International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 8, 2017 ISSN: 2348-6600
Reference ID: IJCS-195 PAGE NO: 1195-1198
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Prevention of DOS Attack by Using Enhanced Malicious Packet Detection Algorithm in VANET Architecture

Dr.V.Sasirekha
Assistant Professor of Computer Science,
J.K.K.Nataraja College of Arts & Science,
Komarapalayam,
Namakkal (DT) - 638 183.
sasirekhailangkumaran@gmail.com

S. Nithyadevi, M.C.A. M.Phil., PGDCA.
Assistant Professor in Computer Science
Anbu Arts and Science College
Komarapalayam,
Namakkal (DT) - 638 183.
nithyamca81@gmail.com

ABSTRACT- The growth of the increased number of vehicles are equipped with wireless transceivers to communicate with other vehicles to form a special class of wireless networks, known as vehicular ad hoc networks or VANETs. Security is one of the safety aspects in VANET. Network Security plays a very important role within event of the VANETs. Due to the unreliable communications in VANETs, security protocols would like a lot of concerns, like privacy, authentication, and consistency of messages. However, VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives. In this paper we proposed Enhanced Malicious Packet Detection Algorithm (EMPDA) which is used to verify and detect the malicious nodes creating DoS (Denial of Service) attack.

Keywords :- VANET, EMPDA.

I. INTRODUCTION

VEHICULAR Ad-hoc Network (VANET) is a kind of Mobile Ad hoc Network (MANET) to provide communication among nearby vehicles and between vehicles and nearby roadside equipment. As mobile wireless devices and networks become increasingly important, the demand for Vehicle to Vehicle (V2V) and Vehicle to Roadside (V2R) or Vehicle -to Infrastructure (V2I) communication will continue to grow .It is supposed that each vehicle has a wireless communication equipment to provide adhoc network connectivity . VANET applications have been broadly categorized into safety and non-safety applications. Safety applications are very important in nature as these are directly related to users and their lives. These applications provide warning-related information to drivers such as post-crash notification on a particular road. Simply, VANET is concern with safety of human life while these people are moving on the roads. Non-safety applications are to comfort the drivers and passengers, and to improve the traffic system, Traveling map, parking availability, and weather information are the examples of these applications. Generally, the purpose of both applications categories is to provide correct information to users/drivers on the roads. However, for safety applications, the information not only needs to be correct but also securely transmitted from a source to a destination. Hence, security is an important issue where little

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 8, 2017 ISSN: 2348-6600
Reference ID: IJCS-195 PAGE NO: 1195-1198
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

interruption, such as intermittent disconnections can create problem to the users. This is particularly crucial if critical life information is being communicated between a sender and a receiver. To achieve this, network availability is a basic requirement. It is defined as when any node wants to access the other node in the network or to access the infrastructure, the network should be accessible to user. The inaccessibility or inavailability may be contributed from any fault or any kind of attacks, such as Denial of Service (DoS).

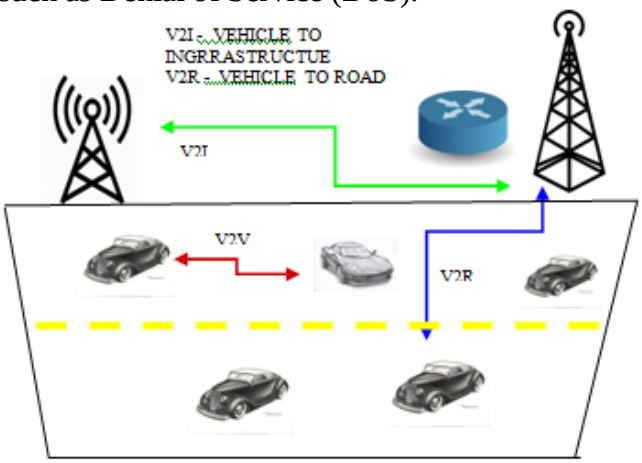

Fig.: VANET ARCHITECTURE

This paper is organized as: Section II discuss possible attacks in VANET. Section III talk about the proposed EMPDA algorithm and IV presents conclusion.

II. POSSIBLE ATTACKS IN VANET

Vanet is susceptible to various attacks, they are:**1.Denial of Service attack:** Denial of service attack can be encouraged by network insiders as well as network outsiders, rendering the network unavailable to authentic users by flooding and jamming with likely catastrophic results. In this attack, the attacker attempts to make a network resource and services unavailable to its intended users. There are three ways the attackers may achieve DOS attacks, namely: jamming communication channel, network overloading, and packets dropping.[2]

2.Alteration attack: In this attack the attacker attempt to modify the data being exchanged between two vehicles, thus delaying the transmission of information and replaying the earlier transmission.[3]

3.Sybil attack: In this attack the objectives of the aggressor is to present a delusion to other nodes by sending erroneous messages and to impose other nodes on the road to flee the pathway for the benefits of the aggressor.[4]

4.Blackhole attack: It can be stated as variation of Denial of service attack in which the malicious node poses the shortest path to the target node and drop all the packets that it can receive and thus can deprived the actual receiver of the packets from receiving the critical information.[5]

5. Node Impersonation : Impersonation is an attempt by a node to send a modified version of a message received from the real originator for the wrong purpose and claim the message as come from the originator. To overcome this problem, a unique identifier is assigned to each vehicle node in VANET, which will be used to verify the real message originator. Police may use it to identify the driver as it is associated with driver's identity [5]. It is important to protect this identifier so that it cannot be misused by the attacker.

6. Sending False Information : In this type of attack, wrong or fake information was

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 8, 2017 ISSN: 2348-6600
Reference ID: IJCS-195 PAGE NO: 1195-1198
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

purposely sent by a node to other nodes in the network to create a chaos traffic scenario, which it may lead to misinterpretation of the actual situation [2]. With the falsified information, the users would likely to leave the road, thus it makes the road free for the attacker to use it for his own purposes.

7. ID Disclosure: Disclose the identity of other nodes in the network and track the current location of the target node. Global observer monitors the target node and sends a 'virus' to the neighbors of the target node. When the neighbors are attacked by the virus, then they take the ID of the target node, as well as the target's current location. Rental car companies are using this technique to track their cars [6].

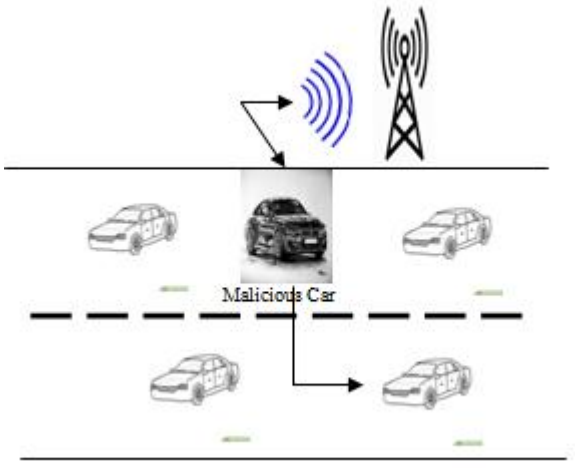

Fig.: DOS ATTACK

The Figure indicates that a malicious black car forges a large number of fake identities and transmits a dummy messages to a legitimate car behind it and even to an RSU(Road Side Unit) to create a jam in the network.

III. PROPOSED MODEL:-

In our work, we will focus on the denial of service attacks in vehicular ad hoc networks. Vehicles communicate with road side units to have access to information. Initially all the vehicles need to be registered in RSU prior to take part in the communication. RSU Verifies the vehicles identity and it send the acknowledgement to the vehicle. At the time of verification RSU use Enhanced Malicious Packet Detection Algorithm to detect suspicious vehicle. According to EMPDA RSU uses different time slot for vehicle communication and also set the range for communication. All the vehicles have to communicate within the range. When malicious vehicle frequently flood the message RSU will calculate the time difference between the sending and receiving the request of the vehicle by using EMPDA. If the time difference is more than the range then RSU announced that the vehicle is malicious and pass the information to its neighborhood RSUs.

Step: 1 The Vehicle ad-hoc network creation in the specified geographical area.
Step: 2 Deployment of Road Side Unit (RSU) and apply EMPDA algorithm .
Step: 3 Divide different Time slots and calculate communication range.
Step: 4 Create Trajectory between one Road Side Unit (RSU) and neighbor RSU along with specified distance.
Step: 5 RSU Verifies the vehicle Identity and generate Acknowledgement.
Step: 6 Entry the time of the traversed details are stored in RSU and OBU(OnBoard Unit) of the vehicle.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 8, 2017 ISSN: 2348-6600
Reference ID: IJCS-195 PAGE NO: 1195-1198
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Step: 6 TimeStamp Calculation in RSU at the particular vehicles time slot:-
TimeSlot = (Sender Timestamp - Received Timestamp) / Total number of Packets send
Step: 7 RSU compares the rate sending packets from each node.
Step: 8 If vehicles rate of sending packets is greater than the usual rate of other nodes, then the packets are discard and detect the vehicle is malicious vehicle.

IV. CONCLUSION:-

Security in VANET is used for enhance road safety. If vehicle and RSU cannot receive correct information due to any type of attacks the VANET network is not secure. So detection of attacks especially DoS is very important for securing network. This paper proposed a new algorithm to detect DoS attack by using timeslots. Thus, Enhanced Attacked Packet Detection Algorithm executes earlier and verification done with lesser delay and increased throughput.

REFERENCES:

[1]. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Springer Science +Business Media, LLC 2010.
[2] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "Denial of Service (DOS) Attack and Its PossibleSolutions in VANET" in International Scholarly and Scientific Research & Innovation 4(5) 2010.
[3] Mushtak Y. Gadkari , Nitin B. Sambre, "VANET: Routing Protocols, Security Issues and Simulation Tools," IOSR Journal of Computer Engineering, July-Aug. 2012.
[4] G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", WISTP 2008, LNCS 5019, pp.106-116.
[5] Amjad Khan, "Minimization of Denial of services attacks in Vehicular Ad hoc networking by applying different constraints" International Journal of Academic Research in Business and Social Sciences July 2013, Vol. 3, No. 7 ISSN: 2222-6990.
[6] S.Roselin Mary, M.Maheshwari, M.Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked packet detection algorithm (APDA)", ICICES, pp.237-243, 2013.
[8] Adityasinha, prof santosh k. Mishra, "Preventing VANET from DoS & DDoS Attack" International journal of engineering trends and technology. vol. 4, pp. 4373-4376, 2013
[9]Verma K, Hasbullah H, Saini HK. Reference broadcast synchronization-based prevention to DoS attacks in VANET. 7th International Conference on Contemporary Computing (IC3); Noida. 2014. p. 270–5.