляді стін, дерев та міської інфраструктури. На транспортному засобі було встановлено ноутбук з Wi-Fi модулем. Було здійснено рух транспортного засобу вздовж дороги з безшовним Wi-Fi покриттям 2.4 ГГц стандарту 802.11n та перевірено якість каналу передачі даних шляхом команди ping з інтервалом 0.2 с. Схема тестування безшовного покриття Wi-Fi 2.4 ГГц вздовж дороги наведена на рис. 4.38.

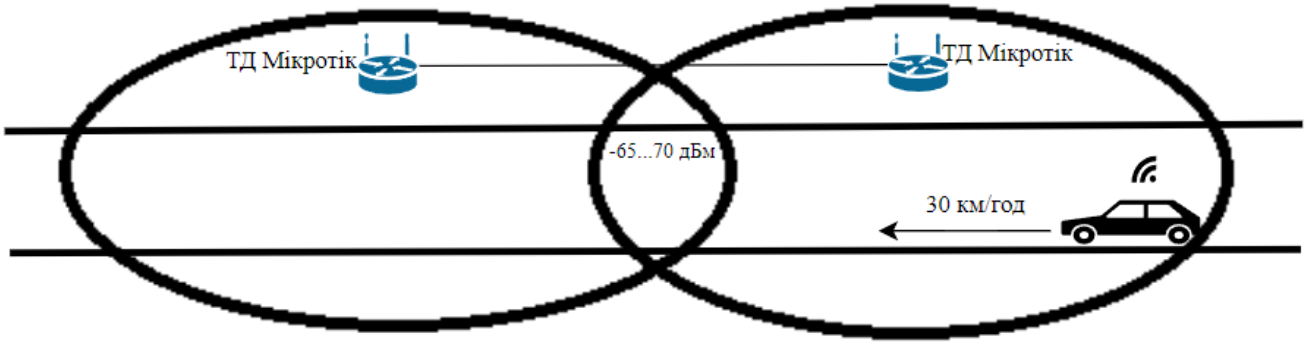


Рисунок 4.38 – Схема безшовного покриття Wi-Fi 2.4 ГГц вздовж дороги

В результаті тестування безшовного покриття Wi-Fi 2.4 ГГц вздовж дороги при русі транспортного засобу 30 км/год було виявлено зростання затримок при передачі пакетів під час переключення ноутбуку між маршрутизаторами до 600 мс, що зображено на рис. 4.39.

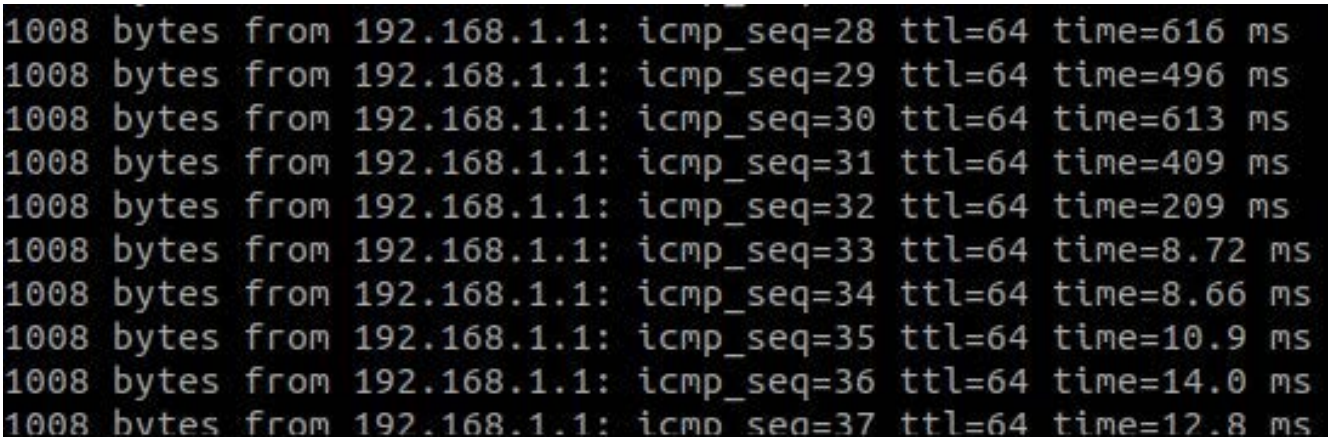


Рисунок 4.39 – Зростання затримок в каналі передачі даних під час переключення ноутбуку між маршрутизаторами

Зростання затримок при передачі даних було тимчасовим і затримки одразу нормалізувалися після переключення ноутбуку на другу точку. Результат тестування якості передачі даних мережі безшовного Wi-Fi 2.4 ГГц вздовж дороги при русі транспортного засобу 30 км/год наведено на рис. 4.40.

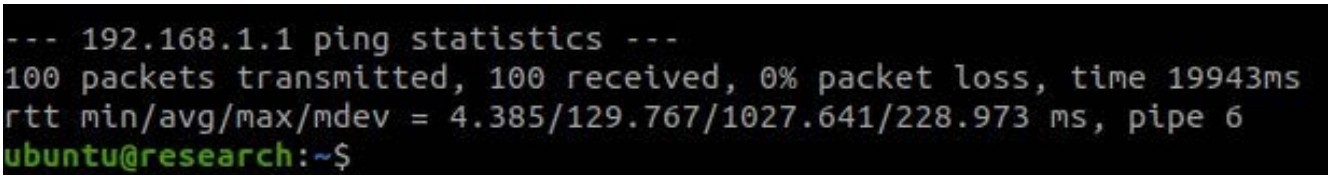


Рисунок 4.40 – Результат тестування безшовного зв’язку W-Fi вздовж дороги при руху транспортного засобу зі швидкістю 30 км/год

Результати тестування показують, що при потраплянні в зону покриття від Wi-Fi точки, транспортний засіб або пішохід може здійснювати безперервний обмін інформацією про своє місцезнаходження, напрямок та швидкість руху. Завдяки безшовному покриттю технологія Wi-Fi компенсує свій мінус у швидкості з’єднання між пристроями, що дає змогу використовувати її як альтернативу технології DSRC на деяких ділянках руху.

Тестування проведені з мінімальним рівнем завад у вигляді дерев, стовпів та міської інфраструктури, тому при моделюванні для кожного окремого випадку необхідно враховувати рівень завад місцевості.

Висновки до розділу 4

Результати дослідження розповсюдження поля сигналу від точок доступу Wi-Fi показали, що для впевненого і швидкого зв'язку між пристроями Wi-Fi необхідно забезпечити рівень сигналу у приймальній антені не менше ніж -70 дБм для Wi-Fi 2.4 ГГц стандарту 802.11n та не менше -80 дБм для Wi-Fi 5 ГГц стандарту 802.11ac. З урахуванням того, що при наявності опадів та густого туману загасання в каналі передавання даних значно зростає, тому доцільно зменшувати відстань між точками доступу у місцях з великим рівнем завад.

В результаті проведеного дослідження встановлено, що незважаючи на те що технологія Wi-Fi забезпечує меншу швидкість з'єднання між пристроями, ніж технологія DSRC, при організації безшовного Wi-Fi покриття можна компенсувати цю ваду даної технології завдяки тому, що пристроям Wi-Fi не треба щоразу встановлювати з'єднання з точкою доступу, поки вони знаходяться в зоні дії безшовного покриття. Таким чином технологію Wi-Fi можна використовувати для оповіщення про місцезнаходження транспортних засобів та пішоходів на небезпечних ділянках руху.

ЗАГАЛЬНІ ВИСНОВКИ

У дисертаційній роботі було проведено аналіз використання сучасних технологій IoT для побудови транспортної мережі smart-міста. Проведено літературні огляди актуальних досліджень в цій галузі, моделювання розповсюдження енергії поля, проведено розрахунки і отримано наступні результати:

1. Проведено аналіз сучасних публікацій в яких проводились дослідження використання технологій IoT у транспортній мережі міста. Згідно проведеного аналізу було встановлено, що в умовах транспортної мережі найкраще використовувати технології стандартів Wi-Fi, технологію DSRC та RFID, оскільки саме ці технології відповідають вимогам транспортної системи.

2. Досліджено розповсюдження енергії поля від активних RFID міток на багато смугових дорогах з обмеженими умовами видимості для транспортних засобів. В результаті аналізу було визначено, що використання активних RFID-міток дає змогу інформувати транспортні засоби на дорогах, які мають більше ніж 2 смуги руху в одному напрямку. Для доріг з однією та двома смугами руху в одному напрямку буде достатньо інтеграції однієї активної RFID-мітки на дорожній знак. Для доріг з трьома та чотирма смугами руху в одному напрямку необхідно інтегрувати активні RFID-мітки з двох боків дороги для забезпечення надійного зв’язку. При кількості смуг більше чотирьох в одному напрямку доцільно використовувати додаткові активні мітки на підвісних дорожніх знаках або світлофорах.

3. Досліджено розповсюдження енергії поля від пасивних RFID міток на багато смугових дорогах з обмеженими умовами видимості для транспортних засобів. В результаті аналізу було визначено, що використання пасивних RFID-міток для інформування водіїв недостатньо для доріг, що мають дві та більше смуг руху в один бік. Такі мітки доцільно використовувати для доріг з однією смугою руху в одному напрямку або для доріг з двома смугами руху в одному напрямку за умови встановлення міток на дорожні знаки з обох боків дороги.

4. Проведено дослідження розповсюдження енергії поля від бортових пристроїв та від дорожніх станцій системи DSRC. Проведений аналіз можливостей системи DSRC для своєчасного попередження водіїв транспортних засобів про можливість зіткнення в умовах щільної міської забудови показав, що в умовах обмеженої видимості пристроїв DSRC, встановлених на транспортних засобах, недостатньо для забезпечення своєчасного інформування водіїв.

Для усунення цього недоліку запропоновано встановлювати дорожні станції DSRC у зонах обмеженої видимості у якості повторювачів (ретрансляторів) сигналів транспортних засобів. Це дає змогу на відрізках з прямою видимістю збільшити відстань впевненого зв'язку у декілька разів, що в свою чергу дозволить завчасно отримати повідомлення про небезпеку. Своєчасне попередження про наявність інших транспортних засобів на дорогах особливо важливо в умовах мокрого або покритого льодом дорожнього полотна.

5. Проведено дослідження можливості використання безшовної мережі Wi-Fi для попередження водіїв та пішоходів при руху транспортних засобів. Результати дослідження розповсюдження поля сигналу від точок доступу Wi-Fi показали, що для впевненого і швидкого зв’язку між пристроями Wi-Fi необхідно забезпечити рівень сигналу у приймальній антені не менше ніж -70 дБм для Wi-Fi 2.4 ГГц стандарту 802.11n та не менше -80 дБм для Wi-Fi 5 ГГц стандарту 802.11ac.

В результаті тестування якості передачі даних мережі безшовного Wi-Fi 2.4 ГГц вздовж дороги при русі транспортного засобу 30 км/год виявлено, що технологія Wi-Fi може використовуватися на транспортній мережі для побудови додатків безпеки руху, де необхідний безперервний зв’язок без втрат в каналі передачі даних.

СПИСОК ЛІТЕРАТУРИ

1. Павлюченко В.А., Макаренко В.В. Використання дорожніх станцій DSRC для підвищення безпеки руху в умовах міської забудови. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. 2022. Випуск 4 (135). С. 63-68. DOI: 10.32782/1995-0519.2022.4.8. ISSN 1995-0519.

2. Павлюченко В.А., Макаренко В.В. Вибір конфігурації та розташування міток RFID для підвищення безпеки руху транспортної мережі міста. *Вісник Кременчуцького національного університету імені Михайла Остроградського. 2023.* Випуск 2 (139). С. 162-168. DOI: 10.32782/1995-0519.2023.2.20. ISSN 1995-0519.

3. Павлюченко В.А., Макаренко В.В. Аналіз можливості застосування технології Wi-Fi у транспортній мережі для підвищення безпеки руху транспорту та пішоходів. *Технології та інжиніринг. 2023.* Випуск 4 (15). С.28-38. DOI: 10.30857/2786-5371.2023.4.3. ISSN 2786-538X.

4. Б.Ю. Жураковський, І.О. Зенів. Технології Інтернету речей. Начальний посібник. 2021. URL: https://ela.kpi.ua/handle/123456789/42078.

5. M.A.Guptha. Internet of things & ITS applications. Lectury notes. 2020-2021. URL:https://mrcet.com/downloads/digital_notes/EEE/IoT%20&%20Applications%20Digital%20Notes.pdf.

6. P. R. Kumar1, Au T. Wan, W. S. H. Suhaili. Exploring data security and privacy issues in Internet of Things based on Five-layer architecture. International Journal of Communication Networks and Information Security (IJCNIS). 2020. P. 108-121. DOI:10.17762/ijcnis.v12i1.4345.

7. Al-Turjman F., Lemayian J. Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview. Computers & Electrical Engineering. October, 2020. P. 106776. DOI:10.1016/j.compeleceng.2020.106776.

8. Abdelgader A., Lenan W. The Physical Layer of the IEEE 802.11p WAVE Communication Standard: The Specifications and Challenges. Proceedings of the World Congress on Engineering and Computer Science 2014. October, 2014. V. 2. P. 691-698.

9. Laboratory Division Office of Engineering and Technology Federal Communications Commission. Phase I testing of prototype U-NII-4 Devices. October, 2018. P. 20-21.

10. Uzcategui R., Acosta-Marum G. WAVE: A Tutorial. IEEE Communications Magazine. May, 2009. P.126-133. DOI: 10.1109/MCOM.2009.4939288.

11. Z. Xu, X. Li,1 X. Zhao, M. H. Zhang, Z. Wang. DSRC versus 4G-LTE for Connected Vehicle Applications: A Study on Field Experiments of Vehicular Communication Performance. Journal of Advanced Transportation. DOI: 10.1155/2017/2750452.

12. S. Ajah; I. E. Achumba, N. Chukwuchekwa, N. Onyebuchi. Standardization of RFID communication and technologies in 5G network. School of Engineering and Technology Conference and Exhibition (SETCONF). 2023. P. 380-389.

13. Gurudatt Kulkarni, Ramesh Sutar, Sangita Mohite. RFID Security Issues & Challenges. International Conference on Electronics and Communication Systems (ICECS'14). February 2014. P.23-26.

14. Rowan T. Negotiating WiFi security. *Network security*. February, 2010. P. 8-12. DOI: 10.1016/S1353-4858(10)70024-6.

15. Aliev H., Kim H. Matrix-Based Dynamic Authentication With Conditional Privacy-Preservation for Vehicular Network Security. IEEE Access. January 2020. DOI: 10.1109/ACCESS.2020.3035845.

16. Yoshimichi S., Makanae K. Development and Evaluation of In-vehicle Signing System Utilizing RFID tags as Digital Traffic Signs. International Journal of ITS Research. January, 2007.

17. Malecki K., Kopaczyk K. RFID-Based Traffic Signs Recognition System. International Conference on Transport Systems Telematics. October, 2013. P. 115-122. DOI:10.1007/978-3-642-41647-7_15.

18. Eun-Kyu L., Soon O., Gerla M. RFID assisted vehicle positioning in VANETs. Pervasive and Mobile Computing – PerCom. 2012. P. 167-179. DOI:10.1016/j.pmcj.2011.06.001.

19. Prasanna K.R., Hemalatha M. RFID GPS and GSM based logistics vehicle load balancing and tracking mechanism. Procedia Engineering. December, 2012. P. 726-729. DOI:10.1016/j.proeng.2012.01.920.

20. Xiang S., Xu L., Wencheng T., Weigong Z. A Fusion Strategy for Reliable Vehicle Positioning Utilizing RFID and In-vehicle Sensors. Information Fusion. February, 2016. P. 76-86. DOI:10.1016/j.inffus.2016.01.003.

21. Shaoping L., Chen X., Ray Y. Z., Lihui W. A Passive RFID Tag-Based Locating and Navigating Approach for Automated Guided Vehicle. Computers & Industrial Engineering. October, 2018. P. 628-636. DOI:10.1016/j.cie.2017.12.026.

22. Hatem E. Optimized And Sub-Metric Indoor Localization System Based On Uhf Rfid Technology. Université Paris-Est; Université Libanaise. 2021.

23. Qin H., Chen W., Chen W., Li N., Zeng M., Peng Y. A collision-aware mobile tag reading algorithm for RFID-based vehicle localization. Computer Networks. August, 2021. P. 108422. DOI:10.1016/j.comnet.2021.108422.

24. Ahmed F., Hunain A., Ahmed Al N., Ab dulrahman A., Raafat A. Role of RFID Technology in Smart City Applications. Computer Science and Engineering. American University of Sharjah. March, 2019. P. 1-6. DOI:10.1109/ICCSPA.2019.8713622.

25. Jiang D., Delgrossi L. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. VTC Spring 2008 - IEEE Vehicular Technology Conference. DOI: 10.1109/vetecs.2008.458.

26. Martinez F., Fogue M., Coll M., Cano J.-C., Calafate C., Manzoni P. Evaluating the Impact of a Novel Warning Message Dissemination Scheme for VANETs Using Real City Maps. Networking 2010, 9th International IFIP TC 6 Networking Conference. May 11-15, 2010. P. 265-267. DOI:10.1007/978-3-642-12963-6_21.

27. Song G., Alvin L. An empirical Study of DSRC V2V Performance in Truck Platooning Scenarios. Digital Communications and Networks. 2. November, 2016. DOI:10.1016/j.dcan.2016.10.003.

28. A. K. Ligo, J. M. Peha, J. Barros. Throughput and Cost-Effectiveness of Vehicular Mesh Networks for Internet Access. IEEE Vehicular Technology Conference. DOI: 10.1109/VTCFall.2016.7881257.

29. N.S. Rajput. Measurement of IEEE 802.11p Performance for Basic Safety Messages in Vehicular Communications. 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). DOI: 10.1109/ANTS.2018.8710108.

30. Sommer C., Eckhoff D., Reinhard G., Dressler F. A Computationally Inexpensive Empirical Model of IEEE 802.11p Radio Shadowing in Urban Environments. Eight International Conference on Wireless On-Demand Network Systems and Services. 2011. P. 84-90. DOI:10.1109/WONS.2011.5720204.

31. Oishi J., Saskura K., Watanabe T. A Communication Model for Inter-vehicle Communication Simulation Systems Based on Properties of Urban Areas. *IJCSNS International Journal of Computer Science and Network Security*. October 2006, V.6 P. 213-219.

32. Yapp J., Kornecki A. Safety analysis of Virtual Traffic Lights. DOI: 10.1109/MMAR.2015.7283927.

33. Bazzi A., Zanella A., Masini B., Gianni P. A Distributed Algorithm for Virtual Traffic Lights with IEEE 802.11p. EuCNC 2014 - European Conference on Networks and Communications. June, 2014. DOI: 10.1109/EuCNC.2014.6882621.

34. Cheng N., Lu N., Zhang N., Shen X. (S.), Mark J. W. Vehicular Wi-Fi offloading: Challenges and solutions. Vehicular Communications. 2014. P. 13–21. DOI: 10.1016/j.vehcom.2013.11.002.

35. Dimatteo S., Hui P., Han B., Li V. O. K. Cellular Traffic Offloading through Wi-Fi Networks. IEEE 8th International Conference on Mobile Adhoc and Sensor Systems. Valencia: 2011. P. 192–201. DOI: 10.1109/MASS.2011.26.

36. Cheng R.-S., Huang C.-M., Pan S.-Y. Wi-Fi offloading using the device-to-device (D2D) communication paradigm based on the Software Defined Network (SDN) architecture. Journal of Network and Computer Applications. 2018. P. 1–12. DOI: 10.1016/j.jnca.2018.03.014.

37. Shuhaimi N. I., Heriansyah, Juhana T. Comparative Performance Evaluation of DSRC and Wi-Fi Direct in VANET. 4th International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME). 2015. P. 298–303. DOI: 10.1109/ICICI-BME.2015.7401382.

38. Tufail A., Fraser M., Hammad A., Kim K.-H., Yoo S.-W. An empirical study to analyze the feasibility of WI-FI for VANETs. Proceedings of the 2008 12th International Conference on Computer Supported Cooperative Work in Design, CSCWD. 2008. P. 553–558. DOI: 10.1109/CSCWD.2008.4537038. DOI: 10.1016/j.phycom.2013.12.003.

39. Fitah A., Badri A., Moughit M., Sahel A. Performance of DSRC and WI-FI for Intelligent Transport Systems in VANET. Procedia Computer Science. 2018. P. 360–368. DOI: 10.1016/j.procs. 2018.01.133.

40. Ahmeda F., Phillips M., Phillips S., Kima K.-Y. Comparative Study of Seamless Asset Location and Tracking Technologies. 30th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2021). 2021. P. 1138–1145. DOI: doi.org/10.1016/j.promfg.2020.10.160.

41. Jiantong C., Ling Y., Yong L., Weihua Z. Seamless outdoor/indoor navigation with WI-FI/GPS aided low cost. Physical Communication. 2014. P. 1–28. DOI: 10.1016/j.phycom.2013.12.003.

42. UHF мітка на метал до 30 метрів OPP130. URL: http://uarfid.kiev.ua/ua/products/uhf-metka-na-metall-do-30-metrov-opp130/.

43. Зчитувач Impinj R700 Series RAIN RFID. URL: https://www.impinj.com/getmedia/c23f175b-b2fa-4d2f-82d7-d33c3f4133ff/Impinj-fixed-reader-spec-table-English-1.pdf.

44. Активна RFID мітка зі звуковою та світловою індикацією SAAT T508. URL:http://uarfid.kiev.ua/products/aktivnaya-metka-so-svetovoj-i-zvukovoj-indikatsiej-t508/.

45. Всенапрямний RSSI активний зчитувач SAAT-F527A. URL: http://uarfid.kiev.ua/products/active-reader-saat-f527a/.

46. Jaktheerangkoon S., Nakorn K., Rojviboonchai K. Blind Corner Propagation Model for IEEE 802.11p Communication in Network Simulators. Journal of Advanced Transportation. 2018. P. 1-11. DOI:10.1155/2018/9482325.

47. Sun Q., Tan S. Y., Kah C. Teh. Analytical Formulae for Path Loss Prediction in Urban Street Grid Microcellular Environments. IEEE transactions on vehicular technology. July, 2005. V. 54. P. 1251-1258. DOI:10.1109/TVT.2005.851298

48. Jardosh P., Belding E., Almeroth K., Suri S. Towards Realistic Mobility Models For Mobile Ad hoc Networks. Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM. September, 2003. P. 217-229. DOI:10.1145/938985.939008

49. Otto J.S., Bustamante F.E., Berry R.A., Down the Block and Around the Corner. 29th IEEE International Conference on Distributed Computing Systems. 2009. P. 605-614. DOI:10.1088/1742-6596/1578/1/012160

50. On board unit OBU-301U Information Sheet. URL: https://unex.com.tw/pdf/OBU-301U.pdf.

51. Technical manual Roadside ITS Station RIS-9160-xx0x. URL: https://fccid.io/XZU9160/User-Manual/User-and-Installers-manual-3874195.

52. Chen Y.-C., Hsia J.-H., Liao Y.-J. Advanced seamless vertical handoff architecture for WiMAX and Wi-Fi heterogeneous networks with QoS guarantees. *Computer Communications*. 2021. P. 281–293. DOI: 10.1016/j.comcom.2008.10.014.

53. Wickramarachchi T., Dias D., Samarasinghe T., Gokull N. Evaluation of DSRC/Wi-Fi Hybrid Communications for Intelligent Transport Systems. *2022 IEEE 25th International Conference on Intelligent Transportation Systems* (ITSC). 2022. P. 3509–3514. DOI: 10.1109/ITSC55140.2022. 9922307.

54. Ott J., Kutscher D. Drive-thru Internet: IEEE 802.11b for "Automobile" Users. *Proceedings – IEEE INFOCOM*. 2004. P. 373.

55. Router Mikrotik HAP AC2 user manual. URL: https://help.mikrotik.com/docs/pages/viewpage.action?pageId=16351533.

ДОДАТОК А. Список опублікованих праць за темою дисертації

1. Павлюченко В. А., Макаренко В.В. Використання дорожніх станцій DSRC для підвищення безпеки руху в умовах міської забудови. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. 2022. Випуск 4 (135). С. 63-68. DOI: 10.32782/1995-0519.2022.4.8. ISSN 1995-0519, (фахове видання категорії Б).

2. Павлюченко В.А., Макаренко В.В. Вибір конфігурації та розташування міток RFID для підвищення безпеки руху транспортної мережі міста. *Вісник Кременчуцького національного університету імені Михайла Остроградського.* 2023. Випуск 2 (139). С. 162-168. DOI: 10.32782/1995-0519.2023.2.20. ISSN 1995-0519, (фахове видання категорії Б).

3. Павлюченко В.А, Макаренко В.В. Аналіз можливості застосування технології Wi-Fi у транспортній мережі для підвищення безпеки руху транспорту та пішоходів. *Технології та інжиніринг.* 2023. Випуск №4 (15). С.20-29. DOI: 10.30857/2786-5371.2023.4.3. ISSN 2786-538X, (фахове видання категорії Б).

4. Павлюченко В.А., Макаренко В.В. Підвищення безпеки руху з використанням дорожніх станцій DSRC. *V міжнародна науково-практична конференція "SCIENCE AND INNOVATION OF MODERN WORLD". Cognum Publishing House.* (м. Лондон, 25-27 січня 2023р.) Лондон. 2023. С. 179-184, (матеріали конференції). ISBN: 978-92-9472-194-5. URL: https://sci-conf.com.ua/wp-content/uploads/2023/01/SCIENCE-AND-INNOVATION-OF-MODERN-WORLD-25-27.01.23.pdf.

5. Павлюченко В.А., Макаренко В.В. Вибір місцезнаходження та конфігурації RFID міток транспортної мережі. *XI міжнародна науково-практична конференція "Scientific progress: innovations, achievements and prospects. MPDC Publishing.* (м. Мюнхен, 23-25 липня 2023р.) Мюнхен. 2023. С. 94-99, (матеріали конференції). ISBN: 978-3-954753-04-8. URL: https://sci-conf.com.ua/wp-content/uploads/2023/07/SCIENTIFIC-PROGRESS-INNOVATIONS-ACHIEVEMENTS-AND-PROSPECTS-23-25.07.23.pdf /.

6. Павлюченко В.А., Макаренко В.В. Використання технології Wi-Fi для контролю транспорту у розумному місті. *І міжнародна науково-практична конференція "Current challenges of science and education". MPDC Publishing.* (м. Берлін, 18-20 вересня 2023) Берлін. 2023, (матеріали конференції). ISBN: 978-3-954753-05-5. URL: https://sci-conf.com.ua/wp-content/uploads/2023/09/CURRENT-CHALLENGES-OF-SCIENCE-AND-EDUCATION-18-20.09.23.pdf EDUCATION-18-20.09.23.pdf.