Security Challenges and Attacks in Vehicular Ad-hoc Network: VANET

[1]Narayanasamy Rajendran, [2]E.R.Naganathan

[1]Department of Computer Science and Engineering, SCSVMV University, Kanchipuram, India.

[2]Symbiosis Institute of Computer Studies and Research, Symbiosis International University, Pune, India.

[1]narayananngt@gmail.com, [2]ern.vec@gmail.com

Abstract - **Vehicular ad hoc network (VANETS) technologies are growing rapidly in the recent times. In VANET environment security is an important concern to perform secured communication between vehicular nodes. VANET can be protected from various passive and active attacks. As compared to other networks VANETs are less immune and more vulnerable to attacks. The additional overheads in VANETs are dynamic nature, bandwidth limitation, reliability, and heterogeneous device configuration in VANET environment leads to unstable network environment. Attacks in VANET leads to serious security issues, affects the performance, drops the packet, and disconnects VANET nodes. Any node in VANET can act as a malicious node and attack other nodes in VANET environment. In this paper we focus the challenges, security attacks, and other issues in VANET, and finally the available security solutions are analyzed to identify the best security method for each type of attacks.**

Keywords—Security attacks, VANET.

I. INTRODUCTION

The Vehicular Ad Hoc Network (VANET) is the most modern upcoming wireless network. It is a collection of independent vehicular nodes, grouped without the support of any wired network. The geographical position of the vehicular nodes may keep on changing and due to this dynamic nature, the VANET topology changes frequently, also it a self-organized network; it does not involve any central control devices to administrate the vehicular network. The self-configurable network architecture leads to the automatic connections and disconnection of vehicular nodes in the network. In VANET, each vehicular node acts as a router, to route the traffic to the destination through the neighbouring vehicular nodes. All the vehicular nodes discovers the neighbouring vehicular node and update the information in the routing table, the routing entries are updated automatically. VANET is a heterogeneous network environment; here different configurations of vehicular nodes are connected together. Due to its dynamic nature and high mobility speed it is lack on the following areas like availability, integrity and confidentiality. Securing the VANET environment without reducing the throughput is a challenging task, because it is a more complex network in nature and due to that it is more vulnerable to security attacks. Security protocols can be implemented to ensure the security of the VANET, but the security solutions are not effective as same as wired network. The aim of this paper is to discuss about the various security threats attacks and vulnerabilities.

1.1 Physiognomies of VANET:

Self-organized and Self-managed:

In VANET, the vehicular nodes communicate by using radio propagation system and self-organise the network themselves. There is no centralized control system to manage the VANET. One of the vehicular node act as a management node, as soon as it leaves the VANET the other node in the group will manage the VANET.

Dynamic topology:

VANET consist of highly dynamic autonomous topology system. Movement of vehicular nodes at a different speed keep on changing the geographical position of nodes and as well as creates a frequent change in the network topology. VANET topology is not similar to fixed network topology.

Complex nature:

Usually VANET's are very simple network but are highly complex in nature. Due to the frequently changing topology, managing the network and monitoring vehicular nodes is a challenging part of the VANET. Here the entire vehicular node will act as a node as well as an intermediate routing node. So the vehicular nodes exchange the data in multi hop communication fashion.

Limited Resource:

In VANET, the device configurations are very low when compared to fixed or wired network. The computing, routing, and storage resources are limited in VANET. Managing a highly complex network with limited resource is a hectic task.

 DOI : 10.18231/2454-9150.2018.1201

Scalability:

Due to its dynamic nature the network size will vary dynamically. Limited computing resources affect the scalability. Security mechanism of VANET are not that much capable to protect the large networks.

Availability:

It ensures the availability of nodes, data and network services. At any time the data or network service should be available to the authenticated users, also it make sure that there is no denial of service attack.

Integrity:

It is one of important security aspect in VANET. It assures that the sent message and received message are the same one; also it ensures the message reached the destination without any changes or modifications.

Authenticity:

In VANET, the authentication of the user and or the vehicular node is a very important security factor. It is also allowed to implement the self-organised security mechanisms to protect the network from various threats and attacks.

Bandwidth limitation:

The capacity of the communication links are low bandwidth in nature. When more vehicular nodes are added due to the lack of bandwidth the performance may be degraded.

Lack of central control system:

In VANET, there is no centralised administration system to manage the network and nodes. It is totally different from wired network; the vehicular nodes cannot send the data directly to router as same as in a fixed router. One of the vehicular nodes is elected as an administrator to manage the network. As soon as the current administrating vehicular node leaves the network, then again one of the vehicular nodes is elected for administration. This process will be continued until the existence of network.

1.2 COMPONENTS OF VANET:

Figure 1: Components of VANET

Central Processing Unit (CPU): It performs arithmetical and logical operations on the data; also it controls and manages all the connected devices.

Monitor: It is an output device; it displays the output in graphical form.

Recorder: It is used to record all the events occur in and out of the vehicle.

Global Positioning Unit (GPS): it is used to identify the global positioning of the device.

Front and Rear Sensor: It is used to sense the nearby devices.

1.3 VANET ARCHITECTURE:

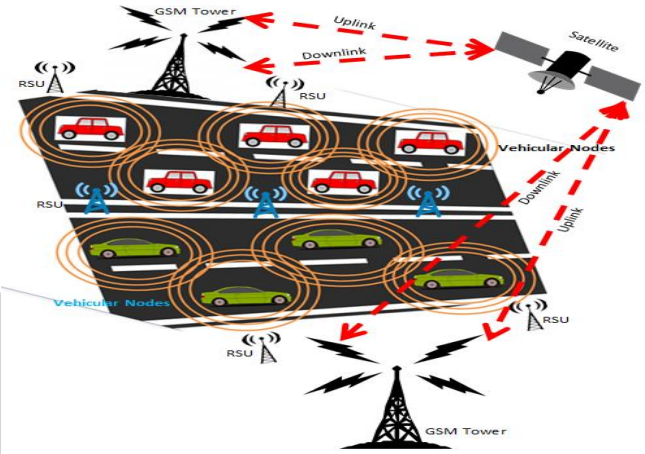

Figure 2: VANET ARCHITECTURE

1.4 APPLICATIONS OF VANET:

VANET can be used in absence of the fixed or wired network infrastructure communication. It is used in emergency rescue operation and during natural disasters like earthquake and Tsunami. It is used to restore the communication rapidly and it has wide range of scope today. It can be used to create a personal area network among the mobile nodes. Various VANET applications are available, they are:

i. Safety Alert Applications
ii. Congestion Warning Applications
iii. Traffic Diversion and Coordination Applications
iv. Infotainment Applications
v. Commercial Applications
vi. Traveller Guide Applications
vii. Traffic Management Applications
viii. Climatic Warning Assistance Applications
ix. Law Enforcement Applications
x. Emergency Management Applications

1.5 ADVANTAGES OF VANET:

A VANET network can be deployed easily without any fixed infrastructure. VANET's are used to increase the vehicle safety, collision avoidance, and cooperative driving and traffic optimization. Easy to implement and cost effective. The complete network can be configured in less time.

SECURITY CHALLENGES AND ISSUES IN VANET

One of the biggest challenges in VANET is security; it is very difficult to secure this stateless network and achieving the security goals. VANET is more vulnerable to attacks and threats due to its fundamental characteristics like (dynamic topology, limited resource, bandwidth constraint, lack of network management and administration facilities).

 DOI : 10.18231/2454-9150.2018.1201

In VANET architecture, the attacks were classified into two major categories active attack and passive attack, apart from this many dissimilar attacks affects the network architecture and different network layers. The internal attacks and external attacks are the part of the active network. Internal attacks are more vulnerable than external attacks because the internal attacks have the complete knowledge about the existing network.

Passive attacks are part of the internal attacks and it is very difficult to identify the attack, the reason behind that is it resides in the network silently and collect all the information without doing any modification in the data. Active attacks are performed from non-members of the VANET group; usually hackers handle active attacks to steal information and to malfunction's the network. Active attacking methods are classified as DOS, Flooding, Bandwidth consumption and Broadcasting false routing information attacks. In past, different researchers were analyzed the following attacks in the paper [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19].

2.0 TYPES OF ATTACKS IN VANET

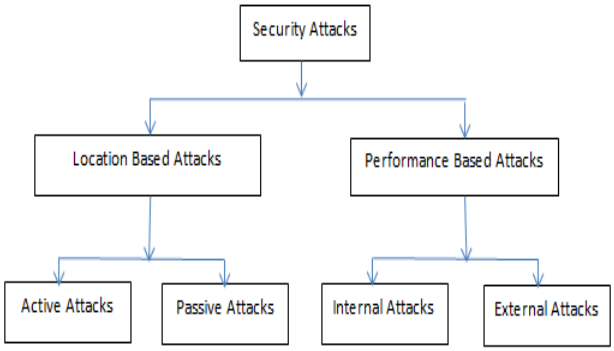

Figure 3: TYPES OF ATTACKS IN VANET

2.1. Location based attacks:

These types of attacks are possible because of the availability of the mobile nodes with built-in GPS system.

2.1.1 Active attacks:

An active attack can be used to do immediate changes on the target data transferred in VANET. The changes will be immediately affecting the target system without any delay. It is highly vulnerable and very difficult to defend and stop.

a. Message Replay Attack:

The vulnerable node sniffs valid messages from the network traffic and breach the authentication by forwarding the same messages later to the destination node in the network. This type of attack can cause higher damage to intermediate nodes.

b. Wormhole Attack:

A group of vulnerable node joins together and attacks the VANET. One of the vulnerable nodes receives the packet from the VANET and tunnels it to another vulnerable node via a private connection. Wormhole attack affects the routing process in VANET. It creates serious consequences and leads to network congestion and collision. There are different types of wormhole attacks are used by the attackers. They are:

I. Open wormhole attack
II. Half open wormhole attack
III. Closed wormhole attack

b (i). Open Wormhole Attack:

In figure 4, the nodes (S) and (D) represent the source and destination. The nodes S, D, X, and Y are considered as good nodes and nodes V1 and V2 are vulnerable nodes affected by wormhole attack. In this attack, both vulnerable nodes present in the same network in order to hack the communication between two parties. The vulnerable nodes add themselves IP header and advertise their availability through the route discovery process and gains attention of target node. It creates an image that the immediate neighbours are the vulnerable nodes, so the target node bypasses the neighbouring node and forward the data through the vulnerable node. [3]

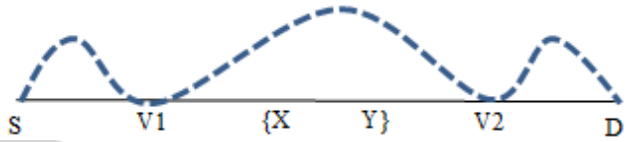

Figure 4: Open Wormhole Attack:

b (ii) Half Open Wormhole Attack:

In figure 5, the nodes (S) and (D) represent the source and destination. The nodes S, D, X, and Y are considered as good nodes and nodes V1 and V2 are vulnerable nodes affected by wormhole attack. In this attack, the initial vulnerable node does not modify anything in the packet at its end, simply it tunnels the packet to the other vulnerable node and that vulnerable node do changes in the packet and rebroadcast the packet.

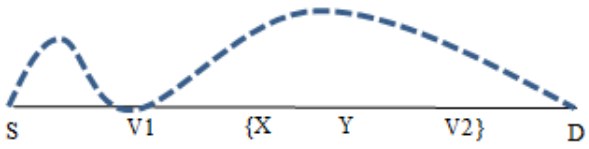

Figure 5; Half Open Wormhole Attack:

b (iii). Closed Wormhole Attack:

In this attack, it hides all the intermediate nodes between the sender and receiver. It creates an image between the sender and receiver that both are directly connected.

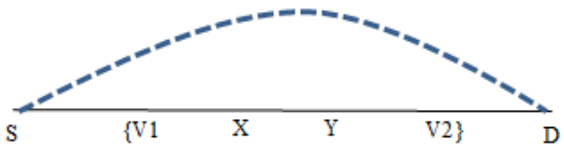

Figure 6: Closed Wormhole Attack:

Mitigation Technique:

In [15], the author proposed an approach that makes forwards the RREP conditionally. The condition checks the validity of neighbouring node that forwarded the packet. When the condition fails that means the identity of the neighbour is not valid. It is best suitable for wormhole attack with out-of-band channel. The simulation result indicates the impact of wormhole attack affects the throughput of packet ratio in the receiver system.

 DOI : 10.18231/2454-9150.2018.1201

c. Byzantine Attack:

In this attack, the vulnerable node has complete governance of a number of authenticated nodes in that network and performs randomly to interrupt the communication on the network. It creates routing loops, drops particular nodes packet or packets from the particular network, forwards packet through non-optimal path [13].

Mitigation Technique:

In [16], the author proposed the solution for byzantine attacks, the challenging task is it is difficult to predict. Trust based cryptographic mechanism and motivation based mechanisms are used to exchange messages. it ensure the authenticity of the message.

d. Sybil Attack:

In this attack, a vulnerable node in the network can claim multiple fake identities. Attackers attack the less secure node and force the node to execute malicious or vulnerable activities like it claims multiple fake identities. The vulnerable nodes are also known as Sybil nodes. It is name after the case study of a woman with multiple personality disorder. It compromises the authenticated node and steals the authentication [2].

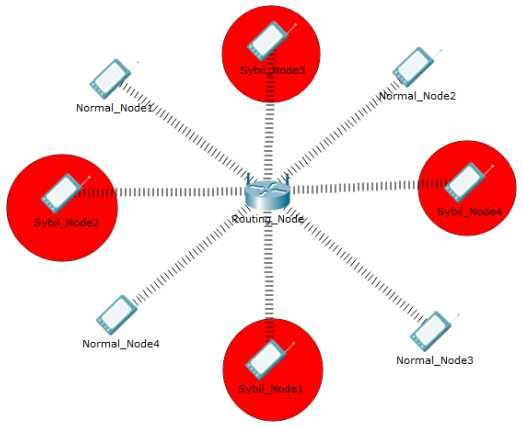

Figure 7: Sybil Attack:

Mitigation Technique:

In [17], the researchers proposed few techniques like trusted certification, Privilege Attenuation, Recurring Costs and resource testing to defend Sybil attack.

e. Denial of service Attack:

In this attack, the attacker node seeks to make a victim node or devices in a network unavailable. The aim of this attack is to interrupts and stops the service provided by the victim node. This kind of attacks are achieved by flooding the redundant message from various attacker node to the target victim node to overload it, because of the overwhelming request the victim node cannot continue its service, finally it not accessible by any users.

Mitigation Technique:

In [18, 19], the authors proposed a mechanism for detecting and preventing denial of service attack in MANET. DoS attacks were detected through collaborative monitoring, Profile-based detection and Specification-based detection. DoS can be defended through reputation-based incentive mechanism, using globally coordinated filters, Tracing the source IP address.

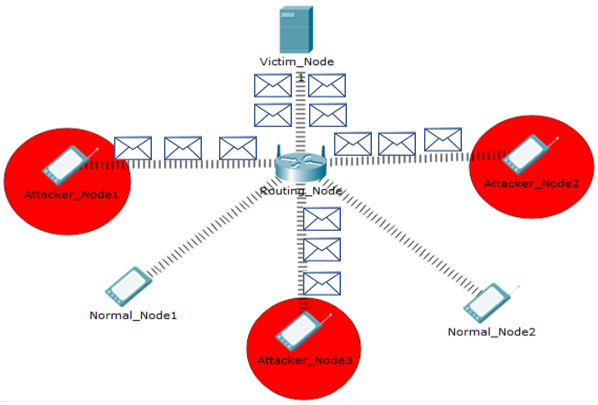

Figure 8: Denial of service Attack:

f. Masquerade Attack:

In this attack, the attacker uses a fake network identity, to gain access to the target node. This attack can happen in many different ways. In one of the method the attacker steals the authorisation information by convincing the victim node, then the attacker access the victim node by using the stolen authorisation credentials. Once the attacker gains the access then he can modify or delete the data or software in the victim node.

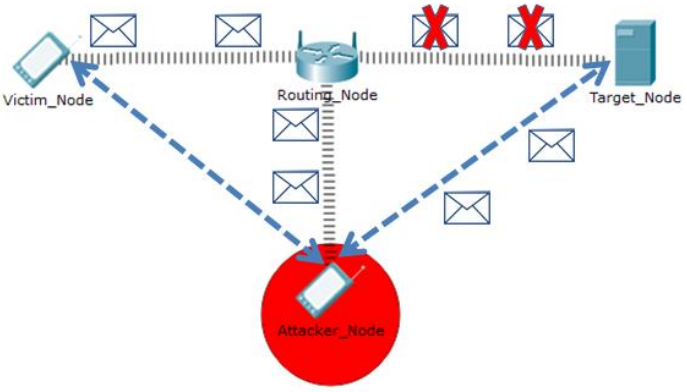

Figure 9: Masquerade Attack:

Mitigation Technique:

The researchers proposed SGA and DDSGA algorithms for effective detection of masquerade attacks.

2.1.2 Passive attacks:

In VANET, passive attacks are intended for monitoring the data and analysing the network pattern. The passive attacker does not do any changes in the data or information transmitted in the network. Passive attacks are very difficult to detect.

a. Traffic Monitoring:

An attacker uses this type of attack initially to understand the network activities. It monitors the network activities and helps the attacker to plans for the attack. It can be used to discover the network traffic pattern and monitor the

 DOI : 10.18231/2454-9150.2018.1201

network performance, bandwidth utilization and monitors the conversation between the sender and receiver.

b. Traffic Analysis

As a next step to traffic monitoring the traffic analysis attack is implemented by the attacker. It analysis the total behaviour of the VANET and generates the statistical data about the VANET usage. It is more useful for the attacker to understand the current network scenario and helps them to plan for a better attack.

Figure 10: Traffic Analysis

c. Eavesdropping:

An attacker hacks the information or data shared between the sender and receiver without their knowledge. This type of attacks easily read the message and also creates distribute fake messages easily in the network.

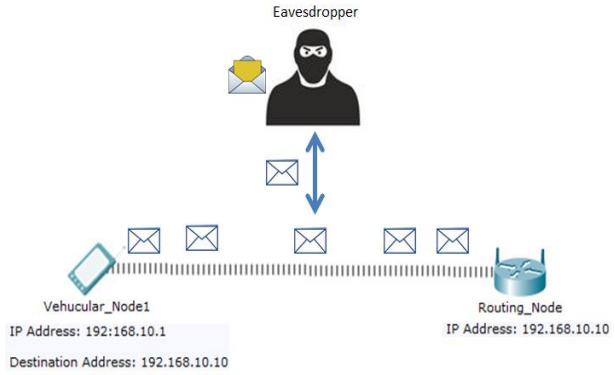

Figure 11: Eavesdropping:

2.2 Performance Based Attack

2.2.1 Internal Attacks:

This type of attacks occurs when a normal node in the same group becomes vulnerable node, it disclose the network authentication with other vulnerable nodes or hackers which are outside the network. The hackers can extract all the sensitive information very easily, or the attackers stops the function of the network and its services very easily.

a. Routing Attacks:

The aim of the attacker is to stop the network services, communication and brings down the performance of the VANET by affecting the network routing process. Different routing attacks are used by the hackers to attack the VANET successfully. They are:

a (i). Black hole Attack:

In VANET, each node acts as host as well as a router. Each node in the VANET will communicate with the help of one or more intermediate router and the intermediate nodes (routers) forwards the packet to destination network. The vulnerable vehicular node router drops the network packet from the particular network or from a particular destination.

a (ii). Flooding Attack:

The vulnerable vehicular node floods the routing information continuously to all the destinations in the network. By repeatedly sending the same packets on the network, it consumes the total bandwidth of the network, so that communication between the vehicular nodes will be affected. The flooding attacks initially affect the network throughput and finally it leads to denial-of-service.

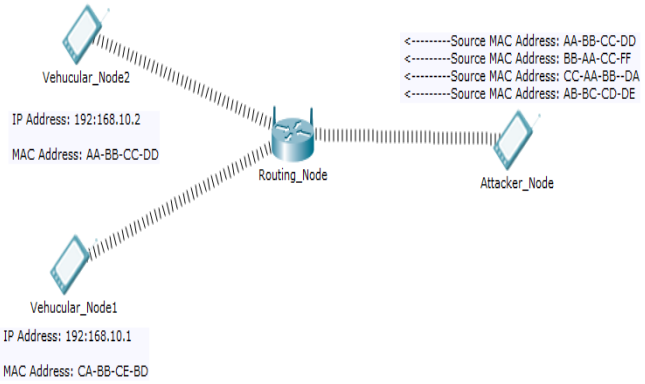

Figure 12: Flooding Attack

a (iii). Spoofing Attack:

A spoofing attack can be used to launch attack against vehicular nodes to steal the information, breach the security and intruding malwares. In this, a vulnerable node impersonate as another vehicular node in order to launch the attack. There are varieties of spoofing attacks.

- IP Spoofing Attack
- ARP Spoofing Attack
- DNS Server Spoofing Attack

a (iii). IP Spoofing Attack:

A vulnerable vehicular node spreads a packet with multiple spoofed addresses to the target machine or network. At the same time it can also spoof the particular vehicular nodes IP address, by using that IP address it'll forward the packet to all the other nodes in the network. In response of receiving the IP packet all the receivers will send their response back to that particular vehicular node, it results in flooding attack and DOS attack

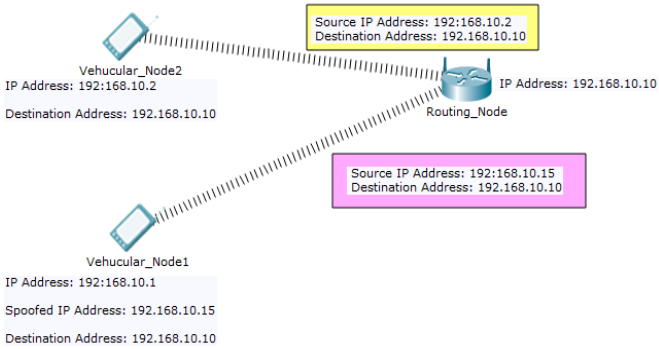

Figure 13: IP Spoofing Attack:

 DOI : 10.18231/2454-9150.2018.1201

a (iii). ARP Spoofing Attack:

ARP spoofing attack is developed to attack a LAN that uses ARP. ARP spoofing attack mechanism is the base for attacks like session-hijacking attack and DOS attack. A vulnerable vehicular node spreads the spoofed ARP packet/message in the LAN in order to link the IP address of the target node with the MAC address vulnerable node.

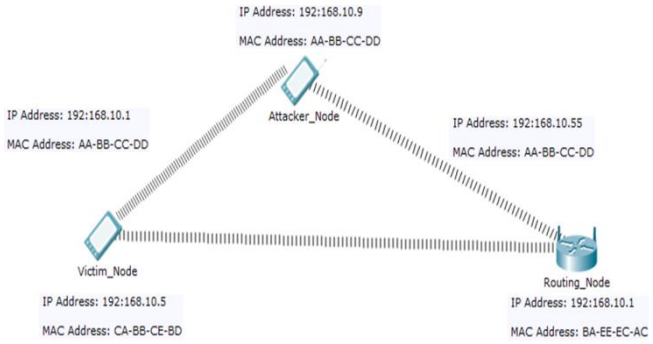

Figure 14: a (iii). ARP Spoofing Attack:

a (iii) DNS Server Spoofing Attack:

The main aim of this attack is to spread virus and worms into the target node. The vulnerable node attacks the DNS table and changes the IP address of the particular domain name to the IP address of the server managed by the attacker. Any node access that particular domain will be redirected to the server managed by the attacker.

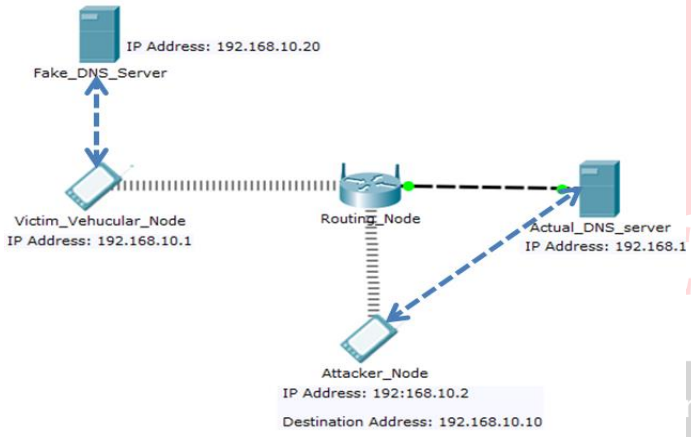

Figure 15: a (iii) DNS Server Spoofing Attack:

2.2.2 External Attacks:

This type of attack is common in VANET, because it's an open network and any node can join or leave the network anytime. Each type of external attack tries to gain the weakness of the network to exploit and affect the network resources.

2.2.2. (a). Jamming:

VANET's are vulnerable for jamming attacks. These types attacks can be easily achieved by transmitting radio frequency RF signals to create interference on the VANET transmission range. The main aim of this attack is to block all the network resources and services. The attacker is not part of the network so this type of attack comes under the external attack. Jammers were categorised into four types [6], they are:

- Constant Jammer
- Reactive Jammer
- Deceptive Jammer
- Random Jammer

Constant Jammer:

In this type of jammer, the high RF signals are continuously transmitted in the same frequency of the VANET to supress and destroy vehicular node signals.

Reactive Jammer:

In this type of jammer, the signals are not transmitted when the VANET is idle. The jammer continuously sense the network to find the communication signals, if it finds any signal it automatically jam the signal.

Deceptive Jammer:

In this type of jammer, it constantly transmits the series of packet in to the wireless medium without any gap between the successive transmissions; also it broadcast the fake messages among the nodes to create confusion.

Random Jammer:

In this type of jammer, it randomly jam the network signal, it will not continuously transmit the signal to jam the network resources. Sometime it transmits the signal and sometime it's quite and idle. This jamming type cannot be identified easily.

2.2.2. (b). Brute Force attack:

In this type of attack, the attacker uses a trial-and-error method to obtain the identity of other users such as username and password. It is also known as dictionary attack. It is time and resource consuming attack. The success rate of this attack is based the computing resource and different key combination algorithm. The main aim of this attack is to steal the information from the authenticated users.

II. CONCLUSION AND FUTURE WORK

VANET's are prone to various types of security attacks. In this paper, we discussed most of the security issues, challenges and various types of attacks in VANET. This paper will create awareness for the researchers and students about the security attacks in VANET. We analyzed the each and every attack and classified according to its behavior, characteristics and impact they create. The root cause of each attack was explained clearly with diagrams. Finally this paper will be useful for the researchers to develop the mitigation strategy against the security attacks. In future study, we will try to provide security solution by developing security algorithms to protect VANET.

III. ACKNOWLEDGEMENT

I would like to thank my guide Professor E. R Naganathan, for his continuous support and constant encouragement in order to complete this paper.

REFERENCES

[1] Arif Sari, Onder Onursal, Murat Akkaya, "Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)", International Journal of Advanced

 DOI : 10.18231/2454-9150.2018.1201

Research in Computer and Communication Engineering, Vol. 6, Issue 4, April 2017

[2] James Newsome, Elaine Shi, Dawn and Adrian Perring "The Sybil Attack in Sensor Networks: Analysis & Defences", IPSN'04, April 26–27, 2004, Berkeley, California, USA.

[3] Marianne Azer, Sherif El-Kassas, Magdy El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.

[4] Ankit Mehto, Prof. Hitesh Gupta, "A Review: Attacks and Its Solution over Mobile Ad-Hoc Network", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013 ISSN: 2231

[5] Narayanasamy Rajendran, & E.R Naganathan. (2017). Adaptive Method For Vehicle Integration And Coordination Among Vehicles In Manet. International Conference on Energy, Communication, Data Analytics and Soft Computing (pp. 3479-3482). Chennai: IEEE.

[6] Neha Thakur, Aruna Sankaralingam "Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks" International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555, Vol. 3, No.2, April 2013

[7] Amandeep Kaur1, Dr. Amardeep Singh "A Review on Security Attacks in Mobile Ad-hoc Networks" International Journal of Science and Research (IJSR) Volume 3 Issue 5, May 2014.

[8] Ashish kumar khare, Dr. R. C. Jain and Dr. J. L. Rana, "A REVIEW: TRUST, ATTACKS AND SECURITY CHALLENGES IN MANET", Informatics Engineering, an International Journal (IEIJ), Vol.3, No.3, September 2015.

[9] Saritha Reddy Venna1, Ramesh Babu Inampudi2, "A Survey on Security Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 7 (1) , 2016, 135-140

[10] Narayanasamy Rajendran, & E.R. Naganathan. (2016). A Detailed Study on Fundamental Characteristics and Functional Operations of Manet. International Journal of Engineering Research in Computer Science and Engineering, 3(6), 151.

[11] Anil Saini, Anu, "Analysis of Security Attacks and Solution on Routing Protocols in MANETs", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.6, June- 2016, pg. 182-189.

[12] Mangesh M Ghonge, Pradeep M Jawandhiya, Dr. M S Ali, "Countermeasures of Network Layer Attacks in MANETs", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011

[13] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in Advances in Ultra-Dependable Distributed Systems, N. Suri, C. J. Walter, and M. M. Hugue (Eds.), IEEE Computer Society Press, 1995.

[14] Umesh Kumar Singh1, Kailash Phuleria, Shailja Sharma2 & D.N. Goswami, " An analysis of Security Attacks found in Mobile Ad-hoc Network", International Journal of Advanced Research in Computer Science, Volume 5, No. 5, May-June 2014.

[15] Dhara Buch and Devesh Jinwala, "Prevention Of Wormhole Attack In Wireless Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[16] Megha D.More , S.B.P.C.O.E Indapur; Amol C.Devkate, S.B.P.C.O.E Indapur; Sonali R.Misal, S.B.P.C.O.E Indapur; Vaibhav G.Pagare, S.B.P.C.O.E Indapur; Yogendra V.Patil, S.B.P.C.O.E Indapur, "Identification and Prevention of Masquerade Attack using DDSGA Algorithm", International Journal for Scientific Research and Development, Volume-6, Issue-11

[17] John, R., Cherian, J. P., & Kizhakkethottam, "A survey of techniques to prevent sybil attacks", 2015 International Conference on Soft-Computing and Networks Security (ICSNS).

[18] Mieso K. Denko, "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme ", Systemics, Cybernetics And Informatics Volume 3 - Number 4.

[19] Sharma, Neeraj & L Raina, B & Rani, Prabha & Chaba, Yogesh & Singh, Yudhvir. (2019). "Attack Prevention Methods For Ddos Attacks In MANETS"

 DOI : 10.18231/2454-9150.2018.1201