Survey on security challenges in VANET

[1]Anup Dhamgaye, [2]Nekita Chavhan

[1] Wireless Communication and Computing, Dept. of CSE, G. H. Raisoni College of Engineering, Nagpur, India

[2] Dept. of CSE, G. H. Raisoni College of Engineering, Nagpur, India

Abstract

Recent advances in development of Wireless Communication in Vehicular Adhoc Network (VANET) has provided emerging platform for industrialists and researchers. Vehicular adhoc networks are multihop networks with no fixed infrastructure. It comprises of moving vehicles communicating with each other. One of the main challenge in VANET is to route the data efficiently from source to destination. Designing an efficient routing protocol for VANET is tedious task. Also because of wireless medium it is vulnerable to several attacks. Since attacks mislead the network operations, security is mandatory for successful deployment of such technology. This survey paper gives brief overview of different routing protocols. Also attempt has been made to identify major security issues and challenges associated with different routing protocols.

.

Keywords: *VANET, ITS, Routing Protocols, Security, Attack.*

1. Introduction

Wireless communication is ubiquitous because of its flexibility to adapt to different scenarios. Mobile Ad Hoc Networks (MANETS) is a term coined for the continuously varying network topology handheld mobiles devices. Vehicular Ad Hoc Networks (VANETS) is one of its types. It deploys the concept of continuously varying vehicular motion. The nodes or vehicles as in VANETS can move around with no boundaries on their direction and speed. Vehicular adhoc network (VANET) involves vehicle to vehicle (V2V), vehicle to roadside (V2R) or vehicle to infrastructure (V2I) communication [1].VANET generally consist of On Board Unit (OBU) and Roadside Units (RSUs). OBUs enables short-range wireless adhoc network to be formed between vehicles. Each vehicle comprises of hardware unit for determining correct location information using GPS. Roadside Units (RSUs) are placed across the road for infrastructure communication. The number of RSU to be used depends upon the communication protocol.

VANET provide assistance to vehicle drivers for communication and coordination among themselves in order to avoid any critical situation through Vehicle to Vehicle communication [2] e.g. road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc. Besides safety applications VANET also provide comfort applications to the road users. Due to the dynamic nature of nodes in VANET the routing of data packets is much complex. Several factors like the type of the road, daytime, weather, traffic density and even the driver himself affect the movements of vehicles on a road. Hence, the network topology change frequently, and the routing protocol used has to adapt itself to these instantaneous changes continuously.

The paper is organized in 7 sections. In Section 2 we discuss about VANET Overview. Section 3 highlights some of the standards for wireless access in VANET communication. Section 4 presents categories of VANET network architecture. Section 5 provides an overview about VANET routing protocols. In Section 6 a brief review is made on Attacks in VANET. The paper closes with a conclusion in Section 7.

2. VANET Overview

2.1 Intelligent Transportation System (ITS)

In Intelligent Transportation Systems (ITS) [3], each vehicle broadcast the information to the vehicular network or transportation agency, which then uses this information to ensure safe and free-flow of traffic. The possible communication configurations in ITS are inter-vehicle, vehicle to roadside, and routing-based communications [4] all this configurations requires precise and up-to-date surrounding information.

2.1.1 Inter-vehicle Communication

Inter-vehicle communication support multi-hop multicast/broadcast over a multiple hops to a group of receivers. ITS is generally concerned with the activity on

the road ahead and not on road behind. Naive broadcasting and intelligent broadcasting [4] are the two message forwarding methods used in inter-vehicle communications. Fig. (1) shows inter-vehicle communication.

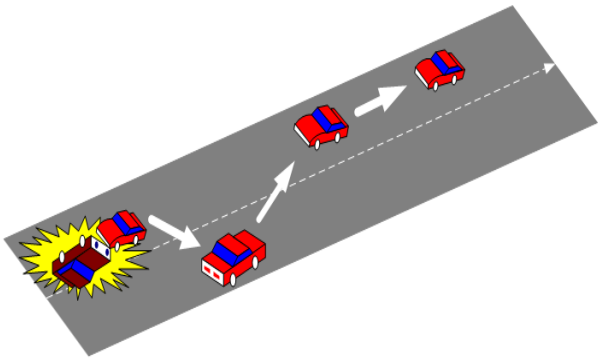

Fig. 1. Inter-vehicle communication

Naive broadcasting believes on the periodic broadcasting of message, if the message is from a vehicle behind it then vehicle ignores the message, but if the message comes from a vehicle ahead then the receiving vehicle sends its own broadcast message to vehicle behind it. Due to the large number of messages, probability of message collision increases which lowers the message delivery rate and increases its time of delivery. This problem is overcome using intelligent broadcasting. It uses acknowledgment address limiting the number of messages broadcast for emergency events only.

2.1.2 Vehicle-to-roadside communication

In this type of communication, vehicle communication is done using single hop broadcasting method. This type of configuration provides ample amount of bandwidth link between communicating parties. In vehicle to roadside communication the maximum load for proper communication is given to the road side unit, it controls the speed of vehicle when it observes that a vehicle violates the desired speed limit, it delivers a broadcast message in the form of an auditory or visual warning, requesting the driver to reduce speed. Vehicle-to-roadside communication is shown in Fig. 2. Here RSU sends broadcast messages to all the equipped vehicles.

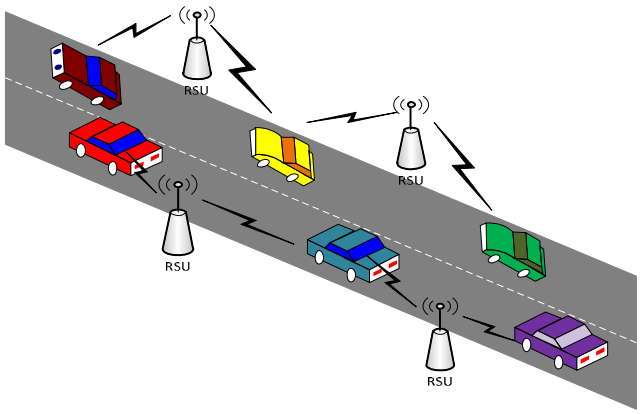

Fig. 2. Vehicle-to-Roadside Unit Communication

2.1.3 Routing-based communication

Multi-hop unicast method is used in routing-based communication configuration. While sending the message, the vehicle sends message using multi-hop fashion until it reaches to the desired vehicle. Receiving vehicle then sends a unicast message to the requested vehicle. Fig. 3. shows the routing-based communication in VANET. Here vehicle A sends message to vehicle C using routing protocols.

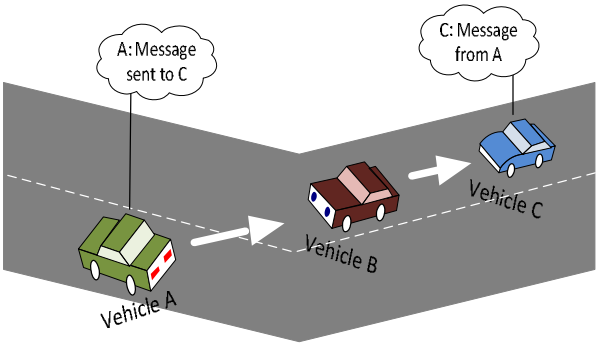

Fig. 3. Routing-based Communication

3. Standards for wireless access in VANET

Vehicular environment supports different communication standards that relate to wireless accessing. The standards are generally helpful for the development of product to reduce the cost and it also helps the users to compare competing products. These standards are as follows:

3.1 Dedicated Short Range Communication (DSRC)

It provides a communication range from 300m to 1Km. The V2V and V2R communication takes place within this range. DSRC [5, 6] uses 75MHz of spectrum at 5.9GHz, which is allocated by United States Federal

Communications Commission (FCC). This provides half duplex, 6-27 Mbps data transferring rate. DSRC is a free but licensed spectrum. Free means FCC does not charge for usage of that spectrum and licensed means it is more restricted regarding of its usage. The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. Out of these 7 channels, one of the channel is reserved only for safety communication. Two channels are used for special purpose like critical safety of life and high power public safety and rests of the channels are service channels.

3.2 IEEE 1609-standards for Wireless Access in Vehicular Environments (WAVE)

It is also known as IEEE 802.11p. It supports the ITS applications, for a short range communications. In WAVE, V2V and V2R communication uses 5.85-5.925 GHz frequency range. It provides real time traffic information improving performance of VANET. It also benefits the transport sustainability. It contains the standard of IEEE 1609 [7, 8, 9]. This is upper layer standard. It uses Orthogonal Frequency Division Multiplexing techniques to divide the signal into various narrow band channels. This also helps to provide a data transferring rate of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels.

4. Vanet Network Architecture

The network architecture [10] of VANETs mainly falls within three categories: pure cellular/WLAN, pure ad hoc, and hybrid. They are discussed as follows:

4.1 Cellular/WLAN

In this type of network architecture, a fixed cellular gateways and WLAN/WiMAX access points at traffic intersections are used in order to connect to the Internet, gather traffic information, or for routing purposes. The network architecture under this scenario is a pure cellular or WLAN structure as shown in Fig.4. VANET can combine both cellular network and WLAN to form the network so that a WLAN is used where an access point is available or a 3G connection otherwise.

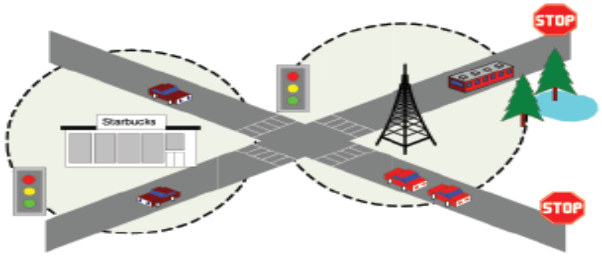

Fig. 4 Cellular/WLAN Network Architecture

4.2 Ad Hoc

The cellular/WLAN network architecture is costlier since it include a fixed gateways and other hardware devices hence to overcome this problem vehicles and all the road-side wireless devices can form a pure adhoc network among themselves. The adhoc network architecture is as shown in Fig. 5. It helps in vehicle to vehicle communications and achieves certain goals, such as blind crossing.

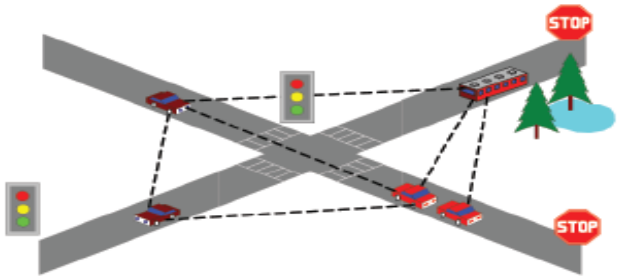

Fig. 5 Ad Hoc Network architecture

4.3 Hybrid

Hybrid architecture in Fig. 6 is a combination of infrastructure network and ad hoc network. This is also a possible solution for VANET. The hybrid architecture though can provide better coverage, arises a new problem such as the seamless transition of the communication among different wireless systems.

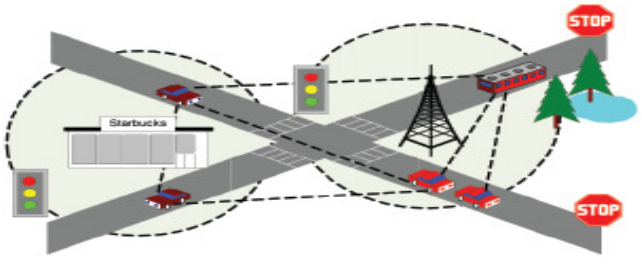

Fig. 6 Hybrid Network Architecture

VANETs can be distinguished from other kind of adhoc networks as follows:

Highly dynamic topology: Due to high speed of movement between vehicles, the topology of VANETs is always changing.

Frequently disconnected network: Due to the same reason, the connectivity of the VANETs could also be changed frequently. Especially when the vehicle density is low, it has higher probability that the network is disconnected. However, a possible solution is to pre-deploy several relay nodes or access points along the road to keep the connectivity.

Mobility modeling and predication: Due to highly mobile node movement and dynamic topology, mobility model and predication play an important role in network protocol design for VANETs. Moreover, vehicular nodes are usually constrained by pre-built highways, roads, and streets, so on giving the speed and the street map the future position of the vehicle can be predicted.

Geographical type of communication: The VANETs often have a new type of communication that addresses geographical areas where packet needs to be forwarded (e.g., in safety driving applications).

Various communication environments: VANETs are usually operated in two typical communication environments they are highway traffic scenarios and city traffic scenarios**.** In highway traffic scenarios, the environment is relatively simple and straightforward (e.g., constrained one-dimensional movement), while in city conditions it becomes much more complex. The streets in a city are often separated by buildings, trees, and other unstated obstacles. Therefore, there isn't always a direct line of communications in the direction of intended data communication.

Sufficient energy and storage: A common characteristic of nodes in VANETs is that nodes have ample energy and computing power (including both storage and processing), here nodes are cars instead of small handheld devices.

Hard delay constraints: In some VANETs applications, the network does not require high data rates but has hard delay constraints. For example, in an automatic highway system, when brake event happens, the message should be transferred and arrived in a certain time to avoid car crash. In this kind of applications, instead of average delay, the maximum delay will be crucial.

Interaction with on-board sensors: It is assumed that the nodes are equipped with on-board sensors to provide information that can be used to form communication links and for routing purposes. For example, GPS receivers are increasingly becoming common in cars, which help to provide location information for routing purposes.

5. VANET Routing Protocols

Routing protocols [10, 11, 12] are the basic building block for efficient communication in any type of network. The goal of routing protocols is to select best path with least time and least expensive route. The routing operation involves finding the best route from source to destination and vice-versa. This is done in two basic ways via source routing or hop by hop routing. It is a challenge to the researchers to develop routing protocols for highly dynamic topology like VANET. The routing protocols for VANET are classified into five different categories which are discussed as follows.

5.1 Topology Based Routing

This routing protocol uses link information that exists in the network to perform packet forwarding. They are further divided into Proactive and Reactive routing protocols.

5.1.1 Proactive routing protocols

Proactive routing means that the routing information, like next forwarding hop is maintained in the background irrespective of communication requests. The advantage of proactive routing protocol is that there is no route discovery since the destination route is stored in the background. The disadvantage encountered with this protocol is that it provides low latency for real time application. The various types of proactive routing protocols are: FSR, DSDV, OLSR, CGSR, WRP, and TBRPF.

5.1.2 Reactive/On-demand routing Protocols

Reactive routing opens the route only when it is necessary for a node to communicate with each other. Reactive routing consists of route discovery phase in which the query packets are flooded into the network for the path search and this phase completes when route is found. The various types of reactive routing protocols are AODV, PGB, DSR, TORA, and JARR.

5.2 Position Based Routing/Geographic routing

Geographic routing is a routing technique in which each node knows it's own & neighbor node geographic position by position determining services like GPS. It doesn't maintain any routing table or exchange any link state information with neighbor nodes. Information from GPS device is used for routing decision. Geographic routing is broadly divided in two types: Position based greedy V2V protocols and Delay Tolerant Protocols.

5.3 Cluster-Based Routing

In cluster-based routing a virtual grouping is formed among the vehicles called clusters. Each cluster has a cluster head which is responsible for intra and inter cluster communication. Nodes in a cluster communicate via direct links. The creation of a virtual network infrastructure is crucial for the scalability of media access protocols, routing protocols, and the security infrastructure. The stable clustering of nodes is the key to create this infrastructure. Cluster-based routing protocols can achieve good scalability for large networks, but a significant hurdle for them in fast-changing VANET systems is delay and overhead involved in forming and maintaining these clusters.

The different types of cluster based routing protocols are COIN, LORA-CBF, TIBCRPH, and CBDRP.

5.4 Broadcast Routing

In broadcast routing, flooding mechanism is used where each node rebroadcasts messages to all of its neighbors except the one it got this message from. Flooding mechanism guarantees that the message will reach to each node in the network. Flooding is easily implemented mechanism for small number of nodes. But for a large number of nodes this mechanism is somewhat time consuming thereby reducing performance of the network**.** Flooding may have a very significant overhead and selective forwarding can be used to avoid network congestion.

Broadcast is a frequently used routing method in VANETs such as sharing traffic, weather, emergency, road condition among vehicles, and for delivering advertisements and announcements. Broadcast is also used in unicast routing protocols (routing discovery phase) to find an efficient route to the destination. When the message needs to be disseminated to the vehicles beyond the transmission range, multihop is used.

The various broadcast based routing protocols are BROADCOMM, UMB, V-TRADE, and DV-CAST.

5.5 Geocast Routing

Geocast routing is a location-based multicast routing. The objective of a geocast routing is to deliver the packet from a source node to all other nodes within a specified geographical area. Geocast can be implemented with a multicast service by simply defining the multicast group over a certain geographic region. Most geocast routing methods are based on directed flooding, which tries to limit the message overhead and network congestion of simple flooding by defining a forwarding zone and restricting the flooding inside it.

The different geocast based routing protocols are IVG, DG-CASTOR and DRG

In this section, the challenges of designing routing protocols in VANETs and several routing protocols have been discussed. In general, position based routing and geocasting are more promising than other routing protocols for VANETs because of the geographical constrains. However, the performance of a routing protocol in VANETs depends heavily on the mobility model, the driving environment, the vehicular density, and many other facts. Therefore, having a universal routing solution for all VANETs application scenarios or a standard evaluation criterion for routing protocols in VANETs is extremely hard. In other words, for certain VANETs application a customizing routing protocol and mobility model need to be designed to fulfill its requirements.

6. Attacks in VANET

Even if there are advances in VANET but still it has many challenges to be overcome. This challenge is attacks on VANET. Raya et al. [13] classifies attacker as having three dimensions: "insider versus outsider", "malicious versus rational", and "active versus passive". The types of attacks against messages, can be described as follows: "Bogus Information", "Cheating with Positioning Information", "ID disclosure", "Denial of Service", and "Masquerade". Irshad Ahmed Sumra et al. [14] proposed different classes of attacks like network, application, timing, monitoring, and social. Each class describes different type of attack, its threat level, and its priority. Along with this model some new attacks are also proposed by them. The aim of their model is to easily identify these attacks and their association to respective classes.

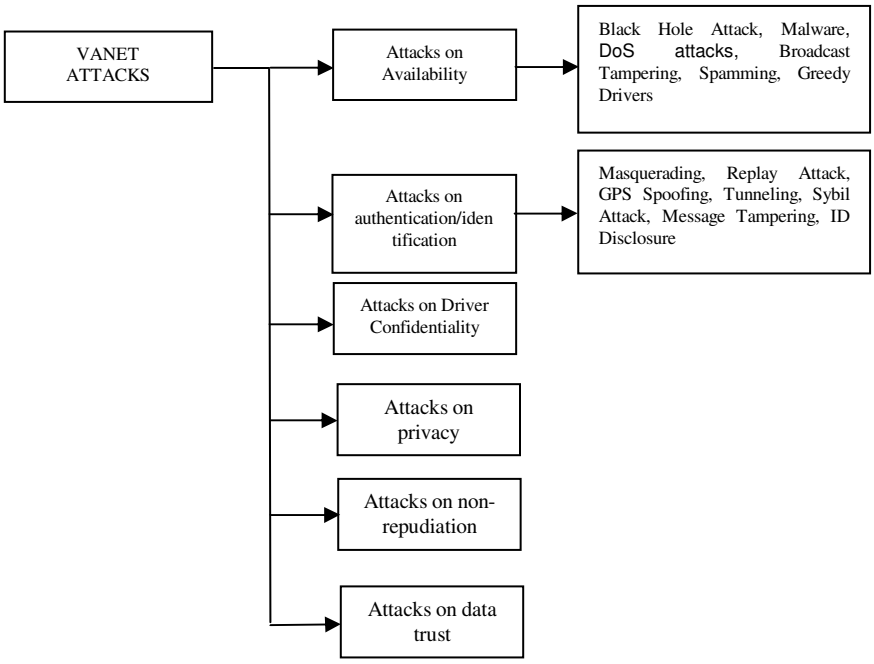

Fig.7 VANET Attacks

Attacks in VANET [4, 15] are classified depending on the Availability, Authentication / identification, Confidentiality, Privacy, Non-repudiation, and Data-trust. Fig.7 gives an idea about classification of VANET attacks.

6.1 Attacks on availability

Availability in VANET means any information at any time of communication. This security requirement is critical in time varying environment. Availability in VANET should be assured both in the communication channel and participating nodes. A classification of these attacks, according to their target, is as follows:

6.1.1 Black Hole Attack

This is one of the security attack occur in VANET. In this attack the attacker node refuses to participate or even drop the data packet [16]. Hence the effect of this type of attack is most dangerous to the vehicular network.

6.1.2 Malware

Malware is a malicious software whose aim to disrupt the normal operation. This attack is carried out by insider. This attack is introduced in the network when the software update is received by car's VANET units and roadside station.

6.1.3 Broadcast Tampering

In this type of attack the attackers introduces false safety messages into the network. This message sometime hides the traffic warnings [17]. This leads to the critical situation like accidents and road congestions'.

6.1.4 Spamming

Spamming are the messages which are of no use to the users like advertisements. The aim of such attack is to consume bandwidth and increase the transmission latency. Due to lack of centralized administration the controlling on such attack is difficult.

6.1.5 Greedy Drivers

Greedy drivers are those who try to attack for their own benefit. These drivers cause overload problem for RSU. This leads to delay in service to the authorized users. On increasing number of such drivers the authorized users faced slow services.

6.1.6 Denial of Service

Denial of Service (DOS) [14] is one of the most serious level attacks in vehicular network. In DOS attack, the attacker jams the main communication medium and network is no more available to legitimate users. The main aim of DOS attacker is to prevent the authentic users to access the network services. DOS attack also

causes the attacks like DDOS (Distributed Denial Of service) which is one of the sever attack in vehicular environment. The aim of this attack is to slow down the network. Jamming is also one of the kinds of DOS attack which jams the channel, thus not allowing other users to access the network services.

6.2 Attacks on Authentication/identification

In these types of attack the affected area is identification/authentication. Whenever any vehicle in VANET needs secure communication its basic requirement is either identification or authentication of nodes under consideration. When the receiving vehicle is identified or authenticated then only a trustworthy transmitter vehicle is allowed to communicate amongst them. The different types of attack on authentication/identification are discussed as follows.

6.2.1 Masquerading

This attack is a result of providing false identities while communication by an attacker. Masquerading [15] involves message fabrication, alteration and replay. For example, to slow down other vehicle speed an attacker tries to act as an emergency vehicle and hence defraud other vehicle.

6.2.2 Replay Attack

This attack happens when an attacker replays the transmission of earlier information to take advantage of the situation of the message at time of sending [20].

6.2.3 Global Positioning System (GPS) Spoofing

The exact position on the earth can be easily known to every vehicle by using GPS. In this attack an attacker provide false information to other vehicle by producing false readings in the GPS devices. This is done by an attacker using GPS simulators that generate signals which are stronger than those generated by genuine satellite.

6.2.4 Tunneling

This attack happens when an attacker connects two distant parts of the Adhoc network using an extra communication channel as a tunnel. As a result, two distant nodes assume they are neighbors and send data using the tunnel [21]. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack.

6.2.5 Sybil Attack

In this attack an attacker pretends to have multiple identities. An attacker can behave as if it were a large number of nodes simply by claiming false multiple identities [14]. It provides illusion to other vehicle by sending some wrong messages like traffic jam message. The objective is to enforce other vehicles on the road to leave the road for the benefits of the attacker.

6.2.6 Message Tampering

In this attack the valuable or even critical traffic safety messages can be manipulated. This is done by attacker by modifying, dropping or corrupting the messages [22].

6.2.7 ID Disclosure

In this type of attack the ID of targeted nodes will get disclosed for tracking the current location of that node. A global observer monitors the target nodes and some time sends a malicious message to neighbor of targeted nodes. This tracked data is used for other purpose like car rental companies to track their own cars [23].

6.3 Attacks on confidentiality

Confidentiality is one of the important security requirement in vehicular communication, it assure that the message will only be read by authorized parties [15]. This kind of security requirement is generally present in group communications, in which only group members are allowed to read such information. The remaining VANET settings transmit public information. Because VANET mobility is higher than MANET, routing with capability of ensuring security in VANET is more problematic than Adhoc. Confidentiality of messages exchanged between the nodes of a vehicular network is particularly vulnerable with techniques such as unlawful collection of messages through eavesdropping and gathering of location information available through the transmission of broadcast messages. In case of eavesdropping, the attacker can collect information about existing users without their permission and use the information at a time when the user is unaware of the collection. Location privacy and anonymity are important issues for vehicle users.

6.4 Attacks on privacy

This type of attack is related with unauthorized accessing important information about vehicles. There is direct relation between driver and vehicle. If the attackers illegally access some data this directly affect the driver's privacy [15]. Usually a vehicle owner is also its driver, so if an attacker is getting the owner's identity then

indirectly vehicle could put its privacy at risk; this type of privacy attack is called as identity revealing. Location tracking is also one of the well known privacy attacks. In this attack the location of vehicle or the path followed by that vehicle at particular period of time is considered as a personal data.

6.5 Attacks on non-repudiation

When two or more user shares the same key then non-repudiation [15] is occurred. Due to this, two users are not distinguished from each other and hence their actions can be repudiated. An identical key in different vehicle should be avoided using a reliable storage.

6.6 Attacks on data trust

Data trust can be compromised by simply inaccurate data calculation and sending affected message, this can be done by manipulating sensors in vehicle, or by changing the sent information [15]. This affects the whole system reliability. And hence some mechanisms must be developed to protect against such attacks in practice in vehicular network.

7. Conclusion

In this paper various aspect of VANET like its environment, standards and network architecture has been discussed; furthermore various characteristics of VANET have been listed which distinguished it from other networks like MANET, Cellular, and WSN. Routing is an important component which used for more prominent and convenient communication. This paper includes detailed working and designing of various VANET routing protocols, finally various attacks in VANET have been classified depending on the availability, authentication, confidentiality, privacy, non repudiation and data trust.
It has been observed that the classification helps to deal with different types of attack on routing protocols in VANET. Since attack creates a more severe condition, it is necessary to analyze the effect of attack on routing protocols which makes more secure vehicular environment.

References

[1] Kawashima, Hironao. "Japanese perspective of driver information systems."Transportation 17, no. 3 (1990): 263-284.

[2] Harsch, Charles, Andreas Festag, and Panos Papadimitratos. "Secure position-based routing for VANETs." In Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, pp. 26-30. IEEE, 2007.

[3] Sun, Jinyuan, Chi Zhang, and Yuguang Fang. "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks." In Military Communications Conference, 2007. MILCOM 2007. IEEE, pp. 1-7. IEEE, 2007.

[4] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular ad hoc networks (VANETs): status, results, and challenges." Telecommunication Systems (2010): 1-25.

[5] Yin, Jijun, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty. "Performance evaluation of safety applications over DSRC vehicular ad hoc networks." In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 1-9. ACM, 2004.

[6] Guo, Jinhua, and Nathan Balon. "Vehicular Ad Hoc Networks and Dedicated Short-Range Communication." Book Chapter. Available at: http://www. nathanbalon. com/project/cis95 (2006).

[7] Stephan Eichler, "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard", in Proceedings of Vehicular Technology Conference, 2007, pp.2199-2203

[8] Jiang, Daniel, and Luca Delgrossi. "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments." In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, pp. 2036-2040. IEEE, 2008.

[9] IEEE (July 2007), "IEEE P802.11p/D3.0, Draft Amendment for Wireless Access in Vehicular Environment (WAVE)".

[10] Watfa, Mohamed. Advances in Vehicular Ad-Hoc Networks: Developments and Challenges. Information Science Reference, 2010.

[11] Paul, Bijan, Md Ibrahim, Md Bikas, and Abu Naser. "VANET Routing Protocols: Pros and Cons." arXiv preprint arXiv:1204.1201 (2012)

[12] Kumar, Rakesh, and Mayank Dave. "A Comparative Study of Various Routing Protocols in VANET." arXiv preprint arXiv:1108.2094 (2011).

[13] Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

[14] Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J-L. bin Ab Manan. "Classes of Attacks in VANET." In Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, pp. 1-5. IEEE, 2011.