A Novel approach for Detection of Distributed Denial of Service attack in VANET

Pooja Bansal
M. Tech Student
Lovely Professional University
Phagwara, Punjab 144411

Shabnam Sharma
Assistant Professor and
*Research Scholar
Lovely Professional University
Phagwara, Punjab 144411

Aditiya Prakash
Lecturer
Lovely Professional University
Phagwara, Punjab 144411

ABSTRACT
Vehicular ad hoc Networks (VANETs) are new upcoming technology providing appropriate communication to the vehicles as well as passengers with no fixed infrastructure. In today's life, maintaining the heavy traffic is very difficult that gives bad impact to roads safety and throughput of network. Researchers have done a lot of work in VANET, but still the security got affected from malicious attacks. To maintain the availability, network must be available at the time when vehicles interact with each other. This paper introduces a scheme to detect DDoS attack, as this attack gives adverse effect to network availability. According to our scheme, a Local Protection Node (LPN) is selected from the hierarchical architecture. PDR value and the threshold value has been compared, when these two values become equal a Monitor mode message is to be transmitted by LPN to other vehicles in the network for the purpose of sensing. Any vehicle that injects large number of false packets will be detected as an attacker and thus packets from evil node will be discarded. The proposed scheme is very simple and efficient.

General Term
Security

Keywords
Availability, DDoS detection, LPN, RSU, VANET

1. INTRODUCTION
Rapid use of VANET has increased day by day as it enhances the protection of passengers. VANET is an ad hoc network so it also have the properties of self-organize, adaptive and temporary network. In VANET nodes are basically vehicles they itself act as a source, destination and router to forward the data packet from source to destination. VANET consists of Vehicles and Road Side Units (RSU), communication units located aside the road that connects with the application server and the trust authority. Communication facilities in VANET can be configured in three ways viz. Inter-Vehicular communication, Vehicle-to-roadside and Routing Based Communication [9].

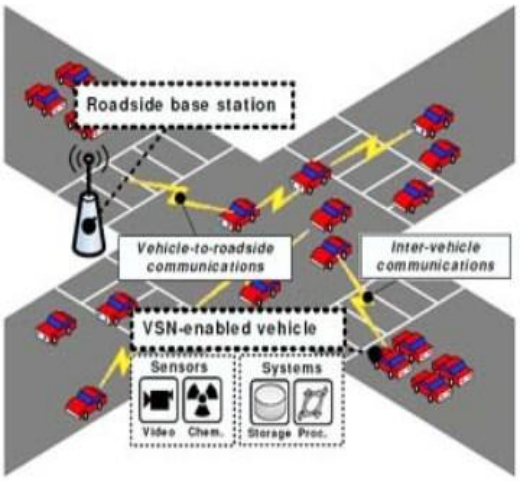

Fig 1. Communication in VANET

The Inter-Vehicle communication configuration uses multi-hop multicast to transmit traffic information over multiple hops to a group of receivers. The communication takes place between vehicles. In Vehicle-to-Roadside communication, vehicles communicate using RSUs. The configuration represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the network. In Routing Based Communication, it is a multi-hop unicast where a message is forwarded in a multi-hop fashion until the vehicle carrying the desired data is reached.

The main components of VANET are:

On Board Units (OBUs): These are the communication devices mounted on vehicles to facilitate communication with other vehicles and roadside units. They enable short-range wireless ad hoc networks to be formed.

Roadside Units (RSUs): They used to facilitate communication. The number and distribution of RSUs depends on the communication protocol to be used.

Trusted Authority (TA): They are third party entrusted with the job of certificate generation, distribution and revocation.

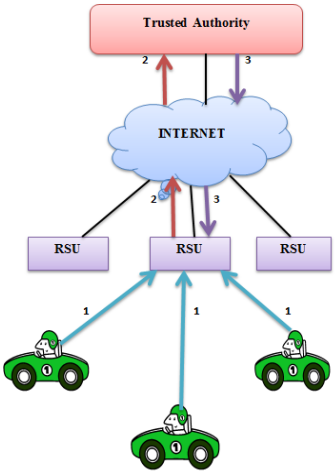

Fig 2: VANETs Architecture

1. Vehicle request RSU to issue certificate.
2. RSU forward to TA.
3. TA sends certificate to RSU.

Many researchers have done their research in VANET network regarding routing protocols, security issues. VANETs are vulnerable to kind of threats like threats to availability, threats to authenticity, threat to confidentiality [10]. DDoS is a kind of threat to availability.

In this paper, we have introduced an approach used to remove the impact of DoS or DDoS attack from the vehicular ad hoc network. This paper is divided into following sections: section II presents introduction to DDoS attack. Section III includes related work to DDoS attack detection schemes. In Section IV, we proposed a new algorithm for detection purpose.

1.1 DDoS Attack

DOS attack causes DDOS (Distributed Denial of Services Attack). This attack takes place in distributed manner. There are number of attackers in the network that attacks from different locations with different timing slots. It is dangerous than the DoS attack because there is only one attacker which can be easily identified but in DDOS attack there are number of attacker in the network. This attack is a kind of threat to availability in which the users cannot be able to access the resources that they are needed.

In VANET, there are number of vehicles communicating with each other. Multiple vehicles known as attackers create attack on the victim from different location and at different time and the victim cannot access the resources in the network. So these kinds of attack are harder to detect. In DDoS, attacker consists of handlers and agents. Handlers are used to handle agents whereas agents are the one that are responsible for the attack on the particular victim.

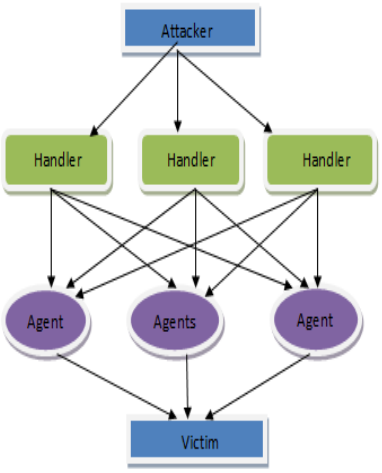

Fig 3. DDoS Attack Mechanism

2. LITERATURE REVIEW

A lot of research work has been carried out to defend against DDoS attack and DoS attack in the Vehicular Ad Hoc Networks.

Al-Khahtani [4] presents the security mechanisms to authenticate and validate message transmission and the approaches to defend against the attacks occurred in the network. This paper defines a number of security and privacy schemes. Few of them are the Public Key Approach (PKI), Symmetric and Hybrid Approaches. For the Prevention of DDOS attack it has defined a Certificate Revocation Technique (CRT) [15], one part of PKI approach. Certified Revocation is done by the CA (Certified Authority) by two ways: Centralised and Decentralised. RSU sends the CRL (Certificate Revocation List) to the OBU (On Board Unit) .When the certificate is detected as invalid, CA sends messages to RSU which sends messages to all vehicles to revoke that particular certificate and stop the communication with it.

A new cracking algorithm is carried out [14] preventing DDoS attack in the 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 than it is considered as normal user. If the user signed in for five or more than five times then it is considered as Attacker.

Minda Xiang proposed a method called Protection Node based strategy [8] to remove the effect of DOS or DDOS attacks in Mobile ad hoc network. 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.

The novel traffic congestion detection and removal scheme [5] was proposed for DDOS attack. It defines the misbehaviour of DDOS attack and the 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.

Aditiya Sinha proposed QLA (Queue limiting algorithm) [3] for protection of VANET from DoS attack. For the protection purpose they have assigned a queue to each node. This purpose provides a limit to each node of receiving packets from other node and also the messages is divided using DSRC (dedicated short range communication). If any node is sending large number of packets to the victim node then the queue will accept the limited number of messages only and the other messages will be discarded. Thus DoS attack cannot be performed by the attacker.

3. PROPOSED METHODOLOGY

The proposed algorithm is used to detect DDOS attack in the network. This algorithm uses the concept of "protection node". One node will be selected on the basis of its importance and divided into multiple levels using hierarchical architecture. Whenever DDOS attack will be triggered by the malicious vehicle into the network, packet delivery ratio will be reduced. The paper consist of two assumptions: DDoS is triggered into the network and the second is the average speed of vehicles in the network. The detection strategy consists of following steps:

1. LPN Selection

A three-way handshaking process is utilized for the selection of LPN node. In the first step the higher level node sends LPN Request (LPNREQ) to lower level node. When the request is received by the lower node, it will not accept any request from other node. In second step, receiver send (LPNACK) acknowledgement back to the sender. In third step, protected node sends confirmation message (LPNCNF).

2. Appointment of LPN

Motivated from SAODV, the hierarchical architecture is adopted for the bisection of nodes based on their importance. The bisect node consist of lower and higher level nodes. Lower level nodes are used to protect higher level nodes and the neighbouring nodes are used for protection of lower level or of same level. Each higher level node has assigned a lower level node for protection known as LPN (Local Protection Node).

Detection Algorithm:

```
Choose LPN
Vehicles send messages, compute PDR;
    When PDR reduces, then

        {
            LPN sends MM message to the
            Vehicles.
        }

        Else

        {
            Ignore.
        }

Vehicles receives MM message,
Vehicle senses its adj V,
If adj Vehicle flooding the rough packets into the network, then

        {
            Consider it as malicious vehicle.
        }

            Else

        {
            Ignore.
        }
Vehicle forward FPN to RPN ;
After receiving FPN, RPN filters all the malicious packet at source side and drop the drops the packet.
```

Fig 4. Proposed Algorithm

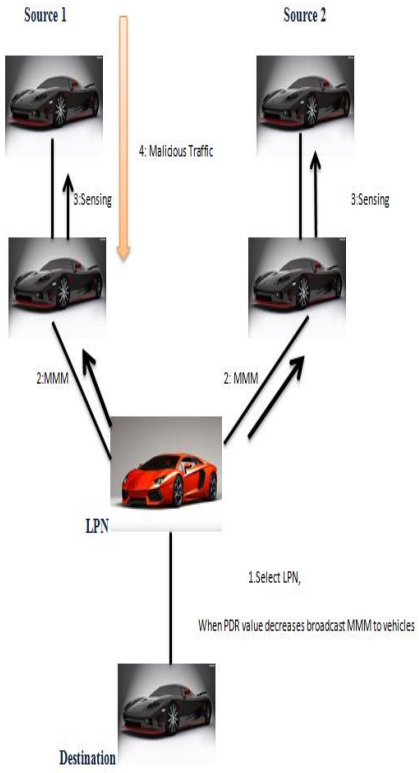

Fig 5. Process of defending DDoS Attack

3. Detection Phase:

Whenever the DDoS is triggered into the network; the PDR (Packet Delivery ratio) value is reduced. When the PDR value becomes equal to the threshold value, LPN node sends MM (monitor mode) message to all the adjacent vehicles in the network. The vehicles which receives MM message will start sensing their adjacent vehicles. The malicious vehicle which is flooding the network with rough packets will be detected. Then an RPN (Remote Protection node) will be selected near to the malicious vehicle. RPN node is used to filter the normal traffic with the malicious one. An RSU will be placed into the network, as VANETs is mobile in nature so RSU maintains the history of all the nodes. When any new vehicle joins the network, the information about the malicious node will be sent to the new entered vehicle.

4. Behaviour Based Profile Creation:

Anomaly based detection methodology is used for the profile creation that represents normal behaviour of vehicles. In this detection process, profiles are created by monitoring the characteristics of the typical activity over a period of time. The behavioural attributes considered for development of profile in VANET are *Bandwidth consumption, Speed of Vehicles, Packet sending rate.* If one of any attributes characteristic changes suddenly like speed of any vehicle then an alert is generated to RSU about the anomaly. This process will be used for the packet filtration on the RPN node.

4. PERFORMANCE

This section discusses the results obtained from the proposed algorithm using MATLAB. It is a 4th generation high level programming language developed by Math Works. It provides an interactive environment for numerical computation, visualization, iterative exploration, and programming. The variation in PDR value in the attack scenario and the detection scenario has been analysed. Performance evaluation has been done on the basis of delay and PDR variation parameters.

Table 1. PDR Variation recorded during simulation

Scenario	Normal	Attack	Detection
PDR Value	1.004	0.9906	1.012

Table 1 defines that how the packet delivery ratio varies w.r.t in the attack scenario and in the detection scenario. In the normal scenario vehicles communicates normally. When DDoS occurred in the network the PDR value reduces, after using proposed algorithm the PDR again becomes normal. Whenever any attack took place into the network packet delivery ratio reduces which leads to bad throughput and greater delay of the network.

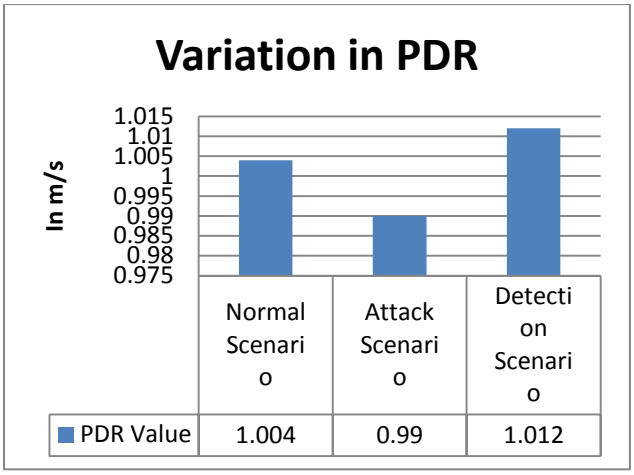

Fig 6. Variation in PDR value

In the given graph, it represents the variation in the PDR value. In the normal scenario when vehicles communicate with each other the value is normal but when the attack triggered into the network it affects the PDR value i.e. PDR reduces. After that when the detection scheme is applied PDR again increases.

Table 2. Delay vs no. of vehicles

	Number of Nodes	**Time in ms**
Attack Scenario	4	0.265
	6	0.274
	9	0.283
	Number of Nodes	**Time in ms**
Detection Scenario	4	0.232
	6	0.225
	9	0.231

The delay graph shows how much time each vehicle consumes while communication. In the attack scenario the vehicles communicates and thus their PDR value calculates. In the detection scenario it takes less time as Euclidean distance is applied to select nearest node. So the delay decreases.

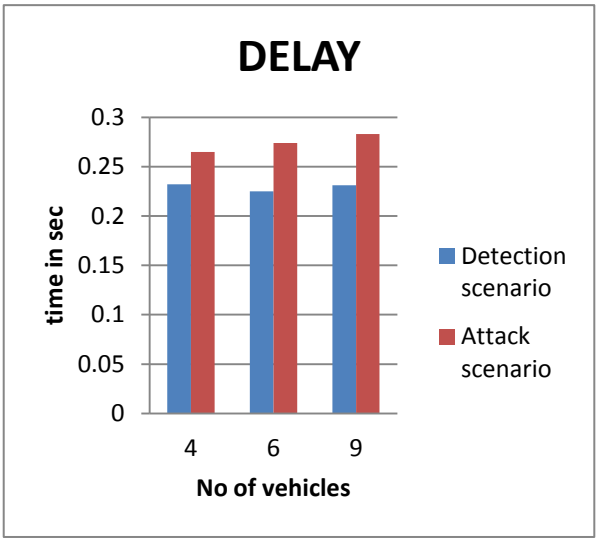

Fig 6. Delay Graph

5. 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 presents detection strategy that detects the evil nodes in the network responsible for the occurrence of DDoS attack. The network is divided into different levels on the basis of priority. The lower level nodes would be allocated as protection node for the superior nodes to grasp the entering load. MATLAB tool is used to analyse the performance of the network that whether the proposed approach is feasible for the detection purpose for DDoS attack from the Vehicular ad hoc network.

6. FUTURE SCOPE

In future we may focus on prevention of DDoS attack. As detection part is completed but there is no prevention mechanism applied for the DDoS attack.

7. REFERENCES

[1] A.Anna lakshmi, D. V. (2012). A Survey of Algorithms for Defending MANETs against the DDoS attack. *International Journal of Advanced Research in Computer Science and Software Engineering* , 155-163.

[2] Aditya Sinha, P. K. (2013). Preventing VANET from DOS and DDOS Attack. *International Journal of Engineering Trends and Technology* , 4373-4376.

[3] Aditya Sinha, P. S. (2014). QLA (Queue Limiting Algorithm) for protecting VANET from DOS(Denial of Service). *International journal of Computer Application* , 14-17.

[4] Al-Kahtani, M. S. (2012). Survey on Security Attacks in Vehicular Ad hoc Networks(VANETs). *IEEE.*

[5] Ayonija Pathre, C. A. (2013). A Novel defence Scheme against DDOS Attack in VANET. *IEEE.*

[6] C Balarengadural, D. S. (2013). Fuzzy Based Detection and predction of DDOS attack in IEEE 802.15.4 low rate WPAN. *International Journal of Computer Science Issues* , 293-301.

[7] Chetan aggarwal, A. J. (2013). Identification of malicious vehicle in VANET from DDOS attack. *Journal of Global Research in Computer Science* , 30-34.

[8] Minda Xiang, Y. C.-S. (2011). Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc Networks. *IEEE Global Communications Conference*, (pp. 1-6).

[9] P., M. E. (2013). Threat Analysis and Defence Mechanism in VANET . *International Journal of Advances research in Computer Science and Software Engineering* , 47-53.

[10] Ram Shringar Raw, M. K. (2013). Security Challenges, Issues and Their Solutions for VANET. *International Journal of Network Security and Its Applications* , 95-105.

[11] Sherali Zeadally, R. H.-S. (2010). Vehicular ad hoc networks (VANETS): status,results, and challenges. *Springer* .

[12] Shweta Tripathi, B. G. (2013). Hadoop Based Defence solution to handle DDOS Attacks. *Journal of Information Security* .

[13] Subir Biswas, J. M. (2013). DDOS Attack on WAVE-enabled VANET through Synchronization. *IEEE.*

[14] TamilSelvan, K. S. (2013). A Holistic Protocol for Secure Data Transmission in VANET. *International Journal of Advanced Research in Computer and Communication Engineering* , 4840-4846.

[15] V.Priyadharshini, D. (2012). Prevention of DDOS Attacks using New Cracking Algorithm. *International Journal of Engineering Research And Applications* , 2263-2267.

[16] M.Raya, J. (2007). Securing vehicular ad hoc network. *Journal of Computer Security*,39-68.