Current Challenges and Security Issues in VANET – A Review

Inderpreet kaur[1], Dr. Rajeev Bedi[2], Dr. R.C.Gangwar[3]
[1]Scholar, Computer Science , Beant College of Engineering & Technology,
Gurdaspur, India
[2]Associate Professor, Computer Science, Beant College of Engineering & Technology
Gurdaspur, India
[3]Head of Department, Computer Science, Beant College of Engineering & Technology
Gurdaspur, India

Abstract-In the modern world, communication in the various networks becomes a big challenge. In Vehicular ad hoc Networks (VANETs), information is exchanged among various nodes of the network which provides the solution to control traffic, efficiency and security to the travelers. Various protocols are used to work with VANET and they work on the basis of different rules and regulations. Security attack is a big challenge in VANET. Many authors have addressed the attacks and their solutions. Thus, we can say that VANET is gaining much attention in the modern era because of its advancement and its modern applications. In VANET, malicious node can attack the network in many ways and detecting such a node is a big challenge. Thus, in this paper we have described the various issues of VANET, its characteristics, security challenges, various routing protocols and its applications in the modern era. Main motive of the paper is to understand the VANET in better way to get idea about the research challenges in the VANET.

Keywords- Vehicular ad hoc network (VANET), malicious, security, protocols, routing.

I. INTRODUCTION

Nowadays, the sheer volume of traffic on road affects the safety, efficiency and security of vehicles in traffic environment. Approximately, an average of 1.2 million or more people lost their lives annually in road accidents. Road traffic safety has become the challenging issue in traffic management. To tackle such phenomenon, one possible way is to provide the traffic information among vehicles earlier, so that they can utilize it to analyze the traffic environment. Vehicles are mobile in nature, so the network we want should be self organized, self creating can self administered and decentralized which operates without infrastructure in a distributed environment. This can be achieved by integrating nodes and the whole network into a single unit through wireless connection called ad hoc network [1].

VANET is a self organized network which is developed by connecting vehicles on the road where each vehicle moves freely in the network coverage area to improve and maintain the safety on road and also to manage traffic. It also provides various infotainment services to each and every end user which is further responsible for an efficient driving environment [2]. In VANET, communication can be manifested in two ways, first is a wireless ad hoc network where vehicles communicate without any infrastructure. In second form, the road side units (RSU) or base stations and vehicles communicate within a fixed infrastructure. Here, each vehicle acquires the two units, On Board Unit (OBU) and Application Unit (AU) as shown in Fig. 1. OBU provides communication whereas AU utilizes the communicational capabilities of OBU to execute various programs [3].

In VANET, all vehicles are capable of sending, receiving messages to and from other vehicles without using any infrastructure. The message contains information regarding the traffic conditions and current position of the data packet [4].

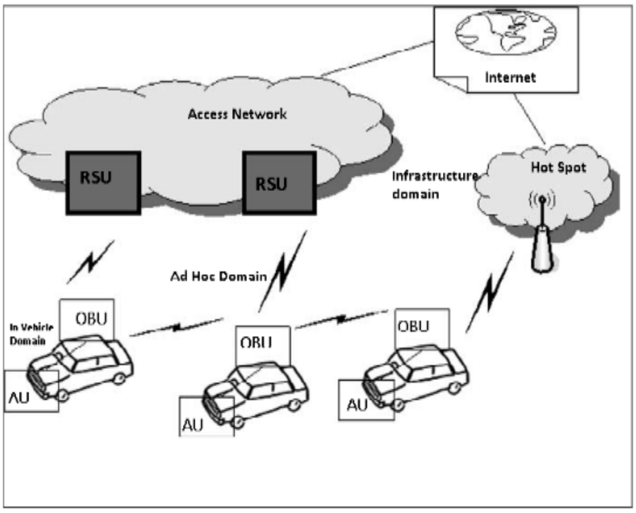

Fig. 1. Architecture of VANET

VANETs have specific characteristics which make it unique from other Ad hoc networks such as higher computational capability, higher transmission power, sufficient storage and predictable mobility that supports longer communication. VANETs have a mobility pattern through which they can travel in a specific path rather any random path.

The rest of this paper is organized as follows: Section II overviews the characteristics of VANET. Section III describes VANET applications. Section IV presents various routing attacks in VANET. Section V shows various routing protocols used in VANET. Section VI concludes the paper.

II. CHARACTERISTICS OF VANET

VANET has specific characteristics which distinguish it from other ad hoc networks.

A. High Mobility

On highways, the vehicles usually move at high speed. This makes harder to predict their position and protect their privacy.

B. Rapidly changing network topology

Due to high mobility and randomness of vehicles, their position changes frequently. So, the network topology in VANET also changes rapidly.

C. Unbounded network size

VANET's network size is geographically unbounded as its implementation is possible within a city, in several cities or within a country.

D. Frequent exchange of information

VANET motivates the nodes or vehicles to interact with road side units and other vehicles which makes information exchange among vehicles more frequent. Also vehicles interact with on board sensors embedded in each vehicle to get node position, its speed and direction to establish Ad hoc communication.

E. Wireless Communication

VANET implementation takes place in wireless environment. Nodes are connected via wireless and exchange the traffic information within a wireless interface.

F. Sufficient Energy

Vehicles have ample energy and sufficient amount of computation resources. They are not power limited and can provide continuous power to their computing and communication devices [5].

III. APPLICATIONS OF VANET

A. Safety Related Applications

These applications increase the safety on the roads by monitoring roads, its surface, road curves and approaching vehicles etc. These can be further classified.

1) Collision Avoidance

Some research proves that 60% of accidents may be avoided if drivers were provided some warning a second before collision. VANET alerts drivers potentially under crash route so that they can change their ways.

2) Cooperative Driving

Drivers can get early notifications for traffic related warnings like curve ahead, landslide ahead, speed warning, sudden downhill, lane change warning etc. This can help and cooperate in safe driving.

3) Traffic Optimization

Traffic on highway can be optimized by sending notifications like traffic jam ahead, collision ahead etc. to the vehicles so that they can mend their paths and saves time [6].

B. User Based Applications

These provide the user with infotainment services.

1) Peer to peer applications

It includes services as web access, movies, streaming audio and video etc. in the vehicle itself.

2) Internet Connectivity

Users always want Internet connectivity. Their vehicles can access internet all the time in VANET using RSU (Road side unit).

3) Other services

VANET can be utilized in other convenience applications such as electronic toll payment, to locate the nearest fuel station, restaurant etc. [7].

IV. ROUTING ATTACKS IN VANET

Various possible attacks can affect the structure and privacy of VANET in terms of confidentiality, integration and authentication. These security attributes must be followed by VANET to prevent attacks from different sources. Figure 2 illustrates different routing attacks.

A. Impersonate

In this attack, attacker pretends to be what he is not to get the access to the information in network or to disturb the normal functioning of the network. This type of attack is mostly performed when some accident takes place on road, at that time attacker impersonate to other persons and refuse. Attacker may be an insider or outsider. This attack can affect the vulnerability of multiple layers in two ways:

1) False attribute possession:

Here, an attacker claims to be a legitimate user and may steal some private information of original user. For example, a normal vehicle driver may claim that he/she is a police or fire protector to free the traffic.

2) Sybil Attack:

In this type of attack, an attacker may send multiple messages from one vehicle to another by using different identities at the same time [8].

B. Black Hole Attack

In this attack, a malicious node indicates to all its neighboring nodes that it has a short route towards the destination node by transferring fake routing information. It may misuse or drop the data packets instead of forwarding them.

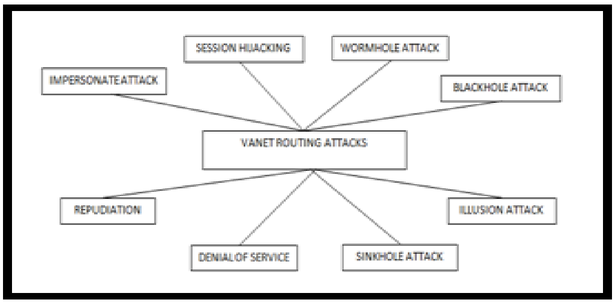

Fig. 2. VANET routing attacks

C. Wormhole Attack

In Wormhole attack, a source to destination communication proceeds through malicious nodes. When a malicious node receives the data packets, it replays them to other nodes by using a wormhole link. Hence, valid route cannot be discovered in this situation [9].

D. Sinkhole Attack

In this attack, malicious node tries to transfer the fake routing information to the network traffic behind it either by altering the received data packets or by dropping them.

E. Illusion Attack

In this kind of attack, attacker tries to manipulate the sensor readings of its own vehicle for giving false information about the vehicle. It tries to broadcast the fake warning messages to its neighboring nodes. It can cause road accidents, traffic jams and reduce the network efficiency.

F. Session hijacking

Most authentication processes are done initially in a session. Hence, it is easy to attack the session immediately after connection establishment. Attacker takes control of the session among nodes.

G. Repudiation

The main threat of repudiation is an attempt to denial by a node involved in the communication. This is slightly different from the impersonate attack as in this attack, two or more entities have common identity which makes it difficult to distinguish them and hence, they can be repudiated.

H. Denial of Service

These attackers can be insider or outsider of the network. An insider attacker can send dummy messages which may cause traffic jam and stops the network whereas outsider attacker may repeatedly disseminates forged messages with invalid signatures to exploit the authentication and confidentiality of information in the network. This attack prevents the legitimate vehicle to make use of services provided by the VANET.

V. ROUTING PROTOCOLS

Routing protocols are needed for communication purpose in a network. Intermediate nodes of a network share information through these protocols. These protocols help to search the reliable route from source node to the destination node. Mainly two types of routing protocols are implemented in VANET which can be classified as topology-based and position-based routing protocols [10]. Figure 3 illustrates the taxonomy of these protocols. Here we will discuss only the topology based routing protocols.

A. Topology-based Protocols

These protocols make use of the link information provided by the network to send various data packets among nodes. They are further classified as given below [11].

1) Proactive Routing Protocols

These are also known as table driven protocols which contain updated list of the routes and their destinations. They establish routes in advance for each node in the network. All the nodes are updated periodically. Hence, they consume a lot of bandwidth [12].

a) Optimized Link State Routing Protocol (OLSR)

It is a link-state protocol, which optimizes the broadcasting of data packets among nodes to reduce bandwidth consumption [13].

b) Fisheye State Routing Protocol (FSR)

A routing table is maintained at each node and it is updated whenever the new information is received from its neighboring nodes and exchanges this updated information with local neighbors.

2) Reactive Routing Protocols

These protocols are also known as on demand routing protocols as route determination is done on demand basis and maintains only the latest or updated routes. Routes are built only when they are required. Vehicles communicate over a very limited number of routes. These routing protocols provide effective bandwidth. But, it also leads to high latency while finding routes. It considers AODV and DSR protocols [14].

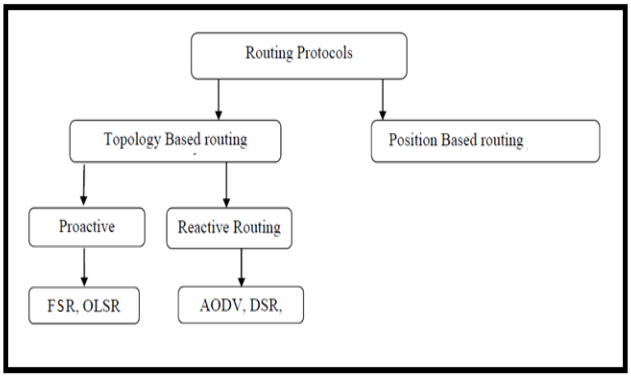

Fig. 3. Routing protocols in VANET

a) Dynamic Source Routing Protocols (DSR)

It is based on source routing means header of the data packet contains the information regarding the path travelled by it. It finds route on demand, and maintains routes to provide communication. But during the route maintenance process, a broken link cannot be repaired and also with increasing mobility, its performance decreases [15].

b) Ad Hoc On Demand Distance Vector Routing Protocol (AODV)

On-Demand routing protocols find their destination node by flooding a request of searching for their destinations to neighboring nodes. Neighbors of nodes can be detected by using neighbor discovery method [16]. High overhead can be produced in AODV by generating routing packets and neighbor discovery messages. To overcome such issues, an Intelligent-AODV (I - AODV) scheme is proposed which reduces the overhead of neighbor discovery processes [17].

VI. Conclusion and Future Scope

As security in VANET is a big challenge and various approaches are used to handle the security issues in the current era. But still it demands a lot of work to handle the malicious nodes to minimize the possibilities of attacks in the VANET to overcome the problems. In a few time span VANET has gain a lot of attention and it is working in a fine way to improve the safety on roads and driving conditions. Thus, in this paper we have discussed the various issues related to VANET by considering the different protocols used in the same area.

Researchers have to work on this area to solve the problem related to the misbehavior of nodes to make VANET more reliable and safe. Thus, the future scope includes adding efficient learning techniques to mine correlation of the events and relationship between vehicular nodes to recognize misconducts. Hence, privacy and security issues are also needed to be handled seriously so that attackers do not target the scenario accurately. So, we can say a well considered approach is needed to find out the solution of all challenges in the VANET which can results in a better performance by using advance protocols.

REFERENCES

[1] Annu Mor, “A study of improved AODV routing protocol in VANET”, International Journal of Computer Applications & Information Technology, Vol. 2, 2013.

[2] T.Priyadarsini, B.Arunkumar, K.Sathish and V.Karthika, “Traffic information dissemination in Vanet using IEEE-802.11”, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 4, Issue 1, 2013, pp. 294 - 303, ISSN Print: 0976-6464, ISSN Online: 0976 –6472.

[3] Yatendra Mohan Sharma and Saurabh Mukherjee, “A contemporary proportional exploration of numerous routing protocols in Vanet”, International Journal of Computer Applications, Vol. 50, No. 21, pp. 14-21, 2012.

[4] E. Schoch, F. Kargl, and M. Weber, “Communication patterns in VANETs,” IEEE Communications Magazine, vol. 46, no. 11, pp. 119–125, 2008.

[5] Chao Song, Ming Liu, Yonggang Wen, Jiannong Cao and Guihai Chen "Buffer and switch: An efficient road-to-road routing scheme for VANETs", Seventh International Conference on Mobile Ad-hoc and Sensor Networks, 2011.

[6] Vincent D. Park and M. Scott Corson, “A highly adaptive distributed routing algorithm for mobile wireless networks”, Proceedings of the INFOCOM '97, Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 1997.

[7] Yaseer Toor et al., “Vehicle ad hoc networks: Applications and related technical issues”, IEEE Communications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3, pp. 74-88.

[8] Marwa Altayeb and Imad Mahgoub, “A survey of vehicular ad hoc networks routing protocols”, International Journal of Innovation and Applied Studies, ISSN 2028-9324, Vol. 3 No.3, pp. 829-846, July 2013.

[9] Alsharif, N., A. Wasef, and X. Shen, “Mitigating the effects of position-based routing attacks in vehicular ad hoc networks in communications”, (ICC), 2011 IEEE International Conference on. 2011: IEEE.

[10] Akhtar Husain, Ram Shringar Raw, Brajesh Kumar and Amit Doegar, "Performance comparison of topology and position based routing protocols in vehicular network environments", International Journal of Wireless & Mobile Networks (IJWMN), vol. 3, no. 4, August 2011.

[11] Jagadeesh Kakarla, S Siva Sathya, B Govinda Laxmi2, Ramesh Babu B3 "A survey on routing protocols and its issues in VANET" International Journal of Computer Applications (0975 – 8887) Volume 28– No. 4, August 2011.

[12] Gongjun Yan, Nathalie Mitten, and Xu Li2, “Reliable routing in vehicular ad hoc networks”, IEEE 30th International Conference on Distributed Computing Systems Workshops, 2010.

[13] Bijan Paul, Mohammed J. Islam, “Survey over VANET routing protocols for vehicle to vehicle communication,” IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661, ISBN: 2278-8727, vol. 7, Issue 5 (Nov-Dec. 2012), pp. 01- 09.

[14] Uma Nagaraj, Dr. M. U. Kharat, Poonam Dhamal "Study of various routing protocols in VANET" IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011

[15] Y.-W. Lin, Y.-S. Chen, and S.-L. Lee, “Routing protocols in vehicular Ad Hoc networks: a survey and future perspectives,” Journal of Information Science and Engineering, vol. 26, no. 3, pp. 913–932, 2010.

[16] Omid Abed, Reza Barangi and M. Abdollahi Azgomi, “Improving route stability and overhead of the AODV routing protocol and making it usable for VANETs”, 29th IEEE International Conference on Distributed Computing Systems Workshops,2009.

[17] P.A. Kamble, Dr. M.M. Kshirsagar, “Improvement over AODV routing protocol in VANET”, IAEME, ISSN 0976 – 6367(Print), ISSN 0976 – 6375(Online) Volume 4, Issue 4, pp. 315-320, July-August (2013).