Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-301-304
Available online at http://www.bioinfo.in/contents.php?id=55

VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS

AJAY RAWAT[1*], SANTOSH SHARMA[2], RAMA SUSHIL[3]

[1]Department of Computer Application, University of Petroleum & Energy Studies, Dehradun, India.
[2]Department of Computer Application, GEU, Dehradun, India.
[3]Department of Computer Application, Shri Guru Ram Rai Institute of Tech. & Science, Dehradun, India.
*Corresponding Author: Email– [1]rawat.ajay@hotmail.com, [2]Santosh.sharma.ddn@gmail.com, [3]ramasushil@yahoo.co.in

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- Vehicular Ad hoc NETwork (VANET) is an emerging paradigm in networking. It is a new form of Mobile Ad hoc NETwork (MANET). Its life saving characteristic has attracted the industry and researchers. In VANET vehicles are the nodes with mobility so does not have fixed infrastructure It serves safe and non safe applications in a wireless medium which makes it vulnerable to several attacks. Security is the most important concern in VANET due to open access medium. In this paper we present the comprehensive study of possible attacks and their possible solutions.
Keywords- VANET, Security, Attacks

Citation: Ajay Rawat, Santosh Sharma, Rama Sushil (2012) VANET: Security Attacks and Its Possible Solutions. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-301-304.

Introduction

Today's transportation system plays an important role in our daily lives. From last few years a new transportation system that has fascinated a lot of attention from both industry and academia is VANETs. It is a new type of network which is expected to support a large spectrum of mobile distributed applications applied on vehicles [1]. VANET is a subset of MANET. In VANET each node is a vehicle or RSU (Road Side Unit) which can move freely within the network range and stay connected. Every node communicates with other nodes in single hop or multi hop. VANET provides safe and non safe services to the drivers. VANET constitutes short-range radios installed in vehicles, Road Side Units (RSUs) and central authorities which are responsible for identity registration and management. Communication in VANET is Vehicle to Vehicle (V-V) and Vehicle to Infrastructure (V-I). However, it is critical for VANET to guard against misuse activities, the overall organization for VANET security architecture must be carefully designed especially when it is a worldwide implemented VANET. The security of VANETs is one of the most critical issues because their information transmission is propagated in open access (wireless) environments. It is necessary that all transmitted data should not be injected or changed by users who have malicious goals. This paper is divided into four sections; Section II describes the possible attacks in VANET on the basis of [17]. Section III describes the possible solution to some of the attacks in the VANET. Section IV concludes the paper.

Possible Attacks

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

Threats to Availability

1. 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. DOS attack can occur by jamming the channel system so that no au-

thentic vehicle can access it [2]. In VANET it is most serious problem as the user cannot communicate in the network and pass information to other vehicle which could result in more devastation in life critical application. Three 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.
b. 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.
c. Drop the packets.

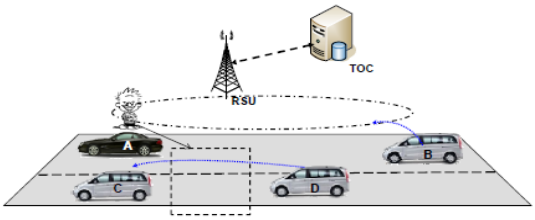

fig. 1- DOS Attacks between V2V and V2I

2. Distributed DOS (DDOS) attack

DDOS attack is more severe than DOS attack as it is distributed in manner. In this attacker uses different location to launch the attack. They may user 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. The main objective is to down the network so the network will not be available to the uses [2]. The two possibilities of DDOS attacks are:

a. Vehicle to vehicle
b. Vehicle to infrastructure (RSU)

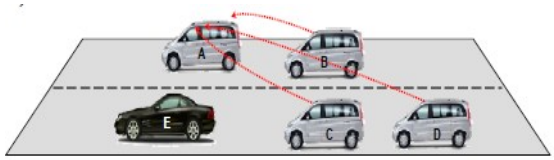

fig. 2- DDOS in vehicle to vehicle communication

3. Spamming

To consume the bandwidth of network and to increase the transmission latency attacker sends spam messages in the network. It is difficult to control this kind of due to lack of necessary infrastructure and centralized administration. In this attacker disseminate spam messages to a group of users [3]. Those messages are of no concern to the user just like advertisement messages.

4. Black Hole

In this problem a node refuses to participate in the network or when an established node drops out to form a black hole. In this all the traffic of the network get redirected towards a specific node which is actually doesn't exists which results in data lost. The malicious code chooses whether to drop a packet to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.

5. Malware

Malware attacks are just like viruses as viruses in VANETs which hamper the normal operation of the network. VANET get infected by these attacks normally when there is software updates in VANET units or RSU [1]. In this attackers are normally malicious insider rather than outsider.

Threats to Authentication

1. Sybil attack

It is a critical attack. In this type of attack an attacker transmits multiple messages with different ids to the other vehicles. In this way other vehicles feels that these messages are coming from different vehicles, so there is a jam further and they are enforced to take alternate route [5]. In other words we can say that the main task of the attacker is to provide an illusion of multiple vehicles to other vehicles and to enforce them to choose alternate route and leave the rod for the benefits of the attacker. This task is done by sending multiple messages with different ids.

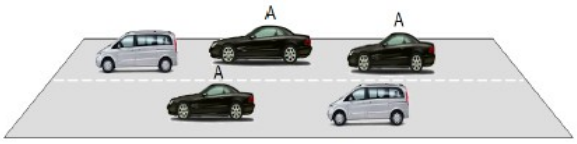

fig. 3- Sybil Attack

2. Node Impersonation attack

In VANET each vehicle has a unique id and with the help of these ids each vehicle is identified in the VANET network. It becomes most important when an accident happens. In node impersonation attack an attacker can changes his/her identity and acts like a real originator of the message. An attacker receives the message from the originator of the message and changes the contents of the message for his/her benefits. After that an attacker sends this message to the other vehicles [2].

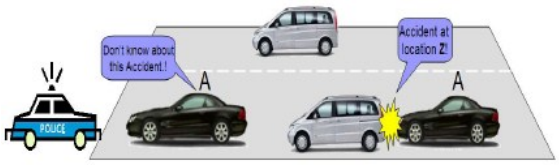

fig. 4- Node Impersonation Attack

3. Message suppression

In this attacker can selectively drop packets from the network which may contain critical information for the receiver [6]. For example an attacker might remove the congestion alerts it receives in order to prevent the nodes to select an alternative path to destination and force them to wait in traffic. The attacker may use these packets again later to get the benefits. The main objective of the attacker would be to prevent the authorities and RSU to know about the collision.

Alteration

As the name suggests this attack means alter or modify the existing data. This attack can occur by delaying the message transmission deliberately, replaying previous transmitted message or altering the particular part of the message [7]. For example attacker obtains the data that congestion is normal in the road but manipulate it and deceitfully indicating a heavily congested highway.

5. Replay

This attack is basically used by authorized or malicious user to masquerade as a legitimate user or RSU. As the name depict this attack is basically happen when attacker replay the transmission of previously generated frames in new connections. Attacker captures a generated frame and use it other parts of the networks [6]. Currently we don't have any protection against replay as it does not contain timestamp or sequence no. The main objective of this attack is to mystify the authorities and prevent identification of vehicle in any accident.

6. GPS spoofing

To maintain the identity and geographic location of all vehicles on the network location table is maintained in GPS satellite. The attacker uses a GPS satellite simulator to generate signals that are more effective than original GPS satellite [1]. The attacker produces bogus GPS reading through simulator to fool vehicles to think that they are in different location.

7. Tunneling

The attacker connects two distant parts of the Ad hoc 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 [8]. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack.

Threats to Confidentiality

Confidentiality of messages exchanged between the nodes of a vehicular network are particularly vulnerable with techniques such as the illegitimate collection of messages through eavesdropping and the gathering of location information available through the transmission of broadcast messages[17]. In the case of eavesdropping, insider and/or outsider attackers can collect information about road users without their knowledge 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. Location privacy involves protecting users by obscuring the user's exact location in space and time. By concealing a user's request so that it is indistinguishable from other users' requests, a degree of anonymity can be achieved.

Miscellaneous threats

1. Timing Attack

Time is a crucial aspect in any application so users need accurate information on right time without any delay. Time is also an important issue in ITS safety applications. In this attack attacker without manipulating the actual content add some time slot to create a delay in the message due to this user will receive the message after the required time [9]. ITS safety applications are time critical application which requires data transmission on time otherwise major accidents can happen. Figure with explanation

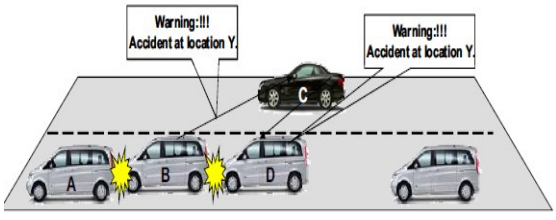

fig. 5- Timing Attack

2. Home attack

Internet is the key component of the VANET. In this attacker take control of the user vehicle by connecting with internet. The three different approaches the attacker can use for home attack [3].

a. In this attacker take over the control of software (AU or OBU) of the user vehicle. Then he can generate some wrong message to the network.
b. In this attacker take over the control of sensor of the user vehicle. Then he can change the behavior of the sensor according to his need.
c. In this attacker take over the control of hardware (ECU) of the user vehicle. Then he can change increase or decrease the speed of the vehicle.

3. Man in the middle attack

As the name suggests the attacker sit in the middle of the two communicating vehicle and launch this attack. In this attacker control all the communication between the sender and the receiver but communicating vehicles assume they are directly communicating with each other [3]. In MiMA attacker listen the communication between the vehicles and inject false or modified message between the vehicles.

4. Traffic analysis

This attack considered to be a serious level threat against the privacy of user in VANET. In this attacker do analyses on the traffic packet between the V2V or V2RSU [10]. Attacker uses the packet which contains location of Vehicle ID, traveling path of the vehicle which may be useful to extract the required information for its own purpose.

5. Social attack

The basic idea of the attack is to confuse and bedazzle the victim by sending unethical and unmoral message so that driver gets disturb. The legitimate user reacts in annoyed manner after getting such kind of messages which is the main objective of the attacker [9]. It effects the driving of the vehicle which indirectly creates the problem in the network.

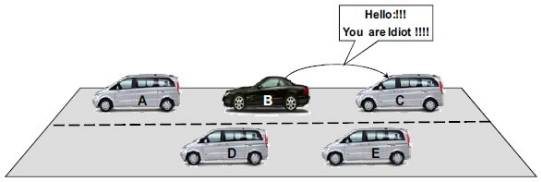

fig. 6- Social Attack

6. Brute force

Safety related information is critical in VANET. For secure VANET appropriate application of cryptographic algorithms and approaches are widely used to protect against the threat. The attacker can use brute force technique to break the cryptography key [10].

7. ID Disclosure

It is a passive attack. In this attacker send the malicious code to the neighbors of the target node and collects the required data. They take the ID of the target node and its current location. Due to this target vehicle's ID will be disclose and they lose their privacy [1]. In this global observer can access their data by monitoring the route of the target vehicle. For this purpose attacker can use the RSU (Road Side Unit). E.g. rental companies use this approach to keep track on their vehicle movement.

8. Bogus information

In this attack, the attacker can be outsider/intruder or insider/ legitimate user. The attacker broadcast false information in the vehicular network to affect the decisions of other vehicles by spreading the false information in the network [11]. For example a vehicle can imitate a heavy traffic on one road to preventing the other vehicle to choose that road. This attack is an example of Application attack.

Solutions For Different Attacks

Following are the proposed solutions to some of the attacks discussed above:

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 [2].

Brute force attack solution is proposed by Langley et al. [12]. In this a secure authentication method which requires use of some unique identification for vehicles concatenated with some large random value and then hashed using some hash algorithm

To deal with traffic analysis attack Cencioni et al. [13] proposed VIPER: a vehicle-to infrastructure communication privacy enforcement protocol. It is resilient to traffic analysis attacks. In this vehicle will send their messages directly to RSU but to have vehicle acting as mix nodes.

To resolve forging attack and Sybil attacks, Yan et al. [15] 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[16] 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 [14].

Conclusion and Future Work

Users want safety and security on the road in future and it may be possible by implementing secure and safe VANET applications which is a rising technology. This technology is a rich area for attackers who try to change the contents of the safe and non safe applications to misguide the users of the network with their malicious attacks. In this paper we present some possible attacks and their solutions. In future we intend to develop the system for detecting the critical attacks and verifying it through simulation by applying our novel idea on the procedure to protect the safe messages.

References

[1] Farzad Sabahi (2011) *Third International Conference on Computational Intelligence, Communication Systems and Networks.*

[2] I. Ahmed Soomro, Hasbullah H.B., J.lb. Ab Manan (2010) *WASET* issue 65, ISSN 2070-3724.

[3] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan (2011) *ICUMT* : 1-8.

[4] Akanksha Saini H.K. (2010) presented at the *National Conference on Computational Instrumentation*.

[5] Douceur J. (2002) *First international workshop on peer to peer (P2P) system*, pp:251-260.

[6] Samara et al (2010) 4*th International Conference on New Trends in Information Science and Service Science*.

[7] Parno B. and Perrig A. (2005) *HotNets-IV, College Park, MD*.

[8] Akanksha Saini H.K. (2010) *National Conference on Computational Instrumentation*.

[9] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah Jamalul-lail bin Ab Manan (2011) *Saudi International Electronics, Communications and Photonics Conference.*

[10] Isaac J.T., Zeadally S., Camara J.S. (2010) *IET communication* vol. 4,Iss 7, pp.894-903.

[11] Raya M. and Hubaux J. (2005) presented at the 3rd *ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria.

[12] LANGLEY C., LUCAS R., FU H. (2008) *IEEE Int. Conf. on Electro/Information Technology*, pp. 223–226.

[13] CENCIONI P., DI PIETRO R. (2008) *Comput. Commun* (12), pp. 2790–2802.

[14] Raya M. and Hubaux J.P. (2005) 3*rd ACM workshop on Security of ad hoc and sensor networks*.

[15] YAN G., OLARIU S., WEIGLE M. (2008) *Comput. Commun* (12), pp. 2883–2897.

[16] Dotzer F., Kohlmayer F., Kosch T., Strassberger M. (2005) 2*nd International Workshop on Intelligent Transportation, Hamburg, Germany.*

[17] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan (2012) *Telecommunication System*, Vol. 51, Issue 2&3.