ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Review on Detection and Prevention Techniques of Denial of Service Attack in VANET

Priya Sharma
Department of Computer Science and Engg.
Amritsar College of Engineering and Technology
Amritsar,India

Er. Amarpreet Singh
Department of Computer Science and Engg.
Amritsar College of Engineering andTechnology
Amritsar,India

Abstract: VANET meaning vehicular ad hoc network is nothing but the group of independent mobile nodes i.e. vehicles which are moving throughout the mobile network liberally. Vehicular ad hoc network is a sub set of mobile ad hoc network. It is a kind of temporary network in which the position of the mobile nodes are not preset. Since the communicating nodes move quickly and keeps on changing position following dynamic topology of Vanet. Such networks are unprotected from the malicious nodes in the network itself. Therefore, they are vulnerable to several kinds of attack such as Sybil attack, Black hole attack, Denial Of Service attack, etc. In this paper we have discussed several techniques for detecting and preventing DoS attack in Vanets.

Keywords :- VANET Security, DOS attack

I. INTRODUCTION

VANET is a sub class of MANET that offers wireless communication among vehicles. Its main concern is providing security and privacy to the vehicles during interaction. It is used to implement ITS which is an intelligent advanced application that provides different services. The wireless access in the vehicles is provided by WAVE and is designated with the standard IEEE 802.11p [1]. Each vehicle is equipped with On-board Unit (OBU) and GPS to identify vehicles' location. In this network basically two kinds of communication are performed i.e, V2V (vehicle to vehicle) and V2I (vehicle to infrastructure). Here the Roadside Infrastructure Units are used to support high mobility and bi-directional traffic in road. Therefore, RSU (road side units) are installed in between both ends on road. These road side units are used to accept data from vehicles and forward to another vehicle in network or send it to the infrastructure monitoring server for data analysis.

Vanet provides safety applications such as collision warning ,traffic information, blind crossing prevention, work zone warning,etc. It also provide comfort applications like parking lot payment, internet service such as sending emails, downloading files, etc. The importance of VANET security becomes prominent when the application is concerned with the safety of life. The basic security requirements of Vanet that ensure the protection from malicious nodes are : Confidentiality ,that ensures message will be comprehended only by authoritative users. Integrity, that ensures messages delivered among nodes are not altered by attackers , and Availability is ensured when the network provides its services even under an attack unaffecting its performance. For Vanet security safety messages should be given high priority and must be delivered on time.

II. ATTACKS

Various kinds of attacks that Vanet is facing are :

a. DoS Attack : Denial of service attack can be carried out by network insiders and outsiders, and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. The attacker attempts to make a network resource and services unavailable to its intended users. By flooding the control channel with high volumes of artificially generated messages, the network's nodes, OBUs and roadside units cannot sufficiently process the surplus data. There are three ways the attackers may achieve DOS attacks, namely: jamming communication channel, network overloading, and packets dropping.[2]

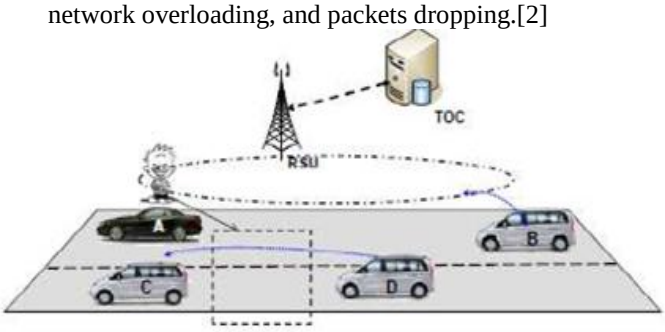

Figure 1. DoS attack between V2V and V2I.

b. Sybil attack: In this type of attack, a node sends numerous messages to other nodes and each message contains a dissimilar formulated source identity in such a way that the originator is not known. The fundamental objectives of the aggressors are 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 attacker.[3]

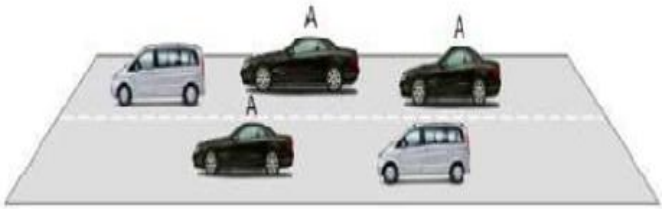

Figure 2.Sybil Attack

c. Blackhole attack: It is a kind of Denial of service attack in which the malicious node can drop all the packets

© 2015-19, IJARCS All Rights Reserved

that it can receive and thus can deprived the actual receiver of the packets from receiving the critical information.[4] When the node drops out, all routes it involved in are broken leading to a failure to disseminate messages. In a black hole attack, a malicious node initiates itself for having the shortest path to the target node and thus, deceives the routing protocol.

d. ***Grayhole attack :*** This attack is known as a variation of Black Hole attack, in which the malicious node deludes the network by agreeing to promote the packets, but it sometimes drops them for a while and then switches to its normal behavior. It is very tricky to outline such categories of attack.

III. LITERATURE REVIEW

There are different Denial Of service Attack detection techniques in Vanets proposed by the researchers over time to time which have some advantages over and vice-versa.

M. Raya et al. [5] explained the need to secure vehicular networks stating its safety related and other applications related to traffic information and liability-related messages. The author proposed a model that identifies the most relevant communication aspects and also identified the threats facing vehicular networks and considered attacks perpetrated against messages rather than vehicles. To overcome these threats a security architecture along with the related protocols has been proposed and they have shown how and to what extent it protects privacy and explained why TESLA-like protocols are not suitable for VANETs. They have analyzed the strength of their proposal from the analysis made and result obtained.

Halabi Hasbullah, et.al [6] solved the security problem of Dos attack with the use of OBU. The model relies on using OBU which resides on each vehicle node, to make a conclusion as to deter a DOS attack. The processing unit transfer information to the OBU, to switch channels technology (or) to use frequency hopping technique. OBU have four options by which it can make decision based on the received malicious message. After necessary processing and decision, OBU send the information to next OBU in the network. Switching options available are channel switching, technology switching, Frequency hopping spread Spectrum, multiple radio transceivers.

Isaac,et.al [7] describes improved road safety and enables a wide variety of value added services. Countless variety of attacks against VANET have emerged recently which crack the security of such networks. Such security assaults on VANET may lead to catastrophic result such as the loss of lives of revenue for those values added services. The author presented some of the main security threats and attacks that can be subjugated in VANET and equivalent security solutions that can be implemented.

A. Baber et.al, [8] proposed two novel approaches providing reliable traffic information propagation: two directional data verification and time based data verification. The traffic condition is sent through message by means of two channels(spatially or temporally spaced). A receiving vehicle verifies the message integrity by inspecting whether the data received from both channels are analogous with the IP address security system.

Nikita Lyamin *et al*.[9] proposed a method for real-time detection of Denial-of- Service (DoS) attacks in IEEE 802.11p vehicular ad-hoc networks (VANETs). The study is focused on the "jamming" of periodic position messages (beacons) exchanged by vehicles in a group. Probabilities of attack detection and false alarm are anticipated for two different attacker models they are Random jamming model and ON-OFF jamming model.

A. Mudasir Malla et al.[10] proposed an effective solution for DoS based attack based on the principle of redundancy elimination mechanism that consists of rate decreasing algorithm and state transition mechanism as its apparatus. This elucidation basically adds a level of security to its already existing solutions of using various alternate options like channel-switching, FHSS, communication technology switching and multiple-radio transceivers to counter affect the DOS attacks. The proposed scheme enhances the security in VANETs without using any cryptographic scheme. The anticipated solution for DOS attacks not only eliminates these attacks but it also improves the efficiency of transmitting the emergency/alert warning messages among vehicular nodes which leads to avoidance of traffic accidents.

S. Roselin Mary, et.al [11] proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial-of- Service) attacks before the verification time. The algorithm detects the invalid requests and attacked packets to avoid the delay that occurs while processing invalid requests and packets. This minimizes the overhead delay for processing and enhances the security in VANET.

Aditya Sinha, et.al [12] Denial of Service (DOS) attack on network availability is presented with its severity level in VANET environment. A procedure to secure the VANET from DOS attack has been introduced and some possible solutions to overcome the attacks have been discussed. In their proposed solution author uses DSRC channels & Revocation techniques . As we know that, DSRC spectrum has seven channels which are used for sending different types of messages. In it, message is send or receives by their priorities . There are four classes; Class1 and Class2 carry safety information whereas Class3 and Class4 carry commercial messages. Class1 has highest priority and second highest priority is given to Class2, Class3 & 4 has low priority. Proposed solution is that, any node in a network will receive limited number of security messages at given timestamp. This makes network to guard itself from DOS attack.

K. Verma et.al,[13] presented a distributed and tough defense against DoS attacks where a malicious node forges a large number of fake identities, in the form of Internet Protocol (IP) addresses in order to disrupt the proper transferring of data between two fast-moving vehicles. In the anticipated approach, these bogus identities are analyzed through the medium of the reliable existing IP address information. Every vehicle frequently exchange beacon packets to claim their presence and to become aware of the neighbors. Each node repeatedly keeps and updates a record of its database by exchanging the information with the group of nodes. If a node detects some similar IP addresses in its record, these identical IP addresses are likely the evidences of a DoS attack. The authors designed a model for DoS prevention called IP-CHOCK that prove the significant potency in locating malicious nodes without the necessity of any secret information exchange or special hardware support. The results depict an encouraging detection rate

© 2015-19, IJARCS All Rights Reserved

that will be even enhanced whenever optimal numbers of nodes are forged by the attackers.

Aditya Sinha et.al [14] proposed Queue Limiting Algorithm that defines a limited capacity of each vehicle in a network for receiving safety message and defend against DoS attack without posing any security risk. The author classified the messages into four classes and assigned priority to each class for accessing different DSRC channels of communication. An OBU on each vehicle is provided with a scheduler to control internal collision and allow high priority messages to be transmitted before low priority messages but the capacity of messages is decided by the QLA algorithm.

Usha Devi et.al,[15] proposed a Request Response Detection Algorithm (RRDA) which is used to detect DOS attack after APDA. By this the DoS attack detection has been extended to multiple requests at a time in contrast to Attacked packet detection algorithm. Request Response Detection Algorithm has been implemented during the verification time. This method efficiently detects the attacks prior to the occurrence at node level. This increases the response time and maximizes the security in VANET.

IV. CONCLUSION

In this way we have studied the existing approaches for detecting denial of service attack in Vanet. The proposed techniques also provide ways to prevent the DoS attack, where each scheme deal with different capacity of messages to be detected. The techniques enhances security in Vanet in one or other way by decreasing overhead or delay or increasing availability and response time. In this paper we present DoS attack and their solutions. In future we intend to develop the system for detecting and preventing the Denial of Service attack and verifying it through simulation by applying our novel idea to protect the safe messages.

V. 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]. G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", WISTP 2008, LNCS 5019, pp.106-116.

[4]. 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.

[5]. M. Raya, J. Pierre Hubaux, "Securing vehicular ad hoc Networks", in Journal of Computer Security, vol.15, January 2007, pp. 39-68.

[6]. 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.

[7]. Isaac, J. T., Zeadally, S., &Camara, J. S, "Security attack and solutions for vehicular ad hoc networks". IET Communications Journal, 4(7), 894–903, 2010.

[8]. Baber, A., Soyoung, P.,&Cliff, Z. C. , "Secure traffic data propagation in vehicular ad hoc networks" International Journal Ad Hoc and Ubiquitous Computing, 6(1), 24–39,2010.

[9]. Nikita Lyamin, Agnus Jonsson, and Jonathan Loo, " Real-Time Detection of Denial-of-Service Attacks" in IEEE 802.11p Vehicular Networks IEEE Communications Letters, Accepted For Publication 1 1089-7798/13$31.00 _C 2013 Ieee.

[10]. Adil Mudasir Malla & Ravi Kant Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET" in International Journal of Computer Applications (0975 – 8887) Volume 66– No.22, March 2013.

[11]. 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.

[12]. Aditya Sinha, Prof. Santosh K. Mishra,"Preventing VANET From DOS & DDOS Attack" in International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 10- Oct 2013.

[13]. Karan Verma, Halabi Hasbullah, Ashok Kumar, "Prevention of DoS Attacks in VANET", in Wireless Personal Communications, November 2013, Volume 73, Issue 1, pp 95-126.

[14]. Aditya Sinha & Santosh K. Mishra, "Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack" published in International Journal of Computer Applications (0975 – 8887) Volume 86 – No 8, January 2014.

[15]. Usha Devi Gandhi &R.M Keerthana, "Request Response Detection Algorithm for Detecting DoS Attack in VANET" International Conference on Reliability, Optimization and Information Technology - ICROIT 2014, MRIU, India, Feb 6-8 2014.

© 2015-19, IJARCS All Rights Reserved