Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack

Aditya Sinha
M.Tech. Scholar
V.N.S. Group of Institutions
Bhopal, India

Prof. Santosh K. Mishra
C.S.E. (Department)
V.N.S. Group of Institutions
Bhopal, India

ABSRACT

Vehicular ad hoc network (VANET) is an important component of Intelligent Transportation Systems. In VANET, active safety systems is seems as the main benefit of it, in which vehicles are exchanging safety messages to increase the passenger safety on road. At the present time, vehicles are exposed to many security threats; and for the security, availability of network is must be obtained at every time. The availability of the network is extremely needed when a vehicle sends any safety information to other one. In this regard, DoS attacks are very dangerous in VANET because they adversely affect the network availability. One of them is oppress the node resources by flooding of messages to the victim vehicle; which is a common form of Denial of Service (DoS) attacks, in which a malicious node sends a large number of (False) safety message to the victim node. In this paper, an efficient method is proposed to defend against DoS attacks. According to our method each vehicle in a network has limited capacity of massage (safety message) receiving, without having any security risk and this limited capacity is defined by our (QLA) algorithm. This is a very simple method and can be easily deploy in network. Simulation results show that the approach is very effective and efficient against denial of service attack in VANET.

Key Words

VANET, DoS attack, DSRC, ITS, OBU

1. INTRODUCTION

For improving the safety, security and efficiency of the transportation system, Intelligent Transportation Systems (ITS) have been introduced. It enables new mobile applications and much kind of services for traveling public. VANET is recognized as an important component of ITS [1]. It consist the field of inter-vehicular communications (IVC), including both vehicle-to- roadside communications (V2R) and vehicle-to- vehicle communications (V2V). The ITS architecture provides a framework for the much needed overhaul of the highway information system infrastructure. The immediate impacts include alleviating the vehicular traffic congestions and improving operation management in support of public safety goals, such as collision avoidance. Equipping vehicles with various kinds of on-board sensors, and V2V and V2R communication capabilities will allow large-scale sensing and decision / control actions in support of these objectives. These systems provide an extended information horizon to warn the driver or the vehicle of potentially dangerous situations at an early stage. VANET applications have been broadly categorized into non-safety and safety applications. These (Safety) applications are very important in nature as these are directly related to users and their lives. It provides warning and important information to drivers such as post-crash notification on a particular road [2]. VANET is concern with safety of human life while these people are moving on the roads. On the other hand non-safety applications are to comfort the drivers and passengers, and to improve the traffic system. Parking availability, traveling map, and weather information are the examples of these applications. To support the above safety and non-safety applications, allocation of 75 MHz in the 5.9 GHz frequency band licensed for DSRC in North America is done, which supports seven separate channels, may also enable the delivery of rich multimedia contents to vehicles at short- to medium-range via either V2V or V2R VANET links [3] [4].

In spite of the ongoing industrial and academic research efforts on VANET, many research challenges remain. From the network perspective, security is one of the most significant challenges. Vehicle safety applications are among the major drivers for VANETs. Where people’s lives are at stake, it is mandatory to secure VANETs against abuse. Denial-of-service (DoS) attacks are one of the most serious problems. These attacks are very dangerous for safety applications and if it affects the safety channel then users are unable access network which causes an accident or any unwanted event.

In this paper, we propose a new scheme for VANET, to protect it from the DOS attack. This scheme works on the safety channels of DSRC to protect the life of drivers on road. In the rest of this paper, we first give a brief background on DoS attack in Section II. Preliminaries in Section III, we present our protection scheme in section IV, followed by simulation and performance analysis in Section V. Conclusions is given in Section VI.

2. BRIEF BACKGROUND OF DOS ATTACK

A Denial of Service attack can be understood by an explicit attempt by attackers to prevent legitimate users of a service from using that service [5]. A DoS attack occurs when multiple flooding packets come to the targeted vehicle in small amount of time (e.g.: 1lakh packets in 1microseconds) which flood the bandwidth or resources of a targeted vehicle.

2.1 Flooding Attack:

Flooding attacks overwhelm the resources of victim’s vehicle with a huge amount of network traffic and end up with long queues, saturated network links and processors with workload [6]. Examples of such attacks are as follows:

2.1.1 Smurf Attack:

In this attack, a large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a network using an IP Broadcast address. Most vehicles on a network will be in their default settings and they respond to this by sending a reply to the source IP address. If the number of vehicle on the network that receive and respond to these packets is very large, the victim's vehicle will be flooded with traffic. This can slow down the victim's vehicle to the point where it becomes impossible to work on.

2.1.2 Ping Floods:

In this type of attack, the attacker overwhelms the victim with Ping (ICMP Echo Request packets). This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. It is most successful if the attacker has more bandwidth than the victim. The attacker hopes that the victim will respond with reply packets, because of that victim consuming both outgoing bandwidth as well as incoming bandwidth. Due to this the target vehicle’s processing is slow down and it consumes enough of its CPU cycles, to notice a significant slowdown.

3. PRELIMINARIES

3.1 Data access in VANET

In VANET, there are two different approaches for accessing data. The first approach is dependent on the road side infrastructures. Each vehicle indirectly communicates with other vehicles or servers via base stations or via access points. The second approach is based on vehicle-to-vehicle communications, by which vehicles can communicate with their router or multi-router neighboring vehicles, for information sharing (or exchanging). Many studies have shown that the first approach (infrastructure based communication) is expensive and not convenient due to the high cost as well as low bandwidth of the cellular communication, along with the limited access opportunity and the infrastructure deployment constraint in the access point based communication. The vehicle-to-vehicle approach, however, is more flexible and cost effective in VANETs, particularly in highway or rural areas [7].

3.2 Message priorities of VANET communications

The DSRC spectrum is divided into seven 10-MHz wide channels. Control messages are communicated through channel number 178, which is generally restricted to safety communications only. The two channels (Ch 172 & Ch 184) at the edges of the spectrum are reserved for future advanced accident avoidance applications and high-power public safety communication usages. The remaining channels are service channels and are available for both safety and non-safety applications. There are four internal queues per OBU (On-Board Unit) for the four different priority message classes, & each message will be queued in a queue according to its priority.

Table1. Example of VANET Applications

Applications	Priority	Network Traffic Type
Life-Critical Safety	CLASS 1	Event
Safety Warning	CLASS 2	Periodic
Electronic Toll Collection	CLASS 3	Event
Internet Access	CLASS 4	Event

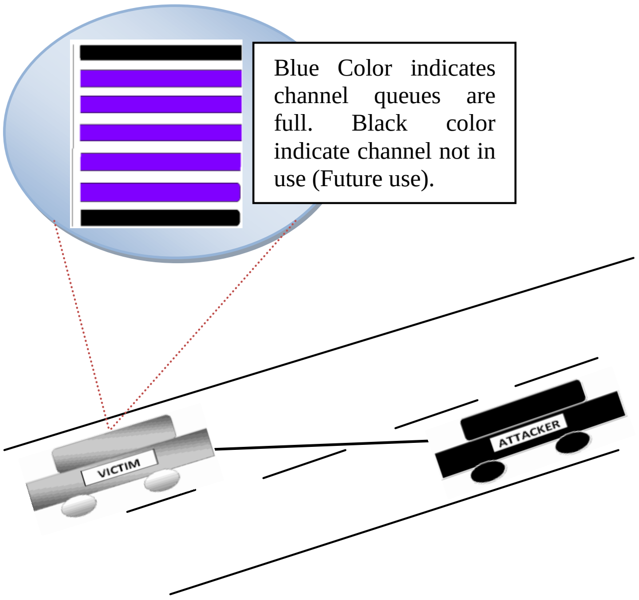
Class 1 message (Table 1) will always access the channel 178 with the highest priority, if the channel 178 is full, then it will access either of the channels 174, 176, 180, or 182 (Table 2) with the highest priority; Class 2 message will always access the channel 178 with the 2nd highest priority, if the channel 178 is full, then it will access either of the channels 174, 176, 180, or 182 with the 2nd highest priority; Class 3 and Class 4 message cannot access the channel 178, and it will access channels 174, 176, 180, or 182 with the 3rd or 4th priority respectively. Internal collision is controlled by a scheduler in OBU. The scheduler will allow higher priority messages to be transmitted before lower priority messages [8].

Table2. DSRC Channels and Classes of message priority

DSRC Channels	Message Priority Classes
178, 174, 176, 180, and 182	Class 1
178,174,176,180, and 182	Class 2
174, 176, 180, and 182	Class 3, Class 4

3.3 System Model

Before presenting the prevention mechanism some introduction is needed about the working of VANETs and how DoS attack will restrain communication between vehicles (Fig. 1). In VANET each vehicle is equipped with OBU and for communication it uses DSRC channels. OBU in vehicle is an intelligent device having sensors, modem, processing unit, and storage capacity [8]. Vehicles can communicate with infrastructure (access point) as well as other vehicles. Where access points are available vehicle send their information regarding crash, collision, and other information to it and AP (Access Point) forward this information to other vehicle that are intended to go that place [9]. Some places where AP is not available (like highways or rural areas) vehicle pass the information to each other. But when attacker comes into frame things will be uncontrolled. Attacker sends enormous amount of (false) safety massages to the victim node. Hence all the channels of DSRC are filled with CLASS 1 messages, thus victim node is unable to communicate with other vehicle and it may be prone to accident or crash.



Blue Color indicates channel queues are full. Black color indicate channel not in use (Future use).

Figure 1 DoS attack, where attacker car sends enormous messages to the victim. Thus; all the channels of victim are filled by the messages. Show in circle.

4. PREVENTION MECHANISM

Attacker sends multiple (false) safety messages to the victim node through DSRC channels. Because safety massages has highest priority over other massages they use all the bandwidth of the victim, thus victim is unable to communicate with other nodes and denial of service is occur. Our protection scheme (QLA) works on that, in our scheme each vehicle have some upper bar for receiving a limited number of safety massages. Thus, receiving limitation of safety massages will protect the node from DoS attack. How? 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. But if only limited number of messages (safety message) come from sender, OBU will perform its task quite easily.

For finding the upper limit of message (safety message) receiving, vehicle sends a hello packet in the network at regular time interval and wait for its reply. When reply come, OBU counts the number of reply; we assume it "Y". We know that class 1 safety massage are generate when any event has take place so at the small time interval if we assume that maximum 10 events have been happen (Max probability). Now compare "Y" with following condition:

If (Y =< 10); where 10 is number of replies

Then receiving (safety message) limit is equal to (Y*10).

Else

If (10< Y =< 50); where 10 & 50 are number of replies.

Then receiving (safety message) limit is (2*Y)

Else

If (50<Y=<max); where "max" is maximum number of replies.

Then receiving (safety message) limit is (Y*1)

This mechanism is able to protect vehicle from DoS attack.

5. SIMULATION SETUP

In this section we present our simulation and analysis to show the performance results of the proposed Queue Limiting Algorithm. There are four way highways and they have two lines each direction. As shown in Figure 2, there are four crossings through which vehicles may cross each other in highway. To have a fixed number of vehicles in the simulation, assume that the exit vehicles will enter the highway at the nearest highway end and immediately start to send messages. Each vehicle in the simulation can initiate queries for safety message. A simulation has been carried out to evaluate the performance of the proposed method.

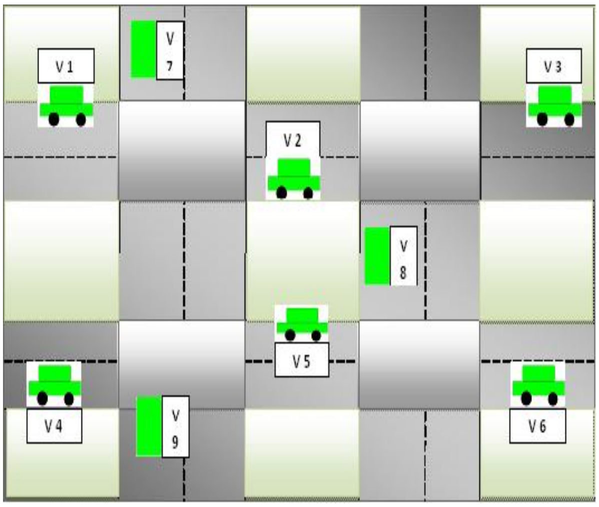


Figure 2 Simulation Scenario

Each vehicle is first randomly scattered on one intersection along the paths. Each vehicle is driven at a randomly fluctuating speed along different streets. In the case, there is no RSU present so all the communication is done between vehicles, other simulation parameters are listed in Table 3.

Table3. Simulation Configuration

Parameter	Default Value
Simulation Area	1000m * 1000m
Simulation Time	300 minutes
Number of vehicles	16
Communication range	400m
Node Speed	60km/hr
Visualization Tool	NAM
MAC layer	IEEE 802.11 p

The simulation results are displayed in the NAM file and from the trace file routing parameters were obtained. For the performance evaluation of the routing protocols, some parameters have been used in the TCL file for measuring the efficiency of vehicle-to-vehicle communication. The study of these parameters is analyzed by the NS-2.31 Trace file. IEEE working group has introduced a new PHY/MAC layer amendment to the 802.11p standard, which is designed for vehicle-to-vehicle and vehicle-to-infrastructure communication only.

Performance of our approach is measured, on the basis of routing overhead, message receiving and packet delivery ratio. There are three different conditions on which we measure routing overhead, message receiving and packet delivery ratio. Those three conditions are a) Normal VANET condition, b) Time when DoS attack happen, c) Time when protection algorithm is applied. Simulation graphs are as follows:

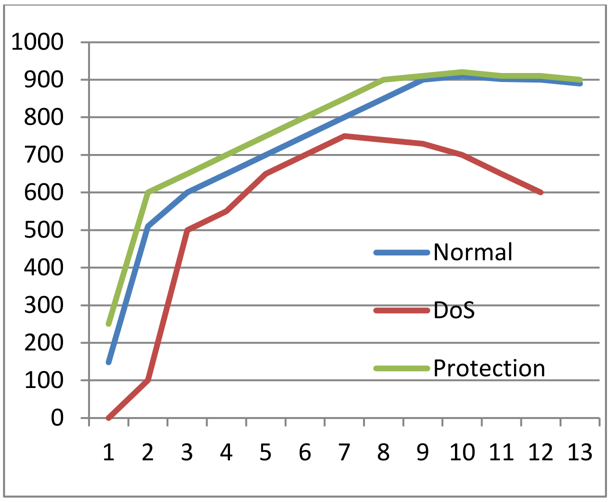


Figure 3 Graph-Packet delivery ratio of Normal, DoS, & Protection condition

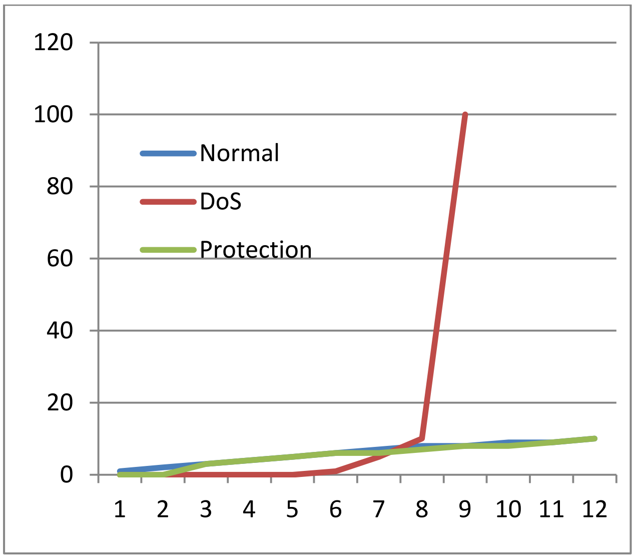


Figure 4 Routing overhead graph, shows comparability of Normal, DoS, & Protection Condition.

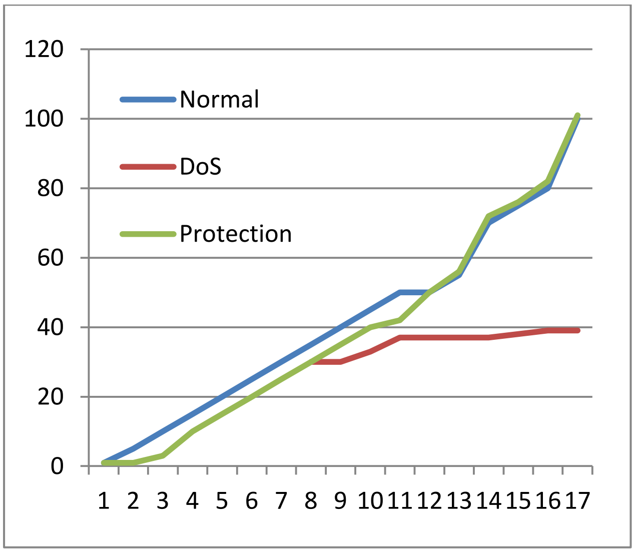


Figure 5 Message receiving graph

6. CONCLUSION

Denial of Service attack is very dangerous in VANET because it directly affects the driver's life. For preventing VANET from this attack we present a new method called Queue Limiting Algorithm. In which, each vehicle have limited capacity of message (safety message) receiving and this capacity is decided by our algorithm. Our Simulation results shows that the proposed approach is capable to prevent VANET from DoS attack and make the communication as easy as normal condition while attack happens.

7. REFERENCES

[1] U.S. Department of Transportation, Intelligent Transportation Systems (ITS) Home, http://www.its.dot.gov/index.htm

[2] J. Jakubiak, Y. Koucheryavy,"State of the Art and Research Challenges for VANETs", 5th IEEE Consumer Communications and Networking Conference, 10-12 Jan. 2008, pp. 912-916.

[3] Dedicated Short Range Communications (DSRC) Home. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[4] Crash Avoidance Metric Partnership, "Vehicle Safety Communication Project Final Report", available through U.S. Department of Transportation.

[5] Willke, T.L., P. Tientrakool, and N.F. Maxemchuk, A survey of inter-vehicle communication protocols and their applications. Communication Survey & Tutorials, IEEE, 2009. 11(2): p. 3-20.

[6] Raymond, D.R. and S.F. Midkiff, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. Pervasive Computing, IEEE, 2008. 7(1): p. 74-81.

[7] Van der Merwe, J., D.S. Dawoud, and R. Peplow. Vulnerability windows in vehicular communications. In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on. 2009.

[8] Yi Qian; Kejie Lu; Moayeri, N., "A Secure VANET MAC Protocol for DSRC Applications," Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, vol., no., pp.1, 5, Nov.302008-Dec.42008.

[9] Mishra, T.; Garg, D.; Gore, M.M., "A Publish/Subscribe Communication Infrastructure for VANET Applications," Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on , vol., no., pp.442,446, 22-25 March 2011
doi: 10.1109/WAINA.2011.87