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

VANETs and Internet of Things (IoT) : A Systematic Review

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

Article Info

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

Page Number : 158-164

Article History
Accepted: 10 Sep 2022
Published: 30 Sep 2022

ABSTRACT

Numerous vehicular data services and applications are made possible by sophisticated tools called vehicular communication networks. The rapidly increasing number of vehicles has also caused the vehicular network to become heterogeneous, dynamic, and large-scale, making it challenging to match the fifth-generation network's stringent standards for extremely low latency, high mobility, top security, and massive connections. Previous research has demonstrated that researchers have worked very hard to enhance vehicular communications as Software-Defined Networking (SDN) on Vehicular Ad-hoc Network (VANET) has become more widely used in industry. This paper offers a thorough analysis of earlier research by categorising it according to wireless communication, IOT, and IOV, particularly VANET. First, a brief explanation of the layers and infrastructure information for the IOV controller and VANET is given. Second, a description of SDN-VANET applications is given in various wireless communications, including the Internet of Things (IoT) and VANET, with an emphasis on the analysis and comparison of SDNVANET works on various factors. This study also offers a thorough overview of the unresolved problems and productive research lines discovered during the integration of the VANET with IOV. In order to solve the various issues with the VANET architecture, it also presents current and developing technologies with examples of their application in vehicular networks.

Keywords : IOV (Internet of vehicle), VANET (vehicle Ad hoc Network), IoT (Internet of things)

I. INTRODUCTION

Due to the massive deployment of intelligent transportation system (ITS) in smart cities, the vehicular adhoc network (VANET) has attracted a deliberate attention in the research domain; the major goals of VANET are to support numerous applications in terms of infotainment, emergency, and traffic safety services [1], [2]. In general, VANET structure has three main components as follows: Firstly,

onboard units (OBUs) mounted on vehicles to allow them connect The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh . with each other by the dedicated short range communication (DSRC) protocol. As long as vehicles move on the road, sharing messages and requesting keys are continuous processes [3]. Secondly, roadside units (RSUs) are wireless units distributed along the road to collect and analyze messages, and take intelligent traffic actions. Thirdly, the trusted authority (TA) is responsible for managing the whole entities in the network and issuing the system parameters. All vehicles and RSUs must register at the TA, which has the highest capabilities in terms of storage and communication, before allowing them to join VANET [1]. Although the secure communication channels are used to exchange messages between the RSUs and TA, the open wireless medium is utilized for transmitting messages between the vehicles and RSUs [4]. Hence, various attacks are subjected on the wireless environment, resulting in a shortage in the security efficiency of VANET. These attacks are rising to track, monitor, and alter the traffic exchanged between the vehicles and infrastructure as indicated in [5]. Accordingly, several authentication protocols are previously proposed to strengthen the security of VANET against attacks [6] In this paper, a new classification of authentication schemes is introduced.

II. Basic Overview of VANETs

Since from 1980, VANETs which are ad hoc network infrastructures grow abruptly, in which vehicles are connected through wireless communication [27]. Recently, VANETs are used in enhancing traffic safety, improving traffic flow, and reducing traffic congestion and driver guidance [28]. The basic model diagram of VANETs which shows the vehicles' communication can be distinguished into V2V and V2I communication, road side units (RSUs), and onboard units (OBUs). Firstly, we will discuss these parameters and then explain the unique characteristics and advantages of using VANETs over MANETs in terms of network topology, bandwidth, reliability, etc. As we discussed above, the VANETs consist of three components such as OBUs, RSUs, and trusted authority (TA); these parameters are discussed below.

2.1. VANET Architecture.

Generally, the communication between vehicles and RSUs is done via wireless technology called as wireless access in vehicular environment (WAVE). The WAVE architecture describes the exchange of security messages [1], and the WAVE communication ensures the safety of passengers by updating vehicle information and traffic flow. This application ensures the pedestrian and driver safety and also improves the traffic flow and efficiency of the traffic management system. The VANETs comprise several units such as OBUs, RSUs, and TA. Specifically, the RSU typically hosts an application that is used to communicate with other network devices, and the OBU is mounted on each vehicle to collect the vehicle useful information such as speed, acceleration, and fuel. Then, these data are forwarded to the nearby vehicles through wireless network. All RSUs interconnected with each other are also connected to TA via wired network. Additionally, TA is the head among all components, which is responsible for maintaining the VANETs [10].

2.1.1. Roadside Unit (RSU).

The roadside unit is a computing device which is fixed alongside of the road or in specified location such as parking area or at the intersection; it is used to provide local connectivity to the passing vehicles. The RSU consists of network devices for dedicated short-range communication (DSRC) based on IEEE 802.11p radio technology. Specifically, RSUs can also be used to communicate with other network devices within the other infrastructure networks.

2.1.2. Onboard Unit (OBU).

OBU is a GPS-based tracking device which is usually equipped in every vehicle to share vehicle information to RSUs and other OBUs. OBU consists of many electronic components such as resource command processor (RCP), sensor devices, user interface, and read/ write storage for retrieving storage information. The main function of OBU is to connect with RSU or other OBUs through wireless link of IEEE 802.11p and is responsible for communication with other OBUs or RSUs in the form of messages. Moreover, OBU takes input power from the car battery, and each vehicle consists of sensor type global positioning system (GPS), event data recorder (EDR), and forward and backward sensors which are used to provide input to OBU [11].

2.1.3. Trusted Authority (TA).

Trusted authority is responsible for managing the entire VANET system such as registering the RSUs, OBUs, and the vehicle users. Moreover, it has the responsibility to ensure the security management of VANETs by verifying the vehicle authentication, user ID, and OBU ID in order to avoid harm to any vehicle. The TA utilizes high amount of power with large memory size and also can reveal OBU ID and details in case of any malicious message or suspicious beha2vior [12]. In addition to these, TA has the mechanism to identify the attackers as well.

2.2. Communication Methods in VANETs.

ITS is consistently focusing on providing secure communication to improve the traffic flow and road safety and also overcoming the traffic congestion by utilizing different networking techniques such as MANETs and VANETs. V2X communications play an important role in the ITS to improve the traffic efficiency, traffic safety, and driving experiences by providing real-time and highly reliable information such as collision warning, road bottlenecks information, traffic congestion warning, emergency situations, and other transportation services [31]. V2X communication can exchange the information between V2V, V2I, and vehicle to pedestrians (V2P) as shown in Figure 1.

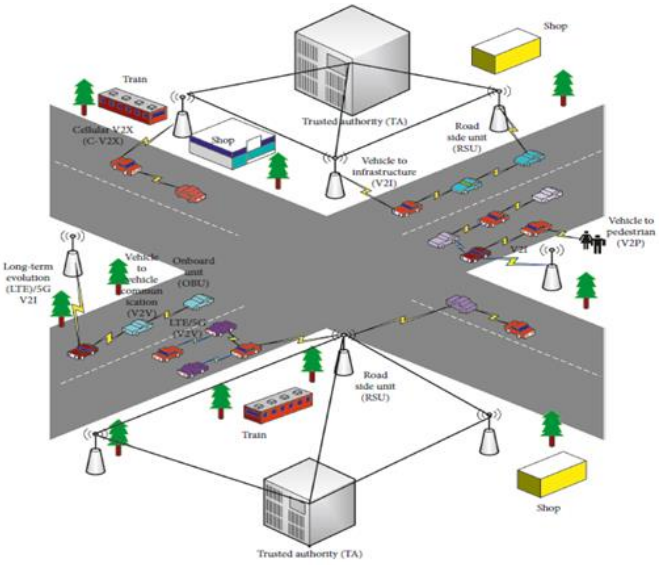

Fig 1: VANET Communication Model

III. VANET and IOT

VANETS AND IOT APPLICATIONS As mentioned in section I, VANET with the aid of IoT has been widely applied for data or message dissemination of safety-based as well as non-safety-based applications to ensure traffic safety and efficiency through broadcasting protocol [23]. It derives the idea of building smart cities where VANET systems are Indonesian J Elec Eng & Comp Sci ISSN: 2502-4752 ρ VANETs and Internet of things (Iot): A Discussion (Shahirah M. Hatim) 221 interconnected to IoT in terms of keeping the data on the internet, or also known as cloud. The concept of smart city is important to increase the quality of services (QoS) provided to citizens and eventually improve their quality of life in this new era of technology. Table 1 shows the relationship or the needs between VANET and IoT. It can be said that both are interrelated to each other. Table 1. VANET and IoT applications

3.1. Safety Applications

Accident prevention is the traditional intention of safety applications, thus lead to the development of vehicular adhoc network where communications among the related components in the environment are involved. [2, 3]. These applications provide life-saving traffic assistance to drivers on the road [2,]. It is categorized into three main categories which are driver assistance, alert information and warning alert [2].

3.2. Non-safety Applications

Non-safety applications are also important in ensuring traffic convenience and efficiency when we are on the road. Information on weather, the location and current traffic movements on the road networks, distance, Point of Interest (PoI) allocation as well as social network (connected to mobile network through smartphones) can be beneficial to the road users connected in the VANET systems using IoT [2]. With the aid of non-safety applications, it can help safety applications to work better and increase efficiency to avoid accidents.

Table 1: VANET and IOT applications

VANET Application	IOT Application
Intersection collision warning	Smart cities
Lane change assistance	Environment monitoring
Road map	Energy management
Overtaking vehicle warning	Medical health care system
Emergency vehicle warning	Building automation
Point of interest (POI)	Transportation
Weather Information	Social network

IV. IOV (Internet of Vehicle)

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 [13]. 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 [14][17]. 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. 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. IoV uses technologies such as navigation systems, mobile communication, and sensor networks for data interchange and instruction systems. Cyber-physical system (CPS) is a combination of cyber (virtual) and physical (real) systems with networking and computation capabilities.

IoT applications typically include three basic layers:

- **Sensor (actuator) layer:** Use to understand (sense) road and traffic conditions.
- **Application (control) layer:** Analysis of data collected by the integration of big data with fog infrastructure in data centres.

• **Communication layer:** Smart wireless connectivity between sensors and fog servers. In IoT, physical devices are connected over the Internet so that they can communicate with each other and make decisions intelligently and exchange information without or with little human intervention [15], for example, driverless cars or drones.

4.1. 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 attacks in traditional networks [16]. 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, so 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 areas, 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][16].

• **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 [17].

• **Sufficient Energy and Storage:** The general feature of nodes in Vehicular networks is that they contain

more power to register (count, maintain and adjust), because nodes are in rows rather than smaller portable gadgets.

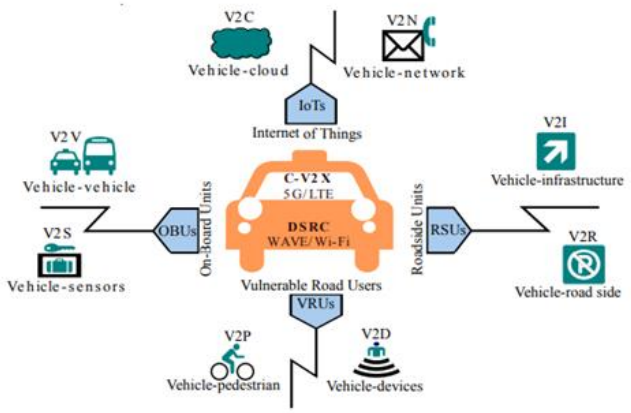

Fig. 2. *V2X Communication approaches in IoV*

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.

frame in which the research was conducted. This kind of research calls for cutting-edge tools and subject-matter experts.

VI. REFERENCES

[1]. M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network," IEEE Access, vol. 8, pp. 170507–170518, 2020, doi: 10.1109/ACCESS.2020. 3024587.

[2]. J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," IEEE Access, vol. 9, pp. 15633–15642, 2021, doi: 10.1109/ACCESS.2021. 3053043.

[3]. M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs," Wireless Netw., vol. 26, pp. 3083–3098, Jun. 2020, doi: 10.1007/s11276- 019-02039-x.

[4]. H. Jiang, L. Hua, and L. Wahab, "SAES: A self-checking authentication scheme with higher efficiency and security for VANET," Peer Peer Netw. Appl., vol. 14, no. 2, pp. 528–540, Mar. 2021, doi: 10.1007/s12083-020- 00997-0.

[5]. A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," Comput. Secur., vol. 89, Feb. 2020, Art. no. 101664, doi: 10.1016/j.cose.2019.101664.

[6]. I. Abdelfatah, N. M. Abdal-Ghafour and M. E. Nasr, "Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions," in IEEE Access, vol. 10, pp. 1096-1115, 2022, doi: 10.1109/ACCESS.2021.3137877.

[7]. W. Qi, Q. Song, X. Wang, L. Guo and Z. Ning, "SDN-Enabled Social-Aware Clustering in 5G-VANET Systems," in IEEE Access, vol. 6, pp. 28213-28224, 2018, doi: 10.1109/ACCESS.2018.2837870.

[8]. 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.

[9]. Rizwan, Dimitrios A. Karras, Mohammed Dighriri, Jitendra Kumar, Ekta Dixit, Asadullah Jalali, Amena Mahmoud, "Simulation of IoT-based Vehicular Ad Hoc Networks (VANETs) for Smart Traffic Management Systems", Wireless Communications and Mobile Computing, vol. 2022, Article ID 3378558, 11 pages, 2022. https://doi.org/10.1155/2022/3378558

[10]. M. Azees, L. Jegatha Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular adhoc networks," IET Intelligent Transport Systems, vol. 10, no. 6, pp. 379–388, 2016.

[11]. Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760–776, 2019.

[12]. T. Neudecker, N. An, T. Gaugel, and J. Mittag, "Feasibility of traffic lights in non-line-of-sight environments," in Proceedings

[13]. M. A. Saleem, Z. Shijie, and A. Sharif, Data transmission using iot in vehicular ad-hoc networks in smart city congestion," Mobile Networks and Applications, vol. 24, no. 1, pp. 248–258, 2019.

[14]. L. Sumi and V. Ranga, An iot-vanet-based traffic management system for emergency vehicles in a smart city," in Recent Findings in Intelligent Computing Techniques. Springer, 2018, pp. 23–31.

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

[16]. 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.

[17]. 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.

Cite this article as :

Pushpa Preyashi, Prof. Suresh Gawande, "VANETs and Internet of Things (IoT) : A Systematic Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 5, pp. 158-164, September-October 2022.
Journal URL : https://ijsrcseit.com/CSEIT228536