International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

IoT-Based Smart and Secure Vehicle Communication Using Advanced Technique

Pushpa Preyashi[1], Prof. Suresh Gawande[2]
[1]Research Scholar (M.Tech) Department of ECE, Bhabha Engineering Research Institute, Bhabha University Bhopal, Madhya Pradesh, India
[2]Assistant Professor, Department of ECE, Bhabha Engineering Research Institute, Bhabha University Bhopal, Madhya Pradesh, India

Article Info

Publication Issue :
Volume 8, Issue 5
September-October-2022

Page Number : 244-250

Article History
Accepted: 10 Oct 2022
Published: 24 Oct 2022

ABSTRACT

The new age of the Internet of Things (IoT) is motivating the advancement of traditional Vehicular Ad-Hoc Networks (VANETs) into the Internet of Vehicles (IoV). This paper is an overview of smart and secure communications to reduce traffic congestion using IoT based VANETs, known as IoV networks. Studies and observations made in this paper suggest that the practice of combining IoT and VANET for a secure combination has rarely practiced. IoV uses real-time data communication between vehicles to everything (V2X) using wireless communication devices based on fog/edge computing; therefore, it has considered as an application of Cyber-physical systems (CPS). Various modes of V2X communication with their connecting technologies also discussed. This paper delivers a detailed introduction to the Internet of Vehicles (IoV) with current applications, discusses the architecture of IoV based on currently existing communication technologies and routing protocols, presenting different issues in detail, provides several open research challenges and the trade-off between security and privacy in the area of IoV has reviewed. From the analysis of previous work in the IoV network, we concluded the utilization of artificial intelligence and machine learning concept is a beneficial step toward the future of IoV model.

Keywords : IOV(Internet of Vehicle)

I. INTRODUCTION

The Internet of Things (IoT) refers to physical devices equipped with sensors, such as smart wearables, autonomous vehicles, mobile phones, home appliances, machines, and other electronic devices connected via an application programming interface (API) for data transmission over the Internet [1]. When vehicles are connected to the Internet and act as an ad-hoc network, it is known as the Internet of

Vehicles (IoV). It is emerging as an innovative model in the wireless and mobile communications sectors with a resolution of new communication and connectivity technologies assisted by the development of IoT [2]. Vehicular Ad-hoc network (VANET) gave rise to the IoV and it refers to the network of dissimilar entities road transport, such as vehicles, foot-travelers, roads, parking lots and city infrastructure and offers real-time communication among them. The IoV is an IoT application that offers a solution for the flow control of traffic and secure communication in cities based on the technology [3]. The increment of the vehicle connectivity to IoT results in the formation of the IoV network. This is a developing field for the automotive industries and one of the significant aspects of the smart cities which helps to monitor the traffic. It is a scattered network that provisions the usage of data formed by linked vehicles and VANETs [4]. The increase in the people drives vehicles results in the corresponding increment of the fatality which occurs because of accidents. A significant objective of the IoV is to permit vehicles to communicate in real-time with their human drivers, foot-travelers, other vehicles, roadside set-up and fleet supervising systems [5]. The IoV supports different types of communication within the network as Vehicle-vehicle (V2V), Vehicle-sensors (V2S), Vehicle-infrastructure (V2I), Vehicle-road side (V2R), Vehicle-cloud (V2C), Vehicle-network (V2N), Vehicle-pedestrian (V2P), Vehicle-devices (V2D) communication. V2V wireless communication is the transfer of information regarding the position and speed of the surrounding vehicle. V2S technology enables sensor communication with neighbor vehicles using pre-installed On-Board Units (OBUs) figure 1 shows the architecture of IOV communication.

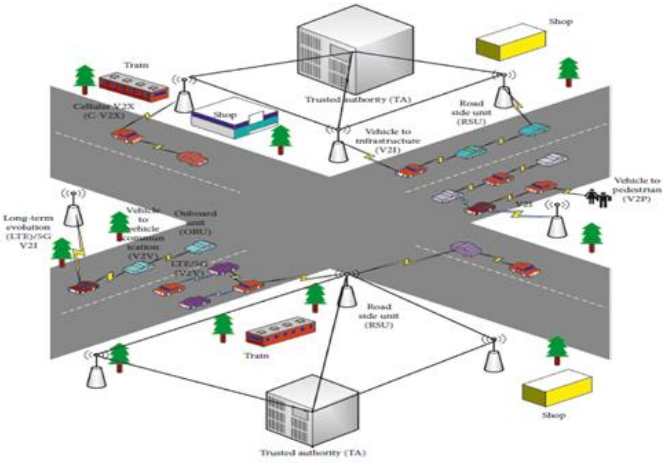


Fig 1: VANET Communication Model

1.1. Issues and Challenges in IoV

The main focus of the Internet of Vehicles is to connect multiple users with vehicles, devices and networks, offering a safe and secure communication capability that is flexible, efficient and reliable. The construction of IoV with such multiple objects makes it a complex system [10]. Also, the use of IoV is less diverse compared to other networks and as a result, there are some particular requirements. Both of these issues add new technological challenges and test the research and development of IoV. During discussion related to the function and construction of IoV, here are some of the issues and challenges that researchers face:

• **Security and Privacy:** Since IoV combines a wide range of various services and standards, there is a requirement for the safety of information. As an open community network, IoV is aimed at cyber-attacks and attacks that can cause physical loss and privacy leaks. Maintaining the balance between privacy and security is one of the key issues in IoV. The acceptance of reliable info from its sender to the recipient is important [11]. However, the senders' privacy requirement may be violated by this reliable information.

• **Vehicles Reliability:** Vehicles, sensors, and network sensors may fail sometime. The system has to deal

with inaccurate data, plus malicious communications, for example denial of service (DOS) attacks. Some technologies can be deployed like Intrusion Detection Systems (IDS) to protect against attack in traditional networks [12]. In general, car safety is very important compared to in-car entertainment.

• **Mobility and Dynamic Topology:** Compared to other vehicles in the network, cars can travel at much higher speeds, resulting in constantly changing network topologies. It requires a test to connect with consecutive nodes and transport the goods from one place to another. Therefore, the flexibility of network topology should be considered important for IoV development.

• **Open Standards:** The absence of standard can make successful V2X communication troublesome interoperability and standardization are required for quick selection. Receiving open standards will empower the flat-sharing of data. Governments ought to take an interest and urge enterprises to work together in the improvement of innovative prescribed procedures and open global standards.

• **Variable network load**: Network size is another big challenge, which can be very high or low due to changing traffic conditions. As the scale of the network in large urban areas can be high, for example, entries in urban area main highways, and metropolitan cities. In any case, if the network has severely broken can now remain fragmented, which cause road accidents. Therefore, a smart traffic surveillance system based on 5G technology will be required to solve this problem [13].

• **Geographical Communication:** Related to different networks that use multicast or unicast routing, where communication is reflected by a particular ID, car networks often have some form of transmission, which affects areas where bulk traffic should be sent.

• **Predictable Mobility**: Vehicular networks are different than different types of specially designated networks where nodes move randomly. Cars, in turn, are forced by topology and design, by the need to pay attention to traffic signals and traffic signals, and by the reaction of moving neighbour vehicles, which makes consistency as far as possible.

1.2. Applications

Most of the IoV applications are in the field of telecom. According to Cyber-physical systems (CPS) some important applications of the IoV model and their functionality are classified into different classes, given below:

• Safety: Cooperative collision avoidance, Lane changing warnings, automatic braking and speed control

• Navigation: Real-time traffic, Route navigation, Locating parked vehicle, Cooperative driving

• Information and Infotainment: Wi-Fi in vehicles for downloading of music, video streaming, content sharing

• Remote Telemetric: Vehicle remote locking, Car surveillance

• Diagnostic: Service spot detection, Self-repair, Fuel usage optimization

• Car sharing: Carpooling, Group parking booking

• Others: Electronic toll payments, Traffic flow monitoring, etc.

The Internet of things and Cyber-physical systems are not isolated technologies. Cyber-physical systems (CPS) and IoT in the IoV network have some other important applications, such as Intelligent transportation systems (ITS), Connected autonomous vehicles (CAV), Smart grid, Smart city, and Smart manufacturing [17].

1.3. Motivation.

In the upcoming time, IoV will become the future of the VANETs based on the expansion of the web services. An essential portion of the Internet of Vehicles having different exploration fields, including intelligent transportation system, wireless communication, cloud and fog computing, mobile computing, autopilot vehicles and era of CPS [18]. On the routing and packet data transmission point of view, both network security and robust data transmission are necessary for different applications.

IoV networks mostly consist of vehicles, which operate in a very different way than wireless sensors. As a result, the IoV network has many features that can influence the formation of IoV technologies. Some features will present difficulties for the advancement of technology, and some may result in benefits.

1.4. Contributions.

sMotivated by existing problems in IoV, we present a new approach for improved traffic management and reliable communication in IoV using behavioural studies of IoT and VANETs. The significant contribution of our work lies in summary as follows: In this paper, we have proposed and designed a novel framework (CSI model) for IoV with studies based on the current VANET environment to prevent traffic congestion, maintain secure communication, and maximize data delivery. The purpose of this study is to analyse various mechanisms for better route selection based on vehicle range, residual energy, and vehicle condition for efficient communication using artificial intelligence The future challenges and current issues for the design and development of IoV networks with the help of big data, IoT, and cloud services have discussed in detail. This paper sheds new light on the full layered architecture of IoV for a better analysis of existing models. This survey presented various communication strategies for IoV by reviewing existing routing protocols, topologies, and applications. In conclusion, comparisons have made for the performance of existing works in terms of Quality of Service (QoS) parameters to explore better possibilities towards faster and reliable data transmission in IoV networks.

II. Literature Review

Chim et al. [5] introduced a method which discussed the security and privacy issues of V2V in VANETs, and this scheme utilizes one-way hash function and secret key between vehicle and RSU. Therefore, this methodology can resolve privacy issue which may occur during communication. Vighnesh et al. [88] introduced a novel sender authentication technique for enhancing VANET security by using hash chaining and authentication code to authenticate the vehicle. This method ensures secure communication between vehicle and RSU, and a confidential data is encrypted through master key. Before sending packets to the authentication centre, the RSU attaches its identity which can eliminate the possibility of rogue RSU abusing the VANET. He and Zhu [8] presented a method which addresses the problem of DOS attack against signature-based authentication. To tackle DOS attack, the pre authentication can be done before signature verification. In this scheme, the pre authentication mechanism is utilized, which takes the advantage of using one-way hash chain and a group rekeying technique. The symmetric cryptography is further extended to timed efficient stream loss-tolerant authentication (TESLA).

In this approach, firstly the sender computes MAC using a known key and attaches a MAC to each sending message, and the receiving messages are buffered without authentication at the receiving part. The main disadvantage of TESLA is that the advance synchronization of the clock at receiving side is required with the clock at sending side. Additionally, TESLA is vulnerable to DOS attack in terms of memory which is caused by unregistered vehicles that utilizing receiver memory with fake messages [6][7].

Jahanian et al. [3] introduced a TESLA-based technique; in this technique, timed method checking approach based on timed color Petri model is used to design and verify TESLA. Later, the researchers have found that the two factors need to be analysed: the first is the security efficiency and the second is the percentage of successful attack. Studer et al. [2] introduced a modified form of TESLA which is known as TESLA++, and it provides the same broadcast authentication which is computationally efficient as TESLA with less memory consumption and also presented a method to effectively verify the

new RSUs and OBUs which encountered during communication. The goal of TESLA++ is to control memory DOS attacks, which can be obtained by receivers self-generated MAC which may lower down the memory requirements for authentication. However, TESLA does not offer multiple hops authentication and nonrepudiation [8].

In general, mostly vehicles contain public or private key for pseudonymous communication. In order to achieve in a secure and reliable way, the public key certificates are the best method which is used in public key infrastructure (PKI) to authenticate vehicles; it contains the digital signature of the certification authority (CA) and vehicle key for authentication [5]. The CA is the centralized management unit which is responsible for certifying nodes, keys, etc. Furthermore, it can also authenticate the vehicles in V2V communication. Every vehicle needs to be registered with CA database before it officially joins the VANET system; the vehicle can communicate with CA in two ways either directly as an offline registration or via RSU as an online registration by indirect way. Raya and Hubaux [9] introduced a new method which utilizes the anonymous public keys to provide privacy. The anonymous keys must be changed in the way that the receiver will not be able to track the vehicle owner key. The main demerits are it required a large amount of storage and memory and also requires huge amount of certificate revocation list (CRL) checks, since using large amount of anonymous keys. Therefore, it may be the reason for DOS attack due to large amount of computational overhead.

Tolba et al. [9] introduced a robust pseudonym-based authentication method to reduce the security overhead, but the robustness of traffic safety is maintained. This scheme alleviates the limitations of a pseudonym by using the combination of baseline pseudonym and group signature which can generate own pseudonym on-the-fly and self-certification. And it minimizes the requirements of handling pseudonym in authentication.

VANET is one of most emerging and unique topics among the scientist and researcher. Due to its mobility, high dynamic nature and frequently changing topology not predictable, mobility attracts too much to researchers academic and industry person. In this paper, characteristics of VANET ate discussed along with its architecture, proposed work and its ends simulation with results. There are many nodes in VANET and to avoid the load on every node, clustering is applied in VANET. VANET possess the high dynamic network having continuous changing in the topology. For stability of network, a good clustering algorithm is required for enhancing the network productivity. Temurnikar et al [12] proposed a novel approach has been proposed to make cluster in VANET network and detect malicious node of network for security network.

III.Proposed Work

Proposed Framework.

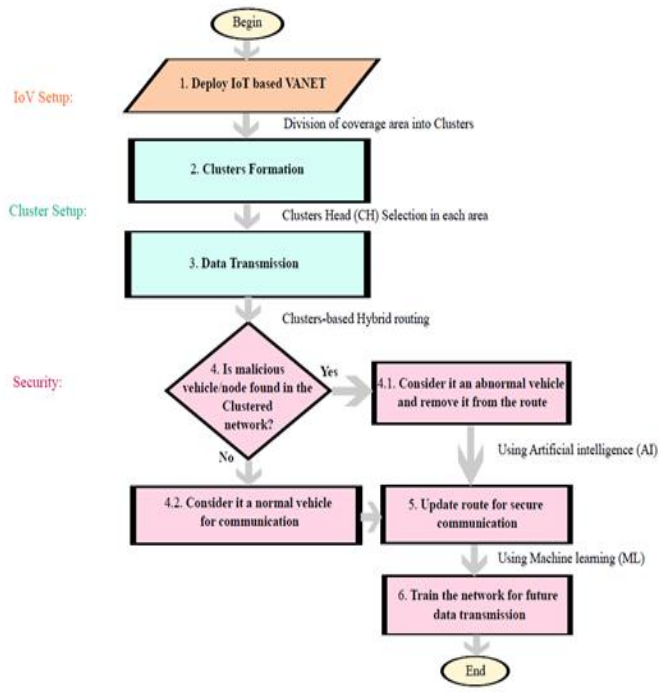
Based on the above survey findings and gaps analysis, IoT-based VANET and intelligent services have used to design a proposed Cluster-based, Self-organized, and Intelligent (CSI) framework that helps in smart and secure communication thereby reducing traffic congestion, as shown in Fig. 1.

· IoV Setup Phase:

Design and deploy IoT based VANET Step 1: IoT has helped develop the ad-hoc network of traditional vehicles into ad-hoc networks of intelligent vehicles.

· Cluster Setup Phase:

Clusters formation and Data transmission Step 2, 3: Define the coverage area for each vehicle/RSU node, which helps to build the route from the source node to the destination node. To solve this problem the selection of Cluster Head (CH) node is best suited for better data transmission.



best suited for better data transmission.

• Security Mechanism:

Malicious node, Update route, and Network training Step 4, 5, 6: When the performance of the network degraded, then the concept of Artificial intelligence (AI) is used to detect malicious or fail nodes in the network, which has not able to communicate with other vehicles/RSU thereby create traffic congestion. The machine learning (ML) algorithm acts as a processing unit that updates itself with changes in routes used for future data transmission. Some important outcomes based on the proposed CSI model have listed below that will help solve real-life problems in existing IoV networks:

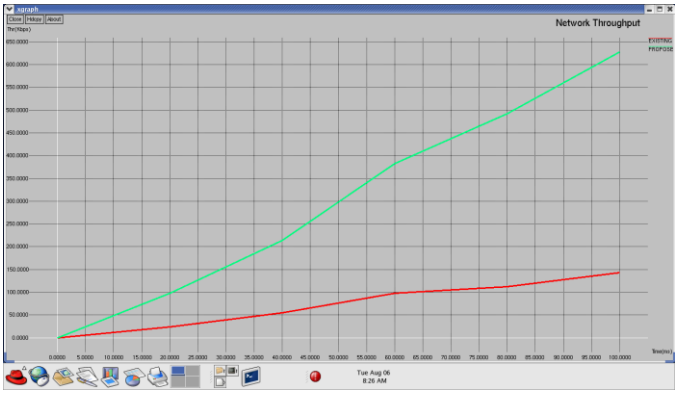
• The use of clustering-based routing approaches with trust management mechanisms will be beneficial for the future internet of vehicles.

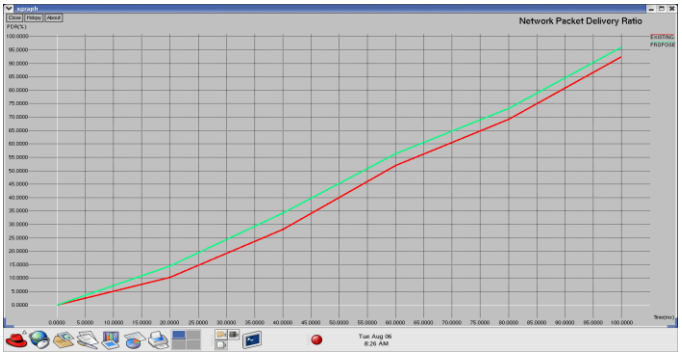
• The integration of artificial intelligence with routing mechanisms helps to detect networks blocked by malicious or dead nodes.

• The concept of traffic congestion minimization will be introduced with the IoV network to provide a fast and robust communication. Moreover, we have decided to use a robust cluster-based routing to validate the proposed work. Hence, future studies on the current topic are required to compare and verify the proposed and existing models based on parameters such as Throughput, Packet loss, Packet delivery ratio, and delay.

IV.Simulation and Result

In this section the simulation result and performance evaluation of our advance clustering algorithm is presented. To Simulate our clustering algorithm the network simulator NS2-2.34 is used to implement proposed algorithm and with the help of simulator we compare the throughput and packet delivery ratio [12].





V. CONCLUSION

New communication technologies for vehicles grow mainly from the improvement of basic communication between Vehicle-vehicle and Vehicle-infrastructure, and Vehicle-network. IoV model is a reality at present which is acquired by interconnections of vehicles and traffic infrastructure including people. This paper presented a detailed

overview of the IoV architecture along with its routing protocols, issues, and challenges, which helps to build secure communication. IoV network designing is still at an early stage of development and requires many technical issues to be resolved before it is recognized globally and deployed in modern networks. With the fast growth of computing and wireless transmission techniques, the Internet of Vehicles network offers large business and research importance for security and fast communication. Therefore, in the future, the IoV network is a better option with the concept of Artificial intelligence and Machine learning technology acting as a classifier used to train IoV networks with a reliable routing mechanism based on hybridization and meta-heuristic optimization algorithms adopted for security and fast communication purposes.

VI. REFERENCES

[1]. M. Nidhal, J. Ben-othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Vehicular Communications, vol. 1, no. 2, pp. 53–66, 2014.

[2]. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[3]. S. Biswas, J. Mi˘sic, and V. Mi´ ˘sic, "DDoS attack on WAVE-´ enabled VANET through synchronization," in Proceedings of the IEEE Global Communications Conference (GLOBECOM), pp. 1079–1084, Anaheim, CA, USA, 2012.

[4]. H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," Vehicular Communications, vol. 7, pp. 7–20, 2017.

[5]. T. W. Chim, S. M. Yiu, L. K. Hui, and V. K. Li, "Security and privacy issues for inter-vehicle communcations in VANETs," in Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Net-works Workshops, pp. 1–3, Rome, Italy, June 2009

[6]. A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in Proceedings of the IEEE Symposium on Security and Privacy, pp. 1–18, Oakland, CA, USA, 2000.

[7]. S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," Vehicular Communications, vol. 9, pp. 19–30, 2017.

[8]. M. H. Jahanian, F. Amin, and A. H. Jahangir, "Analysis of TESLA protocol in vehicular ad hoc networks using timed colored Petri nets," in Proceedings of the 6th International Conference on Information and Communication Systems (ICICS-2015), pp. 222–227, Amman, Jordan, April 2015.

[9]. A. Tolba, Content accessibility preference approach for improving service optimality in internet of vehicles," Computer Networks, vol. 152, pp. 78–86, 2019.

[10]. Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, Social big-data-based content dissemination in internet of vehicles," IEEE Transactions on Industrial Informatics, vol. 14, no. 2, pp. 768–777, 2017.

[11]. Kumar, Sumit & Singh, Jaspreet. (2020). INTERNET OF VEHICLES (IOV) OVER VANETS: SMART AND SECURE COMMUNICATION USING IOT. Scalable Computing. 21. 413-428. 10.12694:/scpe.v21i3.1741.

[12]. A. Temurnikar, P. Verma and J. Choudhary, "Securing Vehicular Adhoc Network against Malicious Vehicles using Advanced Clustering Technique," 2nd International Conference on Data, Engineering and Applications (IDEA), 2020, pp. 1-9, doi: 10.1109/IDEA49133.2020.9170696.

Cite this article as :

Pushpa Preyashi, Prof. Suresh Gawande, "IoT-Based Smart and Secure Vehicle Communication Using Advanced Technique ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 5, pp. 244-250, September-October 2022.
Journal URL : https://ijsrcseit.com/CSEIT228547