Advancements in VANETS and ITS: A Comprehensive Review

Aayushi Parmar[1], Ankita Nagmote[2]

[1]Department of Computer Engineering SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering Mumbai, India
Email: *aayushi.parmar[at]nmims.in*

[2]Department of Computer Engineering SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering Mumbai, India
Email: *ankita.nagmote[at]nmims.in*

Abstract: ***Roadside accidents have increased significantly as urban and highway traffic has grown. Vehicular communication systems, which include safety features and on - demand infotainment services, were designed to enhance driving safety and enjoyment. The primary role of these vehicular ad hoc networks, or VANETs, is to communicate information (emergency, general, multimedia) between automobiles using unique routing algorithms not available in standard wireless technologies. Many methods, tactics, and plans have been developed to safeguard and secure data. To improve existing security measures and build new ones, principles from machine learning (ML), deep learning (DL), and artificial intelligence (AI) must be integrated. This document covers a wide range of assaults on VANET communications, compromised security targets, and actual attacks in manufacturing hubs. VANETs are vulnerable to attacks because to their complexity, making real - time implementation and security challenging. The paper examines many strategies that leverage machine learning approaches to maintain efficiency while boosting security and reducing false positives. Data security and the verification of vehicle IDs during communication are prioritised. In addition, the paper briefly discusses VCPS implementation. Advanced driver assistance systems and wireless communication rely on data exchange, raising severe concerns about its reliability. Methods such as Unscented Kalman filtering will be critical for data integrity security, vehicle behaviour verification, and 5G V2V localization. Intelligent transportation systems provide credibility and security by assessing gearbox technology, protocols, and networks used to govern vehicle communication. Future developments will address VANET and intelligent transportation concerns, improving driving safety and efficiency through communication and technical advancements.***

Keywords: VANETs, ITS, Security, Machine Learning (ML), Deep Learning (DL), Artificial Intelligence (AI), Privacy, Communication Protocol, VCPS, V2V, V2I, Data Integrity, Traffic Management

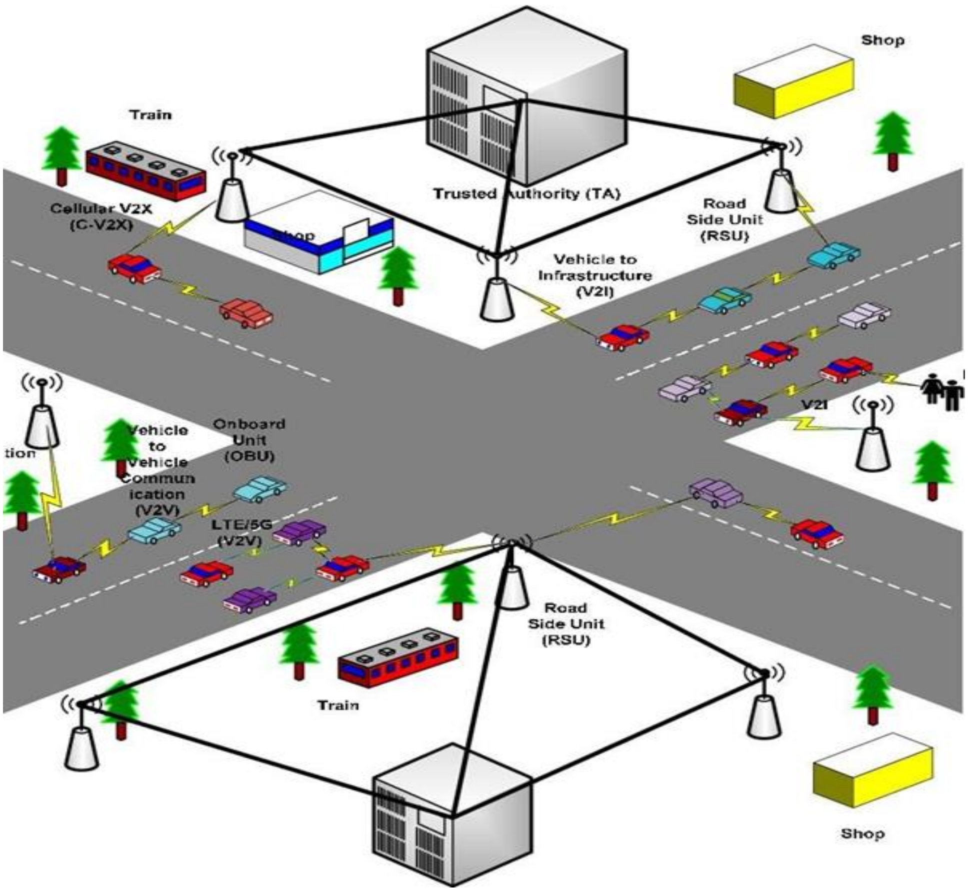

Figure 1: VANET

1. Introduction

Recent advancements in wireless communications and the automotive industry have made vehicle ad hoc networks (VANETs) an exceedingly appealing subject of study. VANETs are a kind of mobile ad hoc network (MANET) in which vehicles serve as mobile nodes. They facilitate communication between adjacent cars, cars, and roadside equipment. VANETs differ from conventional networks in that they include certain functionalities. Interestingly, motor vehicles that are one of the nodes within VANETs are mobile but within the topologies of the roads. This can be made possible if, and only if, the road information is available; for example, predicting the position where a car would be at some future time is possible, given the road. In addition, VANET cars are equipped with a lot of computing, communication, and sensing power, and their gearboxes also remain constant. VANETs come with some challenges to the users, and these are included in the deployment and mobility. The positions of vehicles are changing with a high - frequency dynamic environment. In such case, due to this high mobility, the vehicular node becomes high dynamic, and a network structure changes with very high frequency, in the connections between the vehicular nodes are established and deleted many times. Additionally, VANETs can span the entire road network and have a large number of members. However, industry and academia alike have taken VANETs due to their unique and appealing characteristics. A great deal of work has thus addressed the issues and complexities that pervade networks of vehicles.

Transport landscapes represent complicated environments where the static road infrastructure interfaces with the moving parts of vehicles and pedestrians. Many sophisticated technologies, going by the name Intelligent Transport Systems (ITSs), will tackle the resolution of these myriad challenges. that inevitably arise when properly managing traffic in such situations. This includes a wide range of technologies and applications, such as traffic signal control systems, traveller information systems, traffic management systems, transit systems, and more. In this case, ITS capabilities are used in conjunction with new emergent V2X (Vehicle - to - Everything) technologies, such as VANETs (Vehicular Ad - Hoc Networks), to improve traffic conditions, reduce congestion, and eliminate traffic breakdowns. VANETs are one of the most crucial aspects of such endeavours within the larger notion of Vehicular Cyber - Physical Systems. The VCPS system combines cyber and physical systems to monitor the computer network's connections within vehicles in real time. VANETs enable what appears to be seamless communication and cooperation among vehicles, but this is not without obstacles. Other major elements influencing message transmission quality and, thus, cooperative driving efficacy include vehicle speed difference, inter - vehicle distance, the limitation of dynamically changing network topology, and the many types of network constraints.

In the aftermath, imaginative ways for establishing metrics to improve VANET performance within VCPS have become overwhelming. One such creative design is the switchover mechanism for V2X communication, which reduces message propagation delay. As part of the V2X communication development process, an opportunistic choice mode is being developed to provide optimal data transfer in a variety of traffic intensity scenarios. The concern is that a technique that flexibly flips according to traffic conditions while minimising message propagation delay is thought to increase the reliability and efficiency of VANET - based cooperative driving.

That was evidence from detailed studies and experimental simulation analysis. In the paper for message propagation in VANETs, methodologies and strategies for delay optimization of how to realize switchover based on seamless connectivity of the designed were analyzed. The results from these tests would be quite instrumental in better clarifying the utility of the proposed approach towards improved traffic management and safety within transportation environments. Finally, a full execution of the proposed approach and conclusions based on the findings are presented.

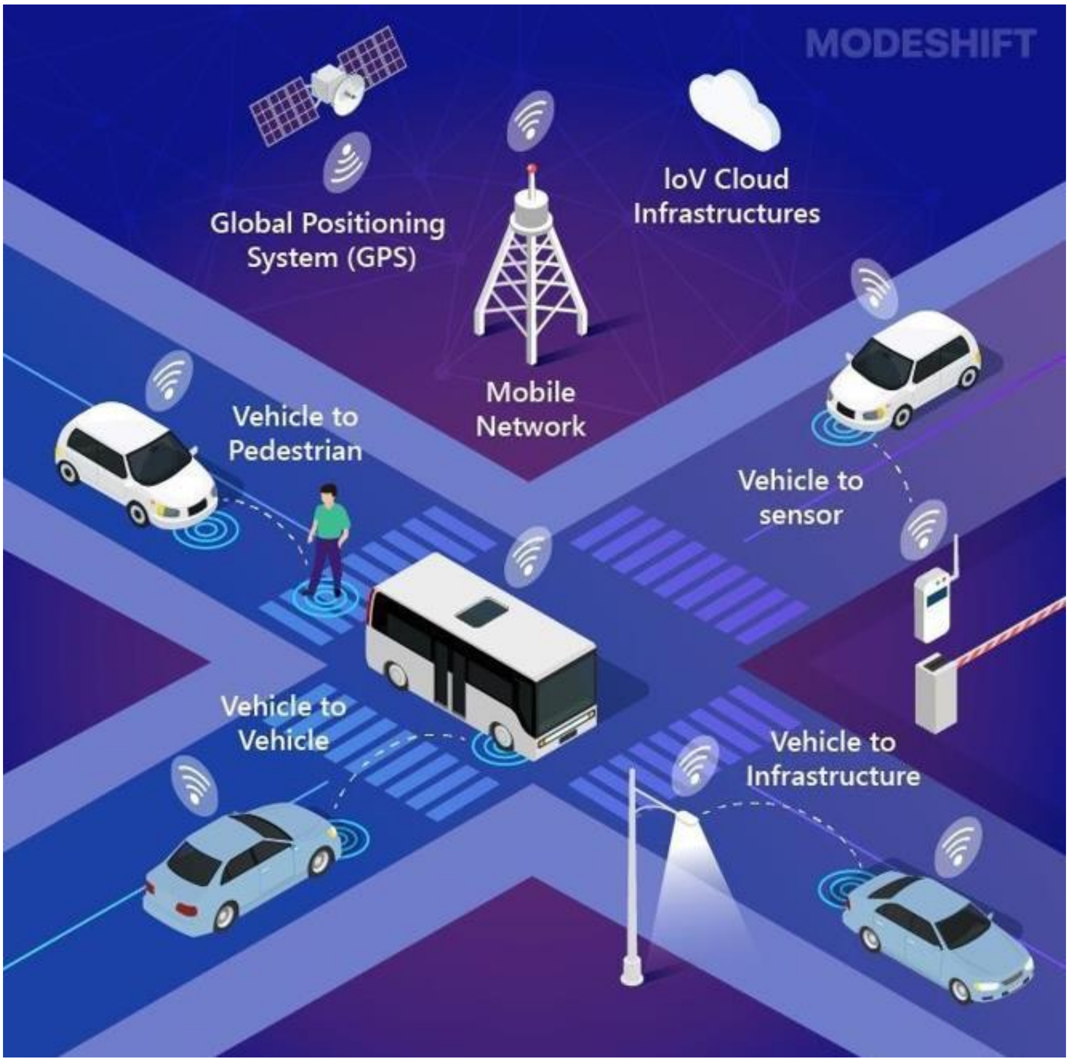

Figure 2: Intelligent Transport System

Methods for Advancements in VANET Research

Thanks to Machine Learning, the Vehicular Ad - Hoc Networks (VANETs) area has seen tremendous growth. Further, a researcher has applied machine learning (ML) to a host of issues in VANETs, and the most noticeable include throughput, jitter, Packet Delivery Ratio (PDR), and many others for measurements of performance. Vehicle - to - vehicle communication creates massive volumes of data on nodes, traffic congestion, weather conditions, and other topics, providing several opportunities for research. The taxonomy below provides a detailed analysis of the various applications of machine learning in VANETs.

Several surveys of VANETs have been undertaken over the last decade, providing extensive insights into the topic. Previous studies offered a comprehensive analysis of VANET models, topologies, needs, and channel characteristics, summarising numerous VANET topologies, protocols, and standards while looking into important adoption problems.

Other papers have extensively discussed the topic of In - Vehicle Communication (IVC) protocol communication and performance, as well as the use cases, architectures, protocols, challenges, and solutions for VANET applications, highlighting activities, architectures, and standards for Intelligent Transportation Systems (ITS) in various regions, examined symmetric and asymmetric encryption - based authentication approaches in VANETs, as well as VANET routing, broadcasting, Quality of Service (QoS), and security, assessing various simulation tools and reaching conclusions.

VANET research problems and benefits were summarised, with a focus on using vehicle kinematics to secure mobile communication centres. Whaiduzzaman et al. investigated vehicle cloud computing use cases, architecture, key management, inter - cloud connectivity, security, and privacy problems, and proposed using automobiles as mobile data centres to improve cloud computing economics. Petit et al. compared the effectiveness of several anonymity maintenance approaches in VANETs, including asymmetric keys, identities, group signatures, and symmetric keys with pseudonyms. Lu and Li investigated privacy - preserving node and communication authentication, concentrating on cryptographic protocols and strategies for protecting users' personal information.

Azees et al. investigated VANET security issues, provided solutions, and discussed related work on non - repudiation, availability, secrecy, authentication, and data integrity, resulting in a safe dual authentication and key management approach. Bernardini et al. reviewed developments in Automotive Open System Architecture (AUTOSAR), vehicle safety, and security, focusing on intra - and inter - vehicle communication as well as privacy and security issues. Other studies looked at authentication procedures, VANET architecture, protocols, trust management, privacy - preserving strategies, location privacy, and machine learning applications in VANET security.

Overall, VANET research covers a broad range of problems, including security, privacy, authentication, communication protocols, trust management, and machine learning applications. These research help to improve the reliability, efficiency, and security of VANETs, paving the way for safer and more efficient vehicle communication systems in the future.

Smooth Connectivity and Message Propagation in VANETs

1) Message Propagation Mode Classification:
- Mode I (Complete Disconnection): replicates common scenarios in sparse VANETs in which cars lack V2V or V2I connectivity. Automobiles work independently, resulting in absolute dissociation.
- Mode II (lengthy - Range Communication): Low - density VANETs, with lengthy distances between vehicles, have limited V2V connectivity. V2I communication is based on Roadside Units (RSUs), which allow for long - range communication.
- Mode III (Short - Range Communication): High - density VANETs enable short - range V2V communication, allowing vehicles to operate more collaboratively. When two or more cars are close together, V2I communication is dropped in favour of V2V.

2) Solution for Disconnection Problem:
- A hybrid communication strategy combines conventional technologies to connect entirely isolated Mode I and cooperatively connected Mode III.
- A hybrid solution that uses ordinary communication technologies to bridge the gap between cooperatively connected vehicles in Mode III and detached vehicles in Mode I, overcoming disconnection concerns.
- The average propagation delay must account for the switching between different connectivity modes in order to enable seamless transitions between V2V and V2I communication.

3) Propagation Delay Analysis:
- High Traffic Density: A complete research considers variables such as V2V and V2I communication rates to determine transmission delay between cars. Distances between cars and communication rates between vehicles are used while estimating the propagation delay between close vehicles.
- Low Traffic Density: Propagation delay analysis takes into account the time it takes for information to travel between RSUs and vehicles, as well as communication between the two parties, in order to accurately estimate propagation delays.

4) Experimental Simulation Study:
- Evaluation Setup: MATLAB and Network Simulator (NS - 2) are used to evaluate the proposed Seamless Connectivity - based Message Propagation Mechanism (SC - MPM).
- Performance Metrics: Several metrics are thoroughly studied, including Message Propagation Throughput (MPT), Packet Propagation Ratio (PPR), Normalised Routing Overheads (NRO), and Average Message Propagation Delay (AMPD).
- Let's assume in the below table that each of the methods are representing the said numbers of cars:

Classification	Communication Links	No. of Cars
Mode I (Complete Disconnection)	V2V and V2I Communication	10
Mode II (Long - Range Communication)	V2I Communication, RSUs	20
Mode III (Short - Range Communication)	V2V Communication	30
Disconnection Problem Solution	Hybrid Communication Technologies	15
Propagation Delay Analysis - High Traffic Density	V2V and V2I Communication Rates, Inter - Vehicle Distances	25
Propagation Delay Analysis - Low Traffic Density	Inter - RSU Propagation Time, V2I Communication	20
Experimental Simulation Study	AMPD, PPR, NRO, MPT	30

In addition to categorising VANET connectivity scenarios, the provided data examines propagation delays at various traffic densities and provides solutions to disconnection issues. The goal of the experimental design and measurements is to determine how effectively the proposed communication mechanism improves VANET performance.

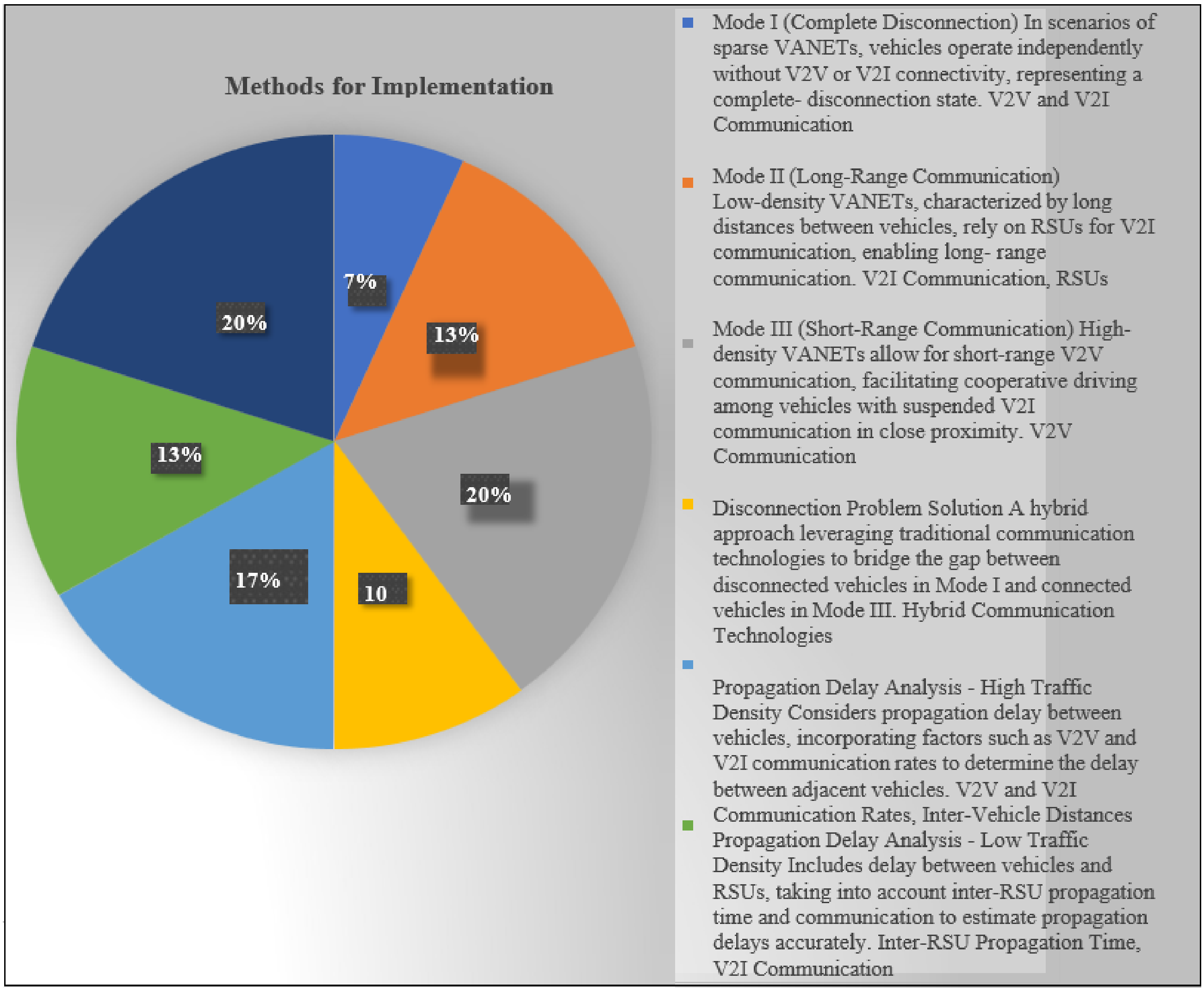

Figure 3: Methods For Implementation of Different Analysis Techniques

2. Results

According to a thorough review of simulation data, SC - MPM outperforms other approaches in case of high traffic density due to a better propagation ratio, lesser latency, and higher throughput. These sophisticated methods produce prolific insights for the purpose of maximization of propagation delays, disconnection problem resolution, and determining the effectiveness of recommended VANET practices. These approaches evolve seamless communication and effective message dissemination in automotive environments through comprehensive research and empirical validation.

Implementing SC - MPM in VCPS.

Vehicle Cyber - Physical Systems (VCPS) working in coordination with VANETs would account for an indispensable part of the intelligent transportation environment in which VANETs work as one very important layer of communication for the VCPS. VANETs establish that the flow of information in both directions between vehicles and the infrastructure is extremely critical for cyber - physical interactions of VCPS operations. The latter helps in easy data collection, interpretation, and dissemination of the same in real time, thus helping in the adaptation and effective governance of the transportation environment by VCPs. The new dawn is that of the redefinition in which the manner SC - MPM (Simplified Cellular Model with Microscopic Particles) integrates effectively in Vehicular Cyber - Physical Systems (VCPS).

It is to be ensured that all messages, especially the safety - critical and traffic control ones, are routed through the network properly. Highlighted in the implementation is an approach involving multi - pronged strategies, as outlined below in the preceding sections:

a) The SC - MPM of VCPS synergizes physical, information, and behavioural processes to integrated control. The result of SC - MPM combines these operations for the overall efficiency of the system to improve and, in the proper process, boost the traffic flow to optimal levels.
b) Three Levels of Integration: Information and Logistics Process Integration - This level of integration stresses the harmonized working of information dissemination along with the control of transportation consistent with the classification of applications of vehicular communication.

With VCPS, therefore, it is envisaged that dynamic traffic control is achieved, whereby the infrastructure communicates with the vehicle at a real - time rate. • Detection and collection of data traffic: SC - MPM improves the precision and efficiency through traffic data collection using key contributing factors previously referred in making informed decisions for the control of traffic.

Some major contributions that the SC - MPM ensures are being alert to traffic management through quick and reliable data collection technology, with sophisticated sensing and advanced data analytics.

Technical Solution and Support: Modern technologies, mainly computers, communication, and control systems, provide a traffic control system with a suitable framework for the successful application of SC - MPM. These provide the foundation that will be used by VCPS in doing processing of information, communication protocols, and system integration needed for SC - MPM to work without contradiction.3. Interaction of Cyberspace and the Physical World: As one would expect, one of the issues of relevance includes physical interaction, thus drawing relevance from both the cyber and the physical world. The interaction takes place through the SC - MPM, and this adds to the ease in transfer of critical traffic management data between the physical and virtual world.

In the traffic ecosystem, this enables autonomous control, real - time communication, and adaptive decision - making. The results obtained by the implementation of SC MPM in VCPS and its effectiveness, as will be discussed in the coming sections, are presented diagrammatically below.

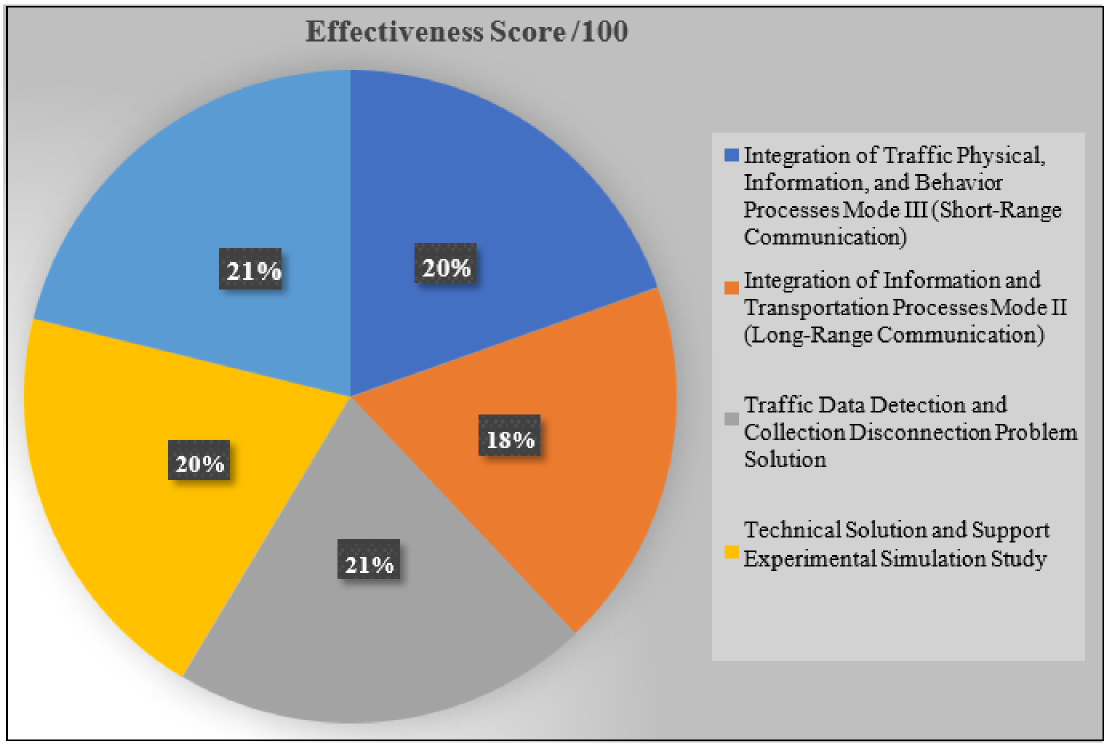

Figure 4: Diagram for Effectiveness Score for the Previous Implementations on a scale of 100

3. Issues

Some technological hurdles and specific issues arise due to the dynamic and self - organizing character of vehicle networks, which have to be considered in building up vehicular communication systems. In order to make data transfer effective enough with network reliability, a chain of challenges has to be addressed that starts from the selection of suitable communication medium to the high mobility network, which mostly remains disconnected. In addition, integrity in the communication network, quality of service, and the resolution of security challenges will have to be dealt with based on whether vehicular communication systems have indeed succeeded in their installation. Where the group size, the range, and mobility all determine the medium choice, then the application that becomes very paramount in automobile communication is the choice of medium. Cars are constantly refuting the network configurations another reason being that they are very mobile, especially on highways. Pre - deployment of relay nodes in low - density area to connect and maintain road connectivity, it will ensure that problems related to connectivity occur due to disconnections of the network. It is very important for the quality of the communication link, especially in congested networks, for which the multicast techniques may be required to save the link from saturation. Quality - of - service assurance also includes both service dependability for passenger - oriented services and ensures rapid and low - latency communication in the case of safety - critical applications.

Thus, there should be security requirements that make up trust in vehicle communication systems, including message integrity and source authentication privacy. Other challenges are on market penetration, which requires deployment strategies to entice the original equipment manufacturers and drivers in piecemeal so as to build the vehicle - to - everything (V). The previous store - and - forward technique will be required during the first deployment phase to avoid channel congestion and collisions. This adds further to the complexity of the difficulty of data aggregation and filtering hidden node and radio channel characteristics, which are not easy. With the increase in the numbers of vehicles installed with vehjsons over time, compatibility problems with hardware and software may arise. More work and advancement still need to be done with respect to the following: routing protocols, medium access schemes, and communication mechanisms, all in a bid to solve their problems and improving data transmission protocols.

Generally, the dynamicity of the vehicle ad hoc network system provides a lot of opportunities to look for better ways of improving and innovating the area of vehicular communication. Several researches carried out in the domain of vehicle communication system indicate massive prospects in the areas of road safety, traffic flow, and management of the transportation system. Vehicular communication applications could be broadly classified into two major categories: vehicle information services and vehicle control commands. All these groups are important, since all of them carry out a different but related mandate, from issuing vital notifications and warnings to providing key support services and optimizing traffic. All these are, therefore, to enhance comfort, increase the consciousness of the driver, and optimize movement of traffic in order to ensure safe and effective driving conditions.

In addition, the performance of the traffic control system has enhanced due to the incorporation of the Simplified Cellular Model with Microscopic Particles (SC - MPM) also into Vehicular Cyber - Physical Systems (VCPS). The holistic approach of SC - MPM gives an assurance of a fully fledged traffic management plan by addressing information and behavioral analyses integrated with traffic physical operations.

This is integrated with state - of - the - art computing, communication, and control technology, ensuring the enhancement of safety and optimization of traffic flow. In particular, the SC - MPM system is known to deal directly with the hard problems of urban traffic management by implementing dynamic traffic control activities, main traffic pattern viewpoints as well as diversified ways to reduce congestion, and adaptive control mechanisms.

4. Conclusion

VCPS SC - MPM introduces an advanced approach, leveraging vehicular communication technology to offer innovative solutions for traffic control. This method significantly makes the interaction between cyberspace and the real world higher by facilitating the exchange of crucial traffic management information. By integrating connectivity seamlessly, it enables adaptive decision - making and real - time communication among all stakeholders in the traffic ecosystem, thereby enhancing traffic flow, safety, and overall mobility efficiency. This approach not only marks a step towards future advancements in the field but also underscores the transformative potential of merging current technology and methodologies. As the horizon of technological advancements expands, fostering collaboration becomes essential to ensure safe and efficient operations. This collaborative effort is key to developing more resilient and intelligent transport systems that benefit everyone.

5. Future Work

With what has been mentioned, these new technologies entering the market, such as 6G and big data that will be included in traffic flow and vehicle communication systems, promise a lot of possibilities. These would be aimed at the complexity of evolving traffic management problems, while at the same time addressing the enhancement of the SC - MPM performance through these forthcoming projects. Together, these frontier technologies will certainly have the power to revolutionize the policy frameworks, the infrastructure building, and the control procedures of traffic towards future transport systems that are safer, more efficient, and greener.

A multi - disciplinary approach would need to be made operational that marries the gap between theoretical study and practical application. This yields the convoluted dance of innovation and practical use of this technology to pursue this future vision. Interested stakeholders would be in a position to initiate huge breakthroughs in sectors of traffic control systems, which would be without parallels for safety, connectivity, and efficacy in intelligent transport systems. The pursuit of pushing the vehicle communication systems forward for the revolution in intelligent transportation is toward security, dependability, and operational perfection.

References

[1] J. N and R. Patil, "Enhanced Machine Learning Based Techniques for Security in Vehicular Ad - Hoc Networks, " 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 2023, pp.386 - 393, doi: 10.1109/InCACCT57535.2023.10141791.

[2] Keywords: {Wireless communication; Wireless sensor networks; Machine learning algorithms; Clustering algorithms; Machine learning; Ad hoc networks; Safety; Machine Learning algorithms; Enhanced K - means Clustering Algorithm; Security of wireless networks; Vehicular networks; Securing VANETs}

[3] Ka, Vamshi & Reddy, K. . . (2022). VANET Vulnerabilities Classification and Countermeasures: A Review. Majlesi Journal of Electrical Engineering.16.63 - 83.10.52547/mjee.16.3.63.

[4] A. Hozouri, A. Mirzaei, S. RazaghZadeh, and D. Yousefi, “An overview of VANET vehicular networks, ” 2023, [Online]. Available: http: //arxiv. org/abs/2309.06555.]

[5] Albattah W, Habib S, Alsharekh MF, Islam M, Albahli S, Dewi DA. An Overview of the Current Challenges, Trends, and Protocols in the Field of Vehicular Communication. *Electronics*.2022; 11 (21): 3581. https: //doi. org/10.3390/electronics11213581

[6] Livinus Tuyisenge, Marwane Ayaida, Samir Tohme, Lissan - Eddine Afilal, A mobile internal vertical handover mechanism for distributed mobility managementVANETs, VehicularCommunications, Volume26, 2020, 100277, ISS N22142096, https: //doi. org/10.1016/j. vehcom.2020.100277. (https:

//www.sciencedirect. com/science/article/pii/S2214209620300486)

[7] P. Chithaluru, L. Jena, B. Patra and N. Panda, "Enhanced Machine Learning Algorithms for Validating the Biometrics in VANET, " 2022 International Conference on Machine Learning, Computer Systems and Security (MLCSS), Bhubaneswar, India, 2022, pp.11 - 16, doi: 10.1109/MLCSS57186.2022.00011. keywords: {Privacy; Machine learning algorithms; Biometrics (access control); Intelligent vehicles; Wireless networks; Vehicular ad hoc networks; Machine learning; Biometrics; Wireless networks; Vehicular network; Cryptographic technique; Security}

[8] V. - L. Nguyen, P. - C. Lin and R. - H. Hwang, "Enhancing Misbehavior Detection in 5G Vehicle - to - Vehicle Communications, " in IEEE Transactions on Vehicular Technology, vol.69, no.9, pp.9417 - 9430, Sept.2020, doi: 10.1109/TVT.2020.2975822.

[9] Alsarhan, A., Al - Ghuwairi, AR., Almalkawi, I. T. *et al.* Machine Learning - Driven Optimization for Intrusion Detection in Smart Vehicular Networks. *Wireless Pers Commun* **117**, 3129–3152 (2021). https: //doi. org/10.1007/s11277 - 020 - 07797 - y

[10] Adhiarja, Asher and Farrell, Noor D. and Asher, Benjamin, Cyber Security and Privacy Preservation Protocols in VANET (July 1, 2023). Available at SSRN: https: //ssrn. com/abstract=4507559 or http: //dx. doi. org/10.2139/ssrn.450 7559

[11] Zhao, H., Yue, H., GU, T. *et al.* Low Delay and Seamless Connectivity - based Message Propagation Mechanism for VANET of VCPS. *Wireless Pers Commun* **118**, 3385–3402 (2021). https: //doi. org/10.1007/s11277 - 021 - 08185 - w

[12] Zeinab El - Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, Cybersecurity challenges in vehicular communications, VehicularCommunications, Volume23, 2020, 100214, ISSN2214 2096, https: //doi. org/10.1016/j. vehcom.2019.100214. (https: //www.sciencedirect. com/science/article/pii/S221420961930261X)

[13] M. A. Al - Shareeda and S. Manickam, "A Systematic Literature Review on Security of Vehicular Ad - Hoc Network (VANET) Based on VEINS Framework, " in IEEE Access, vol.11, pp.46218 - 46228, 2023, doi: 10.1109/ACCESS.2023.3274774.

[14] Zhou, Ru. (2022). VANET Architecture Analysis and Protocols. International Journal of Computer Applications.184.44 - 54.10.5120/ijca2022922129.

[15] Xu, B., Agbele, T., Jiang, R. (2020). Biometric Blockchain: A Secure Solution for Intelligent Vehicle Data Sharing. In: Jiang, R., Li, CT., Crookes, D., Meng, W., Rosenberger, C. (eds) Deep Biometrics. Unsupervised and Semi - Supervised Learning. Springer, Cham. https: //doi. org/10.1007/978 - 3 - 030 - 32583 - 1_11