IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

# A Review on Security Issues in Vehicular Ad Hoc Network (VANET)

**Manpreet Kaur[1], Navjot Bhullar[2]**

Sri Sai College of Engineering & Technology, Manawala[1,2]

**Abstract:** VANETs have been appeared as a new area of data dissemination process in which vehicles provide aid to the end users. Vehicles in vehicular ad hoc network have highly unstable (dynamic) topology which produces hindrances in timely delivery of sensitive messages Vehicular Ad-hoc networks (VANETs) are very likely to be deployed in the coming years because of the safety requirements and thus become the most relevant form of mobile ad hoc networks. Security is the main issue in VANETs because of the main use of the VANETs is for safety related application and in that case the viability of the security may cause harm to human lives. In this paper, we address the security issues of this networks and its consequences overhead in VANETs.

**Keywords**: vehicular ad hoc network (VANETs), cluster head (CH).

## I. INTRODUCTION

The discovery of ad hoc wireless communication networks is the most remarkable development in telecommunication industry. In armed struggled operations over hostile territories, plays an extreme vital role [2]. Although, not only department of defence(DOF) have keen interest in wireless channels but now-a-days automobile industry showing immense interest in vehicular ad hoc networks for safety, entertainment, multimedia purposes[zedan]. With the increased number of private transport users, the possibility for serious road accidents increases day by day, so to provide secure atmosphere to private transport users VANETs comes outs as best possible panacea for above issue. VANETs provide wireless communication among vehicles through communication standards. The federal committee for computer (FCC) has defined the two standards: wireless access in vehicular environment (WAVE) and dedicated short range communication (DSRC) standards. IEEE has assigned the 1609 family to wireless communication whereas the DSRC specified in 802.11p. Furthermore, VANETs provide the vehicle-vehicle communication and vehicle-infrastructure type of communication. The most cardinal units in VANETs architecture are: application units (AU), on-board unit (OBU), and roadside unit (RSU) .Roadside unit act as a router which provides the services to client. The OBU and AU act as the receiver or clients for the services provided by the roadside unit. Wireless communication in VANETs is of two type inter-vehicle and roadside-vehicle type of communication. Inter-vehicle forms the cooperative driving atmosphere in which vehicles communicate with one another known as cooperative communication [1].

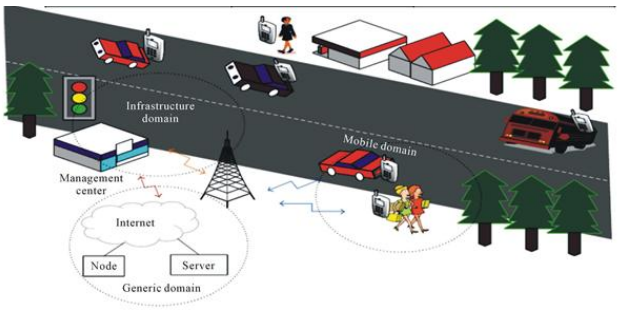


Fig1 VANET System

## II. CHARACTERISTICS OF VEHICULAR ADHOC NETWORK

Vehicular Ad Hoc Network (VANET) is a Dynamic Ad Hoc network containing set of vehicles communicating between each other in ad hoc mode using the wireless medium. The vehicles move on a predefined path due to road topology and at the same time have high speeds. The kind of communication between vehicles is called"Inter-Vehicular Communications". In addition to communicating among themselves, the vehicles also communicate with fixed units on the road also known as Road Side Units (RSUs).Recently, Inter-Vehicular. Communications (IVCs) [3] are highlighted as a way to increase the road safety by utilizing the information exchanged among vehicles utilizing VANET concepts and technologies, in particular, Active Safety which aims at applications like Driver

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Assistance/Information or Decentralized Floating Car Data for improving traffic flows.IVCs are regarded suitable for active safety applications because of their nature to be available anywhere, to require the strict latencies and to cover localized communications. However, ITS can also deal with solutions for better comfort and/or entertainment for drivers and passengers, like(video-) chatting, Internet connection or driving information[4]

## III. ROUTING PROTOCOLS

In this performance analysis, we pick the famous routing protocols: AODV DSDV and OLSR These protocols are optimized for MANETs but also used for VANETs in many occasions. In term of the underlying routing information update mechanism, routing protocols are divided into two major types; reactive (on-demand) or proactive (table-driven). DSDV and OLSR are the examples from the proactive type. While AODV represents the reactive type. For interested readers to the available routing protocols in VANETs could refer to [12].

### A. AODV

In AODV's route discovery process, a source node sets up a route to the destination by sending a Route Request (RREQ) packet. Intermediate nodes forward the packet to other nodes until an active route is found or the maximum number of hops is reached. When an active route has been known, the intermediate nodes will transmit Route Reply (RREP) packet back to the source node. Finally, the source node opens the route after receive the RREP packet. [12].

The use of a destination sequence number (DesSeqNum) to find the latest route to the destination in AODV is a main difference compared to another protocol. If the DesSeqNum of the current packet received is greater than the last stored DesSeqNum, then the node will update the path destination. However, intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. [12].

### B. OLSR

OLSR utilizes a technique called multipoint relaying for optimized message flooding. Each node build and maintains the set of neighbors that can be reached in 1-hop and 2-hops periodically. The dedicated Multi-Point Relays (MPR) algorithm minimizes the number of active relays that is necessary for covering all 2 hops neighbors. OLSR's advantage is as a proactive protocol, the routes to all destinations is known and maintained before the utilization. Nevertheless, it has a strong disadvantage as the nodes in VANETs are moving really fast, calculating the optimal node may be impossible for most cases. [12].

### C. DSDV

DSDV can solve routing loop problem effectively and it is applying the Bellman-Ford algorithm. But it has a weak point that it needs to update the routing table regularly, so it drains more power and more bandwidth[12].

## IV. VANET COMMUNICATION PATTERNS

The use of VANET enables the use of several applications from safety to non-safety applications. These applications exchange messages over VANETs and they are used for different proposes. In the VANET they are four different communication pattern identified [5] [6]. Although other communication pattern exists such as (multimedia access, location based services, etc.).

**1. Vehicle-to-Vehicle (V2V) Warning Broadcast**

This communication pattern is useful in a unicast or multicast situation, where message is been sent to a specific or a group of vehicles. For example and emergency vehicle is approaching, a message can be sent to vehicles coming; this will create an easy passage for the emergency vehicle, or when an accident is detected, a message can be sent to arriving vehicles to warn them and also increase safety on the road [7].

**2. Vehicle-to-Vehicle (V2V) Group Communication**

In this communication pattern, only vehicles that share similar features can participate in the communication. Such features can be static or dynamic in nature, that is vehicles of the same manufacture or enterprise (static nature) or vehicles that appears to be in the same area in a particular time interval (dynamic nature) [8].

## V. SECURITY ARCHITECTURE

All generally includes use of public key signatures. In a public key infrastructure, certificate authorities (CAs) bind between public keys and the nodes. Security and privacy are two critical concerns for the designers of VANETs that, if

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

forgotten, might lead to the deployment of vulnerable VANETs. Unless proper measures are taken, a number of attacks could easily be conducted, namely, message content modification, identity theft, false information generation and propagation, etc. The following are examples of some specific attacks.[10]

1. If message integrity is not guaranteed, a malicious vehicle could modify the content of a message that is sent by another vehicle to affect the behaviour of other vehicles.
2. By doing so, the malicious vehicle could obtain many benefits while keeping its identity unknown. Moreover, the vehicle that originally generated the message would be made responsible for the damage caused.
3. If authentication is not provided, a malicious vehicle might impersonate an emergency vehicle to surpass speed limits without being sanctioned.
4. A malicious vehicle could report a false emergency situation to obtain better driving conditions (e.g., deserted roads), and if non-repudiation is not supported, it could not be sanctioned even if discovered[10]

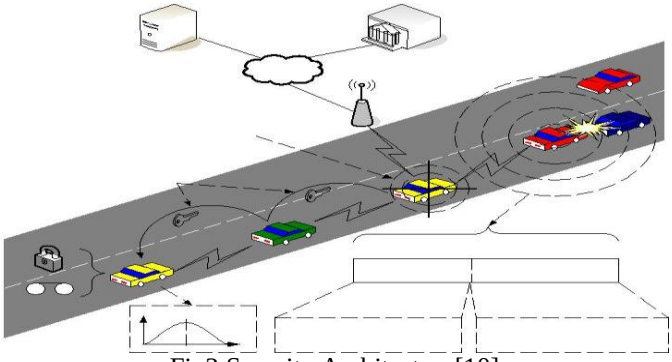

Fig2 Security Architecture[10]

Security is always a challenge for any infrastructure that is been used in communication. Safety in VANET is of high priority because human lives are involved. The security challenges or issues must be put in place during the design of VANET architecture], the author classified attackers into three categories or dimensions; insider versus outsider, malicious versus rational, and active versus passive.

In VANET security issues, the threats are based into three main groups such as; availability, authenticity, and confidentiality. The following 3 subsections expose these issues in details.

**1. Threats to Availability**

The threats to availability of vehicle-to-vehicle and vehicle-to-roadside communication are:[11]

1) Denial of Service Attack: this kind of attack can be done or carried out by an insider, and or outsiders in the network, such attack causes the network to be unavailable to the authentic users. Flooding and jamming with a high volume generated artificial messages causes the VANET components such as the nodes on-board units and roadside units not to sufficiently process the overload caused by the DoS attack.[11]

2) Broadcast Tampering: This attack is carried out by an insider. It inputs false safety messages into the VANET to inflict damage or harm to the road users. An accident can occur when attacker manipulates the traffic on a specific route.

3) Malware: Virus or works can cause serious interference of flow of operation if introduced into VANET. This attack is often carried out by insiders more than outsiders and also it can be downloaded into the network when a firmware update is done.[11]

Spamming: Spam messages in VANET can lead to increased transmission inactivity. This is more difficult to control because there's no centralized administration

**2 Threats to Authenticity**

In VANET authenticity provision is very important. This includes the protecting of legitimate node from the at-tackers "insider or outsider" infiltrating the network with fake identifies, such threats are:[11]

1) Masquerading: This attack is different from others and it's easier to carry out. The attacker joins the net-work by having to get a functioning onboard unit and the attacker possess as a legitimate vehicle in the network, variety of attack can be carried out or feasible such as creating of false message and forming of black holes. [11]

2) Global Positioning System (GPS) Spoofing: Global positioning system keeps a location table that holds the geographical locations of all vehicles on the network and their identities. An attack can be carried out using the

GPS spoofing through GPS satellite simulator to create a false location on the GPS system in the network, the-reby causing the vehicle to think that the corresponding location is the right one. This is because the GPS satel-lite simulator can generate signals that are way stronger than that generated by the authentic or real satellite. [11]

3) Replay Attack: In this attack, the attacker reinsert packets that have been previously used by nodes into the network, this can poison a node's location table by replaying bacons. Although VANET that operate in the WAVE framework are protected from this attack, but to continue protection a precise source of time should be kept and organized because it is used to keep cache of recently received messages in contrast of the incoming messages. [11]

4) Tunnelling: An attacker utilizes the momentarily loss of a vehicle positioning system when it goes through a tunnel before resurfacing on the other side to receive its positioning information. The attacker quickly injects[11]

## CONCLUSION

VANET is an area of research that holds promising future and for vehicular users. However, it has its own challenges in the security prospect. VANET aims at reducing the accidents on our roads and increasing the flow of information among vehicle and the road users. The unique nature of VANET springs up issues like illegal tracking and jamming of the network. In this paper, we introduced VANET, its architecture, components, communication pattern and issues in its security. we found out the routing protocols used in VANET that enabled road users to communicate and receive messages appropriately In this paper we had seen the various security issues in VANET .We had also discuss the various routing protocol and the effects of various threats under various routing protocol VANET transmission method and also discuss the problems of security in VANET

## REFERENCES

[1] Ho, Yao H., Ai H. Ho, and Kien A. Hua. "Routing protocols for inter-vehicular networks: A comparative study in high-mobility and large obstacle environment "Computer Communication 31, no. 12(2008): 2767-2780.
[2] Kumar, Rakesh, and Mayank Dave. "A review of various vanet data dissemination protocols." International journal of u-and e-Service, Science and Technology 5, no. 3 (2012):27-24.
[3] A .Amditis, E.Bertolazzi, and R.Danielsson ,'A holistic approach to the integration of safety applications' IEEE Trans. Intell. Transp. Syst, vol. 11, no. 3, pp. 554–566,2011.
[4] Dr.M.BalaGanesh,MissD.Radha, J.Dhivya, "Warning Message Dissemination Scheme Using Advanced Traffic Assistance System", International Journal of Advanced Computer Technology (IJACT), Vol.3, ISSN:2319-7900 , pp.26–30.
[5] Sun, S., Kim, J., Jung, Y. and Kim, K. (2009) Zone-Based Greedyperimeter Stateless Routing for VANET. Proceed-ings of International Conference on Information Networking, ICOIN 2009, Chiang Mai, 21-21 January 2009, 1-3.
[6] Yu, D. and Ko, Y.-B. (2009) FFRDV: Fastest-Ferry Routing in DTN-Enabled Vehicular Ad Hoc Networks. Proceed-ings of 11th International Conference on Advanced Communication Technology, **2**, 1410-1414.
[7] Ali, S. and Bilal, S. (2009) An Intelligent Routing Protocol for VANETs in City Environments. Proceedings of 2nd International Conference on Computer, Control and Communication, IC4 2009, Karachi, 17-18 February 2009, 1-5. http://dx.doi.org/10.1109/ic4.2009.4909249
[8] Yang, J. and Fei, Z. (2013) Broadcasting with Prediction and Selective Forwarding in Vehicular Networks. Interna-tional Journal of Distributed Sensor Networks, 2013, Article ID: 309041. http://dx.doi.org/10.1155/2013/309041
[9] Chen, W., Guha, R.K., Taek, J.K., Lee, J. and Hsu, I.Y. (2008) A Survey and Challenges in Routing and Data Disse-mination in Vehicular Ad-Hoc Networks. Proceedings of the IEEE International Conference on Vehicular Electronics and Safety (ICVES '08), Columbus, 22-24 September 2008, 328-333.
[10] Ankita Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh Pandey, Tumpa Roy, "Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper", International Journal of Emerging Technology and Advanced Engineering, Vol.3, ISSN: 2250-2459, 2013, pp. 231-235.
[11] Arif Sari, Onder Onursal, Murat Akkaya, " Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)", Department of Management Information Systems, Vol.8, 2015 , pp. 552-566.
[12] Ganis Zulfa Santoso and Moonsoo Kang, "Performance analysis of the Vehicular Ad hoc Networks (VANET) routing protocols AODV, DSDV and OLSR ",5th International Conference on Information & Communication Technology and Accessibility (ICTA), Dec 2015.