2016 International Conference on Computational Science and Computational Intelligence

Detection and Prevention of Distributed Denial of Service Attacks in VANETs.

Munazza Shabbir
Department of Computer Engineering
NUST College of EME, National University of Sciences & Technology Islamabad, Pakistan
yana_libra@live.com

Muazzam A. Khan
Department of Computer Engineering
NUST College of EME, National University of Sciences & Technology Islamabad, Pakistan
muazzamak@ce.ceme.edu.pk

Umair Shafiq Khan
Department of Computer Engineering
NUST College of EME, National University of Sciences & Technology Islamabad, Pakistan
umairshafiqkhan@yahoo.com

Nazar A. Saqib
Department of Computer Engineering
NUST College of EME, National University of Sciences & Technology Islamabad, Pakistan
Nazar.abbas@ce.ceme.edu.pk

Abstract— **Vehicular adhoc networks are becoming a popular and promising technology in the modern intelligent transportation world. As per the safety applications of VANETs any information circulating through the network can be life crucial. So the integrity of the information is a critical need. The mobility of the nodes and the volatile nature of the connections in the network has made VANET vulnerable to many security threats. One of the major attack that exhausts the network by illegitimately using all of its resources is DDOS attack. In this type of attack an attacker fakes multiple identities of nodes i-e uses spoofed IP addresses to exhaust the network by circulating bogus messages and making it deny to cater to legitimate requests for services. So before the proper deployment of this network practically its security needs must be met. In this paper a DDOS attack detection and then prevention scheme is proposed. The basic principle is keeping a check on the number of packets being injected into the network. The proposed structure of this scheme causes almost no overhead on the network resources.**

Keywords-component; : VANET, DDOS, OBU, NS2

I. INTRODUCTION

Every year, as the architectural infrastructure is getting more sophisticated yet crowded and with growing number of vehicles on the road the need to make driving a more organized act is becoming important. For an organized traffic flow vehicles need to have a constant information supply about locations, surrounding traffic scenarios, routes etc.

There can be many categories of information that can be helpful to organize the traffic in a better way e.g. information to assist driver and about the safety of both the driver and the car, traffic jam warning, news about an accident, message from the preceding vehicles about brakes, road maintenance, distance between two adjacent vehicles and many other messages that can prevent an accident or harm [1-2]. Keeping these needs in regard the concept of Intelligent Transportation System ITS emerged. Its main aim is to make driving and safety conditions better and also provide on the go infotainment. For this information between the vehicles and some control units was necessary to share, and to do this sharing an Ad Hoc vehicular network is created [23-32].

VANET is a subclass of MANET with the only difference that here mobile nodes are vehicles, moving in multitude of directions n varying speeds [3]. Nodes in VANET i.e. vehicles or road side units can communicate with each other in single hop or multiple hops [4].

A. DDOS Attacks

For the DDOS attack the attacker can be in two forms; insider and outsider. An insider attacker can pollute the network by sending dummy data packets and hence ceasing the network from doing some productive work. While an outsider will spoof the ids of actual nodes and will repeatedly exhaust the network resources e.g. bandwidth by sending useless/fake messages to a targeted node [14]. In DDOS attacks the outsider attacker manipulates the weaknesses of the legitimate nodes of network and launches attack

978-1-5090-5510-4/16 $31.00 © 2016 IEEE
DOI 10.1109/CSCI.2016.185

through multiple such nodes towards one victim by flooding it with bogus messages so much that it will be too exhausted to communicate with other legitimate requests.

Targeted resources could be bandwidth, memory, CPU cycles, file descriptors, buffers etc. Once the weaknesses of nodes are found they are exploited, malicious code is then run on these nodes called handlers then. These infected machines can now not only launch the attack but can also infect other nodes and can turn them into so called zombies or slaves. Now from the back end the actual attacker commands its army of infected nodes to launch a synchronized attack [20]. Dealing with DDOS attacks is there for a difficult task because the attacks are launched from multiple sources [15]. The manipulated nodes might never know that what they are being used for. In some cases, the target of attackers is not the vehicle but RSU, the purpose of such an attack is to bring down the infrastructure module so that if vehicles want to communicate with infrastructure, the RSU will not be able to respond to them [16].

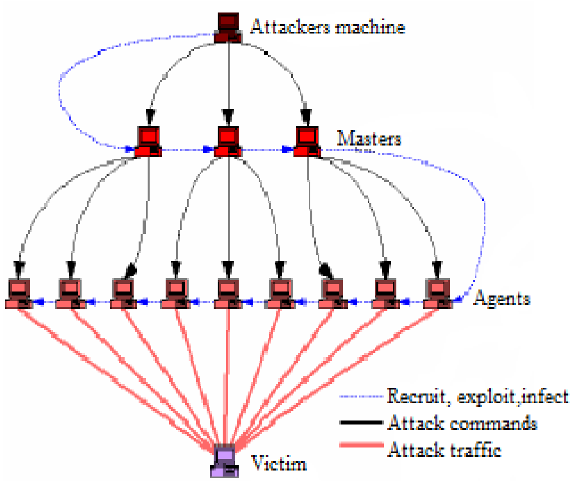

Figure 1. DDoS attack model

As VANET works in real time scenario so a disruption in its normal functionality can cause the loss of life crucial information. Usually the attacker will launch the attack i.e. will start flooding with fake messages parallel to normal broadcast timings. This synchronization between the normal messages and malicious ones will make the packets to collide with each other and hence causes confusion for the receiver that which messages are real and which ones are fake. [13]

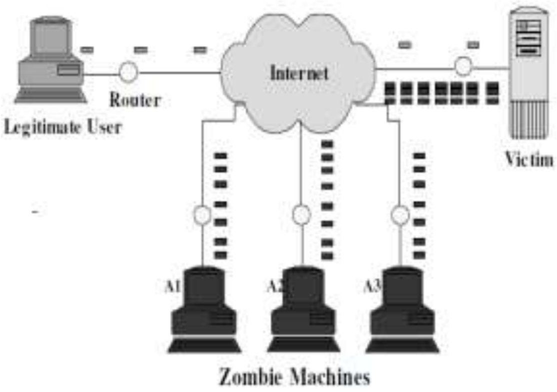

Figure 2. Illustration of the DDoS attack scenario [20]

II. Literature Review

In [16], author's proposed methodology is based upon the knowledge that the DSRC has a separate channel for transmitting safety messages, so a check can be kept on the number of safety packets to be transmitted only. Author suggests that in a specific time period e.g. 30 seconds only 15 safety packets must be allowed to send from a specific IP node to another. The packets will be counted as soon as the first safety message is sent from that IP. If abnormal number of safety packets are sent from that IP, RSU is informed. But a concern arises here that a DDOS attack cannot not be launched only via safety messages. In [17] a method to detect DDOS is presented by analyzing traffic flow in the network. This method uses: The Traffic Analyser, the Fuzzification, the Fuzzy Inference Engine, the Knowledge Base, and Forensic Analyzer. Traffic patterns are read from a trace file and log files are created. Then by using fuzzy algorithm analysis is carried out. The analysis is the crunch of this whole process, it provides information like where why, when and by whom an incident took place in network and then draw conclusion about the happening of an attack. In [18] a filtering based methodology is proposed to detect DDOS attacks. This scheme works against the IP spoofing phenomenon which is the basis of DDOS attack. The algorithm of detection works at victim's side independently and collects the source data of its clients, e.g. source IP addresses, how many hops is the server away in no attack instances. So when an attack is detected, on the basis of already collected data of actual packets, legitimate and malicious packets can be filtered out. In the scheme the source address is classified into different fields making the information extraction fast and easy. In [14-18] the concept of clustering the nodes into groups on the basis of specific parameters is used for scalable communication within a cluster and between clusters a RSUs. The parameters used to form clusters are battery power, connectivity, memory and distances between nodes. The most feasible node from a group of nodes is made a cluster head. The responsibilities of cluster head include collecting the information of group members such as ids, max flooding n max packet drop, as well to communicate with RSU on behalf of all the nodes in a cluster. To communicate with RSU a cluster head locates nearest RSU and sends a message n required info, on the basis of info received RSU passes a conclusion about any node being malicious or not and then informs cluster head to terminate that nodes connection. Once again traffic pattern is scrutinized to look up for any anomalies leading to DDOS attack. According to author in a normal scenario the abrupt disruptions in traffic flow is monitored on the basis of two statistical parameters i.e. volume and flow of data packets in bytes transmitted in network. A cryptographic defense mechanism is used for classification and filtering of attacks packets. If a packet is identified as a malicious packet, it is blocked at the external boarder line router of network and the victim is saved at an initial stage. Before initiating the communication both the participating entities must identify and authenticate themselves to avoid IP spoofing. And for the authentication of the packets being transmitted hash based cryptography is used. In the spoofed IPs of attacker ids are identified by comparing them with the already existing data base of existing IP addresses. Within the network at regular basis, announcing packets are transmitted by each vehicle in the network to all the neighboring vehicles to inform them about their presence and stay updated about theirs and to gain information about next node. In this scenario each node in the network has an updated database about its surroundings. In the case of presence of an attacker a node will find a duplicate IP address in their data log and such identical addresses will be considered as attackers. An attacked packet detection algorithm through which vehicles communicate with RSU. This mechanism gains information about the communicating vehicles exact location. After that details about the packets broadcasted via that vehicles are collected; mainly the frequency and velocity of packets. Depending on these variables values decision is made that it's an attacking vehicle or safe one. [18-26]

In our base papers the idea which is exploited is about the average time of a communication session between two nodes is short, while an attacker node will keep on transmitting packets to the victim node for an extended period and will flood it. So according to the proposed algorithm the average time of communication between two normal nodes is computed and stored as max threshold value. For all the future communication sessions their time interval is compared with threshold value. If the input value increases the max value, the sender node will be considered as malicious and is terminated. [23-30]

III. Proposed Methodology

In base paper the author has exploited the fact that in normal scenario two nodes will communicate for a short interval of time while in case of a malicious and victim node, their communication will be either stretched for an abnormally long period or may be for infinite time. So author is proposing to differentiate between an attacker and a normal node on the basis of comparison of their communication time period with a threshold time.

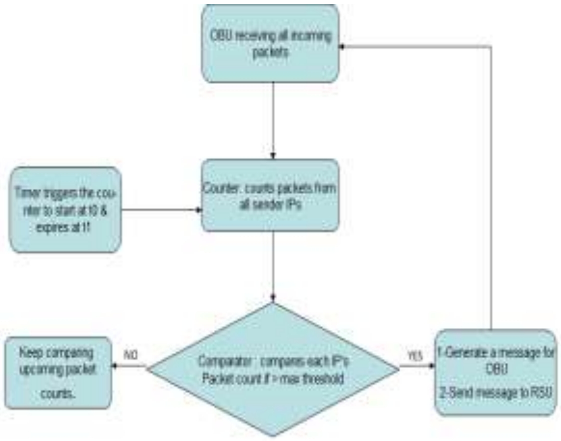
OBU receiving all incoming packets
Timer triggers the counter to start at t0 & expires at t1
Counter: counts packets from all sender IPs
Keep comparing upcoming packet counts.
NO
Comparator : compares each IP's Packet count if > max threshold
YES
1-Generate a message for OBU
2-Send message to RSU

Figure 3. Flow chart of proposed scheme

As DDOS attack is all about flooding a victim to the level of exhaustion by sending abnormally large number of packets, so why not identify the attacker by keeping a check on the number of packets sent by a node, or a potential attacker? In our proposed scheme we are considering the advantage of better battery power resource as the nodes in this case are vehicles. So we can use an algorithm which can run on the OBU of every vehicle continuously to detect an attacker. Let's consider a random vehicle in VANET, which is receiving request messages from multiple IPs (other vehicles) at the same time. In the designed algorithm, OBU will receive these request messages sent from multiple senders and the information about these senders i.e. their IPs and the packets they are sending will be forwarded to the Counter module.

Now as shown in figure 3, this counter takes input from a timer, that triggers the counter to start counting at time t0 and then stops/restarts when a particular time interval is over, in our case this time interval is of 10 seconds. In these 10 seconds counter will count the packets sent by every sender to that particular vehicle and forwards that packet count of each IP to the comparator. After counting packets for 10 seconds the counter will restart to count the upcoming packets. The comparator's job is to compare the packet count sent in that time period, of each sender IP with a max threshold value. This max threshold value is obtained from normal traffic scenario. If the comparator finds any sender's IP more than the threshold value, it will pass that sender's id to the "alarm message module". This module is required to do two tasks, it will send a message to vehicle's OBU to immediately terminate any sort of communication with that malicious IP and also sends a message to RSU to alarm it about the attacker node so that the RSU sends a message to all the vehicles in the networks in advance, to not to initiate communication with attacker IP.

IV. Implementation

For implementation we have used simulator NS 2.35 and for processing the results from trace files of our designed network AWK scripts are used. VANET is implemented using following node configurations:

A. *Simulation Results*

In fig 4 it is evident that with the increasing number of attackers the number of flooding increases but the proposed method is capable of minimizing the flooding more efficiently than the base paper's defense mechanism.

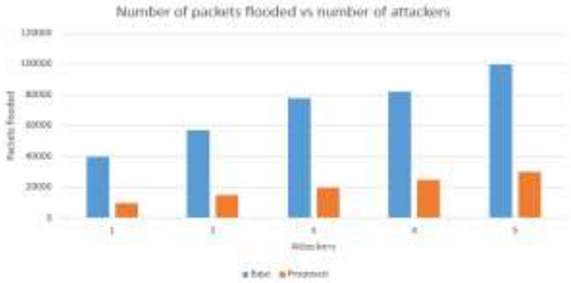

Figure 4. Comparison between base & proposed method's efficiency

In figure 5 the count of packets in the network is given vs the simulation time. It can be seen that before the attack was launched at t=4 sec the number of packets in the network was according to the normal communication between the nodes. At t=4 when the attack is launched we can see a sudden and a huge increase in traffic resulting in a sharp peak but within few seconds the packet count was reduced back to a reasonable number as the proposed algorithm defended the attack.

In figure 6 the packet delivery ratio is shown. It can be noticed that the packet delivery ratio of proposed algorithm is better than the existing algorithm.

.

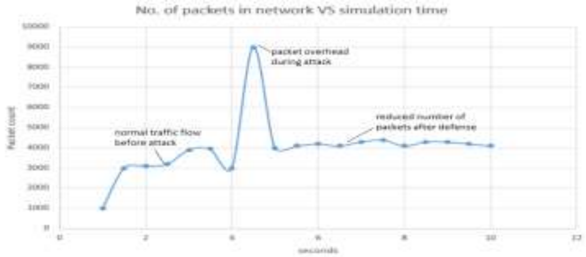

Figure 5. Approx. number of packets in the network during the simulation time

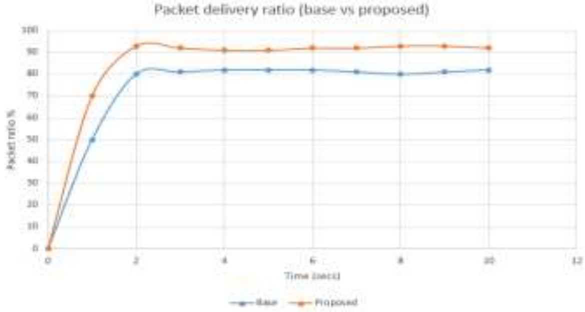

Figure 6. Comparison between packet delivery ratio of proposed and existing defense mechanism

V. Conclusion

Vehicular Adhoc networks is an emerging technology with many promising features to offer. Only if the security hazards in these types of networks are taken care of, VANET can be integrated with the upcoming era of automobile technology as an essential. In our proposed scheme we have attempted to secure the network against the most common form of network attacks- DDOS. Our focus was to do the task with posing minimum overhead on network and using the available resources. The results of our designed algorithm are satisfying enough but still there is a lot more scope for future work to achieve maximum efficiency.

References

[1] Mohamed Nidhal Mari, Jalel Ben-Othman and Mohamed Hamdi, "Survey on VANET security

challenges and possible cryptographic solutions", Vehicular communications: Elsevier, 2014.

[2] Rainer Bauman, "Vehicular Adhoc network (VANET)", Master's thesis, 2004.

[3] Ghassan Samara, Wafaa A.H. Al-Salihy and R.Sures, "Security analysis of Vehicular Adhoc networks (VANET)", in Second international conference on network application, protocol and services, 2010.

[4] Sherali Zeadally et al., "Vehicular Adhoc networks (VANETs); status, results and challenges", Springer Science and Buisness Media, 2010.

[5] Ram Shringar Raw, Manish Kumar and Nanhay Singh, "Security challenges, issues and their solutions for VANET", International Journal of network security and its application (IJNSA), Vol. 5, Sept 2013.

[6] Vishal Kumar, Shailendra Mishra and Narottam Chand, "Applications of VANETs: Present and future", Scientific research, communication and network, Feb 2013.

[7] Jagadeesh Kakarla, S Siva Sathya, B Govinda Laxmi and Ramesh Babu B, "A survey on routing protocols and its issues in VANET", International journal of computer applications, Vol. 28-No. 4, August 2011.

[8] Pino Caballero-Gil (2011). Security Issues in Vehicular Ad Hoc Networks, Mobile Ad-Hoc Networks: Applications, Prof. Xin Wang (Ed.), ISBN: 978-953-307-416-0,

[9] Ghassan Samara, Wafaa A.H. Al-Salihy and R. Sures, "Security issues and challenges of vehicular adhoc networks (VANET)", IEEE Xplore, 2010.

[10] Subir Biswas, Jelena Misic and Vojislav Misic, "DDOS attack on WAVE-enabled VANET through synchronization", 2012.

[11] Priyanka Sirola, Amit Joshi and Kamela C. Purohit, "An analytical study of routing attacks in VANETs", International journal of computer science engineering (IJCSE), Vol. 3, July 2014.

[12] Abdulmotaleb El Saddik et al., "Detecting and preventing IP spoofed distributed DoS attacks", International journal of network security, 2008.

[13] Aditya Sinha and Prof. Santosh K. Mishra, "Preventing VANET from DOS and DDOS attack", International journal of engineering trends and technology (IJETT), Vol. 4, 2013.

[14] Komal B. Sahare, DR. L G. Malik, "An approach for detection of attack in VANET", International journal of engineering research `and application (IJERA) and International conference on industrial automation and computing (ICIAC), 2014.

[15] Vikash Porwal, Rajeev Patel and Dr. R.K. Kapoor, "An investigation of DoS flooding attack in VANET", International journal of advance foundation and research in computing (IJAFRC), Vol. 1, Dec 2014.

[16] Archana S. Pimpalkar and A. R. Bhagat Patil, "Defense against DDOS attacks using IP address spoofing", International journal of innovative research in computer and communication engineering, Vol. 3, issue 3, March 2015.

[17] Kamlesh Namdev and Prashant Singh, "Efficient and secure communication in vehicular adhoc network", International journal of computer application, Volume 127, October 2015.

[18] Karan Verma, Halabi Hasbullah and Ashok Kumar, "Prevention of DOS attacks in VANET", Published in Wireless personal communication, November 2013.

[19] S. Roselin Mary, M. Maheshwari and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using attacked packet detection algorithm (APDA)",2013.

[20] Adil Mudassir Malla and Ravi Kant Sahu, "Security attacks with an effective solution for DDOS attacks in VANET", International journal of computer application, Vol. 66, March 2013.

[21] Er. Pallavi Bansal and Er. Lokesh Pawar, "Reducing impact of flooding in VANET due to distributed Denial of service attacks". IJESC, 2015.

[22] Pranav Kumar Singh, Kapang Lego and Dr. Themrichon Tuithung, "Simulation based analysis of Adhoc routing protocol in urban and highway scenario of VANET", International journal of computer application, Vol. 121, January 2011.

[23] Muazzam A. Khan, Jawad Ahmad, "An Efficient and Secure Partial Image Encryption for Wireless Multimedia Sensor Networks using Discrete Wavelet Transform , Chaotic maps and Substitution Box" Journal of Modern Optics, by Taylor & Francis, IOct 2016.

[24] Nazish Rafique, Muazzam A. Khan, F. Bashir, "Black Hole Prevention in VANETs Using Trust Management and Fuzzy Logic Analyzer" International Journal of Computer Science and Information Security, IJCSIS, Vol. 14 No. 8, Sep 2016.

[25] Zainab Nayyer, Muazzam A. Khan, F. Bashir, "Two Tier Clustering Technique in Vehicular Ad Hoc Networks in Highways' Scenarios" International Journal of Computer Science and Information Security, IJCSIS, Vol. 14 No. 8, Sep 2016.

[26] Shawar Gul, N. Amin, Faisal Bahdur, Muazzam A. Khan "A Light Weight Secure Protocol for Data Transmission in Vehicular Ad-hoc Networks(VANETs)" International Journal of Computer Science and Information Security, IJCSIS, Vol. 14 No. 8, Aug 2016.

[27] Waqar Farooq, Muazzam A. Khan, Saad Rehman, "A Novel Real Time Framework for Cluster-based Multicast Communication in Vehicular Ad Hoc Networks" International Journal of Distributed Sensor Networks, IF 0.665, Mar, 2016.

[28] Zainab Nayyer, Muazzam A. Khan, Nazar A. Saqib "Secure Clustering in Vehicular Adhoc Networks" International Journal of Advanced Computer Science and Applications, Vol 6, No 9, 2015.

[29] Waqar Farooq, Muazzam A. Khan, Saad Rehman, "A Survey of Multicast Routing Protocols for Vehicular Ad Hoc Networks (VANET)" International Journal of Distributed Sensor Networks, June, 2015.

[30] Afza Kazmi, Muazzam A. Khan, F. Bashir " DeVANET: Decentralized Software-Defined VANET Architecture" The EAI International Conference on Future Intelligent Vehicular Technologies, Porto, Portugal, Sep 15–16, 2016.

[31] Waqar Farooq, Muazzam A. Khan, Saad Rehman "A Cluster based Multicast routing protocol for Autonomous Unmanned Military Vehicles (AUMVs) communication in VANET" IEEE International conference, ICE Cube 2016, Pakistan, 11-12th April 2016.

[32] Afza Kazmi, Muazzam A. Khan " DeVANET: Decentralized Software-Defined VANET Architecture" IEEE Symposium on Software Defined Systems SDS'2016 Berlin, Germany between 4-8 April 2016.