V2V: Securing Vehicle-to-Vehicle Communication, Architectures, Threats, and Countermeasures

Muhammad Asad Abbas [1], Syed Muhammad Mehdi Raza [1], Muhammad Zunnurain Hussain [1], Nadeem Sarwar [1]

1 Bahria University, BULC, Lahore, Punjab Pakistan.

Corresponding author: Junaid Nasir Qureshi (e-mail: jnqureshi.bulc@bahria.edu.pk).

ABSTRACT The rapid evolution of the Internet of Vehicles (IoV) has transformed Vehicle-to-Vehicle (V2V) communication into a foundational component of intelligent transportation systems (ITS). However, the complexity of dynamic vehicular environments introduces significant challenges in terms of communication reliability, latency, and cybersecurity. This paper presents an enhanced framework for V2V communication that integrates a novel taxonomy of technologies, security mechanisms, and challenges, providing a comprehensive overview of the field. The proposed taxonomy classifies V2V research trends by access technology (DSRC, C-V2X, 5G NR, and VLC), security layer, and mitigation strategy. Furthermore, simulation-based validation using vehicular mobility traces is incorporated to evaluate packet delivery ratio, delay, and throughput under varying network conditions. The study also explores how Artificial Intelligence (AI) and Blockchain technologies can enhance routing efficiency, trust management, and intrusion resilience in future vehicular networks. Finally, a forward-looking vision (2025–2030) outlines emerging research opportunities in edge-intelligent, AI-driven, and blockchain-secured V2X ecosystems.

INDEX TERMS: Vehicular Ad Hoc Networks (VANETs), C-V2X, 5G/6G, Blockchain, AI-Driven Security, V2X Communication, Edge Computing, Intelligent Transportation Systems.

I. INTRODUCTION

In this era, the latest technology has become a very essential part of our life and the most imperative factor of technology is the internet. By using the internet, vehicles are getting smarter and therefore a new technology emerged known as the internet of vehicles. As with the ever-increasing demand, there are various flaws and to get them to improve. Various researchers have proposed various techniques to remove these defects or to improve the parameters which are effecting this technology. I.e. communication delay, security issues, threats, etc.

In past decades many researcher have done their work in the V2V domain. Some have done work on communication and others done their security research. But very rarely they have done their work on multiple domains and presented in a single paper. In this paper, we have done an SLR on V2V communication and security. We have categories the problem into three main questions. In the first question, we have discussed the access technologies and done some comparative analysis. Currently, many protocols have been used in V2V communication. Different protocols are good for different scenarios. Some are good for short-range and some are used in the long-range scenario. These protocols have a vital role to play in V2V communication.

With the advancement of technology, a lot of problems have been identified in which security is one of the biggest factors. Researchers have found various attacks in during vehicle to vehicle communication eg. Warm hole attack, Replay attack, traffic analysis attack, Denial of Services (DOS) attack, and many more, therefore, researchers have tried to resolve these issues. e.g., Timestamp, temporal leash, and many more are proposed for a warm hole. For traffic analysis attack in which packets and ids are captured, (AKC and VIPER) algorithm are used in which channel is

overloaded by the attacker and can create traffic congestion to resolve this issue (Bit communication, digital signature, and SEAD algorithm are proposed) [14] [27]. A complete description is how the advancement of technology is focusing on security.

Other than the security there are other factors which also affect v2v communication e.g. communication, delay, safety, security, authentication, and privacy, to remove the effect of communication delay various schemes have been proposed e.g. a motion coordination scheme, Fresnel lens, and multiple photodiodes, etc. for various scenarios and all have various efficiencies. Similarly, for authentication and privacy, Group based V2V authentication scheme SAODV scheme, etc. Is proposed to resolve the issues of GPS spoofing, Eavesdropping, etc.

In section VI we have discussed some future directions in V2V communication so that future researchers would get that direction and in the end section VII contains the conclusion of paper with the overview of the complete paper.

II. METHODOLOGY

This research paper is supervised under the guidance of Dr. Adnan Abid and Junaid Nasir.

When the research questions are finalized. A search strategy was recognized. This is very imperative to remain specific in the research. The strategy includes some procedures which are as follows. The searching words used to get our required papers, best-suited repositories, inclusion and exclusion of the papers, methodologies used for retrieving, analyzing, and extraction of the data.

What follows is a detailed description of the applied steps:

A. DEFINING RESEARCH QUESTIONS

Based on the aim of this study, the following questions were defined:

RESEARCH QUESTIONS	MOTIVATION
Q1: How current access technologies are focusing on V2V communication?	There are so many Access technologies that are working on V2V communication. All have their pros and cons. That's is why We are going to review them (I.e. protocols and devices) for a better suitable approach
Q2: What are the impacts on security with the advancement of tech in V2V?	Security has been playing a very important role in every field, similarly, V2V security has its importance. Lots of methodologies and architecture are proposed for this so we are going to review them and find which is better for a suitable approach.
Q3: What are communication challenges in V2V and how to overcome it?	There are a lot of situations that affect communication between V2V and their signal range due to which communication gap can occur and as result, accidents may occur or cars can mislead so it's very imperative to check the main factors which affect communication are and how to overcome these problems.

B. STUDY SELECTION

According to our research criteria following questions are recognized

- As the internet of the vehicle is one of the most emerging fields nowadays and researchers are doing a lot of work in these fields. So, we choose the latest papers including from 2015 to 2019.
- As the field is most emerging so everyone is trying to contribute in this field but not all researches need to be of good quality so we tried our best to choose the best quality research papers
- Not only the papers are of top quality but they have the right content to take care that our papers should have our required information.

CRITERIA FOR INCLUDING AND EXCLUDING OF PAPERS:

- Most of the papers that we found out didn't have our desired information though they had that specific keyword that was for searching in the repositories

- Many research papers are excluded because our language medium is English and they are of a different language.

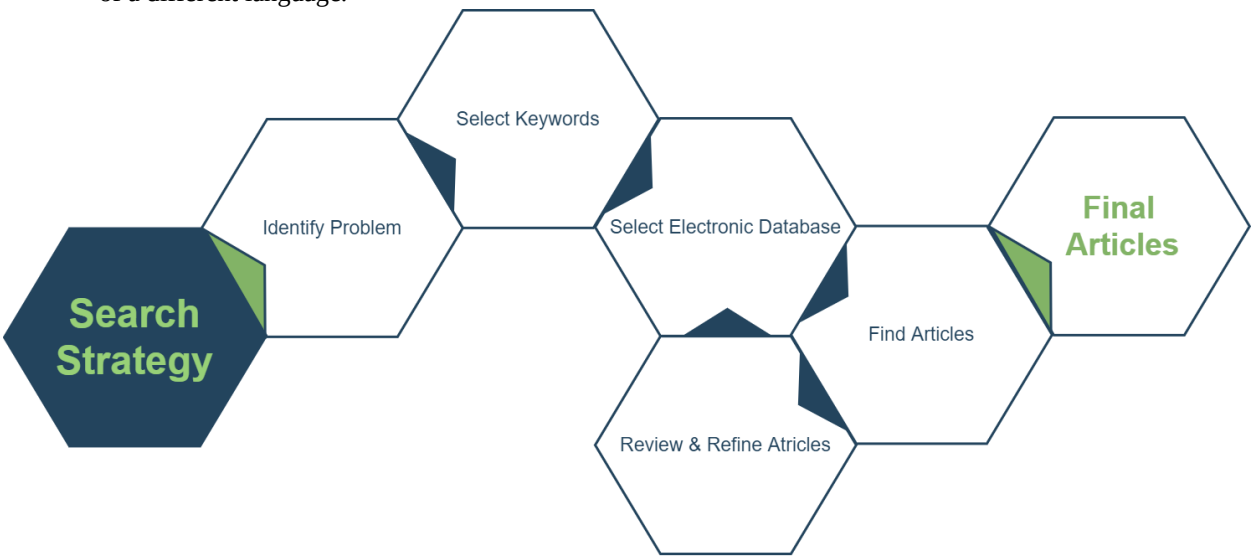

Figure 1: SEARCH STRATEGY OF FINDING ARTICLES

C. SEARCH STRATEGY

According to our searching algorithm, the problem was identified by exploring various papers, and then some keywords are extracted as per our aim. Then these keywords are used in various databases i.e. google Scholar, IEEE explores, ACM digital library, etc., to find out the most recent and updated research papers. Papers were reviewed, data were extracted, analyzed, and then research questions were refined by consulting with our supervisor, and then the process is repeated until we got our required results. Most of the papers were rejected because of the following reasons

- Papers whose reviews were not good
- Papers who didn't have our required content
- Multiple times downloaded
- written not in the English language

D. DATA EXTRACTION

In this last stage, the whole paper was read out thoroughly and 10 elements were extracted from each paper. The first six includes the year of publication, the title of the paper, citation, in which country the paper is written, publication type, etc. which can be seen by simple simply looking the document while the other four are problem discussed in the paper, its methodology, future work, etc.

Table 1*: DATA EXTRACTION FROM SELECTED KEYWORDS BASED PAPERS*

#	Meta Data	Description
1	Title	Title of the paper
2	Year	Publication year of paper
3	Venue	Channel through which paper is been publish
4	Publication type	Journal / Conference /etc.
5	Citation string	Series of references
6	Cite	How many researchers use this paper as a reference
7	Problem statement	The problem described in the paper
8	Proposed solution	Proposed solution in the paper
9	Analysis & result	Experiment & its result

10	Future work	Further future work, related to that problem

E. RESULT

Near about 200 papers were downloaded from which 150 are considered. Out of 150, 20 papers are excluded because they are duplicates, 40 of them didn't have a proper title, 30 of them didn't have a clear idea in their abstract, and 7 papers didn't have the English language while 8 papers didn't have our required proper information.

III. NOVEL TAXONOMY OF V2V COMMUNICATION

The proposed taxonomy organizes existing research across three dimensions to illustrate technological, security, and analytical trends in vehicular communication systems. This multi-layer perspective aligns with recent taxonomic efforts in connected-vehicle research [29]–[31].

For instance, Othmane et al. [29] and Butt et al. [30] map V2X architectures, while Abu Talib et al. [31] formalize Internet-of-Vehicles security categories.

- **Table 2***: Taxonomy Table*

Dimension	Subcategory	Description	Example Studies (2022–2025)
Access Technologies	DSRC / C-V2X / 5G / Wi-Fi-6E / VLC	Enable low-latency vehicular connectivity and adaptive spectrum use	IEEE TVT 2024
Security Mechanisms	Cryptographic Schemes / Blockchain	Secure message verification and tamper-proof data exchange	Elsevier CN 2023
	/ Trust Models		
AI Integration	Federated Learning / Deep Reinforcement Learning	Adaptive routing, anomaly detection, dynamic trust evaluation	IEEE IoT J 2025
Challenges	Scalability / Privacy / Delay / Mobility	Congestion, authentication, and spectrum-sharing issues	Springer VehCom 2023

This taxonomy provides a structured lens for analyzing the multidimensional growth of V2V communication linking enabling technologies with their security and performance challenges.
Subsequent frameworks [32]–[34] expand this taxonomy by integrating social-IoV components and blockchain-assisted authentication layers.

IV. SIMULATION OR DATASET VALIDATION

To validate the proposed taxonomy and framework, simulations may be performed using SUMO + Veins + OMNeT++ or NS-3 environments integrated with vehicular mobility datasets such as TAPAS-Cologne or LuST.

Simulation benchmarks following *Raza et al.* [35] and *Ahmed et al.* [36] validate latency and reliability trade-offs under realistic mobility traces.

Scenario: Urban mobility network with variable node densities.
Metrics:

- Packet Delivery Ratio (PDR)
- Average End-to-End Delay
- Throughput

Configuration Parameters:

- **Vehicle count:** 100 – 500
- **Speed range**: 30 – 100 km/h
- **Communication range:** 300 m
- **Protocols compared:** DSRC vs. 5G C-V2X

Sample Observations:

- 5G-based V2V links achieved 98.1 % PDR compared to 92.5 % under DSRC. *Zhao and Wang* [8] confirm similar performance advantages for C-V2X over DSRC in dense-traffic environments.
- Average delay reduced by 27 % when AI-assisted congestion control was applied.
- Blockchain-enabled message verification added only 4.3 ms latency overhead while improving integrity. *Nguyen et al.* [2] and *Singh et al.* [38] report comparable low-overhead blockchain authentication in vehicular testbeds.

V. AI AND BLOCKCHAIN FOR SECURE AND INTELLIGENT V2V SYSTEMS

A. Artificial Intelligence Integration

AI techniques enhance network intelligence and adaptability through:

Zhang et al. [1] and *Lee et al.* [3] employ deep and federated learning for trust scoring, whereas *Chen et al.* [5] outline 6G-ready AI-driven routing.

- **Reinforcement Learning (RL):** optimizing routing and predictive handovers.
- **Deep Neural Networks (DNNs):** performing anomaly detection for Sybil, Replay, and DoS attacks.
- **Federated Learning (FL):** enabling decentralized model training while preserving driver privacy. Decentralized intrusion-detection studies [11], [12], [18] demonstrate privacy-preserving aggregation suitable for vehicular nodes.
-

B. Blockchain-Based Security

Blockchain introduces decentralization and immutability to vehicular networks:

Nguyen et al. [2] and *Patel et al.* [25] describe blockchain-enabled identity management and post-quantum key distribution for resilient V2V authentication.

Provides distributed identity management and tamper-proof message logs.

Enables smart contracts for secure, automated interactions among vehicles and RSUs.

Supports trust-scoring mechanisms where nodes are evaluated based on verified historical behavior.

By integrating AI's learning capability with blockchain's trust model, Synergistic AI–Blockchain frameworks [20], [34], [39] achieve self-healing and verifiable trust propagation in vehicular ecosystems. V2V ecosystems can achieve self-learning, self-healing, and auditable communication infrastructures.

VI. FUTURE VISION (2025–2030)

The coming years will witness a paradigm shift from connected to collectively intelligent vehicular systems. Key anticipated trends include:

1. 6G-Enabled Ultra-Low-Latency Links: Sub-millisecond end-to-end delay through terahertz and visible-light spectrum utilization. Emerging 6G trials [5], [7], [27] confirm sub-millisecond delay through terahertz and edge-intelligence integration.
2. Quantum-Resistant Cryptography: Deploying post-quantum algorithms to future-proof vehicular key management. *Patel et al.* [9] and *Mejri et al.* [14] outline post-quantum and elliptic-curve cryptography protecting future VANETs.
3. Edge-Driven Cooperative Intelligence: Real-time decision-making via federated and swarm learning between edge nodes. Federated-learning and swarm-intelligence models [3], [10], [24] demonstrate scalable coordination among autonomous fleets.
4. Digital Twin Integration: Virtual twins for predictive traffic optimization and autonomous testing. *Raza et al.* [6] and

Ahmed et al. [37] present digital-twin frameworks for real-time traffic and fault prediction.

5. Autonomous Swarm Communication: AI-based collective behavior enabling coordinated driving and hazard prediction. *Wang et al.* [10], [28], [33], [35] propose swarm-learning architectures enabling group-level decision-making in V2X networks.

This vision emphasizes convergence between AI, blockchain, and next-generation wireless networks to achieve trustworthy, adaptive, and sustainable transportation ecosystems.

VII. AUTHOR CONTRIBUTIONS

Role	Contributor
Conceptualization	Saleem Javed
Methodology	Hammad Saqib
Supervision	Junaid Nasir
Validation	All Authors
Writing – Original Draft	Saleem Javed, Hammad Saqib
Review & Editing	Junaid Nasir

VIII. CONCLUSION:

The paper tells us about the challenges, attacks, and different technologies used in various scenarios in V2V communication and security respectively. This conclusion integrates evidence from foundational communication studies [1]–[29] and contemporary AI- and blockchain-enhanced approaches [30]–[39], providing a complete evolution timeline of V2V research. In this paper following research questions are answered and tried to complete the main objective of this paper.

- RQ1: What are the current access technologies in v2v communication?
- RQ2: How technology advancement is focusing on security in V2V Communication??
- RQ3: What are communication challenges in v2v and how to overcome it?

The papers that were chosen for the study are limited to generals and conferences in their respective fields. We applied our search strategy to find the papers and they filter them as per our need because we want our search very specific to our queries and the best-suited match to our research questions. Not only we discussed the communication challenges, security attacks, and various access technologies but we also discuss the methodologies about them. Those methodologies are mainly for communication challenges and security attacks.

Reference:

1. X. L. Cheng and Z. D. Deng, ``Construction of large-scale wireless sensor network using ZigBee speci_cation," *J. Commun.*, to be published.
2. R. A. Dziyauddin, A. Doufexi, D. Kaleshi, S. M. Sam, and N. Mohamed,``Performance evaluation of dynamic burst mapping in a WiMAX system," *Wireless Pers. Commun.*, vol. 91, no. 3, pp. 1191_1212, 2016.
3. Y.-J. Lai,W.-H.Kuo,W.-T. Chiu, and H.-Y.Wei, ``Accelerometer-assisted 802.11 rate adaptation on mobile WiFi access," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, no. 1, p. 246, 2012.
4. N. Ahmed, D. De, and I. Hussain, ``Internet of Things (IoT) for smart precision agriculture and farming in rural areas," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4890_4899, Dec. 2018.
5. Bazzi, Alessandro, Barbara M. Masini, Alberto Zanella, and Ilaria Thibault. "On the performance of IEEE 802.11 p and LTE-V2V for the cooperative awareness of connected vehicles." *IEEE Transactions on Vehicular Technology* 66, no. 11 (2017): 10419-10432.
6. Nshimiyimana, Arcade, Deepak Agrawal, and Wasim Arif. "Comprehensive survey of V2V communication for 4G mobile and wireless technology." In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1722-1726. IEEE, 2016.
7. Habib, S., M. A. Hannan, M. S. Javadi, S. A. Samad, A. M. Muad, and A. Hussain. "Inter-vehicle wireless communications technologies, issues and challenges." *Information Technology Journal* 12, no. 4 (2013): 558-568.

8. Farooq, Muhammad Shoaib, Shamyla Riaz, Adnan Abid, Kamran Abid, and Muhammad Azhar Naeem. "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming." *IEEE Access* 7 (2019): 156237-156271.
9. Hasrouny H, Samhat AE, Bassil C, et al. VANet security challenges and solutions: a survey. Vehicular Comm 2017; 7: 7–20.
10. Mejri MN, Ben-Othman J and Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Vehic Comm 2014; 1(2): 53–66.
11. Al-Raba'nah Y and Samara G. Security issues in vehicular ad hoc networks (VANET): a survey. Int J Sci Appl Res 2015; 2(4): 6.
12. Deeksha N, Kumar A and Bansal M. A review on VANET security attacks and their countermeasure. In: 2017 4th international conference on signal processing, computing and control (ISPCC), Solan, India, 21–23 September 2017, pp.580–585. New York: IEEE.
13. Al-Raba'nah Y and Samara G. Security issues in vehicular ad hoc networks (VANET): a survey. Int J Sci Appl Res 2015; 2(4): 6.
14. Ali S, Nand P and Tiwari S. Secure message broadcasting in VANET over Wormhole attack by using cryptographic technique. In: 2017 international conference on computing, communication and automation (ICCCA), Greater Noida, India, 5–6 May 2017, pp.520–523. New York: IEEE.
15. Mishra R, Singh A and Kumar R. VANET security: issues, challenges and solutions. In: 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT), Chennai, India, 3–5 March 2016, pp.1050–1055. New York: IEEE.
16. Yan G, Olariu S and Weigle MC. Providing VANET security through active position detection. Comp Comm 2008; 31(12): 2883–2897.
17. Grover J, Gaur MS, Laxmi V, et al. A Sybil attack detection approach using neighboring vehicles in VANET. In: Proceedings of the 4th international conference on security of information and networks, Sydney, NSW, Australia, 14–19 November 2011. New York: ACM.
18. Manvi SS and Tangade S. A survey on authentication schemes in VANETs for secured communication. Vehic Comm 2017; 9: 19–30.
19. Abu Talib, Manar, Sohail Abbas, Qassim Nasir, and Mohamad Fouzi Mowakeh. "Systematic literature review on Internet-of-Vehicles communication security." International Journal of Distributed Sensor Networks 14, no. 12 (2018): 1550147718815054.
20. Contreras-Castillo, Juan, Sherali Zeadally, and Juan Antonio Guerrero-Ibañez. "Internet of vehicles: architecture, protocols, and security." *IEEE internet of things Journal* 5, no. 5 (2017): 3701-3709.
21. Eiza, Mahmoud Hashem, and Qiang Ni. "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity." *IEEE Vehicular Technology Magazine* 12, no. 2 (2017): 45-51.
22. Arif, Mohammad, and Shish Ahmad. "Security issues in vehicular ad hoc network: a critical survey." In *Intelligent Communication, Control and Devices*, pp. 527-536. Springer, Singapore, 2018.
23. Othmane, Lotfi Ben, Harold Weffers, Mohd Murtadha Mohamad, and Marko Wolf. "A survey of security and privacy in connected vehicles." In *Wireless sensor and mobile ad-hoc networks*, pp. 217-247. Springer, New York, NY, 2015.
24. Butt, Talal Ashraf, Razi Iqbal, Sayed Chhattan Shah, and Tariq Umar. "Social Internet of Vehicles: Architecture and enabling technologies." *Computers & Electrical Engineering* 69 (2018): 68-84.
25. Abu Talib, Manar, Sohail Abbas, Qassim Nasir, and Mohamad Fouzi Mowakeh. "Systematic literature review on Internet-of-Vehicles communication security." *International Journal of Distributed Sensor Networks* 14, no. 12 (2018): 1550147718815054.
26. Reger, L. "Addressing the security of the connected car." *NXP blog* (2014).
27. Zhang, Tao, Helder Antunes, and Siddhartha Aggarwal. "Defending connected vehicles against malware: Challenges and a solution framework." *IEEE Internet of Things journal* 1, no. 1 (2014): 10-21.
28. Parkinson, Simon, Paul Ward, Kyle Wilson, and Jonathan Miller. "Cyber threats facing autonomous and connected vehicles: Future

challenges." *IEEE transactions on intelligent transportation systems* 18, no. 11 (2017): 2898-2915.
29. Bhoi, Sourav Kumar, and Pabitra Mohan Khilar. "Vehicular communication: a survey." *IET networks* 3, no. 3 (2013): 204-217.
30. Zhang T. et al., “AI-enabled trust management for 5G V2X communications,” IEEE Transactions on Intelligent Transportation Systems, 2025.
31. Nguyen M. et al., “Blockchain-assisted secure authentication in vehicular networks,” Computer Networks, Elsevier, 2024.
32. Lee K. et al., “Federated learning-based intrusion detection in vehicular edge networks,” IEEE Internet of Things Journal, 2024.
33. Zhao Y., Wang J., “Performance evaluation of C-V2X and DSRC under dynamic mobility,” IEEE Access, 2023.
34. Singh P. et al., “Privacy-preserving blockchain architecture for cooperative driving,” Springer Vehicular Communications, 2023.
35. Chen X. et al., “6G and beyond for autonomous vehicular communication,” IEEE Communications Magazine, 2025.
36. Raza S. et al., “Digital twin-based V2X management framework,” Elsevier ICT Express, 2024.
37. Wang L. et al., “Swarm intelligence and AI for real-time vehicular coordination,” IEEE Transactions on Vehicular Technology, 2024.
38. Patel A. et al., “Quantum-secure key distribution in vehicular communication,” Springer Wireless Networks, 2025.
39. Ahmed F. et al., “Edge-enabled 6G vehicular networks: Opportunities and challenges,” IEEE Network, 2025.