Isolation of Distributed Denial of Service Attack in Vehicular Ad Hoc Networks

Aaditya Barak, Vikas Sindhu

Student, Assistant Professor

Electronics and Communication Engineering

University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak.

Abstract

A network in which the vehicular nodes are free to join or leave the network is known as vehicular ad hoc network (VANET). Either vehicle to vehicle or vehicle to infrastructure types of communication is performed in this decentralized type of network. The identification and elimination of Distributed-Denial of Service (DDoS) attacks from VANETs is the major objective of this research. The nodes that can flood victim nodes with large numbers of rough packets are chosen by the malicious nodes in this kind of attack. The technique which is proposed in this research is based on the two step verification. In the two steps verification technique, when the network performance is reduced to threshold value then the traffic is monitored that which node is sending data on such high rate. NS2 simulator is used to implement the proposed technique. With respect to various performance parameters, the proposed technique is analyzed. A comparative evaluation of results achieved from proposed and existing techniques is also done to conclude the level of improvement achieved.

KEYWORDS: DDoS, Threshold, VANET

Introduction

A self-configuring type of network that provides vehicle to vehicle and vehicle to roadside communications is known as vehicular ad hoc network. The information is shared across the network through the nodes that represent themselves as servers or clients [1]. The computerized system comprises of various components such as computers, communications, and management technologies as well as the sensor and control innovations. There are vehicles as well as Road-Side Infrastructure units (RSUs) present in the VANETs. The vehicles are able to communicate with each other as well as with the RSUs using VANETs. The RSUs are referred to as the fixed entities and the vehicles are considered as mobile entities [2]. There can be one-hop communication amongst vehicles in VANETs or multi-hop communication in which the vehicles can act as routers and retransmit the messages. So, the vehicles can communicate directly with each other or can pass messages amongst a series of vehicles. The nature of the message is an important factor which determines the type of communication [3]. The one-hop communication can be provided if the vehicles wish to communicate on individual basis. In order to travel within the network, the node or vehicle needs to have a certificate which approves its participation in that network. The certificate authority helps in issuing this certificate [4]. If the vehicle requires a certificate authority (CA) to travel along with it, a message is broadcasted and passed across the network. This stops once the RSU is reached and this type of communication is known as multi-hop communication. For the purpose of enhancing the transportation safety as well as efficiency, the VANETs are proposed. An example of one such application is the cooperative collision avoiding. The speed of wireless communications is high due to which the drivers can receive alerts in a timely manner due to which the accidents can be prevented. The driver stops the vehicle before the accident can occur. This helps in providing safer transportation. However, these networks are not only deployed within the safety applications. The basic ad hoc routing protocols cannot be used adequately within the VANETs because of the change is configurations, the mobility patterns, the entering and leaving of various vehicles and various other reasons [5]. The utilization of least communication time while using minimum amount of network resources, is the major objective of routing protocols in VANETs. On the basis of the position accusation and route update technique, the VANETs routing protocols can be categorized. A class of routing algorithm is provided within the position based routing in which the geographic positioning of information is shared amongst the nodes. Within the clusters that are generated within the network, the cluster based routing protocols are used [6]. The nodes that are similar will form clusters and one cluster head will be chosen which will help in broadcasting the packet to the cluster present. There is an occurrence of delay and overhead within the highly mobile

VANETs even when there is high scalability of these networks. In order to share the traffic, weather and any emergency related information from the roads, the broadcasting routing is utilized within VANETs. The important information can be delivered and the announcements can be made amongst the vehicles through this protocol. A location based multicasting routing which helps in delivering the packets from source node to the all other various nodes present in a geographical area is known as geo cast routing [7]. Any unnecessary hasty reaction can be avoided by not informing the vehicles outside the Zone of Relevance (ZOR) which is also done through geo cast routing scenarios. The information related to the links which are present within the network is utilized by the topology based routing protocols. This is done in order to perform packet forwarding across the network.

An attempt made by an attacker from different locations to stop legitimate users from accessing the required objects from the system is known as DDOS attack. The distributed arrangement adds "many to one" algorithm which creates difficulty to prevent entry of intruder in the network [8]. The denial of service attacks consists of four parts namely; firstly, it has a victim that is a target host which is attacked by the interference of the attack. Secondly, it has attack daemon agents. They are specially designed to conduct the attack on the target victim. They are generally present in the host computers. The daemon affects the working of target as well as host computers. The purpose to deploy these attack daemons is to gain access and infiltrates the host computers. Control master program is the third component of denial of service attack and the presence of real attacker, the master mind behind every attack, is the fourth component of denial of service attack.

Literature Review

Wesam Bhaya et al. (2017) [9] introduced in this paper the combination of unsupervised data mining methods. The Clustering Using Representative (CURE) method was a data mining method which helped in providing an entropy concept within the windowing of incoming packets. This helped in identifying the DDOS attack present within the network. Amongst the various approaches which already existed this proposed method was evaluated and compared in order to check what kind of enhancements have been made. The evaluation was done with respect to various parameters which helped in determining the performance of the proposed method. As per the results, it was seen that the proposed method outperformed all other existing approaches by providing higher level of accuracy.

Surendra Nagar et al. (2017) [10] proposed in this paper a secure routing protocol which could be applied in scenarios where DDOS attack was possible. The proposed algorithm was used to scan the infected nodes. The identified infected nodes were blocked in such a manner that they could not participate within the further activities. The intrusion prevention mechanism was used in order to protect the network. The neighbors were scanned by these nodes in regular manner. When a misbehavior node was identified by the IPS node from the frequently passing message the IPS node blocks it in such a manner that the information was sent to all the sensor nodes. Here, the routes were changed within this method. The network was protected against the DDOS attack as seen within the simulation results achieved by applying proposed method.

Munazza Shabbir et al. (2016) [11] presented a mobile Adhoc network which transformed into a mainstream and most promising technology of the modern time. Any time of information moving around the network is very important. The free movement of nodes and unpredictable path of the associated network degrades the working of VANET. DDOS is one of the dangerous attack present in the VANET, it exhaust the network working by using its greater part as its assets. In this attack, the attacker forges the identity of another node and uses spoof IP address to degrade the network circulation. So, before the proper working of the VANET all the security based requirements should be fulfilled.

Kirti A. Yadav et al. (2016) [12] reviewed in this paper the different types of routing protocols that are being applied in vehicular ad hoc networks. The security related scenario was to be generated through the presence of routing techniques within these systems. There was also a need to identify the need of providing security applications to the users involved here. The various security measures being provided in VANET are also studied in this paper. Within the security scenarios, there was a need to provide a future scope which could help in ensuring the security, availability as well as non-repudiation of the techniques. It was analyzed through this study that there was a need to provide enhancement in the intelligent transport system in order to provide higher level of secure environment within these networks.

Mohamed Nidhal Mejri et al. (2015) [13] proposed a new detection mechanism which was known as Greedy Detection for Vehicular ad hoc Networks (GDVAN). The proposed technique was executed by any node present in the network which was a major benefit of this proposed technique. There was no need to modify the IEEE 802.11p standard within this mechanism. With the help of various simulations and experiments the effectiveness and efficiency of the proposed method was computed which showed that the proposed algorithm outperformed the already existing techniques in terms of various performance parameters.

Nirav J.Patel et al. (2015) [14] studied in this paper that there was vehicle to vehicle communication provided over the vehicular ad hoc networks. There is a continuous

change within the locations of the vehicles within VANETs. During the routing process, there was a need to provide secure routing in order to provide a mutual trust amongst the nodes present in the network. In order to provide trust-based techniques within these networks, various researchers have proposed many studies. The enhancement of various ad hoc routing protocols had been reviewed in this paper, in order to study the secure the routing processes. On the basis of this review, the various enhancements to be made within the trust-based techniques were also understood.

Research Methodology

In this research work, various methods are proposed which can identify and isolate malicious nodes from the network which are responsible to trigger DDOS attack. The DDOS attack is the denial of service type of attack in which malicious node can select some of the nodes which can flood victim node with raw packets. In this work, mutual authentication technique is proposed for the detection of malicious nodes from the network. The nodes which are not able to prove their identity will be detected as malicious nodes from the network.

In the work, a novel technique is presented which will detect malicious nodes from the network and to detect malicious nodes following are the steps which will be followed:-

1. In the first step, the network will be employed with the finite number of vehicle nodes. The fixed bandwidth will be allocated to each vehicle node in the network.

2. The road side units will start analyzing the bandwidth consumption of each vehicle node and node which will use the bandwidth above allocated value will be the malicious node.

3. In the third step, the road side units will check the type of packets the node is sending which is using the bandwidth above the allocated value. When the node transfers the data packets to the victim node, then that node may or may not be the malicious node.

4. In the last step, the nodes which will send the malicious data packets, if that node will receive control packets from any node then that node will be identified as the malicious node which will be responsible to trigger DDOS attack .

The proposed technique is based on two type of message which are data packets and control packets. The vehicles and road side units are used for the detection of malicious nodes in the network. The DDOS attack is the special type of attack in which malicious nodes select the nodes which flood the victim node. The malicious nodes which forward maximum number of packets in the network and flood maximum number of packets are detected as the IDS nodes. The IDS nodes detect the malicious nodes. When the network throughput reduced to threshold value, then the monitor mode technique is applied in which each node watch its adjacent node. The node which is sending the data packets above the threshold value is the marked as the malicious nodes. On the same time, if the nodes which are marked as malicious receive control packets, the nodes which send control packets is marked as malicious nodes. The proposed technique does not require any extra hardware or software for the detection of malicious nodes from the network.

The proposed flowchart explaining the discussed research methodology is given below.

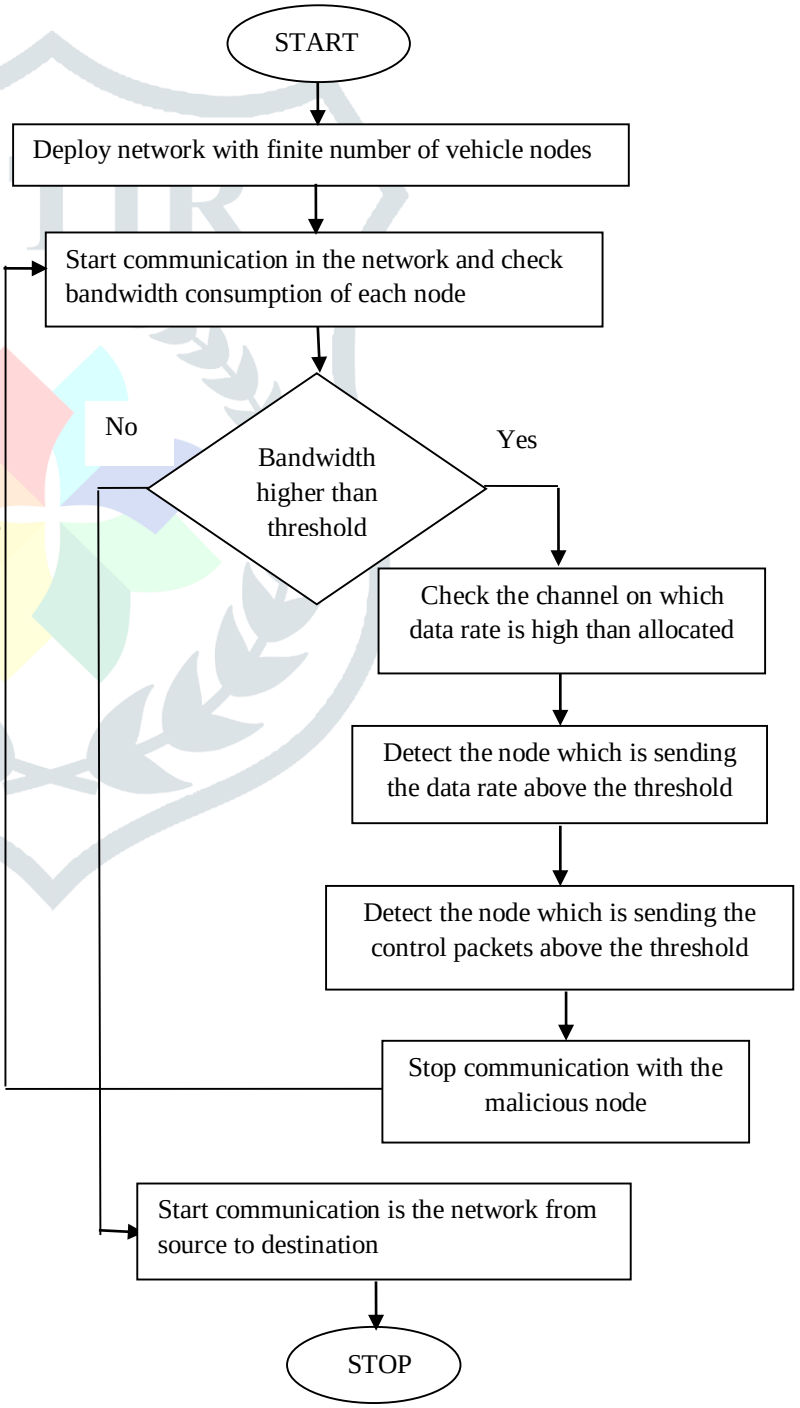

Figure 1: Proposed Flowchart

Experimental Results

The proposed research is implemented in NS2 and the results are evaluated as shown below.

Table 1: Routing Overhead Comparison

Time	Proposed Technique	Existing Technique
5.5	22	52
6	25	60
6.5	80	220

Table 2: Packet loss Comparison

Time	Proposed Technique	Existing Technique
5.5	40	90
6	45	120
6.5	55	220

Table 3: Throughput Comparison

Time	Proposed Technique	Existing Technique
5.5	220	100
6	300	120
6.5	500	220

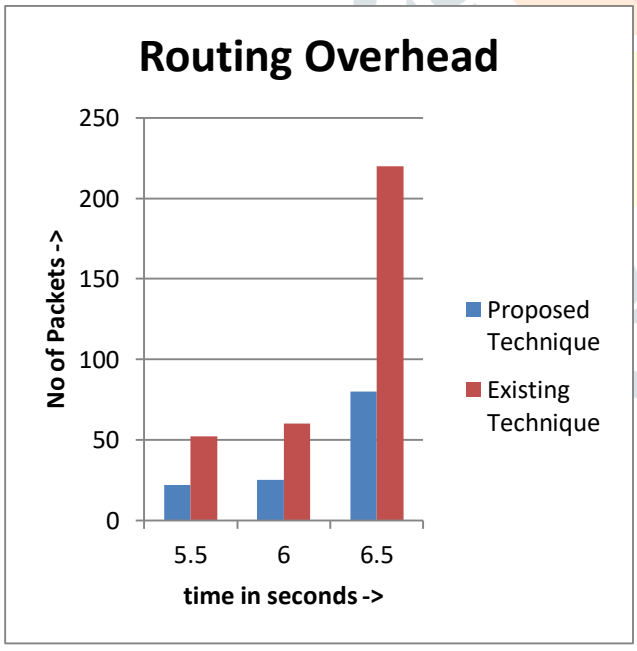

Fig 2: Comparison of Routing Overhead proposed vs existing technique

Figure 2 shows the comparison between the routing overhead of the proposed and existing technique. It is found from research that due to the presence of DDOS attack in the network, the routing protocol is very high. When the network detects the malicious node then the routing overhead is reduced.

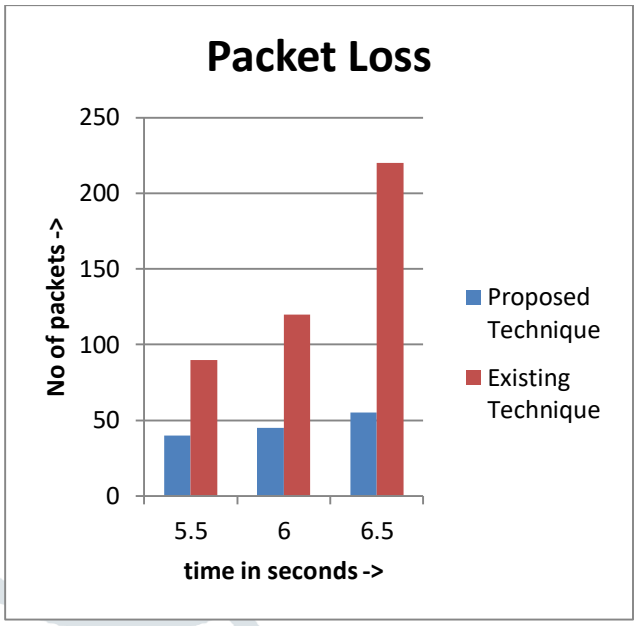

Fig 3: Comparison of Packet loss proposed vs existing technique

As shown in figure 3, the packet loss of the proposed and existing algorithms is compared for the performance analysis. Due to occurrence of DDOS attack in the network, the packet loss is high and when the malicious nodes are detect from the network, the packet loss is reduced and efficiency of the network is increased

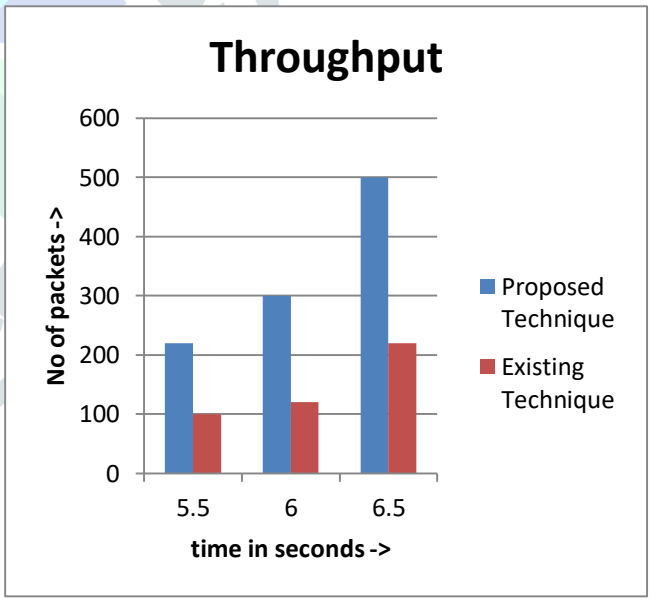

Fig 4: Comparison of Throughput proposed vs existing technique

As shown in figure 4, the throughput of the proposed and existing techniques is compared for the performance analysis. It is analyzed that throughput of the proposed technique is high due to isolation of malicious nodes from the network when compared to scenario which has malicious nodes.

Conclusion

VANETs are gaining popularity in the field of research due to their increase in demand within the real-time applications. There is no infrastructure required within these networks and all the vehicles as well as roadside units are linked with each other to exchange the information. In this research work, the technique will be designed which will be based on the threshold technique. In the threshold technique when the malicious node is transmitting data above the threshold value will be identified as the malicious nodes. The improvement leads to increase network performance and detection of malicious nodes from the network. The proposed algorithm is implemented in NS2 and it is seen that the network's performance is improved in terms of throughput, packet loss and delay.

References

[1] Navneet Kaur, Er. Sandeep Kad, "Data Dissemination In VANETS- A Review", International Journal of Engineering and Technical Research (IJETR), Volume-6, Issue-4, pp. 33-42 2016.

[2] Leandro Aparecido ,"Data dissemination in vehicular networks: Challenges, solutions, and future perspectives", IEEE International Conference on New Technologies, Mobility and Security (NTMS), volume 7, issue 11, pp-220-243, 2015.

[3] Rakesh Kumar and Mayank Dave, "A Review of Various VANET Data Dissemination Protocols", International Journal of u- and e- Service, Science and Technology ,Volume 5, issue 3, , pp. 38-44, 2012.

[4] Surya Nepal, Julian Jang, John Zic, "Anitya: An Ephemeral Data Management Service and Secure Data Access Protocols for Dynamic Collaborations", IEEE computer society, volume 7, issue 23, pp-219-226, 2007.

[5] Hoang D. T. Nguyen, Le-Nam Tran, and Een-Kee Hong, "On Transmission Efficiency for Wireless Broadcast Using Network Coding and Fountain Codes", IEEE communications letters, Volume 15, issue 5, pp-130-145, 2011.

[6] Xia Shen, Xiang Cheng, Liuqing Yang, Rongqing Zhang, and Bingli Jiao," Data Dissemination in VANETs: A Scheduling Approach", IEEE Transactions On Intelligent Transportation Systems, Volume 15, issue 5, pp-110-132, 2014.

[7] Subir Biswas, Jelena Misic, Vojislav Misic, "DDOS Attack on WAVE-enabled VANET Through Synchronization", IEEE Global Communications Conference (GLOBECOM), volume 10, issue 8, pp-131-154, 2012.

[8] Li He and Wen Tao Zhu, Mitigating "DOS Attacks against Signature-Based Authentication in VANETs", IEEE International Conference on Computer Science and Automation Engineering (CSAE), volume 2, issue 10, pp-101-109, 2012

[9] Wesam Bhaya, Mehdi EbadyManaa, "DDoS Attack Detection Approach using an Efficient Cluster Analysis in Large Data Scale", Annual Conference on New Trends in Information & Communications Technology Application, volume 16, issue 3, pp- 236-241, 2017.

[10] Surendra Nagar, Shyam Singh Rajput, Avadesh Kumar Gupta, Munesh Chandra Trivedi, "Secure Routing Against DDoS Attack in Wireless Sensor Network", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" volume 3, issue 9, pp- 114-128, 2017.

[11] Munazza Shabbir, Muazzam A. Khan, Umair Shafiq Khan, Nazar A. Saqib, " Detection and Prevention of Distributed Denial of Service Attacks in VANETs", IEEE Computational Science and Computational Intelligence , volume 8, issue 14, pp- 123-129, 2016.

[12] Kirti A. Yadav and P. Vijayakumar, "VANET and its Security Aspects: A Review", Indian Journal of Science and Technology, volume 9, Issue 18, pp- 104-118, 2016.

[13] Mohamed Nidhal Mejri and Jalel Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs", Journal of IEEE Transaction on Mobile Computing, volume 4, issue 7, pp- 53-62, 2016.

[14] Nivraj J.Patel, Rutvij H.Jhaveri, "Trust based approaches for secure routing in VANET: A Survey", ELSEVIER, volume 19, issue 71, pp- 194-203, 2015.