An Analytical Study of MITM Attack in VANETs

Saeid Alizadeh Bahrami
Saeid.Alizadeeh@GMail.Com
Islamic Azad University Malard Branch
Ramin Karimi
Rakarimi1@GMail.Com
Islamic Azad University Malard Branch
Pejman Abdolahifard
Islamic Azad University Malard Branch
P.fard@yahoo.com

Abstarct

Vechiular ad-hoc network (VANET) is developing advanced technology to achieve progress in the transport industry and road safety.VANET using a wireless technology to connect to the server to get the necessary information for all activites and this connection provides a way for some of the attacks in wireless network. Wireless networks are vulnerable because of the use of wireless communication, multiple attacks on these networks is to implement some of these attacks using routing topology , malicious nod , Denial of Service (DoS) and MITM Attack (Man in the Middle).

Keywords: Vehicular ad-hoc network (VANET), Intelligent transportation system (ITS) , Security Attack , MITM Attack

Introduction

Needs and new technologies and road safety and to benefit from the new technologies and the Internet together have created a structure Now called Ad-hoc networks (VANET).this special category of wireless networks We have overcome many of the needs of today and tomorrow.

The inter-vehicle network that satisfies the needs of such warning accident, the traffic, the weather, road facilities, restaurants, resorts, recreation centers and Internet services, pay toll events, recreation is.

Today U.S Federal Comunication Commision Called FCC allocated 75 megahertz of spectrum for intelligent transportation services to improve highway safety and efficiency as part of the U.S. Department of Transportation's "Intelligent Transportation Systems" (ITS) national program.fCC decided to use the 5.850-5.925 GHz band for a variety of Dedicated Short Range Communications (DSRC) uses, such as traffic light control, traffic monitoring, travelers' alerts, automatic toll collection, traffic congestion detection, emergency vehicle signal preemption of traffic lights, and electronic inspection of moving trucks through data transmissions with roadside inspectionfacilities(FCC, 1999).

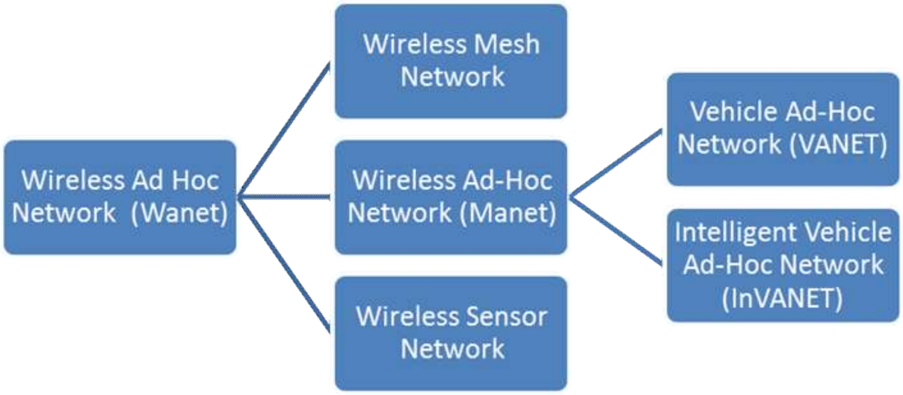
Wireless Ad Hoc Network (Wanet)
Wireless Mesh Network
Wireless Ad-Hoc Network (Manet)
Wireless Sensor Network
Vehicle Ad-Hoc Network (VANET)
Intelligent Vehicle Ad-Hoc Network (InVANET)

Fig 1. Hierarchy of wireless ad hoc networks

In VANETs Communication in Two Type: I.RoadSide Units (RSUs) AND II.OnBoard Unit (OBU)

I. Transceiver that is located along the road the above
II. Receiver and transmitter (vehicle) that is used for communication between vehicles

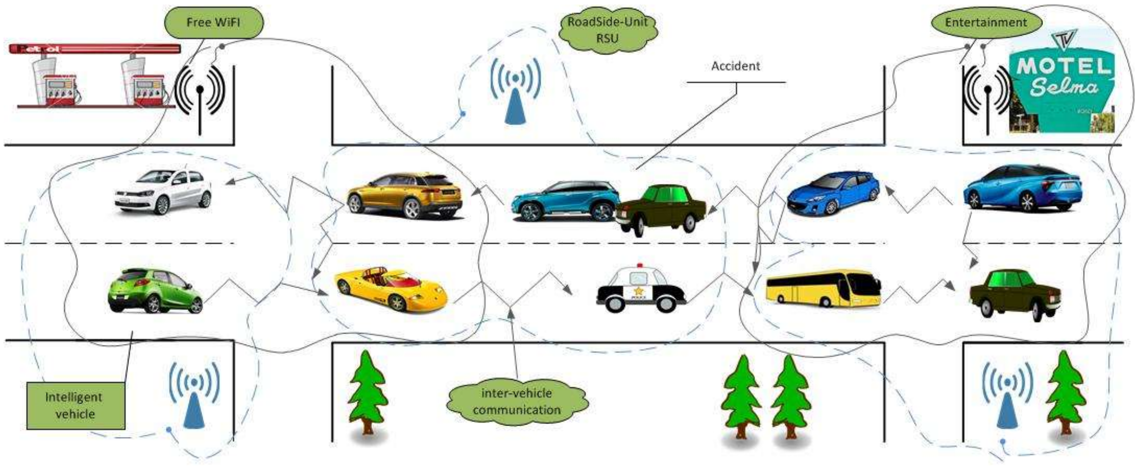

Fig 2.A basic structure of VANETs

Fig2. an overview of the vent network And Vehicle-to-vehicle communication with the roadside -Unit private and public networks and the Internet for advertising and entertainment.Because the vent speed networks, nodes are constantly in motion. Node transferred from one group to another or from a Vehicle may be associated with a group.Man In The Middle (Mitm) a Security attack with High Risk Degree in this attack (Kim& Lee, 2014).

In these attacks, an attacker using hardware and software, start listening on the network and after collect any data can Put yourself in the middle of a connection to host and clinet .After being in the middle attacker can connect to the host referred to the victim and the victim's personal information wing and Can also host as the client receives.
Attacks can be divided into several categories, each with its own dangerous.

Security CHARACTERISTICS

Many security component used to secure the VANET but the attacks on some of these components will attack(Kim& Lee, 2014).

- Authentication

  inThe VANET the transceiver network authentication is one of the most important factors of security check. (Kim& Lee, 2014).
- Confidentiality

  Privacy is one of the main components of the VANET network.for this use the encrypted data and Symmetric-key algorithms. (Kim& Lee, 2014).
- Integrity

  All messages to prevent fraud and protect the corrosion between the host and client To ensure the reliability of the content of messages. (Kim& Lee, 2014).
- Non-repudiation

  Identify the attacker after the attack was carried out to prevent the next attack. (Kim& Lee, 2014).
- Availability

  create network to allow authorized user to work even in network under attack. (Kim& Lee, 2014).
- Accsess Contorl

  Mechanisms to allow access to any of the resources on the network This mechanism makes it possible to each user request permission to use any resource. (Kim& Lee, 2014).
- Mac-Address sketching

  MAC is used to communicate on the network and can not be forged unique design and one of them.The standards can be referred to the standard CSMA. Adopted by the IEEE organization for these networks (Sumra et al,2011).

Attack in VANETs

The attacks are classified into several groups , Depending on the extent of damage and the degree of threat and risk and overall category.

- **Overall Category**

Attack classified in Tow Category

- Active Attack

  The Attack Started as soon as symptoms develop specific & Exposure

  In Active Attack , attacker can be make new packet and send to Victim

- Passive Attack

  Attack not show Signs and symptoms that are specific

  In Passive Attack , passive attackers active only eavesdrop the wireless carrier but cannot make new packets (La Vinh,& Cavalli,2014).

- **Malicious Vs Rational**

  Aggressive methods to destroy and damage in the attacks, and the benefits it gets On the adverse, a realistic attacker predicts
  personal assistance from the invasion. Thus, these attacks are
  more certain and follow some arrangements (La Vinh,& Cavalli,2014) (Raw et al ,2014).

- **Level of Damage**

  Assess the damage to the resource and disclosure of personal information

- **Degree of Threat**

  Depending on the type of attack, the damage was done , Down Time and the time required to detect attacks.

- **Insider Attacker**

  An attacker who is within your network as a node can communicate with other nodes of the network.

- **Outsider Attacker**

  Network members were not aggressive and can not directly communicate with other network members.Mitam Attack with a high degree of threat, and the irreparable damage to both the active and passive attacks based on the type.

- **Coverage zone**

  The area covered by one of the factors that according to their attack into the attacker finds,Striker according to the type of attack that is sometimes referred to as non-covered areas are attacked and sometimes covered the RSU transmitter (Tyagi & Dembla ,2014)

Description of Attack

The man in the middle attack, attack in which an attacker between the main connection between the host and the client and Causing the attacker to impersonate the client as the default host to send information to an attacker , The attacker to forge customer information it communicates with connect to the host.

The MITM consists of several different types of attacks

- **interception**
  - When the attacker can listen to the information exchanged between the client and the host With this aggressive action to collect messages exchanged and can Decrypt from the code to find out information
- **Modification**
  - When the data between the client and the host to be manipulated by an attacker in any way With this operation, attacker can change messages with

your own customer information such as key, to obtain banking information, etc.

- **Fabrication**
    - When an attacker is able to produce bogus messages to the host impose

      It was hard because I have to be able to introduce a client to server or vice versa but can gain important information

- **Interruption**
    - If the attacker can disable the system or service during the attack

      Note: In the first stage, professional Attacker Down Main server from the client side, they are will be drawn

ARP Cache Poisoning Is another type of MITM Attacks , According to VANET networking protocols TCP under surveillance network can be used to attack , Arp mechanism can be used to update the cache with arbitrary values can be updated by the weakness of the listen to the network.

Mitm In RSU(Road Side Unit)

In this attack, the attacker in the last long wave transmitter placed alongside the road and communicates with the main transmitter and the other side was strengthened and sends waves , Vehicles that are fooled into attacking waves, with the original sender communicate and to start the exchange of information.

Here waves aggressive acts like an amplifier with the exception that instead of connected nodes are connected to the original sender of the aggressive and invasive, which is linked to roadside transmitters.All information exchanged between the node and the sender is saved by the attacker, listen, manipulate and decrypt is.

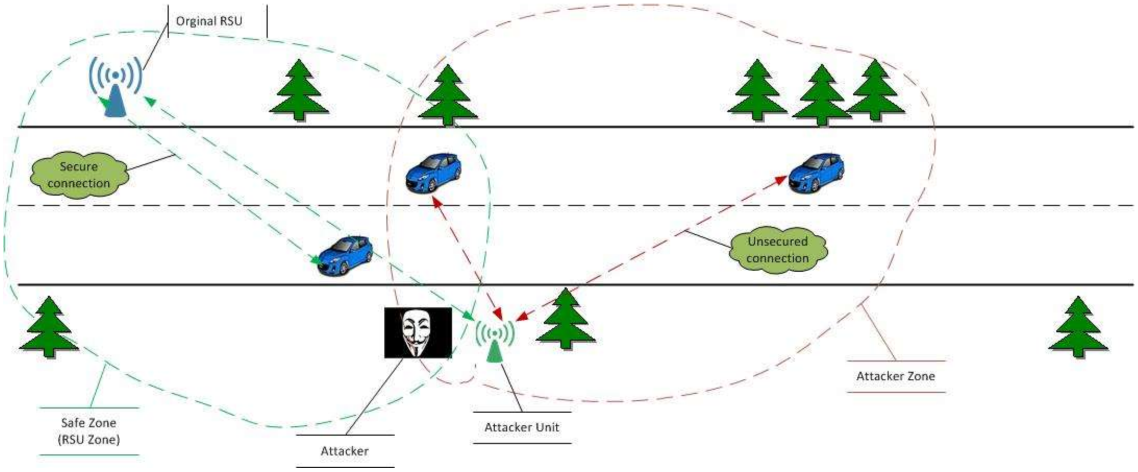

Fig 3.RSU Mitm Attack

Fig 3.Mitm RSU scenario The first car entered the attacker Zone limited and as long as they are within range of aggressive waves linked with the network and then enter the RSU Zone.

Mitm Attack In OnBoard Unit (OBU)

In this attack, the attacker is a node within the network between other nodes on the move and share information with other nodes. Malicious Node start listening connection between two other Node, and can save their data, recovery, and in some cases even change(La Vinh,& Cavalli,2014).

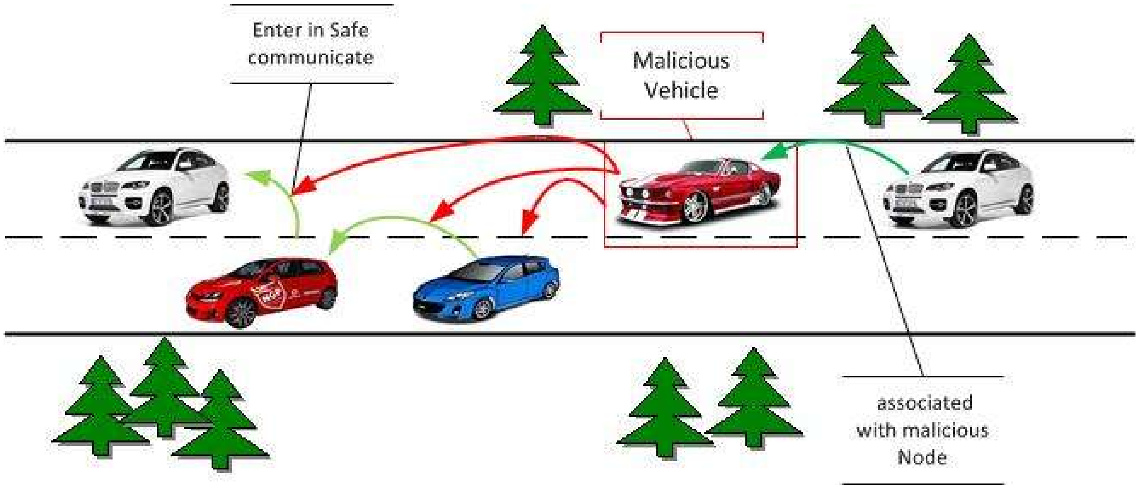

Fig 4.Obu Mitm Attack

Fig 4 Sees the that malicious Node can communicate between two other Node in and start listening, and even change the data Node healthy and malicious due to ignorance of the Node begin to communicate with them.

Risks and Possible Damage

The VANET Network according to user needs a variety of exchanging information. This information can include: weather information, highway patrol, traffic & accident, entertainment And internet, buy and recharge the account.
It makes extensive information exchange on a wide attacker can access all your data. Even with the development of technology and the rise of intelligent vehicles without drivers, the attacker can take control of your car.The attack resulted in several Harm and damages that may reduce the amount of loss can be very dangerous and is sometimes true reflection.

- Heavy damage
  - Damage that occurs during the attack and is very dangerous, it can cause damage, chain accident, very heavy traffic and long, steal credit card information
- Light damage
  - Not very heavy losses that can be as simple as they passed Damage as the definitive online entertainment network outages, lack of weather information.

Discussion

To protect the security of information and to avoid possible risks of this solution can be used. Other solutions can be used for these attacks will be mentioned in future articles. Here are two solutions will be introduced to protect them. The first scenario is based on the model of the relationship and the key is to use the algorithm Bloom, The second scenario is based on an algorithm that is robust encryption to prevent this scenario is to break the encryption algorithm used Diffie–Hellman Cryptography .

Secure Communication By Using Bloom Filter

A good solution is reasonable to block the OBU& RSU Attacks. In this model, all Vehicles are already pre-registration with a TA (Trusted Authority) befor join to the network In this proposal, all vehicles must be a hardware device called TRH (Tamper-Resistant Hardware) before related by OBU truly equipped to be surveyed , All vehicles through OBU synchronized with the time .After the operation, there is the assumption that vehicles can enter the network and is reliable RSU (Fig 5)(Raya & Hubaux ,2007).

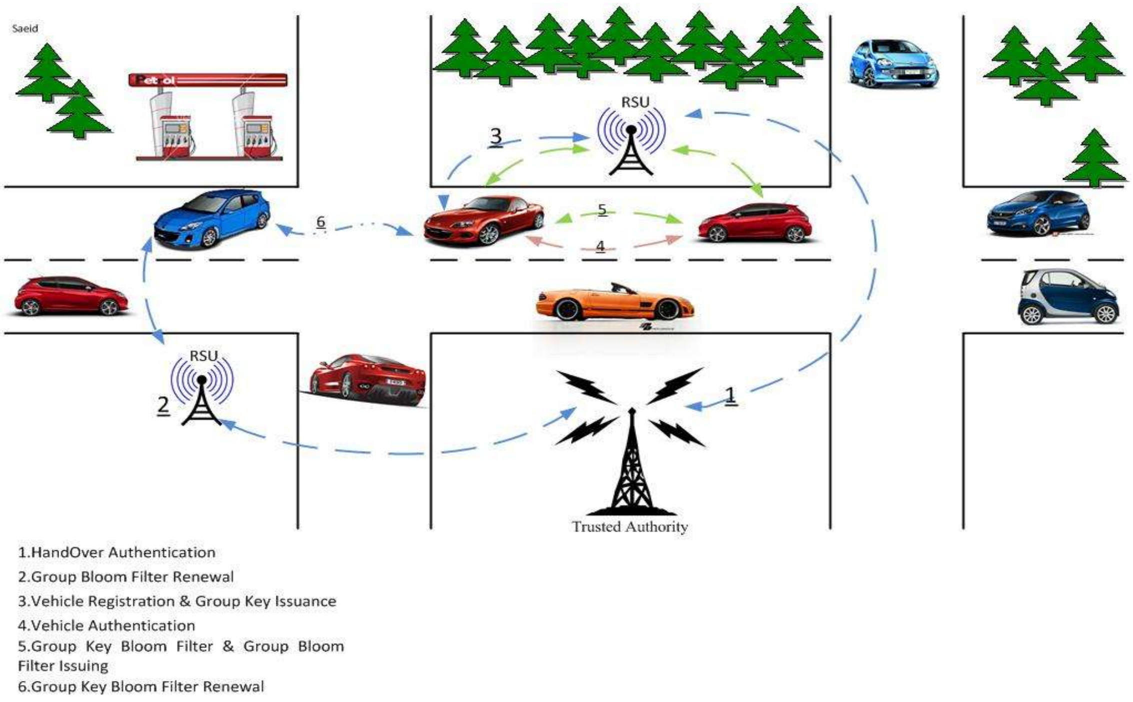
Saeid
Petrol
RSU
3
6
5
4
RSU
2
1
Trusted Authority
1.HandOver Authentication
2.Group Bloom Filter Renewal
3.Vehicle Registration & Group Key Issuance
4.Vehicle Authentication
5.Group Key Bloom Filter & Group Bloom Filter Issuing
6.Group Key Bloom Filter Renewal

Fig 5. Secure V2V Communication By Using Bloom Filter

Summary

Table1 VANETs a summary of several attacks, including attacks on networks, the degree of risk, In addition, a brief analysis of the attacks and proposed solutions for the disposal of these attacks is.

Table 1

Attack	Inside Or Out Side	Communication	Type of Attack	degree of risk	solution
Mitm	I,O	V2V & V2I	A,P,M,R,L,E	High	Protocol By Bloom OR Diffie–Hellman Cryptography
Sybil	I	V2V & V2I	A,M,R,L,E	High	Approach based on Movement Patterns OR Approach based on Neighboring nodes
Dos & dDos	I,O	V2V & V2I	A,M,L	Medium	Pre authentication Approach OR BFICR Approach OR APDA
illusion	I	V2V & V2I	A,R,L	Medium	PVN Approach
Black Hole	I	V2V	A,M,L	Low	DPRAODV Protocol OR BAMBi Approach OR Modified AODV Protocol
Worm Hole	I	V2V	A,M,E	High	HEAP Approach OR Plausibility Check Approach OR WHOP Protocol
Sink Hole	I	V2V	A,M,L	Low	LQI based Approach Or IDS Model

I:Inside Attack , O:Outside Attack , A:Active , P:Passive ,M: Malicious ,R:Rational,L:Local, E: Extended (La Vinh,& Cavalli,2014) (Sirola, et al 2004)(Zhang & Lee,2005)

Reference

F.C. (1999). Commission, F.C., FCC Allocates Spectrum in 5.9 GHz Range for Intelligent Transportation Systems Uses. Report No. ET. (p. 99-5.), p. 99-95.

Kim, S.-H., & Lee, I.-Y. (2014). A secure and efficient vehicle-to-vehicle communication scheme using bloom filter in vanets. *International Journal of Security & Its Applications, 8*(2).

La Vinh, H., & Cavalli, A. R. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey. *International journal on AdHoc networking systems (IJANS), 4*(2), 1-20.

Raw, R. S., Kumar, M., & Singh, N. (2013). Security challenges, issues and their solutions for VANET. *International Journal of Network Security & Its Applications, 5*(5), 95.

Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39-68.

Sirola, P., Joshi, A., & Purohit, K. C (2004). An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs). *International Journal of Computer Science Engineering (IJCSE), 3*(04).

Sumra, I. A., Ahmad, I., Hasbullah, H., & Manan, J.-l. B. A. (2011). *Classes of attacks in VANET.* Paper presented at the Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International.

Tyagi, P., & Dembla, D. (2014). A Taxonomy of Security Attacks and Issues in Vehicular Ad-Hoc Networks (VANETs). *International Journal of Computer Applications, 91*(7).

Zhang, Y., & Lee, W. (2005). Security in Mobile Ad-hoc networks *Ad hoc networks* (pp. 249-268): Springer.