Approaches to Reduce the Impact of DOS and DDOS Attacks in VANET

Aaditya Jain¹, Divya Sharma²

¹ M.Tech Scholar, Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, India
² B.Tech Student, Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, India

ABSTRACT

Growing number of vehicles in use has ushered in the service to provide human and resource safety. The present trend calls for the application of technology to automate safety measures in road traffic and since has been known as Intelligent Transport System (ITS). Vehicular Ad Hoc Networks (VANETs) are envisioned to be used in practical ITS systems around the world. Privacy and Security have become an indispensable matter of attention in the VANET Networks, which is vulnerable to many security threats these days. One of them is the Denial of Service (DoS) attacks, where a malicious node forges a large number of fake identities, i.e., Internet Protocol (IP) addresses in order to disrupt the proper functioning of fair data transfer between two fast moving vehicles. In this paper various level of Denial of Service attack in VANET are discussed and various approaches that mitigate the impact of DOS, Jamming and Distributed DOS attacks are surveyed and a simple scheme is proposed to overcome DOS.

Keywords: VANET Security, DOS, Jamming, DDOS Detection.

1. INTRODUCTION

The growth of population is leading to an increase in the growth of transportation. Road accidents are more frequent in the present time than before because of high traffic. These days advancement of technology provides an intelligent transportation system. These transportation facilities are equipped with communication devices and internet facilities. Such facilities are based on fixed wired networks, mobile wireless networks and hybrid networks. The fixed wired infrastructural network faces a lot of problems such as access points, cell sites and a lot of digital equipment’s and cables. On the other hand a wireless network is easy to be installed and maintained [1, 2]. A wireless network is divided into two sections; one section is with infrastructure and another is without infrastructure. Such networks are called Mobile Ad Hoc Networks (MANETs) [3]. MANETs applied in intelligent transportation systems are called Vehicular Ad Hoc Networks (VANETs). VANET provides great flexibility, an efficient transportation service and also an efficient management of the transportation service but every network in modern day is susceptible to security attacks and VANET is no exception. A simple architecture of VANET is described in the figure1 which include all the essential components.

2. OVERVIEW OF VANET

Vehicular ad hoc network is a communication network for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications developed mainly for establishing an Intelligent Transport System (ITS) in road traffic for the purpose of prevention of accident, post-accident investigation, mitigation of traffic jams and other non safety applications. The three main components of VANET are on board unit (OBU), application unit (AU) and road side unit (RSU) [4]. Analogous to computer networks each vehicle is represented as a network node and OBU and AU sit on the node. The term “ad hoc” implies that these kinds of networks are self organizing and providing extemporaneous services. Although MANETs as in [5], the parent networks, are supposed to be non-infrastructure self establishing communication network but a road side unit is needed in VANET to facilitate internet connectivity and information collections for maintenance of network. Thus we can say VANET are hybrid networks whose design has its root in MANET but with few modifications to meet the requirement of feasible vehicular environment. It provides great flexibility, an efficient transportation service and also an efficient management of the transportation service but every network in modern day is susceptible to security attacks and VANET is no exception. A simple architecture of VANET is described in the figure1 which include all the essential components.
Fig -1: DOS Attack in V2V and V2I communications [7]

4. SOLUTIONS FOR DENIAL OF SERVICE ATTACK

Halabi Hasbullah et al. [8] work on Denial of Service (DOS) attack and its possible solutions in VANET which use the redundancy elimination mechanism. This solution basically adds a level of security to its already existing solutions of using various alternative options like channel switching, frequency hopping; communication technology switching and multiple-radio transceivers to counter affect the DOS attacks. Proposed scheme enhances the security in VANETs without using any cryptographic scheme.

Adil Mudasir et al. in [9] proposed solution to DOS attacks use more than one lines of defense as to counter attack its (DOS) effect. Due to various defense lines along with the decreasing message retransmission rate mechanism, the solution is good enough in handling any type of DOS attack. Apart from this it also controls network traffic congestion, broadcast storm and delay while propagating emergency warning messages among vehicular nodes even in absence of DOS attacks. In short, it efficiently handles both DOS attacks and network transmissions.

Amjad Khan et al. [10] works on “Minimization of Denial of services attacks in Vehicular Ad hoc networking by applying different constraints”. It improves the level of trust on the neighboring nodes instead of using some specialized hardware. The main aim of introducing different constraints is to improve the reliability of the node which will receive the data packets or acts as packet forwarder. and ultimately minimizing the possibility of jamming which is one of the major cause of DoS attack.

S. Roselin et al. [11] works on “Early detection of DOS attacks in VANET using Attacked packet detection algorithm (APDA)” which is used to detect the DOS (Denial-of-Service) attacks before the verification time. This minimizes the overhead delay for processing and enhances the security in VANET.

Usha Devi Gandhi et al. [12] works on “Request Response Detection Algorithm for detecting DoS Attack in VANET”. RRDA algorithm is used for the further verification of new requests that wants to join the network. This algorithm compares the previous validated data base with new requests and further reduces the false alarms by allowing only the validated nodes.

Ashok Kumar et al. [13] proposed a technique against DoS attacks. The malicious vehicles are identified with the help of consistent IP address information. The Beacon packets are periodically exchanged by all the vehicles to declare their presences and get aware of the next node. Each node keeps the record of it in their database. If a node observes that they have similar IP address in the network, then this IP addresses are identified as the Dos attackers. The security attacks are going to increase in the future. A DoS attack on the network is elaborated in this paper. The DoS prevention has been
developed called “IP-CHOCK” used for the prevention of DoS attack. There is no requirement for special hardware and without exchanging any secret information.

Karan Verma et al. in [14] proposed a IP-CHOCK (filter) based detection scheme for Denial of Service attack in VANET. Author suggests the bloom filter based detection method, which provides the availability of a service for the genuine vehicles in the VANET. This approach is used to detect and defend against the IP spoofing of addresses of the Denial of service attacks. This method is useful because it provides a secure communication as well as it also frees the bandwidth of the network. This approach requires a fewer resources and is easy to deploy. Results of this approach show that this method is efficient and effective to defend against and detect Denial of service attacks.

5.SOLUTIONS FOR JAMMING ATTACK

Nikita Lyamin et al. in [15] 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 platoon. Probabilities of attack detection and false alarm are estimated for two different attacker models i.e., Random jamming, ON-OFF jamming.

I. Azogu et al. in [16] proposed a Anti Jamming Strategy for VANET. Authors have studied the security issues that VANET can encounter and focused on jamming style DoS attacks. The paper measured the effeteness of defense mechanism against jamming and proposed a new direction to utilize RSU to make VANET defense more feasible. Authors defined a scheme called Hideaway strategy which uses the packet send ratio (PSR) to determine if a network is jammed and consequently all nodes should go into silent mode. The paper didn’t discuss detection and presumed it is out of the paper scope.

S. Babar et al. in [17] describe jamming attack behavior and modeling. It classified jamming attack into active and reactive jamming. Authors evaluated the impact of different type of jammers using NS2 simulation. The data was analyzed to show that reactive jamming is more difficult to detect than other attacks because of the intelligent behavior. The paper contribution suggested to use the behavioral modeling and analysis tools to understand jamming attacks behaviors to develop an efficient defense strategy.

A. Nguyen et al. in [18] studied jamming affect on VANET and proposed a new algorithm to detect jamming attack. The proposed detection method is based on the PDR and its diminution. PDR reduction is used to decide whether a network is jammed as soon as the change of PDR surpasses a threshold. Then warning messages will be issued with high priority. The basic concept is when a vehicle enters a jammed area the parameter Down PDR is considered to detect that it is jammed. That’s because when a vehicle is jammed its PDR is high but the rate of PDR decrease is great. Hence, the vehicle considered jammed and (state jam) will be true. This will lead to broadcast a warning message contains information of its state, direction, jammed time and jammed position. The paper provides a new scheme to detect jamming attack in VANET however; it only considers one type of jamming. In real world, jammers can use different strategies to block all communication and have more capabilities which were not considered in the paper.

6.SOLUTIONS FOR DISTRIBUTED DENIAL OF SERVICE ATTACK

Minda Xiang et al. in [19] proposed a method called protection node based strategy to remove the effect of DOS or DDOS attacks in VANET. Hierarchical network architecture is adopted to divide the nodes into multiple levels. Lower level nodes used to protect the higher level nodes and lower level nodes are protected by the same level neighbouring nodes. The node selected at the lower level to protect the higher level node is considered as Local Protection Node (LPN). When an attack route is built by the attacker, the very first hop or node from the source is selected as the protection node sometimes called as Remote Protection Node (RPN). RPN filters the false or rough packets at the source side coming from the source node and a message called ANM (Attack Notification Message) is broadcasted into the network to inform all other nodes about the malicious node. Thus every node in the network drops the packet coming from the malicious node. So this technique reduces the effect of DDos attack, but it takes time for the whole process for mitigation.

Ayoniya Pathre et al. in [20] proposed a novel traffic congestion detection and removal scheme for defence against DDOS attack in VANET. It defines the misbehavior of DDOS attack and the road side unit (RSU) mechanism for detection and removal purpose. The number of vehicles that receives the false packet is affected from the attack called as abstract node. The main aim of DDOS attack is to prevent legitimate access to any resource. So it provides RSU mechanism for prevention from this type of attack. RSU monitors the communication between the vehicles. It identifies the vehicle or the attacker
vehicle that injects the false information packet into the network and then it blocks the activity of the attacker node and manages the traffic schedule affected by the attacker.

Tamil Selvan et al. in [21] proposed a new cracking algorithm for preventing DDoS attack in the wireless network. It maintains a status table that keeps the IP address of the users and their status. The algorithm consists of three parts. Packet Filter that works by inspecting the packets which transfers between computers on the internet, MAC Generator that distinguishes the packet that contains the genuine source IP address from those who contains fake address and IP Handler which describes when the attacker uses genuine address, the proxy server use the deflect Round robin technique to collect the address from the client side. It also takes into account that if the user is sign in address for the first time then it is genuine user. If it is for two or more times then it is considered as normal user. If the user signed in for five or more than five times then it is considered as Attacker.

7. PROPOSED SCHEME

This scheme is based on two approaches that described in paper [11, 12]. For detection of DOS attack they use mechanism namely Attacked Packet Detection Algorithm (APDA) and Request Response Detection Algorithm (RRDA). In APDA the malicious attacker node is detected during the initial verification phase. The node which is sending request messages at more than 25 packets per second has been detected as malicious. Then RRDA detects all the verified vehicles. In our proposed scheme, we have tried to reduce the impact of DOS by limiting the request time communication interval between the two vehicles. The normal time of sending the request messages and receiving the same message is recorded. The legitimate vehicles which do not cause DOS & DDOS in the network usually communicate for a short interval of time whereas the attacker node will send request messages for a longer interval of time. So if we limit the communication interval for request messages then the impact of DOS can be reduced to a significant amount, at the same time the vehicle which is trying to communicate for longer time interval can be detected easily as malicious attacker.

8. CONCLUSION

VANET is a kind of network that provides consistent communication to the vehicles in some described range. The adaptable nature of network brings problems related to traffic safety and security. This paper surveyed various approaches that deal with VANET to overcome DOS type attacks in it. Also a simple but effective approach is proposed that detects the malicious nodes in the network which is responsible for the occurrence of Denial of Service attack. Even though, much research has been conducted to defend VANET against DOS attacks, there is not a perfect solution that can be used effectively to solve DOS, Jamming and DDOS related problem in Vehicular Ad Hoc Network. Hence, it is still an open challenge in the case of VANET and much research are still undergoing.

Acknowledgment

I would like to express my deep sense of respect and gratitude towards “Dr. Bala Buksh”, Professor Department of Computer Science & Engineering, who has been the guiding force behind this work. Without his unconditional support it wouldn’t have been possible.

REFERENCES


AUTHORS

Aaditya Jain is currently pursuing M.Tech in Computer Science & Engg. from Rajasthan Technical University, Kota (Raj). He received his B.E. degree in Computer Science & Engg. from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (MP) in 2013. He published research papers in various International and National Journals and Conferences. His areas of interests are Network Security, Cryptography, and Wireless Ad Hoc Networks.

Divya Sharma is currently pursuing B.Tech final year in Computer Science & Engg. from Rajasthan Technical University, Kota (Raj). Her area of interests are Vehicular Ad Hoc Networks and Information Security.