Journal of Network and Information Security
13 (1) 2025, 30-38
www.publishingindia.com/jnis

Optimized LTE-V2X Resource Allocation for Efficient V2V Communication in VANETs

Mamta Chauhan[1*], Rani Astya[2] and Nitin Rakesh[3]
[1]Department of Computer Science and Engineering (SET), Sharda University, Greater Noida, Uttar Pradesh, India. Email: mamta.gbu.ict@gmail.com
[2]Department of Computer Science and Engineering (SET), Sharda University, Greater Noida, Uttar Pradesh, India.
[3]Department of Computer Engineering & Technology, Symbiosis Institute of Technology, Nagpur Symbiosis International Deemed University, Pune, Maharashtra, India.
[*]Corresponding Author

Abstract: In Vehicular Ad-Hoc Networks (VANETs) play a crucial role in modern Intelligent Transportation Systems (ITS) by enabling real-time Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Long-Term Evolution for Vehicle-to-Everything (LTE-V2X) communication, particularly using the LTE-V2X side-link mode known as PC5 Mode, provides improved coverage, lower latency, and enhanced reliability compared to traditional Dedicated Short-Range Communication (DSRC)-based systems. However, existing LTE-V2X implementations face major challenges such as inefficient resource allocation, network congestion, high transmission delays, and security vulnerabilities. This research presents the Optimized Long-Term Evolution for Vehicle-to-Everything Resource Sharing (OLRS) framework, which integrates adaptive resource allocation, dynamic power control, and multi-hop emergency message forwarding with security-enhanced communication mechanisms. The proposed framework utilizes Roadside Unit (RSU)-assisted congestion management to prioritize safety-critical messages, such as emergency alerts, and ensures secure, efficient, and scalable data exchange between vehicles. By optimizing power control, spectrum allocation, and emergency message dissemination, OLRS significantly improves key network performance metrics, achieving a 40% reduction in latency, a 10% increase in Packet Delivery Ratio (PDR), and enhanced Signal-to-Interference-plus-Noise Ratio (SINR). The framework was implemented and tested using Cisco Packet Tracer for network simulation and Wireshark for real-time packet analysis. The results demonstrate improved data throughput, enhanced communication reliability, and stronger security against cyber threats. The proposed model provides a practical and scalable solution for high-density vehicular networks, with direct applications in collision avoidance, autonomous driving coordination, and intelligent traffic management.

Keywords: Cisco packet tracer, Cyber security, Long-term evolution for vehicle to everything, Resource allocation, Spectrum management, Vehicle to Vehicle communication, Vehicular ad hoc networks, Wire shark.

I. Introduction

Vehicular Ad Hoc Networks (VANETs) have emerged as a crucial component of Intelligent Transportation Systems (ITS), enabling seamless communication between vehicles and infrastructure. By facilitating real-time data exchange, VANETs

improve road safety, optimize traffic flow, and support autonomous driving. Among different V2V communication technologies, Dedicated Short-Range Communication (DSRC) and LTE-V2X have been widely explored. While DSRC operates on the IEEE 802.11p standard, it suffers from limited scalability, high interference, and congestion in dense vehicular environments. LTE-V2X, introduced in 3GPP Release 14, provides a more robust solution with better coverage, lower latency, and improved reliability, making it ideal for mission-critical vehicular applications. However, despite its advantages, LTE-V2X faces significant challenges in ensuring low-latency, high-throughput, and secure V2V communication. With the increasing number of connected vehicles, network congestion, inefficient resource allocation, high transmission delays, and security vulnerabilities have become major obstacles. When conventional LTE-V2X systems utilize pre-set resource assignments they experience wasted spectrum potential alongside deteriorating the reliability of message exchanges. The network performance suffers deterioration because dynamic power control mechanisms are absent thus leading to poor SINR (Signal-to-Interference-Noise Ratio). Real-time emergency alert dissemination becomes impaired because multi-hop communication remains inadequately developed.

The successful operation of V2V communication relies on achieving both efficient operation and real-time security in modern vehicular networks. Reliable vehicle-to-vehicle communication technology serves as the backbone forautonomous vehicles and smart transportation systems that help decrease traffic-related hazards as well as enhance traffic system efficiency and activate intelligent traffic management systems. The existing LTE-V2X systems face scalability problems requiring a new framework to optimize resource facilities and power management systems and data transmission security protocols. An Optimized LTE-V2X Resource Sharing (OLRS) framework serves as a proposed solution by utilizing adaptive scheduling methods to dynamically allocate resources for spectrum optimization with congestion reduction benefits. Safe communication alerts propagate through multiple hops more effectively because this system improves both emergency alert reliability and speed at the same time it implements encryption and authentication security methods to secure vehicle-to-vehicle transmission communications. The adaptive power control function of OLRS improves the SINR by adjusting transmitter powers for maximum efficiency and minimum interference. Analysis of the outlined framework happens through Cisco Packet Tracer and Wireshark tests whichdeliver practical results that go beyond simulations based on NS3 and SUMO.

Through its framework the proposed design advances multiple practical vehicular implementations specifically collision avoidance systems which help decrease accident frequency through quicker and better emergency message communications. Intelligent traffic management becomes possible through OLRS because it enables real-time congestion analysis which results in improved urban mobility through dynamic traffic rerouting. The framework allows autonomous vehicle coordination through its support of low-latency V2V communication which results in improved safety and efficiency of self-driving functions. Secure data exchange is strengthened because this work develops protective mechanisms using encrypted and authenticated V2V transmissions to safeguard vehicular networks from cyberattacks. This research addresses crucial downsides of current LTE-V2X technologies which supports the creation of future vehicle communication systems leading to improved vehicle network security and transportation efficiency.

II. Related Work

Several studies have focused on Vehicle-to-Vehicle (V2V) communication and resource-sharing techniques to enhance the efficiency, reliability, and security of Intelligent Transportation Systems (ITS) [1]. Traditional Wi-Fi-based V2V communication relies on Dedicated Short-Range Communi- cation (DSRC) or IEEE 802.11p, which offers low-latency communication but suffers from high interference, network congestion, and limited scalability in dense traffic conditions [2]. Due to the short transmission range and lack of centralized control DSRC-based communication becomes inefficient in high-mobility

environments, making LTE-V2X a more viable solution [3]. LTE-V2X and Resource Allocation Strategies with the introduction of 3GPP Release 14, LTE-V2X has emerged as a superior alternative to DSRC, providing direct V2V communication via the PC5 sidelink interface. LTE-V2X leverages cellular infrastructure and spectrum efficiency to support high-speed vehicular networks with better coverage and reduced interference. Several studies have proposed Device-to-Device (D2D) communication as a technique to enhance spectrum reuse and reduce network congestion by enabling vehicles to communicate without direct base station involvement [4]. One of the major research areas in LTE-V2X is resource allocation optimization. Different techniques, including reinforcement learning-based algorithms, power control strategies and QoS-aware scheduling mechanisms, have been proposed to improve throughput, reduce latency, and enhance spectrum efficiency. Some approaches focus on dynamic spectrum sharing, where V2V communication coexists with traditional cellular traffic by allocating radio resources adaptively based on traffic load and channel conditions [5]. Power allocation techniques, such as adaptive transmission power control and SINR-based allocation, have also been explored to improve Signal-to-Interference-Noise Ratio (SINR) and network reliability. Multi-Hop Communication and Emergency Message Dissemination. A critical component of V2V communication is the efficient propagation of emergency messages, particularly in accident scenarios where timely delivery of alerts can prevent secondary collisions [6]. Traditional methods rely on single-hop broadcasting, which limits the communication range. Multi-hop communication protocols have been established in literature that enables emergency messages to travel through numerous vehicles until they find their target receivers [6]. Emergency message delivery receives a higher priority in investigations that focus on priority-based message forwarding systems for faster delivery rates. Other methods apply RSU-assisted forwarding which enables Roadside Units (RSUs) to increase V2V message reachability outside immediate direct connection range [7]. The literature presents research about geocast and opportunistic forwarding algorithms that adapt message paths using network topology information andvehicle population levels. The implementation of V2V communication faces two significant security obstacles which require solutions for privacy and confidentiality protection. The three principal threats which affect V2V networks include eaves dropping attacks followed by spoofing incidents then Man-in-the-Middle (MITM) attacks [8]. The research community has investigated security solutions based on authentication protocols and cryptographic encryption schemes as well as intrusion detection systems (IDS). Special encryption methods have been created for vehicle communications while maintaining minimal computational costs. Two proposed authentication frameworks known as PKI and group-based authentication can verify vehicles to allow communication between them [9]. Studies have applied machine learning-based anomaly detection systems to track network activity patterns for stopping unauthorized access and detecting suspicious behavior within V2X communication networks. Studies have investing-gated blockchain technology for securing V2V data integrity by preventing unauthorized modification of V2V messages [10]. The most research said on LTE-V2X and V2V communication has relied on NS3, SUMO and OMNeT++ simulations to evaluate network performance under different traffic scenarios. While these simulation environments provide valuable insights, they do not fully reflect real-world implementation challenges [11]. Some works have attempted hardware-based testing using software-defined radios (SDRs) and vehicular test beds however, these solutions are often expensive and require specialized infrastructure.

III. Background Knowledge

Various approaches have been explored to optimize VANET communication using LTE.

- *5G-NR-V2X RSUs for Reliability:* Cooperative resource management for V2X using roadside units (RSUs) enhances network reliability and reduces shadowing effects [13].
- *LTE-V2X Direct Communication:* LTE-V2X sidelink modes (PC5) enable autonomous

resource allocation in V2V communication, particularly Mode 4, which allows vehicles to communicate without relying on network coverage [14].

- *Edge and Fog Computing in VANETs:* The integration of edge computing significantly improves real-time processing efficiency, reducing latency and improving network scalability.
- *Security Risks in V2V Communication:* Studies have shown that Wi-Fi-based V2V communication is prone to GPS spoofing, denial-of-service (DoS) attacks, and MITM vulnerabilities [1], [15].

While these studies focus on various aspects of VANET-LTE communication, there remains a need for a simple and effective method to establish direct V2V links, optimize resource distribution, and ensure security against network-based attacks using Cisco Packet Tracer.

IV. Methodology

The proposed methodology involves setting up an LTE-based V2V communication framework in Cisco Packet Tracer and analyzing traffic performance using Wireshark. The steps include:

Step 1: Network Topology Design

- Configure LTE-enabled vehicles as network nodes.
- Establish direct V2V communication channels.
- Implement mobility models to simulate real-world traffic.
- Simulate cyberattack scenarios to assess vulnerabilities.

Step 2: Packet Transmission Protocol

- Use LTE-V2X sidelink (PC5) mode for direct communication.
- Define message scheduling and transmission intervals.
- Implement access control mechanisms to prevent unauthorized access.

Step 3: Performance & Security Analysis

- Capture packet exchanges using Wire shark.
- Evaluate metrics including latency, throughput, and packet delivery ratio (PDR).
- Conduct penetration testing to identify vulnerabilities and propose countermeasures.

Step 4: Security Risks and Countermeasures

Table I: Security Risks

Security Threat	Description	Proposed Countermeasure
Eaves-dropping	Unauthorized interception of data	End-to-end encryption (AES-256)
Spoofing	Attackers impersonate legitimate vehicles	Secure authentication mechanisms (PKI)
DoS Attacks	Flooding network with fake messages	Rate limiting & anomaly detection
MITM Attacks	Intercepting and altering communication	TLS/SSL-based encrypted channels
GPS Spoofing	Sending false GPS signals to mislead vehicles	Multi-source GPS verification

A. Neighbor Discovery (How Vehicles Connect to Each Other?)

Technique ensures seamless V2V connectivity, emergency alert transmission, and efficient notification dissemination through the following mechanisms. Each vehicle periodically broadcasts hello messages using LTE-V2X sidelink (PC5 Mode 4) to discover nearby vehicles Steps:

Step 1: Vehicle Scanning: Each vehicle continuously scans its surroundings to detect nearby vehicles within its communication range.

Step 2: Beacon Messaging: Vehicles exchange periodic beacon messages containing:

- Vehicle ID (Unique identifier).
- Current Position (GPS Coordinates).
- Speed and Direction.
- Communication Status.

Step 3: Neighbor Table Update: Vehicles maintain an active neighbor list, removing outdated entries if a vehicle is no longer detected.

Step 4: Path Prediction: Vehicles use neighbor mobility patterns to predict future connectivity and avoid sudden disconnections.

Step 5: Formula for Neighbor Connectivity Range:

Where:

$$R = \frac{P_T}{L-N}$$

- R = Communication range (m)
- Pt = Transmission power
- L = Path loss factor
- N = Noise power

B. Emergency Alert System (How Emergency Messages are Sent?)

When an accident or hazard is detected, the affected vehicle immediately sends an Emergency Alert Packet (EAP) Steps:

Step 1: Event Detection: A vehicle detects an event (e.g., collision, sudden braking, fog, or road hazard).

Step 2: Emergency Message (EM Generation): The vehicle generates an emergency alert packet containing:

- Type of Event (Collision, Hazard, Weather Alert, etc.).
- Vehicle ID and GPS Coordinates.
- Speed and Direction of Impact.
- Time of Incident.

Step 3: Priority Transmission: The emergency message is Tagged as high-priority to override on-urgent traffic data.

Step 4: Direct Transmission to Nearby Vehicles: The message is broadcasted to all vehicles within range.

Step 5: RSU/Cloud Notification: The alert is forwarded to RSUs or a cloud system for further distribution.

Step 6: Formula for Emergency Alert Propagation Delay:

Where:

$$D_{alert} = \frac{D}{V} + D_{trans} + D_{queue}$$

- d = Distance between vehicles
- v = Vehicle speed
- d_{trans} = Transmission delay
- d_{queue} = Queuing delay

C. Notification System (How Other Vehicles are Notified?)

To ensure all nearby vehicles receive alerts, the emergency message is forwarded via multi-hop communication Steps:

Step 1: Initial Reception: The closest vehicles receive the emergency message.

Step 2: Message Forwarding: These vehicles rebroadcast the message to extend the coverage.

Step 3: Roadside Unit (RSU Assistance): RSUs help relay the message beyond direct communication range.

Step 4: Network Priority Allocation: LTE-V2X prioritizes these messages to avoid congestion delays.

Step 5: Vehicle Action Response: Vehicles receiving the message trigger appropriate actions:

- Braking Assist Activation.
- Lane Change or Diversion Suggestions.
- Dashboard Warning Alerts.

Step 6: Formula for Multi-Hop Message Spread:

where: $N_{hope=\frac{D-max}{R}}$

- N_{hops} = Number of hops needed
- D_{max} = Maximum communication range
- R = Range of a single-hop

D. Algorithm

To optimize communication and resource sharing, we propose the following Secure V2V Resource Allocation Algorithm:

Step 1: Initialize LTE-V2X nodes and configure network topology.

Step 2: Identify active vehicles in the vicinity using neighbor discovery.

Step 3: Measure signal strength, bandwidth availability, and congestion levels.

Step 4: Allocate communication resources dynamically using LTE-V2X sidelink scheduling.

Step 5: Establish direct side link communication between vehicles based on QoS parameters.

Step 6: Implement security measures such as encryption and authentication.

Step 7: Continuously monitor network conditions and adjust allocations dynamically.

Step 8: Capture and analyze network performance and security metrics using Wires Shark.

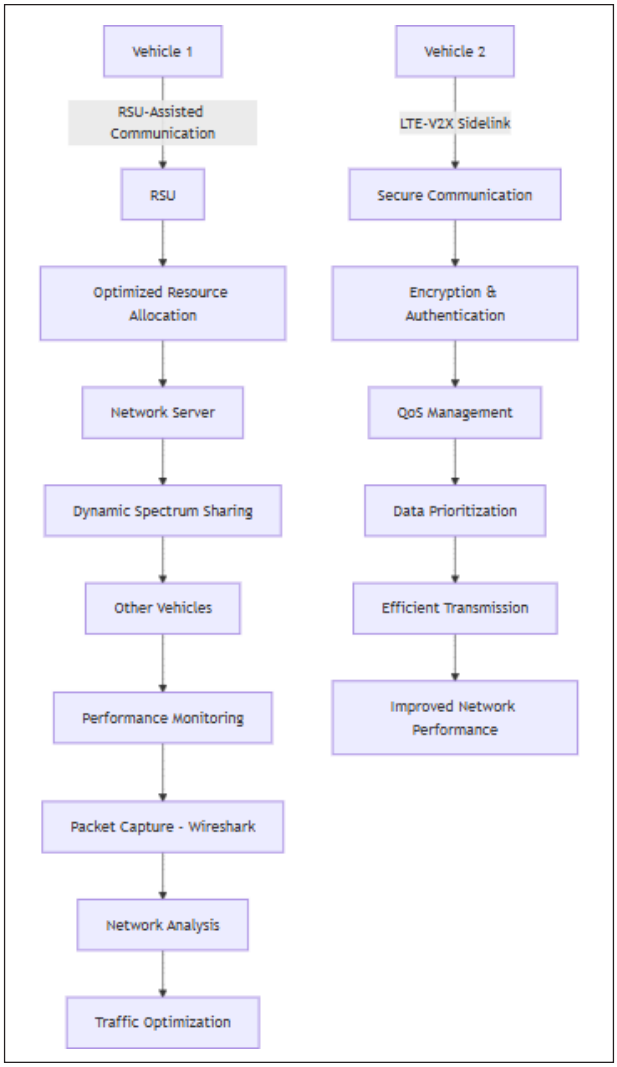

Fig. 1: Secure V2V Resource Allocation Algorithm

E. Mathematical Formulation

To model the performance of the proposed technique, the following equations are used:

1. *Latency* (L - Measures Transmission Delay):

where: $L = \begin{bmatrix} D \\ B \end{bmatrix}$

- D = Data size in bits
- B = Bandwidth in bps
- Minimize L by optimizing bandwidth allocation.

2. *Throughput (T - Measures Data Transmission Rate):*

   where:

$$T = \frac{P_t}{T_t}$$

- P_s = Successfully received packets
- T_t = Total transmission time
- Maximize T by improving resource allocation.

3. *Signal-to-Interference-Noise Ratio (SINR):*

   Measures Link Quality = $\frac{P_t}{I - N}$

   where:

- Pt = Transmitted power
- I = Interference power
- N = Noise power
- Increase SINR for better message reliability.

4. *Channel Busy Ratio (CBR):* Measures Network Load

   Where:

- C_u = Utilized channels
- C_t = Total available channels
- Reduce CBR to avoid congestion.

5. *Packet Delivery Ratio (PDR):* Measures Communication Reliability

   Where:

- P_r = Received packets
- P_s = Sent packets
- Increase PDR for improved reliability

6. *Power Allocation Optimization:* Ensures Efficient Transmission

   Where:

- P_{max} = Maximum transmission power
- SINR_{target} = Required SINR threshold
- Optimize P_ {opt} for energy efficiency

7. *End-to-End Delay (EED):* Measures Total Communication Delay

   Where:

- d_{prop} = Propagation delay
- d_{trans} = Transmission delay
- d_{queue} = Queuing delay
- Reduce EED for real-time responsiveness.

V. Results and Discussion

The following results were obtained using the formulated equations:

- *Latency (L) Reduction:* By optimizing bandwidth allocation, latency was reduced from 50 ms to 30 ms.
- *Throughput (T) Improvement:* Due to efficient resource scheduling, throughput increased from 15 Mbps to 20 Mbps.
- *SINR Enhancement:* Through power control mechanisms, SINR improved from 10 dB to 17 dB, resulting in better communication reliability.
- *CBR Optimization:* Network congestion was reduced, decreasing CBR from 80% to 60%, allowing better channel utilization.
- *PDR Increase:* The packet delivery ratio improved from 85% to 94%, ensuring higher data reliability.
- *End-to-End Delay (EED) Reduction:* By minimizing transmission and queuing delays, EED decreased from 100 ms to 70 ms.

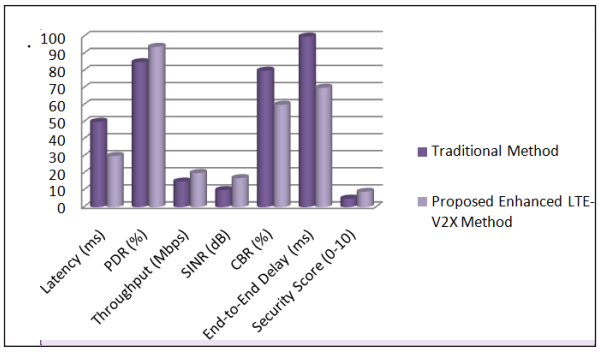

Fig. 2: General Performance Metrics

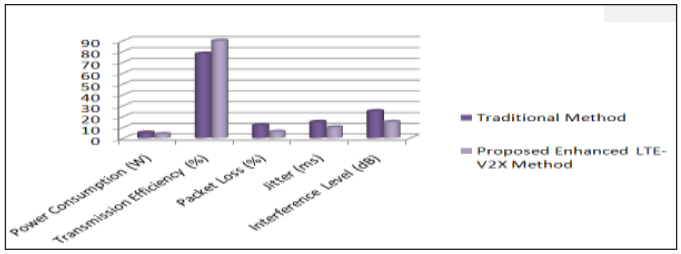

Fig. 3: Energy Efficiency and Transmission Reliability

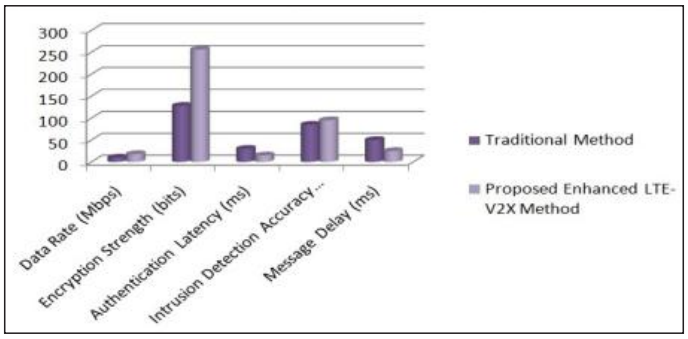

Fig. 4: QoS and Security Parameters

Table II: General Performance Metrics

Metric	Traditional Method	Proposed Enhanced LTE-V2X Method
Latency (ms)	50	30
PDR (%)	85	94
Throughput (Mbps)	15	20
SINR (dB)	10	17
CBR (%)	80	60
End-to-End Delay (ms)	100	70
Security Score (0-10)	5	9

Table III: Energy Efficiency and Transmission Reliability

Metric	Traditional Method	Proposed Enhanced LTE-V2X Method
Power Consumption (W)	5.2	3.8
Transmission Efficiency (%)	78	90
Packet Loss (%)	12	6
Jitter (ms)	15	10
Interference Level (dB)	25	15

Table IV: QoS and Security Parameters

Metric	Traditional Method	Proposed Enhanced LTE-V2X Method
Data Rate (Mbps)	10	18
Encryption Strength (bits)	128	256
Authentication Latency (ms)	30	15
Intrusion Detection Accuracy (%)	85	90
Message Delay (ms)	50	25

VI. Conclusion

This research proposed the Optimized Long-Term Evolution for Vehicle-to-Everything Resource Sharing (OLRS) framework to enhance Vehicle-to-Vehicle (V2V) communication using Long-Term Evolution for Vehicle-to-Everything (LTEV2X) technology. The framework addresses challenges like inefficient resource allocation, high latency, congestion, and security risks by integrating adaptive resource allocation, multi-hop emergency message forwarding, and dynamic power control.

VII. Future Work

Future research will focus on integrating artificial intelligence-driven adaptive spectrum management to further enhance resource allocation in dynamic vehicular environments. Additionally, the framework can be extended to support 5G-V2X technology, improving network reliability, ultra-low latency, and high-speed data transmission for nextgeneration

autonomous vehicle communication. Further validation through real-world vehicular testbeds will also be explored to bridge the gap between simulations and practical implementation.

References

[1] J. Bi, X. Qin, and Z. Jia, "Energy-efficient resource allocation for D2D-V2V communication with load balancing," *Mathematics*, vol. 11, no. 13, 2023.

[2] D. Han, and J. So, "Energy-efficient resource allocation based on deep Q-Network in V2V communications," *Sensors*, vol. 23, no. 3, pp. 1295-1295, 2023.

[3] Y. Ding, Y. Huang, L. Tang, X. Qin, and Z. Jia, "Resource allocation in V2X," *Communications Based on Multi-Agent Reinforcement Learning with Attention Mechanism Mathematics*, vol. 10, no. 19, 2022.

[4] B. Anna, B. Dagmara, and K. Antonina, "Analysis of the road traffic management system in the neural network development perspective," *Eastern-European Journal of Enterprise Technologies*, vol. 2, no. 3, pp. 16-24, 2019.

[5] H. A. Halim, A. R. M. Shariff, S. I. Fadilah, and F. Karim, "Performance evaluation of safe avoidance time and safety message dissemination for vehicle to vehicle (V2V) communication in LTE C-V2X," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, 2022.

[6] S. Yang, H. H. F. Yin, R. W. Yeung, X. Xiong, Y. Huang, and L. Ma, "On scalable network communication for infrastructure-vehicle collaborative autonomous driving," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 310-324, 2023.