International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at :www.ijsrcseit.com
doi : https://doi.org/10.32628/IJSRCSEIT

IoT-Based Smart and Secure Vehicle Communication Using Advanced Technique

Abhishek Anand[1], Susheel Kumar Tiwari[2]

[1]M Tech Scholar, [2]Professor

Department of Computer Science & Engineering, Millennium Institute of Technology and Science

Bhopal-462001, Madhya Pradesh, India

ARTICLEINFO

Article History:

Accepted: 01 Dec 2023

Published: 10 Dec 2023

Publication Issue

Volume 9, Issue 6

November-December-2023

Page Number

361-368

ABSTRACT

Attractive solutions like the Internet of Vehicles (IoV) have changed the automotive industry. IoV is the foundational idea of connected and autonomous vehicles. In order to facilitate conversation both inside and outside of a car, numerous wireless networking options are provided. Thanks to these interfaces, the car may communicate with other automobiles and the outside world. With the development of technology for IoV and linked cars, autonomous driving will become a viable option for motorists. Autonomous vehicles and the IOV concept can learn a lot from big data technology, which describes massive, interconnected databases. A new method of planning has been proposed in this work for use with autonomous vehicles that are also connected to the internet. In particular, we detail the in-car gateway's role in the larger hardware and software architecture for autonomous vehicles, outlining the communication flows, data interchange requirements, and fundamental service capabilities that must be in place before an autonomous driving service can be developed.

Keywords- IOT, Internet of Vehicles, MANET, VANET

I. INTRODUCTION

VANET is also known as Vehicular Ad-hoc Network and the future of Vehicle Crash avoidance. VANET has resemblances with MANET However VANET Safety capabilities and its unique traits that make its specific from MANET. Vehicular Network means communication between vehicle and vehicle & communication between vehicle and Road Side Unit. VANET's main purpose is safety. Apart from safety, it also provided other information like email, video/ audio [1]. VANET Convert every participant as a node and covert into them in a NETWORK. In VANET, vehicles are free to move in 360 directions.

Classification of Network

A network that allows information to be circulated among all of these entities, based on well-defined rules. A group of objects which are connected is known as Network. Classification of network is shown in figure 1.1.

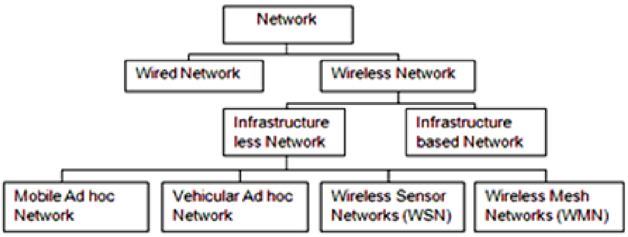

Figure 1.1: Classification of network

Wired Network

Connections (network links) between nodes employ media such optical fibre and twisted pairs to join together a collection of laptops and other devices. All of the nodes in this network are hardwired into the central computer where the website is hosted[2].

Wireless Network

In a wireless network for linking nodes or cars, wireless links such as computers to the Internet utilizing radio waves. Wireless link is used for Wi-Fi hotspots in cafes, airport lounges, or other public locations.

Infrastructure based network

These networks are based on a base station that controls communication between two nodes and these networks have advantages over an Ad-hoc network. For example, the security level will be increased, and faster data, transmission speeds in this type of network.

MANET (Mobile Ad Hoc Network)

MANET is defined as a network in which nodes move autonomously and interact without a structure. It integrates peripherals without a centralized structure and can run.

Infrastructure less network (Ad-hoc network)

The Ad hoc network has no base station, and the network is ad hoc, for nodes in wired networks communicate with each other without a base station. The network is ad-hoc since it does not rely on pre-existing infrastructure such as wired network routers or wired network access points.

VANET (Vehicular Ad-hoc Networks)

VANET is intended to facilitate contact between road vehicles and between vehicles andinfrastructure on the roadside. For this communication to be possible, it is essential to position devices known as Road Side Units (RSUs) and On-Board Units (OBUs) on each vehicle and each road. These devices can send or receive data from roadside units to or from them. However, suppose a vehicle is unable to transmit its data directly to an RSU. In that case, it will relay its data to other vehicles before the RSU data is reached using a multi-hop transmission technique. Without any pre-existing units, VANET vehicles are linked to each other. It also contains a unit on the lane. Roadside units operate as gateways to provide mobile nodes with access to infrastructures[3,4,5]. The OBU functions in the vehicle network as a radio system, while the Road Side Unit (RSU) functions as a fixed unit. Figure 1.2 depicts the Network of VANET.

Each car has OBU and the 802.11p protocol is used to connect to other vehicles. OBU is made up of sensors, managing modules, and a system for communication. The discovery of routes in VANET is a great challenge because we know VANETs often change their topology.

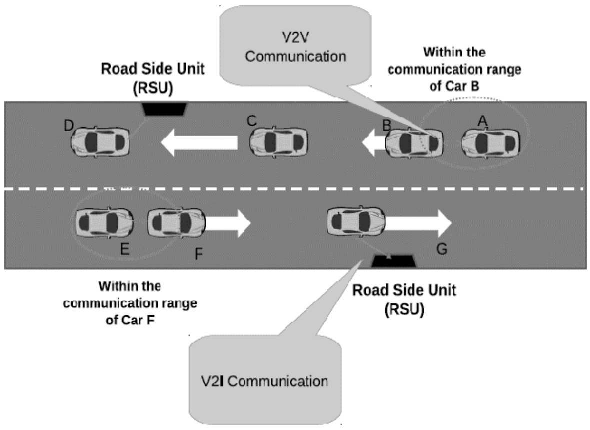

Figure 1.2: Network of VANET

This coordination helps to improve traffic safety, traffic management, and traffic quality. Speed, direction, and location are the required vehicle details for OBU. It will lead to improved coordination on road safety.

Intelligent Transport system

To improve the safety, reliability, and efficiency of transport systems, new standards for vehicles are required. Intelligent Transportation Systems (ITS) are widely recognized as software or gadgets connected to transport networks. Intelligent Transportation Systems (ITS) have no specific significance, and the nation or territory attempting to execute Intelligent Transportation Systems (ITS) has its vision and purpose. Europe, for example, has a different view of Intelligent Transportation Systems (ITS) as a modern framework for urban transport information and communication technology, which is often referred to as telematics for transport. The Intelligent Transportation Society of America (ITSA) in the United States describes ITS as a wide range of technology that can solve many of the transport problems that exist. ITS consists of a wide range of technologies, including the processing of information, communications, and electronics. To save lives, time, and money, the incorporation of all these technologies into existing transport networks is expected[6].

Japan finally sees ITS as a primary solution to the challenges of the transport sector that, in turn, cover accidents, accidents, and environmental degradation. ITS tackles these concerns using the latest sophisticated contact and control technologies. As we said earlier, each nation has its vision of ITS, but they all have the same coherent purpose: the use of modern technologies to fix issues related to transport systems. Generally, ITS aims to use networking and information technology in vehicles and vehicle infrastructures to control all the components (such as vehicles, traffic loads, and routes) that make up the transport network. Protecting reducing travel times, optimizing traffic flows, and reducing fuel consumption are the ITS' priorities. By incorporating modern technologies such as cordless sensor, cellular, and mesh networks, it aims to resolve these issues by implementing it carefully. By carefully incorporating relevant new technology into transport networks and cars themselves, pollution will both be evicted and road safety enhanced along with increased efficiency. The biggest task, though, is to incorporate these technologies into a cohesive and cooperative framework that can resolve multiple transport concerns[7]. This modern cooperative climate, in which all networking, electronics, and computer technology are well integrated, would allow safer highways, more efficient mobility, and reduce environmental effects [8]. VANET is a type of wireless Ad-hoc network that serving a broad range of applications and advantages, including in areas such as automotive protection, entertainment, and regulation of traffic, one of the most powerful components of ITS

II. RELATED WORK

Numerous research projects and initiatives pertaining to vehicle communication systems have recently been conducted. As a result, we publish the most recent research publications on three keywords that are connected to our contribution—IoV, CSC, and autonomous driving—in this part2.1 IoV related worksAs a matter of fact, we classify these works according to the technologies they use. We detail the strategies that have been recommended to make use of modern technologies like Blockchain, Software Defined Networking, and Information Centric Networks (ICN). In addition, we briefly discuss how big data technologies can be applied to automotive networks.

New architecture CCN-IoV was introduced in [9] that delivers Content-Centric Network (CCN) content chunks at the network layer. Using a Named Data Networking (NDN) simulator, the authors analysed CCN efficiency. IoV's Their initial results support implementing CCN in the car sector. There is a specific and lasting name for every piece of stuff. We used the NS2 simulator to evaluate CRoWN's capabilities in comparison to the standard IP-based method. Simulation findings show that the proposed method is effective in establishing differentiated traffic management while maintaining a manageable traffic volume. An ICN concept centred on the location of vehicles was described in [10]. The authors of wanted to use ICN capabilities to send multimedia across a VANET for cheap. The method put an emphasis on the supply-demand equilibrium and the portability of material, both of which have significant effects on efficiency. The research used adaptive heuristic algorithms to enhance on-demand caching, priority-driven path selection, and source upkeep with the fewest possible resources. Results -from assessing the plan showed an increase in efficiency. In [11], for instance, the GeoZone NDN-based solution for forwarding interest packets in automotive networks was proposed, which helps to lessen network flooding. Their contribution is a geo-referenced content name strategy for making a dissemination zone with node GPS coordinates and a zone forwarding approach to prevent content request overload. More research is needed to fully understand the potential benefits and drawbacks of this method, including the impact of factors like vehicle speed. In addition, a service-oriented system architecture based on NDNs was proposed in [12]. This idea included a standardised naming convention for several types of services (including safety, transit info, and entertainment), a service sublayer to facilitate request management and information sharing techniques, and a network load-based service prioritisation system. Simulation-based performance evaluation proved the system's service management prowess, although improvements in this area are still needed, especially with regards to time-sensitive service management. In this study, we provide a system for managing redundant messages, a mechanism for reducing the impact of source mobility, and a method for advertising material so that providers can let users know when their content is available. MobiVNDN has been proven to be an effective solution for addressing mobility challenges and the unreliability of wireless communication media. The study [13,14, 15] simulated the impact of different speeds on VANET performance to learn more about how ICN was incorporated into vehicular networks. The two most crucial indicators were throughput and packet delivery ratio.

III.PROPOSED WORK

Based on the results of the survey and the gaps analysis, we suggest a Cluster-based, Self-organized, and Intelligent (CSI) framework (shown in Figure 4.5) to facilitate efficient and secure communication while reducing gridlock.

The Internet of Things (IoT)-based VANET must be built and deployed during the IoV installation phase. The Internet of Things (IoT) has helped standard ad hoc automobile networks mature into smart ad hoc car networks.

Cluster Formation and Data Transmission in the Initial Setup Phase Coverage areas for each vehicle and RSU are established in Steps 2 and 3. node, best suited for better data transmission.

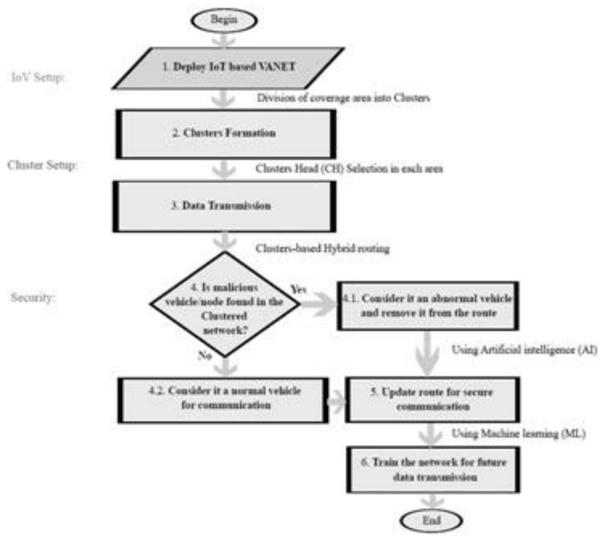

Figure: 4.6 Proposed Architecture flow diagram

Updating routes, rogue nodes, and network configuration is a part of the security mechanism. Step 4, 5, 6: When there is a drop in network performance, the concept of artificial intelligence (AI) is utilised to identify malicious or failed nodes in the network that are preventing vehicles/RSU from communicating with one another and contributing to gridlock. Machine learning (ML) algorithms serve as processing units that self-update in preparation for future shifts in how data is transmitted. Key takeaways from applying the proposed CSI model to actual problems in current IoV networks are as follows:

To provide a constant and quick connection, the IoV network will employ the principle of traffic congestion minimization. In addition, we will be using a robust cluster-based routing system to evaluate the proposed work. In light of this, more research is needed to compare and contrast the suggested and existing models in terms of throughput, packet loss, packet delivery ratio, and latency, and to test these metrics against one another.Consequences and foresight In this section, we zero in on object detection as one of the many services that perceptual approaches can provide for autonomous vehicles

IV.RESULT ANALYSIS

In this Paper, we provide the results of our simulations using the APROVE clustering algorithm. Clustering performance, average clustering algorithm overhead, and robustness to channel error were compared between APROVE and MOBIC using the NS2 simulator. Average cluster head duration, average cluster member duration, average rate of cluster head change, and average cluster size are some metrics used to evaluate clustering performance[16]. All three APROVE formulations described inare simulated to evaluate their clustering efficiency: APROVE with clustering interval, APROVE with cluster head contention, and asynchronous APROVE.

First, this chapter provides an overview of the simulation environment, which comprises the network and traffic simulators. The clustering performance metrics are then outlined. After then, the self-similarities and the Future Prediction Period are adjusted through simulations. Once the settings have been adjusted, simulations are run to analyse APROVE's and MOBIC's clustering efficiency versus average velocity. Similarly, the typical cost of using APROVE with aggregated message forwarding is shown next to MOBIC. Finally, we provide the clustering performance metrics as a function of channel error for APROVE and MOBIC to assess the approach's resilience. It evaluates the channel error performance of the three different APROVE formulations.

a. Simulation Set-up

Network Simulator: The APROVE methodology is well accepted in the networking research field, therefore it was naturally adopted by the NS2 [15] programme used for this type of research. The NS2 tests employed the 802.11 MAC and a 914MHz Lucent Wave LAN DSSS network card with a radio range of 250m. The MOBIC code was included in an older version of NS2 that was distributed with reference [17]. All APROVE simulations were run with the TH parameter set to 1s and other values for self-similarities, f, and CI manipulated. A virtual freeway with one hundred cars was used for the tests. While 500s were spent in each simulation, only the last 200 were used to determine effectiveness. This was done to ensure that the duration metrics (cluster head and member duration) were stabilised prior to obtaining any readings. Eight separate traces were used to run the simulations, and the average of the results was taken.

b. Non-Repudiation

This prevents fraudsters from concealing their offences since, even if the attack occurs, the ability to detect attackers will be accelerated. Vehicle networks will demand real-time for numerous functions and should hence be available at all times. If there is a hold of seconds in various applications, these apps require high speed from sensory networks or through the Ad-hoc network, and the subsequent elimination or massage may be a bit pointless.

c. Confidentiality

This security requirement ensured that information was only read by authorised users. In group communications, where team members are not permitted to read such information, confidentiality is necessary.

d. Authentication

It ensures that the data was entered by an authorised user. Because in IoV, the reaction nodes are based on data established from the other end, the data accessing the physical stream must be precise and established by an authentic individual[18].

e. Integrity

It assures that the data in the sender and the data on the sender side are same. Only authorised users can convert messages. The recipient follows the identical procedure as the sender to generate the second call from the message and compare it to the first message. This procedure ensures the data's integrity.

Table 4.1 QoS Parameters Comparison S.no Authors Average Throughput (Mbps) Packet Loss Rate (%)

S.no	Author	Throughput	Packet loss
1	Muhammad Asim Saleem et al.	5.34	13.77
2	Lucy Sumi and Virender Ranga	54.94	25.74
3	Amr Tolba	90.17	7.83
4	Sumit et al.	74.33.	7.87
5	**Proposed**	**94.45**	**6.74**

(Also called Total Packet/Success Transfer Rate.) The simulation parameters used in these studies were derived under varying conditions, making direct comparisons between them impossible. Table 4.1 compares previous research using Quality of Service (QoS) characteristics like throughput and packet loss, whereas Fig. 4.1 provides a visual depiction of these results. In Table 4.1, we compare the IoV models proposed in recent years by different methods and algorithms in terms of the QoS parameters. (a) shows a comparison of the observed throughput in various scenarios for IoV; however, the work proposed in [3] and [4] fares much better than the others because it proposes maintaining vehicle connectivity through the estimation of headway distances, a Wiener process that can be exploited thanks to the Kolmogorov equation. (b) depicts a comparative examination of the transmission loss in several Internet of Vehicles (IoV) scenarios, revealing that the transmission loss in the works proposed by [3] and [4] is lower thanks to the reliable connections established between the vehicles. As can be seen in, different researchers have come up with different models, each with their own set of pros and cons. However, using AI to improve upon the state of the art in terms of secure communication in IoV networks is a welcome development. More research is needed to develop an intelligent and trustworthy VANET model based on the Internet of Things utilising AI methods

V. CONCLUSION

in order to facilitate communication and the sharing of data between these three categories. Both the hardware and software architecture of this in-car gateway were shown. The architecture that we have proposed is innovative, and it has the potential to make it possible to provide a wide range of sophisticated services which include autonomous driving. Consequently, in the part that came before this one, we placed an emphasis on fundamental characteristics and the flow of information for autonomous driving services. In addition, in order to bolster our approach, we proposed a way for changing lanes without human intervention. The deployment of our gateway within the network of our choice is something that we plan to do in the future in order to evaluate its effectiveness.

VI. REFERENCES

[1]. A. J. Kadhim and J. I. Naser, "Proactive load balancing mechanism for fog computing supported by parked vehicles in IoV-SDN," in China Communications, vol. 18, no. 2, pp. 271-289, Feb. 2021. doi: 10.23919/JCC.2021.02.019

[2]. Approach for the Internet of Vehicles (CCA-IoV)," 2020 Second International Conference on Embedded & Distributed Systems (EDiS), Oran, Algeria, 2020, pp. 58-63.

[3]. B. Sarra, M. Saleh and H. Saad, "Ensuring QoS and Efficiency of Vehicular Networks by SDVN-IoV," 2020 International Conference on Advanced Aspects of Software Engineering (ICAASE), Constantine, Algeria, 2020, pp. 1-6.

[4]. D. B. Rawat, M. Garuba, L. Chen and Q. Yang, "On the security of information dissemination in the Internet-of-Vehicles," in Tsinghua Science and Technology, vol. 22, no. 4, pp. 437-445, Aug. 2017. doi: 10.23919/TST.2017.7986946

[5]. G. Raja, P. Dhanasekaran, S. Anbalagan, A. Ganapathisubramaniyan and A. K. Bashir, "SDN-enabled Traffic Alert System for IoV in Smart Cities," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2020, pp. 1093-1098. doi: 10.1109/INFOCOMWKSHPS50562.2020.9162888 M. Bersali, A. Rachedi and H. Bouarfa, "A New Collaborative Clustering

[6]. H. Sikarwar and D. Das, "Towards Lightweight Authentication and Batch Verification Scheme in IoV," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3244-3256, 1 Sept.-Oct. 2022. doi: 10.1109/TDSC.2021.3090400

[7]. J. Eze, E. Eze, S. Zhang and E. Liu, "Design Optimization of Resource Allocation in OFDMA-based Cognitive Radio-enabled Internet of Vehicles (IoVs)," 2019 25th International Conference on Automation and Computing (ICAC), Lancaster, UK, 2019, pp. 1-8.

[8]. M. A. Hossain, M. Schukat and E. Barrett, "MU-MIMO Based Cognitive Radio in Internet of Vehicles (IoV) for Enhanced Spectrum Sensing Accuracy and Sum Rate," 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 2021, pp. 1-7. doi: 10.1109/VTC2021-Spring51267.2021.9449068

[9]. N. Verma, S. Kumari and P. Jain, "Post Quantum Digital Signature Change in IOTA to Reduce Latency in Internet of Vehicles (IoV) Environments," 2022 International Conference on IoT and Blockchain Technology (ICIBT), Ranchi, India, 2022, pp. 1-6. doi: 10.1109/ICIBT52874.2022.9807757

[10]. O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," in IEEE Access, vol. 8, pp. 91028-91047, 2020. doi: 10.1109/ACCESS.2020.2992580

[11]. P. Sharma and S. Jain, "Review of VANET Challenges and Protocol for Architecture Design and Intelligent Traffic System," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-4. doi: 10.1109/IDEA49133.2020.9170685

[12]. P. Soleimani, M. R. B. Marvasti and P. Ghorbanzadeh, "A Hybrid Traffic Management Method Based on Combination of IOV and VANET Network in Urban Routing for Emergency Vehicles," 2020 4th International Conference on Smart City, Internet of Things and Applications (SCIOT), Mashhad, Iran, 2020, pp. 58-65. doi: 10.1109/SCIOT50840.2020.9250198

[13]. Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari and M. K. Khan, "Efficient Certificateless Aggregate Signature With Conditional Privacy

Preservation in IoV," in IEEE Systems Journal, vol. 15, no. 1, pp. 245-256, March 2021. doi: 10.1109/JSYST.2020.2966526

[14]. S. Bhuvaneswari and R. Saranya, "Internet of Vehicle based Accident Detection and Management Techniques by using VANET: An Empirical Study," 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2020, pp. 237-244. doi: 10.1109/ICISC47916.2020.9171224

[15]. S. S. Vladimirov, D. A. Karavaev, A. B. Stepanov, M. A. Yurchenko and A. G. Vladyko, "An Application of LoRa Technology for SD-IoV Network," 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 2019, pp. 1-4. doi: 10.1109/ICUMT48472.2019.8970938

[16]. S. Yu, J. Lee, K. Park, A. K. Das and Y. Park, "IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment," in IEEE Access, vol. 8, pp. 167875-167886, 2020. doi: 10.1109/ACCESS.2020.3022778