International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May- June, 2018)

A Co-operative Neighbor Approach (C.N.A.) to Detect Sybil and DoS Attack in Vehicular Ad-hoc Network

Shailendra Singh Bhadoriya, Prof. Vimal Shukla
Department of Information Technology,
K.N.P. College of Science & Technology,
Bhopal, Madhya Pradesh, India

Abstract— *Vehicular ad hoc network (VANET) has attracted the attention of many researchers in recent years. It enables value-added services such as road safety and managing traffic on the road. Security issues are the challenging problems in this network. Denial of Service with Sybil attack is the serious security threat, in this attack attacker sends bulk of false messages to the target node from forge identities. One of the main purposes for creating invalid identities is disruption in detection of attacker in network. In this paper we propose a scheme which is able to protect nodes from "DoS along with Sybil attack", we proposes two modules one for DoS attack and second for Sybil attack incoming packet first go through the Sybil detection module and then DoS detection module. We used NS-2 simulator for result calculation.*

Keyword —VANET, DoS Attack, Sybil Attack, NS-2.

INTRODUCTION

Vehicular ad hoc network (VANET) is a type of mobile ad hoc network (MANET) employing wireless communication for vehicle to vehicle communication (V2R communication mode) and vehicle to fixed infrastructure called Road Side Unit communication (V2R communication mode). These communications are through two devices called the Roadside Unit (RSU) as the fixed infrastructure and onboard unit (OBU) installed on the vehicles. The Dedicated Short Range Communications (DSRC) band has been allocated at 5.9 GHz for V2I and V2V communications. VANET is a comprehensive response to the increasing requests for safety services in Intelligent Transportation Systems (ITS). Vehicular communications can be used in a wide range of applications are related to the safety, traffic management, and passenger comfort. The main applications in each domain are stated in [1].

It is obvious the performance of VANET applications is depending on the reliability of the received messages. Any malicious behavior, such as injecting false information, modifying and replaying disseminated messages, discarding routing packets in the network and impersonation has irreversible effects on people's lives. Moreover, drivers show prime interest in privacy to protect their private information leading to unique identification in the network. So, it is clear that security and privacy preservation are two critical challenges for VANET deployment in real world. One of the well-known harmful attacks in VANET is Sybil attack. Sybil attack was first described by Douceur [2] in peer-to-peer networks. In this attack a malicious vehicle claims to be several vehicles by creating multiple dummy entities (Sybil entities) to use them simultaneously or separately in the network. The Sybil attack is harmful for network topologies, connections, network bandwidth consumption, and there are some threats even related to human life [3]. There are some protocols for secure communication and Sybil attack detection in VANET. We stated a comprehensive comparison of different methods in [4]. Proposed methods for Sybil attack detection have some disadvantages include: depend on some factors for a high detection rate and fail to detect all of entities for some protocols such as Footprint [5], some of them do not hold other security requirements such as privacy [6] [7], and the best case called P2DAP [8] can detect the attack centrally by the Center of Authority (CA) or RSU by a heavy overhead on the CA. The overhead of P2DAP can be reduced by reducing the rate of attack detection. Therefore, in this paper, the Sybil attack detection is considered with the features: preserving the privacy of drivers, detection of Sybil entities, having an acceptable detection time and possibility for attack detection by each vehicle receiving messages from other vehicles in the RSU's group. The rest of the paper is organized as follows. Section II describes the characteristics of vehicular ad hoc network. Section III describes the security threats in vehicular ad hoc network followed by Denial of Service (Dos) Attack section V describes about proposed methodology followed by simulation results in section VI. Finally we conclude the paper in section VII.

CHARACTERISTICS OF VANET

The vehicular network has some unusual kind of performance and features that recognizing them from different sorts of networks. Compare with the different network this network have an exclusive and stimulating characteristics given below:

2.1 Unlimited transmission power: power problems are fundamental oblige yet in the ad-hoc device on account of this network node/vehicle give constant and adequate energy to process and specialized devices for doing another assignment.

2.2 Computational limits high: Functioning vehicles may have a most important computing ability that done via circuit and sensor within vehicle with ample power, sensing abilities.

2.3 Predictable mobility and communication: In VANET where the mobility of vehicle is so tough to measure, vehicles have most expected movements, which are restricted to roadways. The Roadways data are

frequently displayed from situating frameworks and map depending tools for example GPS.

2.4 High mobility: vehicular network perform very dynamically. Speed In the event that takes the case of expressway where moderately speed of about 190-230 Km/h canaries during density 1-2 vehicle in 1 Km on the opponent where comparative speed about 65-70 Km/h and in rapid hours particularly very high node density.

2.5 Partitioned network: vehicular network may often divide and dynamic movement behavior can result in enormous inter vehicle crevices in inadequately occupied scenarios in many general clusters of nodes.

2.6 Connectivity and network topology: Scenarios in vehicular network differ from site to site. When a vehicle moves and alters their location continually in dynamic scenarios. Connection between nodes detached and connect many times because network topology alters frequently [9].

SECURITY THREATS IN VANET

There are numerous sorts of attacks, which may interrupt the VANET system and its security. Each type of attack principally affects many services within system.

3.1 Denial of Service (DOS): It is a simple and harmful attack. This attack utilizes other identity and stops another services or it can also block the communication service of VANET.

3.2 Fabrication Attack: This attack fabricates or alert the message holds and transmits the wrong information within network. It changed the information or data and transmits wrong information clam to another one.

3.3 Interception Attack: This is like a man in middle attack. In this attack attacker is middle in network, interrupts the information among them, and transmit to another destination.

3.4 Eavesdropping Attack: This is most common attack that completed secretly. This is inactive in nature, performed upon network layer, and very hard to observe. It achieves the control of secrete information for example vehicle identity or site or other secrete information.

3.5 Impersonate Attack: The attacker in this attack is impersonating to another. As simply some accidents are happen on highway, at this time attacker impersonate to numerous and decline.

3.6 Sybil Attack: This attack sends much Information with several harmful characters from single vehicle node to another. This is constantly conceivable with the exception of the great circumstances and the probability of source equality and control among entities [9].

DENIAL OF SERVICE (DOS) ATTACK

In this sort of attack, the attacker prevents the availability of the network by jamming the channel or makes some difficulties in network accessing for nodes. The primary goal of the attacker is to corrupt the execution of a network by preventing a legitimate user from accessing the network resources and the network services [10].

The above figure demonstrates three legitimate users A, B and D where C is an attacker. The attacker transmits many safety messages as compared to the genuine users. Safety messages have greater priority than other messages. So, most of the bandwidth of the victim is consumed by an attacker that creates object node incapable to reply to genuine packets [11].

Three levels of DOS attacks are following.

1) Basic Level: Overwhelm the Node Resources there is a common level attack in DOS; attacker main aim is to node resources overwhelm such that the nodes cannot achieve numerous significant and required tasks. The node becomes busy and uses each resource to verify the data.

2) Extended Level: Jamming the Channel Here DOS attack where attacker jams in a specific channel, hence not permitting other users to access the network.

3) Distributed Denial of Services [11]: DDOS attacks are harmful in the vehicular atmosphere because the mechanism of the attack is in disseminating way where the effect is scattered in the network. In this type of attack, the attackers launch attacks from different locations. There are two conceivable cases as take after.

PROPOSED METHODOLOGY

Attacker sends multiple messages to the victim vehicle through DSRC channels as well as it may also use spoofed IP addresses for this. Because safety massages has highest priority over other massages they use all the bandwidth of the victim and messages come from different IP address also create problem to detect attack, thus victim is unable to communicate with other vehicles and denial of service with Sybil attack is occur. Our protection scheme works on that, in our scheme each vehicle keeps its neighbor's IP address in a table at regular interval and after that it checks all incoming traffic, if coming packet is matched from IP present in a table than data will go through DoS detection module and then en-queue in a queue, otherwise new queue will be created with upper bar for receiving a limited number of massages and number of new queue shall be equal to the count in Node Identity Table. By this way we shall able to protect network from Denial of Service with Sybil attack. Our Limited Queue Algorithm module create receiving limitation of massages as well as new queue allocation, this prevent the node from DoS attack. When DoS attack happen all the internal queues of OBU are filled with messages and all the resources of OBU

are busy in processing of these messages so communication with other vehicle. But if only limited numbers of messages are received from sender, OBU will perform its task quite easily.

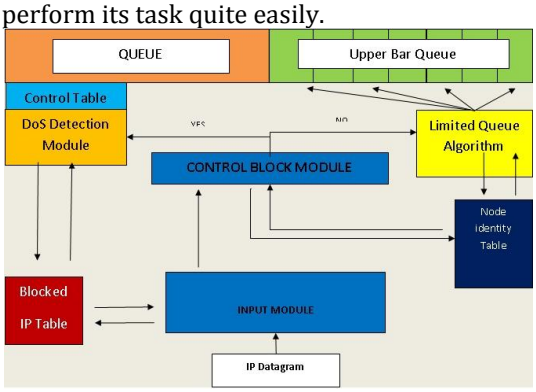

Figure 1 Logic Diagram

SIMULATION & RESULTS

Performance of CNA (Co-operative Neighbor Approach) approach is measured on the basis of Throughput, end-to-end delay and Packet delivery ratio. In this section we are comparing our approach with two existing approaches on the basis of time. Previous approaches are IP-trackback and other one is referenced broadcast synchronization. Simulations parameter table is as follows:

Parameter	Values
No. of Nodes	20
Node speed	60 m/sec
Simulation Time	400
Environment Size	1000 x 1000 meter
Packet Size	500 KB
Antenna Model	Omni-directional Antenna
Packet Type	TCP/UDP
Traffic Type	CBR
MAC Layer	IEEE 802.11p
Visualization Tools	NAM

Simulation Parameter

Simulation graphs are as follows:

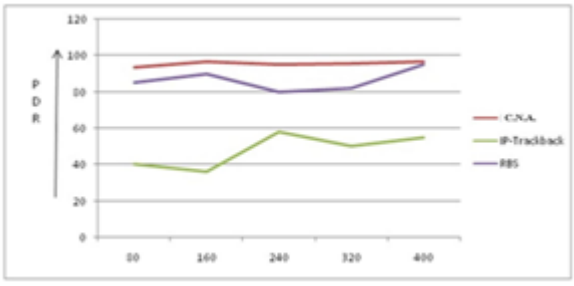

Figure 2 Comparison graph on the basis of PDR

In the Figure2 Horizontal plane represents time in seconds & vertical plane represents packet delivery in percentage. Red line represents our proposed approach "Co-operative Neighbor Approach Algorithm" or CNA in the packet delivery ratio graph, blue line represents Reference Based Synchronization in the packet delivery ratio graph and green line represents IP-Trackback in the packet delivery ratio graph.

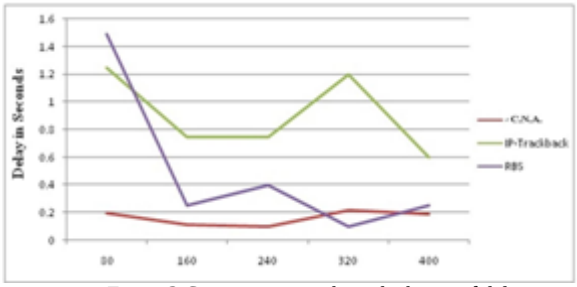

Figure 3 Comparison graph on the basis of delay

In the Figure3 Horizontal plane represents time in seconds and vertical plane Delay in seconds. Red line represents our proposed approach (CNA) in the end-to-end delay graph, blue line represents Reference Based Synchronization in the end-to-end delay graph & green line represents IP-Trackback in the end-to-end delay graph.

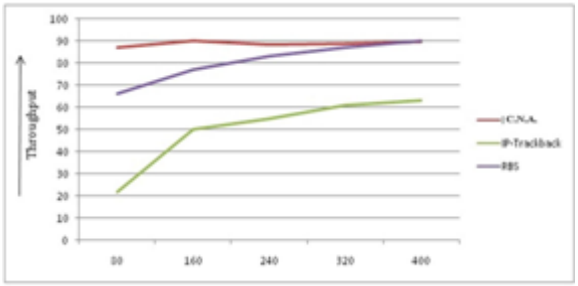

Figure 4 Comparison graph on the basis of throughput

In the Figure 4 Horizontal plane represents time in seconds and vertical plane shows throughput in bytes. Red line represents our proposed approach (CNA) in the Throughput graph, blue line represents Reference Based Synchronization in the Throughput graph & green line represents IP-Trackback in the Throughput graph.

CONCLUSION

CNA or Co-operative Neighbor Approach scheme is able to protect VANET in concern of the security threats such as union of Sybil and DoS attacks. Dependence of this work is on the node's faith on its Neighbor Nodes for communication; by this we can protect VANET from fake IP problem. The proposed CNA (Co-operative Neighbor Approach) model is work into two sections: one is for the known Neighbor Node nodes and the other is for the new nodes coming to its surroundings. For known Neighbor Nodes model implements DoS detection scheme and for new nodes, limited queuing is to be used. This approach is local and simple so it can be easily implemented in a network. Results of C.N.A. are promising.

REFERENCE

[1] Alimohammadi M., Pouyan A. A.; Vehicular Ad Hoc Networks: Introduction and a proposal for vehicle positioning; 13th International conference on Traffic and Transportation Engineering; 2014.

[2] Douceur J. The Sybil attack. Proc. of International Workshop on Peerto-Peer Systems 2002; 251–260.

[3] Isaac, J. T., Zeadally, S., & Camara, J. S. Security attacks and solutions for vehicular ad hoc networks. Communications IET 2010; 4(7): 894
[4] Alimohammadi M., Pouyan A. A.; Defense Mechanisms against Sybil Attack in Vehicular Ad hoc Network, Security and Communication Networks, John Wiley & Sons, 2014.
[5] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. IEEE Transactions on Parallel and Distributed Systems 2012; 23(6): 1103-1114.
[6] Xiao, B., Yu, B., & Gao, C. Detection and localization of Sybil nodes in VANETs. Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks 2006; 1-8.
[7] Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. Lightweight Sybil Attack Detection in MANETs. IEEE, Systems Journal 2013; 7(2):36-248.
[8] Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks. Selected Areas in Communications, IEEE Journal 2011; 29(3): 582-594.
[9] Jaydeep P. Kateshiya and AnupPrakash Singh," Review To Detect and Isolate Malicious Vehicle in VANET", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 2, February 2015, pp: 127-132.
[10] Komal Rani and Meenakshi," Prevention Of Denial Of Service Attack On Dynamic Source Routingvanet Protocol", IJRET: International Journal of Research in Engineering and Technology, Volume: 04 Issue: 09 | September-2015,pp: 251-255.
[11] Halabi Hasbullah, Irshad Ahmed Soomro and Jamalullail AbManan," Denial of Service (DOS) Attack and Its Possible Solutions in VANET", World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol:4, No:5, 2010