A Survey of Attacks on Vehicular Ad-Hoc Network

Karthikeyan. P. S[1], Javeed Basha. S[2],
Gayathrie. P. K[3], Gajalakshmi. M[4]
[1,2,3,4]U.G. Student Computer Science and Engineering,
S.A.Engineering College, Chennai.

Mary Anitha.E. A[5]
Professor Computer Science and Engineering,
S.A. Engineering College, Chennai.

***Abstract*-Vehicular Ad-hoc network, a subset of MANET and an unstructured network formed by the vehicle on the road. Exchanging information among the vehicles which act as mobile nodes, in turn, improves security on the roads. Being a wireless medium VANET is more vulnerable to many malicious attacks. This paper presents a few existing security attacks and ways to deal with safeguard against them in an elaborate manner.**

Keywords: Attacks; testing; range; spectrum; radio

I. INTRODUCTION

VANET is a dedicated short range communication. It is nothing but a 360 degree protection to each and every vehicle. In VANET, vehicles communicate with each other in order to ensure their own security. Each vehicle has a communication range within which they can be able to communicate. This method enables the vehicles to inform about accidents and other critical damage to their neighbors on the road which in turn ease the work of traffic officers. This trending technique is a booming technique for road safety.

II. VARIOUS ATTACKS

The various attacks that are related to Vehicular ad-hoc network are discussed in brief and various solutions that are used to overcome these attacks like Black Hole Attack, Sybil Attack, Timing Attack, Denial of Service Attack, Wormhole Attack, Man-in-the-middle Attack.

RELATED WORK

A)Black hole Attack and its avoidance protocols for wireless networks
A famous attack, which is common in many wireless networks. Where a router discards a packet in the place where it has to relay them. For example, if suppose two vehicles are indulged in an accident and this information is passed to the other vehicles which are in their own communication range. But the receiving vehicles discard this information instead of relaying the information to the other vehicles heading towards the same route. This scenario creates a lot more confusion instead of solving them.
The solutions suggested towards the black hole attack include maintaining a Coming Route Reply Table as suggested by the author [7]. It is also suggested if it is possible to have a trust management between the cars i.e. the nodes in VANET. A tricky problem in this case is implementing trust management between the cars is very difficult as they are not centralized in nature. Therefore trust values of the nearby nodes needs to be collected.
Also another method imposed by the authors in [2] says that cryptographic methods are used to find the solution to black hole as well. S. Amutha and K. Balasubramani proposed an algorithm to detect this attack. They just preferred the sequence number concept to solve the problem. They state that if the first reply is from the black hole node then compare the destination sequence number with the source sequence number. By identifying the difference to be too large the malicious node is detected.
Encryption verification method is another detection mechanism. The encrypted verification message is used to identify the black hole node. The information contained in the messages cannot be modified by any malicious nodes.

B)The Sybil attacks in sensor networks, analysis and defences It is a famous attack slack hole node. The information contained in the messages cannot be modified by any malicious nodes. It is a famous attacks. In this attack the malicious node will create fraud identities to violate the protocol. Here the attacker‟s subverted the system by creating more identities to have a large influence. Usually, entities use multiple identities for redundancy, resource sharing, reliability and integrity. Here many identities correspond to a single local entity.

DOUCEUR proved that only trusted certification can eliminate Sybil attack. Here there is a need of a centralized authority to ensure all the entities have a unique identity. This method is the most effective method and also create performance bottleneck.

It includes storage ability and network bandwidth Having heterogeneous IP addresses prevents these attacks as well.

Resource Testing method is used to detect the Sybil attack in a fair manner as given in [11]. One of the most common sub-technique in this Sybil attack is Radio resource testing.

In radio resource testing, the sending node sends the message to all the nodes in its network and uses a channel for sending these response messages. If the recipient is not real then it may result in a failure of sending the response messages in different channels at the same time as stated by the author [5]. This method is very much cheaper for any Vehicular ad-hoc network because in radio testing there is a requirement of the source node to broadcast its identity which in turn violating the characteristic of vehicular network.

Another popular method which is specifically designed for VANET is computational resource testing. This method states that if a particular node can"t be able to solve a puzzle in VANET then it is Sybil. This method further requires various tools for message tracking.

A famous approach as stated by the author which plays a vital role in finding these attacks are range-based and range-free methods.

These methods used to initially find the distance between the source and the receiver.

Alternate approach is the „seeing in believing", in this technique each vehicle is used to collect the GPS information from the other vehicles which are in their transmission range in order to confirm their originality and to find the fake identities.

C)Timing Attacks in vehicular Networks Timing attacks is one of the major attacks in vehicular ad-hoc networks. This attack just causes a delay at which the message has to be transmitted from one vehicle to another. Scenario:When malicious nodes receives a message it do not forward that message instead it just add the time slots to them, as a result the message is delayed.

Solution to this Timing Attacks

Data Integrity verification is the only way to avoid timing attacks. This technique eliminates the time slots that are added to the message packet. Trusted Platform Module is another technique of maintain the integrity of the messages.

D)A survey of Denial of Service Attack in vehicular networks The main approach of DOS is to prevent the resources to be accessed by its authenticated users. There are three sub-approaches under this attack And they are Jamming, Syn flooding, and Distributed denial of service attack. Jamming

This technique is a most common technique of the attackers. Here the attackers introduce dummy messages into the network and thereby jamming the network.

Syn Flooding

This attacks normally happens during the connection setup between the client and server. In this case the client is the malicious user.

A normal connection setup between the client and the server happens from

a) SYN MESSAGE (client to server)

b) SYN-ACK MESSAGE (server to client)

c) ACK (client to server)

Here the client won"t send the expected ACK to the source or it just spoof the source IP address and just cause the source to send the SYN-ACK to the wrong client.

Distributed Denial Of Service Attack

This attack is much more severe than any other attack. Here the many number of malicious cars attack a specific car in a distributed manner from different locations and at different times.

Related Work towards the Denial Of Service Attack:

The method to overcome DOS attack is based on the methods suggested by the authors [8],[9],[10]It is advisable to use a On board unit here. Actually, these methods are used whenever a DOS attack occurs the network must be in a position to hop to other frequency channels.This method is further categorized based on the amount of data being hopped and they are slow frequency hopping and fast hopping. Slow frequency hopping allows the transmission of one or more data bits while fast frequency hopping is used for the transmission of one bit at a time but ensuring secured transmission than the other one.

Actually, Dedicated Short Range Communication channel is a very important technique for allowing the network to varying frequency channels. Here the source and destination nodes already know the hopping sequence and hence can exchange the safe messages.

Solution to DDOS attack

DDOS Mitigation is the most popular technique to avoid DDOS attacks. The first process in this solution is to identify the human traffic and separate it out from the traffic generated by BOTS like human beings.

Another approach to pass the message to the target using scrubbing filters(a high power network). unit is attached on each of the vehicles in order to solution to avoid a DOS problem. Whenever an attack is detected the OBU is given an instruction by the processing unit in order to change to a different node. Frequency Hopping Spread Spectrum is a major technique to alleviate the DOS attack. Here the bandwidth of the signal is usually expanded. Another common sub-techniques used are Direct Sequence Spread Spectrum and Frequency Hopping Spread Spectrum.

E)A Survey on Wormhole attack in VANET

A Wormhole attack is the one of the most dangerous attack which breaks the security of the VANET. In this attack a malicious node captures messages at one location and send to another malicious node which replays them locally.

In this paper [14], it tries to overcome wormhole attack by using a cryptographic method and proposed algorithm. Packets are broadcasted from one node to other nodes in a secured and efficient manner. The ID of node is used to broadcast the messages which are carried out by the shared key.

F)Man-in-the-Middle attack in Vehicular Ad Hoc Network
Man-in-the-middle attack is one of the most common attacks. In this attack, the attacker intercepts the communication between two nodes. The attacker may also try to deliver a false or incorrect message to another node.This attack can be overcome by the lightweight authentication and key agreement protocol [15]. The authors mainly try to maintain an attack free network by using three different types of mutual authentication between vehicle to vehicle, between vehicle to respective cluster head and between cluster heads and their computing device. And it also uses secret key to maintain secure communication between computing devices (road side units).

G)Survey on Security Attacks in Vehicular Ad Hoc Network
In illusion attack, the sensors in the vehicles broadcast wrong information to its neighbors leading to traffic disturbances. Actually the driver's behavior is completely dependent on these messages. These unauthorized information leads to traffic collision, accidents etc. Plausibility Validation Network is one of the specific ways to overcome the illusion attack. Here [3] the sensor‟s information is collected and then PVN will intimate whether it is reasonable or not. PVN specifically has a module for checking the data called Data Checking Module.

H)Authentication Solution for Security Attacks in VANET
Message Suppression attack occurs in a rare fashion where the attackers drop the packets from the network which is intended for a particular recipient. This data may be used by the attacker for future times. The attacker may be intended to hide his own personal information about collisions and so as to cause accidents. As a result it may indulge many of the vehicles not obtaining enough information about the roadways and hence causing traffic. In some of the cases the attacker may hide congestion alert. This paper [4] provides a solution to overcome the message suppression attack by using the virtual certification authority. This authentication will help in identifying the malicious nodes easily. Thus the trusted nodes can avoid the message from the malicious nodes.

III. CONCLUSIONS

The various attacks in the Vehicular ad-hoc networks are discussed in a standard manner and each topic in this paper focused on the curious attacks in VANET and the corresponding solutions to overcome those attacks. Furthermore, various views of the networking specialists on each one of those specified attacks are listed for better clarity. Nearly half of the attacks are actually caused due to malicious nodes. The usage of DMV algorithm in VANET avoids the major problems caused due to malicious nodes. In addition to all these brief compilation various studies have been on the stage in creating a SMART VANET, a single solution to all of the mentioned attacks.

IV. REFERENCES

[1] D. He, S. Zeadally, and B. Xu, “An efficient identity –based conditional privacy-preserving authentication scheme for vehicular ad-hoc networks,” IEEE trans. Inf. Forensics Security, vol. 10, no. 12, pp.2681-2691, Dec. 2015.

[2] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, ”An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,” IEEE Trans. Vech. Technol., vol. 59, no. 7,pp. 3589-3603, Sep. 2010.

[3] Mohammed Saeed Al-kahtani,” Survey on Security Attacks in Vehicular Ad hoc Networks,” IEEE Transaction Vehicular transaction, 2012.

[4] Bharat, Santhi Sree and Mahesh Kumar,”Authentication Solution for Security Attacks in VANETs,” International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 3, Issue 8, August 2014.

[5] Q. Xu, Z. Su, and S. Guo, “A game theoretical incentive scheme for relay selection services in mobile social networks,” IEEE Trans.Veh.Technol., vol. 65, no. 8, pp.6692-6702, Aug.2016.

[6] C. X. Zhang, X. D. Lin, R. Lu, P-H. Ho, and X.Shen, “An efficient message authentication scheme for vehicular communications,” IEEE Trans.Veh.Technol., vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[7] Vimal Kumar , Rakesh Kumar., "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network," in Procedia Computer Science 48 (2015) 472 – 479,International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) , ,Science direct-published by ELSEVIER 1877-0509, 2015.

[8] Raya, Pierre, Hubaux, ”Securing vehicular ad hoc Networks,”Journal of Computer Security, Vol.15, Issue 1, January 2007, pp. 39-68.

[9] Stampoulis, Chai, ”A Survey of Security in Vehicular Networks,” IEEE Transaction Vehicular Technology.

[10] R. Prasad, R. Kanjee, H. Zui, Pishro, ”DSRC Accident Warning system at Intersection”, Technical Report, October 19, 2006.

[11] J. Newsome, E. Shi, D. Song, A. Perrig, “The Sybil attack in sensor networks: analysis & defenses,” In Proceedings of the 3rd international symposium on Information processing in sensor networks, 259-268, 2004.

[12] Saurabh Gupta, SubratKar , S Dharmaraja "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network " in International Conference on Computer & Communication Technology (ICCCT)-2011, 978-1-4577-1386-611, 2011 IEEE .

[13] Irshad Ahmed Sumra, Jamalul-Lail Ab Manan, Halabi ,“Timing Attack in Vehicular Network,” IEEE Transaction Vehicular Technology.

[14] Shahjahan Ali, Parma Nand, Shailesh Tiwari.,” Secure message broadcasting in VANET over Wormhole attack by using cryptographic technique,” in Computing, Communication and Automation (ICCCA), Dec 2017,doi: 10.1109/CCAA.2017.8229856.

[15] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar,” Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks,” IEEE Access, vol. 5, July 2017.