ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Overview of security Attacks in Vehicular Ad-hoc Networks (VANETs)

Rakesh Rani
MCA III Student
Department of Computer Science, Guru Nanak College Budhlada
rakeshrani4488@gmail.com

Abstract: *Vehicular Ad hoc Network (VANET) are the promising approach to provide safety and other beneficial applications to the drivers as well as passengers. It is recognized as an essential component of intelligent transport system. In this paper, we have discussed about some security attacks in vehicular Ad hoc Network. We have also discussed about some solutions that can be implemented against these attacks. Life saving characteristics of VANET has attracted the industry and researchers. In VANET vehicles are nodes so they have no fixed infrastructure. It serves safe and non safe application in wireless medium which makes it venerable to several attacks.*

Keywords: *VANET characteristics*, Overview of attacks, Solutions.

1. INTRODUCTION

Vehicular Ad Hoc Network (VANET) is application of Mobile Ad Hoc Network (MANET). So that every node can move freely within the network coverage and stay connected and each node can communicate with other nodes in single hope or multi hop and every node could be vehicle, Road Side Unit.

The advancement and wide deployment of wireless communication technologies improved human lifestyle by providing the convenience and flexibility in accessing internet services, also providing various types of communication applications for driver and passengers' safety.

Recently, car manufactures and telecommunication companies have been gearing up to equip each car with technology that allows drivers and passengers to communicate with each other as well as with roadside infrastructure that may be located in some critical sections of the road, such as at every traffic light or any intersection or stop sign, in order to improve the driving experience and make driving safer. For example, Microsoft Corp.'s MSN TV and KVH Industries, Inc. have introduced and automotive vehicle internet access system called TrackNet, which can bring internet service to any in-car video screen. It also turns the entire vehicle into an IEEE 802.11-based Wi-fi hotspot so passengers can use their wireless enabled laptops to go online, by using such equipped communication devices, also known as On Board Units(OBUs), vehicles can communicate with each other as well as with Road Side Units(RSUs) located at critical points on the road[1]. A self organized network can be formed by connecting the vehicles and Road Side Units (RSUs), called a Vehicular Ad hoc Networks (VANET) [1].

In VANETs, RSUs can provide assistance in finding facilities such as restaurants and gas stations, and broadcast traffic related messages such as maximum curve turning speed notifications to give drivers a heads up. On the other hand VANETs can enabled vehicles to communicate with each other so that drivers can have better awareness of what is going on in their driving environment and take early action tp respond to an abnormal situation. For achieving this, an OBU regularly broadcasts routine traffic-related messages with information on position, current time, direction, speed, brake status, steering angle, turn signal, acceleration/deceleration, traffic conditions, and traffic events[1].

Security is the most important concern in VANET due to open access medium, there are different attacks can occur at any time. Different attacks with solutions are presented in this paper , also conclude these different attacks and solutions.

Emergency messages can be generated and sent by OBUs in case of emergent breaking, traffic jam or any accident. For example fig. 1 shows whenever there is a accident on highway, several lanes can be blocked, drivers can experience long delay. If drivers informed in advance about the situation so that drivers can follow the detour route or change the lanes to avoid the traffic jam. Standard 802.11p is a communication technology that provide short range communication with low latency. 802.11 support wireless communications among vehicles for the roadside infrastructure.

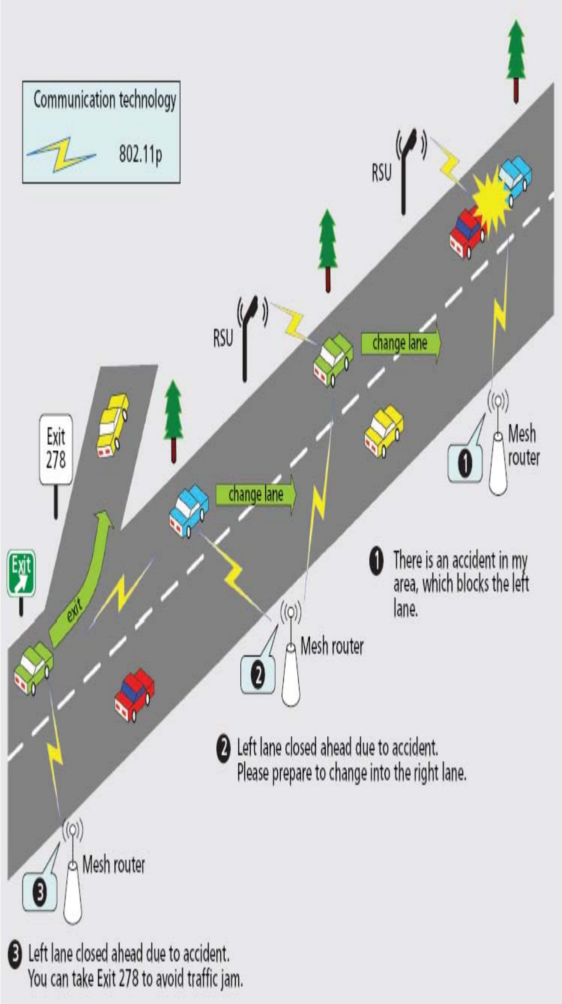

Communication technology
802.11p
RSU
RSU
change lane
change lane
Exit
278
Exit
exit
Mesh router
Mesh router
Mesh router
1
2
3
1 There is an accident in my area, which blocks the left lane.
2 Left lane closed ahead due to accident. Please prepare to change into the right lane.
3 Left lane closed ahead due to accident. You can take Exit 278 to avoid traffic jam.

Figure 1. *An example of road emergency response operation under VANET.[1].*

2. VANET CHARACTERISTICS

Vehicular Ad hoc Network (VANET) is an application of Mobile Ad hoc Network (MANET) but it has its own different characteristics, we summarized as :

A. High Mobility:

The nodes in VANET usually are moving at high speed. This make harder to predict a node's position and making protection of node privacy [2].

B. Rapidly changing network topology :

Due to high node mobility and random speed of vehicles, the position of node change frequently.

C. Unbounded network size:

Unbounded network size means that network size in VANET is geographically unbounded, can be implemented for one city, several cities or for countries.

D. *Frequent exchange of information:*

The ad hoc nature of VANET aims the nodes to gather information from other vehicles and Road Side Units (RSUs)so that the exchange of information becomes more frequent.

E. *Wireless communication:*

Vehicular Ad hoc Network is designed for wireless. Nodes are connected and exchange their information via wireless [2].

F. *Time critical:*

The information in VANET must be delivered to the nodes within time limit so that the decision can be made by the node and perform action accordingly[2].

G. *Sufficient Energy:*

The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power [2].

3. OVERVIEW OF SECURITY ATTACKS IN VANET

Attacks on VANET can be categorized into three groups : those that pose a thret to availability, those that pose a threat to authenticity those that pose a threat to driver confidentiality and miscellaneous.

Threats to availability

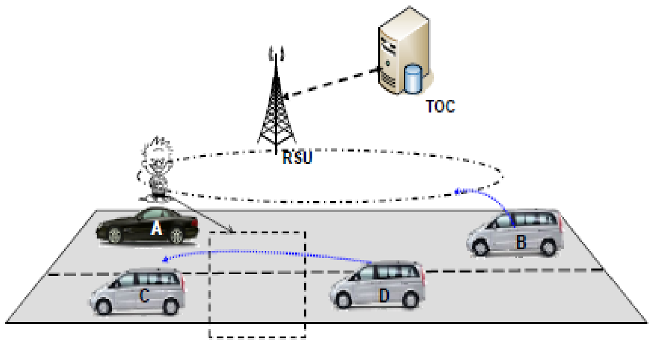
As any other communication network, availability in VANETs should be assured both in the communication channel and in participating nodes. A classification of these attacks, according to their target, is as follows:

Denial of service (DOS) attack

In DOS the main objective is to prevent the legitimate user from accessing the network services and from network resources. This attack can occur by jamming the channel system so that no authentic vehicle can access it [3]. It is the most serious problem in vehicular ad hoc network the user cannot communicate in network and pass information to other vehicle which could result in more devastation in life critical application.

There are different ways through attacker can achieve it

a. In basic level the attacker overwhelm the node resource so that it cannot perform other necessary tasks which results in becoming the node continuously busy and not able to do anything else. In extended level the attacker jam the channel by generating the high frequency in the channel so no vehicle is able to communicate to other vehicle in the network. Drop the packets[3].



. **fig. 1-** DOS Attacks between V2V and V2I [3].

Distributed DOS (DDOS) attack

DDOS is distributed in nature, complicated than DOS. In this attacker uses different location to launch the attack, user may different time slot for sending the message. The time slot and the nature of the message may be different varied from vehicle to vehicle of the attackers.

There are two chances of DDOS attackers are:

1. vehicle to vehicle

2. vehicle to infrastructure(RSU)

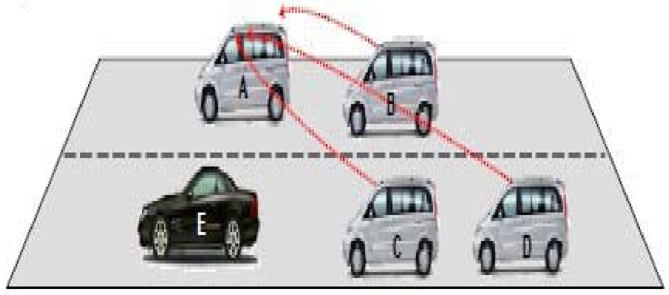


fig. 2- DDOS in vehicle to vehicle communication[3]

Spamming

Attackers send the spam messages to consume the bandwidth of network and to increase the transmission latency. Due to lack of necessary infrastructure and centralized administration, it is difficult to control. In this attacker send the spam message to the group of users[3].

Message suppression attacks

An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points. For instance, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive the warning and forced to wait in the traffic [4].

Alteration Attack

This attack happens when attacker alters an existing data, it includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted .
For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested[4] .

Replay Attack

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending [4].

Threats to Authentication

There are two main attacks related to identification and authentication:

Sybil attack

The Sybil attacker uses different identification at the same time and transmit multiple messages. It is critical attack. So the vehicle feels that these messages are coming from different vehicles, so there is a jam further and they are enforced to take alternative way.

Prankster

Include bored people probing for vulnerabilities and hackers seeking to reach fame via their damage [4].

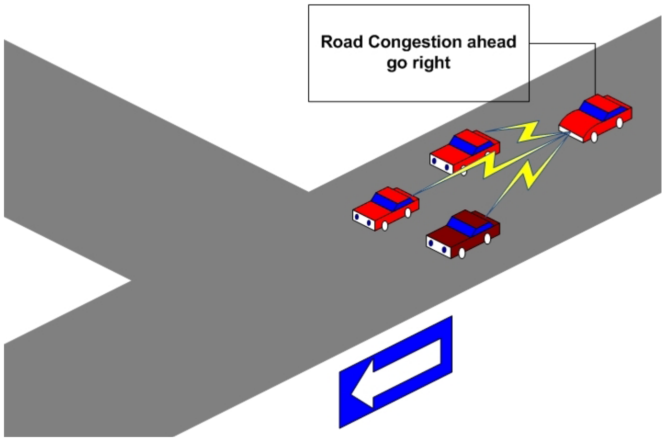


Fig. 4 Selfish Driver [4]

For example the prankster convence one vehicle to slow down, and tell the vehicle behind it to increase the speed.

4. SOLUTIONS FOR DIFFERENT ATTACKS

There are different solution are available to mitigate these attacks. Different solutions are as follow:

ARAN (Authenticated Routing for Ad hoc network) is based on authentication. ARAN uses the public key cryptography and requires a certificate server whose public key is known to all nodes. It uses timestamp for the freshness of the route. A source node broadcasts the route discovery packet (RDP) to all its neighbors for route discovery. Each node keeps the record of its neighbor from which it receives the message. After receiving the message all the neighbor again forwards this message to their neighbors with their sign and own certificate. When the message received by the destination, it replies to the first node from which it received the message. No intermediate node can reply the RDP other then destination even if that intermediate node knows the path of destination[5].

SMT (Secure Message Transmission) P. Papadimitratos et al proposed Secure Message Transmission protocol which is light weight and operates on end to end manner. It requires a security association between source and destination. It does not use the cryptographic operation for intermediate nodes [5].

DOS attack solution is based on the use of OBU (On Board Unit) that is installed in vehicles. In case of DOS attack the processing unit will suggest to the OBU to switch channel, technology, or to use frequency hopping technique or multiple transceiver [3].

To resolve forging attack and Sybil attacks, Yan et al. [3] proposed a novel solution that uses on-board radar as the virtual ‘eye’ of a vehicle. Although the ‘eyesight’ is limited because a modest radar transmission range, a vehicle can see surrounding vehicles and receive reports of their GPS coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicles

To prevent replay attacks in vehicular networks[3] there can be two options: The first option is using a globally synchronized time for all nodes and other is using nonce (Timestamp).

One proposed solution to mitigate this attack is to verify the received data in correlation with the data received from other sources. The important issue in this context is the correctness of the received data rather than its source [3].

5. CONCLUSION

Every user want safety and security on the road in future it may be possible by implementing safe and secure vehicular Ad hoc Network (VANET) applications which is useful technology. In this paper already discussed about different attacks and their solutions also. In our future work we will propose new solutions that will help to maintain a securer VANET network, and test it by simulation.

REFERENCES

[1] Xiaodong Lin,Rongxing Lu, Chenxizhang, Haojin Zhu, Pin-Han and Xuemin (Sherman) Shen, “Security in Vehicular Ad Hoc Networks”,IEEE communication magazine,April 2008, pp. 88-89.

[2] Ram Shringer Raw, Manish Kumar, Nanhay Singh,”SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET”, Ambedkar institute of Advanced Communication Technology &Research Delhi, India. pp.97.

[3] AJAY RAWAT, SANTOSH SHARMA, RAMA SUSHIL,” VANET: Security Attacks And Its Possible Solutions”, Jurnal of Information and Operationa Management.Bioinfo Publications.

[4] Ghassan Samara, Waffa A.H. AI-Salihy R.Sures, “Security Analysis Of Vehicular Ad Hoc Network (VANET)”, 2010 second International Conference On Network Applications, Protocols and services.

[5] Ram Shringer Raw, Manish Kumar, Nanhay Singh,”SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET”, Ambedkar institute of Advanced Communication Technology &Research Delhi, India. pp.101-104.