A Review on Security Aspects in VANET

Kajal Saini[1], Dr Kamlesh Namdev[2] and Dr Kalpana Roi[3]

[1]Kajal Saini, Department of CSE, Sagar Institute of Research Technology-Excellence, Bhopal (M.P), India
[2]Dr Kamlesh Namdev, Department of CSE, Sagar Institute of Research Technology-Excellence, Bhopal (M.P), India
[3]Dr Kalpana Roi, Department of CSE, Sagar Institute of Research Technology-Excellence, Bhopal (M.P), India
[1]sainikajal0508@gmail.com

* Corresponding Author: Kajal Saini

Abstract: *Vehicular ad hoc networks (VANETs) are an emerging type of mobile ad hoc networks (MANETs) with robust applications in intelligent traffic management systems. VANET has drawn significant attention from the wireless communication research community and has become one of the most prominent research fields in intelligent transportation systems (ITS) because of the potential to provide road safety and precautionary measures for drivers and passengers. This paper presented is an overview of VANETs and their architecture. And the attack classification, security risks, and requirements are introduced in this study.*

Keywords: *VANETs, MANET, ITS, Security System.*

I. Introduction

In recent years, due to economic and population growth, a rapid increase has been observed in the numerous vehicles. This has automatically increased road accidents, driver exhaustion and worsening of roads and support framework. According to a healthcare report by the World Health Organization (WHO), the main cause of deaths of people between 15–29 years is road accidents, also 1.3 million people are killed in accidents annually worldwide. This rapid increase in traffic accidents can be managed by practicing the latest technology to report real-time information to the driver about vehicle health parameters, circumstances of roads, traffic jams and forewarning of weather. Progressive advancement of Intelligent Transport Systems (ITS), associated vehicles internet of vehicles known as the (IoV) is the fundamental of communication required to share data about crisis and developing traffic dynamics has been expanded. A current study by the IoT tracker service declared that the linked car market would expand by an additional 270% by 2022 including more than 125 million cars. This also expands the size and complication of current working vehicle ad hoc networks, usually known as VANETs. In addition to running challenges, the rapid proliferation of vehicle connections has also created critical security and information confidentiality concerning the evolution and expansion of VANETs design. From the literature review, it can be asserted that some threats related to privacy and infringing location privacy are more dangerous as they can lead to more advanced physical attacks such as trail and robbery.

II. Related Work

M. Arif et al. [1] have presented about the Intelligent Transportation Systems to VANET and discussed the security and privacy issues. They addressed the VANET and cloud computing effectiveness and solution to security and privacy concern. Finally, they discussed the applications and open issues in VANET.

Z. Lu et al. [2] have discussed VANET architecture, security classification and solutions. The author also discussed the trust in VANET, its challenges and mitigations. Also, various simulators were discussed.

Manivannan et al. [3] have presented the security, privacy and message dissemination in VANET. They reviewed ten years of work done (2009-2010) and presented open challenges in VANET.

Wang et al. [4] have discussed existing certificate revocation scheme and classified these schemes based on its place of storage. They gave challenging issues and key techniques at each stage.

Al-Shareeda et al. [5] discussed the security and privacy issues and solutions based on the security and privacy requirement and also done comparison based on computational overhead and security threat.

O. S. Al-Heety et al. [6] an overview of VANET and SDN controller has been presented. They have explained the SDN layers and infrastructure. The author also discussed open issues and the requirement of robust routing protocol, latency, connectivity, and security challenges for future SDN-VANET architectures.

Farooq et al. [7] have discussed the VANET authentication schemes and its mitigation in several attacks. It discussed the advantages and disadvantages of various schemes and also provided research direction in the area of VANET authentication].

III. VANETS Overview

The VANETs architecture consists of the OBU, roadside unit (RSU), and trusted authority (TA). There are two communication patterns, V2V and V2I communications, as shown in Figure 1. In the V2V communication, the vehicle can communicate with each other to exchange the traffic-related information within the wireless range. For instance, when an incident occurs on the road, the vehicle can immediately send the traffic information to the other vehicles nearby, suggesting them to avoid that area. In the V2I communication, the vehicle can exchange the safety information with the infrastructure such as RSUs which are deployed on the road. The V2I communication aims to avoid the crashes and severe incidents and provide multiple safety measures and precautions to the vehicles.

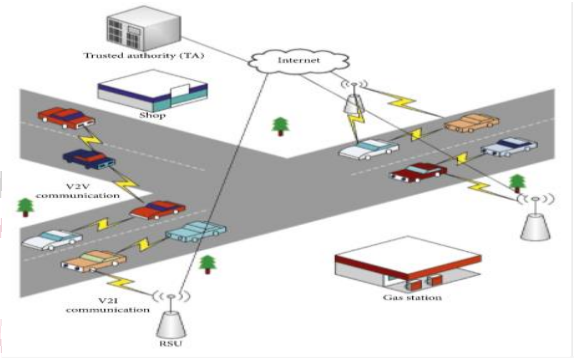

Figure 1 VANET system

IV. Architecture of VANETs

The architecture of VANET can be described based on the components [8]. A generic VANET architecture is illustrated in Figure 2. It demonstrates various components and parties involved in a VANET and also shows communication techniques. VANETs are made up of many components like vehicles (electric and nonelectric), on-board units of vehicles, roadside units, and pedestrians, communication channels like Dedicated Short Range Communication (DSRC), cellular networks, and charging grids of electric vehicles[9,10]. Two types of communication can be observed in VANETs: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), and reversely, Infrastructure-to-Vehicle (I2V). Infrastructure-to-Infrastructure (I2I) communication takes place among roadside units and also with base stations. They use the internet as a backbone. To distribute the credentials or keys, trusted authorities also use this communication type. The components of the architecture are shown in Figure 3.

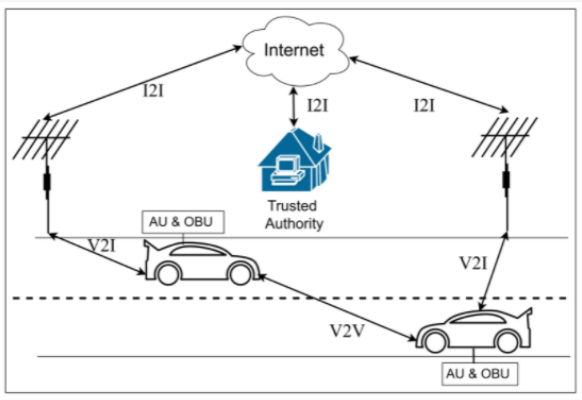

Figure 2. General architecture of VANET.

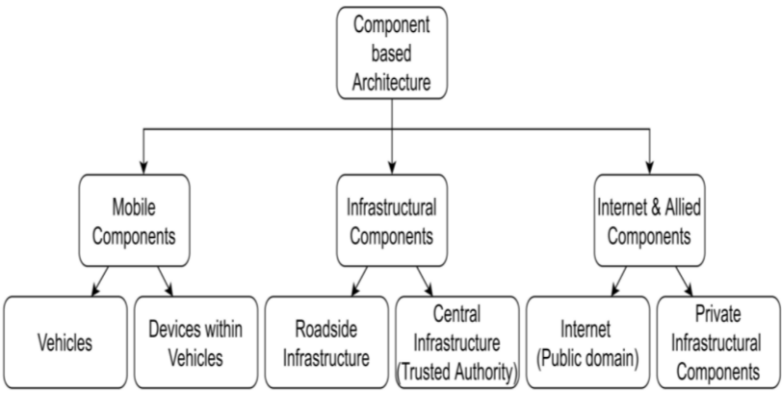

Figure 3. Component-based architecture of VANET.

A. Mobile component:

All vehicles like cars, jeeps, trucks, buses, motorcycles, and pedestrians fall in this category. It also includes all those components or devices which are carried by passengers and those components which remain in the vehicle. Examples of these components and devices are on-board units, Personal Digital Assistant (PDA), navigation devices such as Global Positioning System (GPS), laptops, and smart mobile phones, etc.

B. Application Unit:

It is the front end of the driver module. It is an application that is either provided by the manufacturer of the On-Board Unit (OBU), or it may be obtained from an external source. For example, in the case of PDA, applications may be downloaded from various resources using cloud applications.

C. Onboard Unit:

An Onboard Unit (OBU) is a device that is placed in the vehicle used for communication with other vehicles using various communication technologies. It can also communicate with infrastructural components or Road-Side Units (RSUs) such as traffic lights, charging spots of electric vehicles, and trusted authority. For this, it may use some other mechanism of communication like 3G, LTE, VoLTE, or 4G networks. OBU further consists of multiple components like sensors, storage, GPS, a processor, and an interface for communication. Other components that may be used here are a Tamper-Proof Device (TPD)[11], event data recorder (EDR)[12], and GPS receiver [13]. OBUs are designed to consume less power so that the vehicles' functions can be executed smoothly.

D. Infrastructural components:

These components don't move, but play important role in network communication. Some components are placed on the roads and are called the Road-Side Units (RSUs). For example, charging spots, poles, and traffic lights are considered as RSUs.

E. Road-Side Unit (RSU):

These units are configured with antennas, processors, sensors, charging spots, and storage systems. They are generally placed alongside the road, but in many cases, these are also placed in parking areas and sometimes at other locations feasible for communication coverage.

F. Trusted Authority (TA):

To implement security in VANETs, there is always a need for a trusted authority which handles the security issues. A trusted authority (TA) is a centralized or decentralized authority responsible for various activities like registration of vehicle users, OBUs, and RSUs [14,15]. These authorities are located in such a place where all the traffic is easily manageable. TAs have systems with high computational power, large storage capacity, and consume large amounts of power without any interruption. All these systems form the central infrastructure of the VANETs. These TAs can observe data traffic flowing in between various vehicles and can identify any suspicious activity. Various types of attacks may also be identified and stopped by taking appropriate action like removing a malicious node or stopping traffic from that malicious node. Different types of cryptographic keys are also initiated by these TAs.

Communication system: Vehicles can communicate with other vehicles using Dedicated Short Range Communication (DSRC) [16]. The information collected using this mechanism is not sufficient for managing vehicles and traffic. To get a wide range of information, the internet is used along with its infrastructure. Wireless Access in Vehicular Environment (WAVE) is also used for communication in VANETs [16]. On the other hand, 3G/4G/LTE cellular networks may be used for communication with other networks. Various types of communications take place in VANETs, which includes in-vehicle communication [17,18], vehicle to vehicle communication (V2V) [19], vehicle to infrastructure (V2I) [20], vehicle to pedestrians (V2P) [21], vehicle to grid (V2G)], vehicle to broadband cloud (V2B), and vehicle to everything (V2X)[22]. Based on the above communication schemes one classification may be done which categorizes the VANETs in three types: pure ad hoc networks, cellular, and hybrid. In pure ad hoc networks, vehicles and RSUs use DSRC for communication, and networks are completely transient. On the other hand, cellular networks are fixed and persistent even if these are used in VANETs or not. RSUs may use these cellular networks for communication with other RSUs or trusted authority. Hybrid VANET architectures use a combination of both the architectures.

V. Attackers Classification, Security Attacks And Requirements

VANET is susceptible to security attacks and hence it is important to identify the attack and mitigate so that attacker cannot alter the safety message. An attacker can be classified based on their behavior and scope of damage they can do in VANET [23]. The description of attacker classification is as follows:

- Active attacker: These attackers generate bogus message as well as stop forwarding the received message.
- Passive attacker: These attackers only eavesdrop on the wireless channel collecting traffic information and forward it to other attackers.
- Inside attacker: These attackers possess complete knowledge of the network configuration and hence are very dangerous compared to other attackers.
- Outsider Attacker: These attackers being not authenticated are less dangerous than the insider attackers.
- Malicious Attacker: These attackers have the main goal of harming other nodes without any personal benefit. They can severely damage the network.
- Rational Attacker: These attackers harm the network for their personal benefit and can be easily tracked.
- Local Attackers: These attackers can perpetrate only to limited area.
- Extended Attackers: These attackers have higher range and can attack across the network.

Researchers have identified various attacks in VANET which are explained as follows:

- Impersonation attack: In this the vehicle uses the identity (ID) of other vehicle and shows to be trustworthy.
- Modification attack: Here the attacker modifies the message to put false information
- Replay attack: In this, the attacker creates a dilemma to vehicles in VANET in case of emergency situation by continuously injecting old beacons and messages.
- Bogus information attack: Here, the attacker puts false and incorrect information in the broadcasted message.
- Sybil attack: A Sybil is any vehicle which forges the identity of other vehicle to abrupt the normal functioning of the VANET.
- ID disclosure attack: When a vehicle is able to steal or get the ID details of another vehicle.
- Location tracking: In location tracking, an attacker tries to locate the vehicle, i.e. they track the location.
- Denial of service (DoS): This attack happens when an insider or outsider jams the communication channel or overrides the VANET resources.

For secured communication, the requirements such as node authentication, message authentication, privacy preservation, non-repudiation, low communication and computational overhead, traceability and un-linkability must be satisfied by the authentication schemes in VANET.

V. VANET Characteristics

VANET Characteristics VANET is well-known as the subspace of MANET. However there are few characteristics of VANET that makes different from MANET, whereas VANET exhibited complexity in designing it as well as more challenges compared to MANET.

- Frequent Disconnected Network Vehicles are moving while exchanging information. Due to the rapid topology changes, the connections between two vehicles are easily disconnected. Usually the disconnections occur in infrequent networks.
- Rapid Topology Changes Due to the fast moving of vehicles, VANET topology changes quickly.
- Battery Power and Storage Capacity The communications in MANET consumes battery power conversely in VANET, the power and storage is boundless.
- Communication Environment. Obstacles in VANET are presented in dense network as well as sparse network. Trees, buildings, and other objects could obstruct the communications in VANET especially in dense network. For this reason, routing protocol for sparse and dense networks should be considered.

Security Challenges in VANET Security issues in VANET are critical due to vulnerabilities exist during information transmission which causing VANET exposed to the attacks. In order to maintain a secure vehicular communication and networks, VANET security system should satisfy with the requirements. Some of the requirements are essential for all networks, but some are definite for VANET only [23].

Those requirements are;

- Authentication In order to allow the communication between vehicles which sending and receiving information, VANET should authenticate each of them. This process may comprise the identification of the sender identity and the legitimacy of the sender to use the network.

- Availability Availability is defined as the degree of the VANET system that must be operable and available when needed. A fast response time also must applicable for some applications.
- Privacy Privacy is one of the most important requirements in VANET. Privacy must ensure that the identity of the drivers and the location of the vehicles are not being exposed.
- Integrity The information exchange in between the sender and the receiver should be free from the alteration attacks. Thus, information can be trusted.
- Non-repudiation it ensures that the origin of the information cannot be denying that it has sending the information.

VI. Conclusion

The VANET is a vital and promising research area in ITS due to high mobility and dynamic network topology. It aims to ensure the safety of human lives on the street by broadcasting safety messages among the vehicles and provide comfort services to the passengers. Since the safety messages are broadcasted in an open access environment, VANETs are vulnerable to attacks. Therefore, sophisticated and robust security algorithms must be designed to tackle the dangerous security and privacy attacks. In this survey, we discussed the basic overview of the VANET from the architecture, characteristics, and VANET security services.

References

[1] M. Arif, G. Wang, M. Z. Bhuiyan, T. Wang, and J. Chen, ''A survey on security attacks in VANets: Communications, applications and challenges,'' Veh. Commun., vol. 19, pp. 1–36, Sep. 2019, doi: 10.1016/j. vehcom.2019.100179.

[2] Z. Lu, G. Qu, and Z. Liu, ''A survey on recent advances in vehicular network security, trust, and privacy,'' IEEE Trans. Intell. Transp. Syst., vol. 20, no. 2, pp. 760–776, Feb. 2019, doi: 10.1109/TITS.2018.2818888.

[3] D. Manivannan, S. S. Moni, and S. Zeadally, ''Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANETs),'' Veh. Commun., vol. 25, pp. 1–18, Oct. 2020, doi: 10.1016/ j.vehcom.2020.100247.

[4] Q. Wang, D. Gao, and D. Chen, ''Certificate revocation schemes in vehicular networks: A survey,'' IEEE Access, vol. 8, pp. 26223–26234, 2020, doi: 10.1109/ACCESS.2020.2970460.

[5] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, ''Survey of authentication and privacy schemes in vehicular ad hoc networks,'' IEEE Sensors J., vol. 21, no. 2, pp. 2422–2433, Jan. 2021, doi: 10.1109/JSEN.2020.3021731.

[6] 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,'' IEEE Access, vol. 8, pp. 91028–91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[7] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, ''Survey of authentication techniques in vehicular ad-hoc networks (VANETs),'' IEEE Intell. Transp. Syst. Mag., early access, May 12, 2020.

[8] Mohammad, S.A.; Rasheed, A.; Qayyum, A. VANET Architectures and Protocol Stacks: A Survey. *Commun. Technol. Veh.* **2011**, 95–105.

[9] Tomar, R.; Prateek, M.; Sastry, G.H. Vehicular Adhoc Network (VANET)—An Introduction. *Int. J. Control. Theory Appl.* **2016**, *9*, 8883–8888.

[10] Balu, M.; Kumar, G.; Lim, S.-J. A review on security techniques in vanets. *Int. J. Control. Autom.* 2019, *12*, 1–14.

[11] Paranjothi, A.; Khan, M.S.; Nijim, M.; Challoo, R. MAvanet: Message authentication in VANET using social networks. In Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 20–22 October 2016.

[12] Papadimitratos, P.; Buttyan, L.; Holczer, T.; Schoch, E.; Freudiger, J.; Raya, M.; Hubaux, J.-P. Secure vehicular communication systems: Design and architecture. *IEEE Commun. Mag.* 2008, *46*, 100–109.

[13] Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* 2014, *44*, 1–13.

[14] Purkait, R.; Tripathi, S. Fuzzy Logic Based Multi-criteria Intelligent Forward Routing in VANET. *Wirel. Pers. Commun.* 2020, *111*, 1871–1897.

[15] Salem, F.M.; Ali, A.S. SOS: Self-organized secure framework for VANET. *Int. J. Commun. Syst.* 2020, e4317.

[16] Silva, C.M.; Masini, B.M.; Ferrari, G.; Thibault, I. A Survey on Infrastructure-Based Vehicular Networks. *Mob. Inf. Syst.* 2017, *2017*, 1–28.

[17] Ho, K.Y.; Kang, P.C.; Hsu, C.H.; Lin, C.H. Implementation of WAVE/DSRC devices for vehicular communications. In Proceedings of the International Symposium on Computer, Communication, Control and Automation, Tainan, China, 5–7 May 2010; pp. 522–525.

[18] Pauzie, A. In-vehicle communication systems: The safety aspect. *Inj. Prev.* 2002, *8*, 26–29.

[19] Neumann, A.; Mytych, M.J.; Wesemann, D.; Wisniewski, L.; Jasperneite, J. Approaches for In-vehicle Communication—An Analysis and Outlook. *Commun. Comput. Inf. Sci.* 2017, 395–411.

[20] Yang, X.; Liu, L.; Vaidya, N.H.; Zhao, F. A vehicle-to-vehicle communication protocol for cooperative collision warning. In Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), Boston, MA, USA, 22–26 August 2004.

[21] Jurgen, R. V2V and V2I Technical Papers. In *V2V/V2I Communications for Improved Road Safety and Efficiency*; SAE: Warrendale, PA, USA, 2012.

[22] Anaya, J.J.; Merdrignac, P.; Shagdar, O.; Nashashibi, F.; Naranjo, J.E. Vehicle to pedestrian communications for protection of vulnerable road users. In Proceedings of the 2014 IEEE Intelligent Vehicles Symposium Proceedings, Dearborn, MI, USA, 8–11 June 2014; pp. 1037–1042.

[23] S. S. Shinde and S. P. Patil, "Various Issues in Vehicular Ad hoc Networks : A Survey," vol. 1, no. 2, pp. 399–403, 2010.