International Journal of Computer & Information Technologies (IJOCIT)
www.ijocit.ir & www.ijocit.org
ISSN = 2345-3877

Various Types of Attacks in VANETs

Yasser Safinejhad[1], Mehran Abdali [*2]
Department of Software Engineering, Azad University, Baft Branch, Kerman [1,2]
Email: Yassernejhad@gmail.com

Abstract:- Any attempts to cross the border of security in a network, is called an attack. Attack may be cause to lose or modify the transferred data. The success amount of an attack is depends on network's vulnerabilities. VANETs can be disturbed by attackers for different reasons such as: fun, creating disorder in functionality of networks and etc. In this investigation, we attempt to introduce VANET and then concentrate on different attacks which are happening in this network.

Keywords: V2V network, Security Protocols, Network performance, Attack, Signals strength, VANET

1. Introduction

Nowadays, there are millions of cars which are moving in various states of each country and each year thousands of collisions and incidents occur between them in all around of the world. Several research efforts have been done by researchers in various countries, in order to figure out the reasons of these accidents [1]. The results of most of these studies have shown that, error or delay in the notification is one of the main reasons for car accidents in the most cases.

It seems that, with increasing distribution of information to drivers, an evolutionary change in transportation safety will be happen. Currently, car companies, governments, universities, researchers are interested on developing a system, which allows vehicles to communicate with each other and with the road side infrastructures and inform the hazards, obstacles and important information to each other for the purpose of controlling or preventing accidents and collisions [2].

V2V is defined the communication between vehicle with other vehicle and V2I is defines communication between vehicle with road side infrastructures. Therefore, three main tasks are defined for these networks:

- Identify the information that requires to exchanges between vehicles and stations.
- Sending and receiving information between vehicles with each other or with communication network.
- Creating security for transferred data.

This paper is organized in four sections. Second section describes the general classification of various attacks in VANET. Third section includes special classification of attacks. Fourth section concludes the paper.

2. General Attacks Classification

Generally, attacks that are happening in V2V or V2I communication are divided into three categories which are discussed in below [4].

- Messages reading: in this type of attack, in the time of sending message from source node (vehicle or station) to destination (vehicle or station), attackers allocate in the path and read the content of message.

- Juggle: in this type of attack, attacker take place and replace in other node location.

- Eliminate the Message: in this attack, attacker by staying in the route of messages eliminates all messages which are transferring in that path.

- Modifying the Messages: this attack is similar to the attacks which are eliminating the messages. The performance of this message is such as combining the effects of three attacks including message reading, juggle and eliminating messages. only difference is that in this type attack, attacker changes the authority of itself and receive all messages which are receiving from source nodes and with modifying messages, delivers those messages to the destination.

- Flood of Messages: in this type of attack, attacker is sending messages continually and cause to happen high traffic in network, therefore, create problem in main services.

3. Special Attacks Classification

Attacks against on availability are including:

- *Denial of Service attacks (DoS)*: this type of attack, makes network inaccessible to users. For example by sending a flood of messages to the nodes or with the production of noise and disturbance at the physical layer, this attack may be suffered by members of the internal external network or located out of the network [5].

- ✓ *Flooding Send:* An efficient way to build networks between vehicles is producing massive amounts of fictitious or false messages and sends it to the channel. So that nodes in network includes on-board unit and the roadside infrastructure are unable to process unnecessary information. Therefore, important messages will be lost in the meantime.
- ✓ *Disorder:* with creating interference in the channel, the attacker can prevent the timely delivery of the messages. In addition, a disorder makes an coverage for attackers and cause to not recognizing of that.
  - ✓ *Bad Behave Software:* having software such as viruses with badly behave into VANET can cause serious disruption in the operation of the network.
  - ✓ *Anonymous messages:* this types of messages creates delay in sending messages in VANET.

- *Attacks against the authenticity of the messages*: ensure the authenticity of network includes: recognizing Virtual node from unauthorized nodes or in network from external attackers, black holes Detection, detecting the attacks that virtual interactions are repeated, Disclosure signals from Global Positioning Detection System and also, Neutralizing false news which are published on the network.
  - ✓ *Identity Change:* The external members who are not members of the network, by posing itself instead of one of the nodes in VANET can be authorized to send the wrong messages.
  - ✓ *black holes:* A black hole is created by the nodes that participate in the process of publication or broadcast messages on the network. This attack carried out by domestic abuse nodes. Because, external nodes do not have permission to replicate and spread their messages.
- ✓ *Repeated message attack:* VANETs due to their WAVE structure protected from repeated messages. Because,

each node are stored in its memory the recently received messages. When receive a new message, it compares with the saved messages to determine if that is not repetitive.

- ✓ *Signals from false GPS:* With using the GPS satellite simulator to generate radio signals stronger than signals that are receive from main GPS satellites. An attack that may happen is that the nodes are expected an incorrect position for each other and it can cause accident in network.

- ✓ *Interference in the broadcast:* It may be an abuser node tries to create fake safety messages and inject into network.

- ✓ *Interference in transactions:* In this type of attack, an attacker sends a message that is exchanged between a vehicle and fixed network communication infrastructure with the aim of requesting changes in damaged transaction.

- *Attacks against privacy of messages:* Since in VANET air is exchange messaging environment, messages are accessible in this environment. Attacks on the confidentiality of messages are done. Illegal transaction information collected through surveillance and spatial data network nodes via broadcast messages is happening [6].

  - ✓ *Eavesdropping Foreign Nodes:* Broadcast messages usually includes information related to traffic safety and therefore are not suitable for eavesdropping. With the accumulation of a series of requests for service, an abuser can use the file which is made for regular users that are using special services in defined time.

  - ✓ *Eavesdropping Internal Nodes:* As long as the internal nodes, start to collect network information with the user agreement, that will not be happen any problem. But it is possible that an internal node without notifying users collect their information. For example, a ticket sales agency makes agreement with an employer that track activities and movements at all hours.

✓ *Track Position:* since tracking position of vehicles are necessary, therefore, it is very likely that the attackers to take the disadvantage of this location information. By collecting separate information related to the location of each vehicle in particular, this information can be used to track the vehicles and create files used to store information for each vehicle.

- *False attacks and false attack detection:* attacks from the point of view of the impact on performance of network, are divided into three categories: minor, major and critical attacks. False attack when assessing the risk, due to the attacker's motive for attack, and the high probability of the attack on the VANET network and high effect of this attack on the performance of network, despite technical difficulties when attempting to do it in the groups of critical attacks in VANET. Various types of false attacks are proposed. Two main types of these attacks are: attacks based on location and attacks based on vehicle ID.

4. Conclusion

For sending timely notification to drivers on the roads to reduce accidents and traffic we need communication systems. This system can be used for sending messages from vehicle to other vehicle or between vehicles to road side infrastructure. For this purpose, should ensure the security of transmitted data and prevent unauthorized access to information or prevent from information modifying and etc. Therefore, in the first step, it is necessary to identify all attacks. Then, make solutions for each type of the identified attacks decide. In this paper, we attempt to make a complete survey about various types of attacks in VANETs.

References

[1] http://www.sae.org [Accessed on Feb 2015]

[2] C. J. Adler, (2006), " Information Dissemination in Vehicular Ad Hoc Networks", Diploma Thesis, University of Munich, Germany.

[3] H. Kawashima, (1990), " Japanese Perspective of Driver Information Systems", Transportation, Vol. 17, No. 3, pp. 263-284.

[4] S.Tsugawa, (2005), "Issues and Recent Trends in Vehicle Safety Communication Systems", IATSS Res.

[5] Pat Jang Yodsuk, (2010), "Reliable Broadcasting in VANET, San Jose State University.

[6] Intelligent Transport Systems (ITS), Vehicular Communications, Geo-Networking, (2013), ETSIEN 302636-2 Vol.1, No.2.

[7] Mina Rahbar Gogani, “Various types of attacks and identifying the false attackes in VANET”.