Minimizing DDOS Attack by Applying Clustering Scheme & Threshold value in VANET

Md.Tanvir Hossain
[1] Department of Computer Science and Engineering, Internation University of Business Agriculture and Technology, Dhaka 1230, Bangladesh
19303038@gmail.com

Abstract. A vehicular ad hoc network (VANET) is a Network Technology where vehicles and RSU (roadside units) are connected by OBU (On Board Unit) to make transportation safer and faster than the Traditional transportation system. VANET can be implemented in self-driving cars, which will make those cars more intelligent and effective in terms of quickly making the right and most effective decisions to improve passenger safety and experience. Network Technology is the number one victim of cyber attacks, for which concerns about secure communication are always there. To maintain the normal workflow, VANET requires availability between VANET components (RSU, vehicles). Most of the time, Hackers will try to hack the RSU because all the road information and car conditions are sent to the roadside units(RSU) and RSU sends all the received information to other RSU and vehicles. So to stop the VANET or make a large area out of the network, a hacker has to target the RSU. Most Hackers prefer to perform Distributed Denial of Service (DDoS) attacks to hamper or shut down VANET. In a DDoS attack, hackers create a malicious script that can be turned on and off over the network and automatically generate and sent a large number of packets in a short time to the target IP. The malicious scripts are then sent to other computers or nodes. When hackers think the number of affected computers or nodes is enough, the hacker triggers those scripts and at a time all the computers or nodes start sending false data packets to the RSU. Which make a very heavy load on the RSU and RSU got hanged or stop working. This forces VANET to stop. Hackers prefer DDoS because it's effective for hampering the network and hard to find out the real attacker. To prevent DDoS attacks effectively, we have proposed an algorithm that will enable 2 layers of security. This algorithm includes clustering techniques and a DDoS detection module. In our proposed algorithm we have given major priority to the safety of RSU and then to the vehicle. This could makes this algorithm's success rate more than 98 percent in terms of RSU Protection And 90 percent in terms of vehicle protection. Less amount of simulation tool learning resource, algorithm complexity, and Only 3 scenario consideration were scopes of this research. All the tests were conducted in SUMO (Simulation of Urban Mobility) with the help of ns-3 and C++ knowledge. Our proposed algorithm is updatable. This algorithm can also be used in servers to prevent DDoS attacks in servers.

Keywords: VANET, DDOS, OBU, NS2,SUMO

1 Introduction

A vehicle Ad-Hoc Network (VANET) is a wireless network technology that allows the vehicle to communicate with other nearby vehicles and Road Side Units (RSU) or Roadside infrastructure. In VANET, each vehicle is referred to as a node which contains two electronic devices called On-Board Unit(OBU) and an Application Unit(AU) which helps nodes to communicate with each other(i.e., Vehicle to Vehicle(V2V)) and with roadside infrastructure(i.e., Vehicle to Infrastructure(V2I)).In VANET nodes can receive important information(such as road is the jammed or not good situation) from near nodes which will make driving safe and enjoyable. VANET will reduce traffic jams, which will save people's time and help to increase the growth rate of a country. The most important point to look at is that VANET will reduce the number of road accidents which is nowadays a very important issue to concern. VANAT is a network technology that will face many cyber attacks such as DDOS, reple, etc. Distributed Denial of Service or DDoS is a cyber-attack where a hacker attempts to disturb regular traffic of a targeted device over the network by sending a huge amount of invalid requests In a short time. In short DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination. The

DDoS attack is considered an organized attack because in a DDoS attack an army of zombie devices (Affected devices with malicious code) is first created then they all start sending false requests to the targeted devices to stop or block service.DDoS is the most common attack in the hacking community and it is one of the main threats to VANET.

2 Background Study

The paper in [1] describes how traffic accidents and its sequences are dramatically rising throughout the world, leading to a demand for solutions to ensure vehicle security and control while driving. Improving the quality of life for citizens by establishing an intelligent transportation system is one of the main priorities for modern governments (ITS). The use of Vehicular Ad hoc Networks (VANETs) in making their notion a reality is acknowledged. The VANET has the potential to improve commuters' comfort and traffic safety. The significant security risks that VANET technology still faces must be resolved before it can be used efficiently and reliably. One of the main threats to the VANET's availability is Distributed Denial of Service (DDoS).The paper in [2] explains that's vehicular ad hoc network (VANET), also known as a mobile ad hoc network, road vehicles often act as the network nodes (MANET). VANETs present a distinct spectrum of challenges and potential for routing protocols because of the semi-organized structure of vehicular movements subject to the limitations of road layout and rules as well as the barriers which limit physical connectivity in urban situations. Many studies are being conducted, in particular, on the reliability and scalability problems with routing protocols in large metropolitan VANETs. Clustering can be used to improve the scalability and reliability of routing in VANET as it leads to the scattered creation of hierarchical network structures by grouping vehicles together based on correlated spatial distribution and relative velocity. The paper in [3] explains Vehicle networks (VANETs), a specific type of ad hoc network, offer the infrastructure for communication between vehicles and connected parties like roadside units (RSU). Secure communication worries are on the rise as technology is used in transportation systems more and more. One of the key objectives of VANET is to keep the system operational. One of the most frequent forms of attacks that target the system's availability is the distributed denial of service (DDoS) attack. They consider the quick detection and mitigation of DDoS attacks on RSU in Intelligent Transportation Systems (ITS). A novel approach for ITS detection and mitigation of low-rate DDoS attacks is proposed and is based on nonparametric statistical anomaly detection. Low-rate DDoS assaults are a danger to RSU availability and can get by standard data filtering techniques because of their highly distributed nature. The full simulation results for a real-world road scenario are shown using the SUMO traffic simulation software. Their suggested strategy greatly beats two parametric methods and the traditional data filtering approach in terms of average detection time and false alarm rate, according to the Cumulative Sum (CUSUM) test.The paper in [4] explains Machine learning (ML), one of the technological instruments that is currently undergoing the most rapid development, is frequently utilized to address critical difficulties in a range of sectors. Traffic jams and traffic fatalities are expected to be significantly decreased because to the vehicle ad hoc network (VANET). To ensure the role, a significant volume of data must be sent. Nevertheless, the wireless access allotted by VANET is insufficient to manage such enormous amounts of data. Spectrum scarcity is a challenge for VANET as a result. Cognitive radio (CR) appears to be a practical solution to this issue. The communication must be ultra-reliable and low latency for CR-based One of the many performance improvement measures that must be accomplished is VANET or CR-VANET. By incorporating ML techniques, CR-VANET may become extremely intelligent, achieving quick adaption to the environment's dynamic nature and boosting service quality while saving energy. In their paper, they go into great detail about the architectures, functions, challenges, and open problems of ML, CR, VANET, and CR VANET. They also discuss the roles and applications of ML techniques in CR-VANET scenarios, the use of machine learning in driverless or autonomous vehicles, and the advancements and potential future research directions of these well-known technologies.The paper in [5] explains, The transmission through the VANET is subject to a variety of security threats, including Distributed Denial of Service (DDoS) attacks. It is challenging to defend against these attacks on VANET. Most current DDoS detection techniques are unreliable and involve a lot of processing. To overcome these problems, they offer a brand-new Multivariant Stream Analysis (MVSA) method. The suggested MVSA technique maintains the many steps for network detection of DDoS attacks. The Multivariant Stream Analysis produces distinctive results based on vehicle-to-vehicle communication via Road Side Unit. The plan keeps separate regulations for different traffic classes throughout

different time intervals and keeps track of the flow of traffic in a variety of conditions and conditions. Using an NS2 simulator, the MVSA's effectiveness is assessed. The simulation's results show that the MVSA does a good job of reducing interference with VANET connectivity and boosting detection accuracy.The paper in [6] explains, Multi-hop broadcast is necessary for ad-hoc wireless networks. Broadcast communications are heavily utilized in several vehicular network (VANET) applications. They advocate using the distance-to-mean technique to simplify these applications. Their method's performance is strongly influenced by the decision threshold's value, making it difficult to choose a threshold that works well across different network scenarios. The ideal measurable limit esteem is influenced by hub thickness, spatial conveyance example, and remote channel conditions. Since these elements differ greatly between VANETs, protocols created to support these applications must be adaptable. Using the distance-to-mean approach, a decision threshold value that is Black-box optimization algorithms based on machine learning methods like genetic algorithms and particle swarm optimization in their work are automatically identified to be simultaneously adaptive to node density, node distribution pattern, and channel quality. The quadrat statistic Q, the Rician fading parameter K, and the number of neighbors N combine to form the Statistical Location-Assisted Broadcast (SLAB) protocol. JiST/SWANS studies show that SLAB achieves great reachability and effective bandwidth consumption in both urban and highway environments with different node densities.

3 Research Methodology

A. Algorithm Scenario

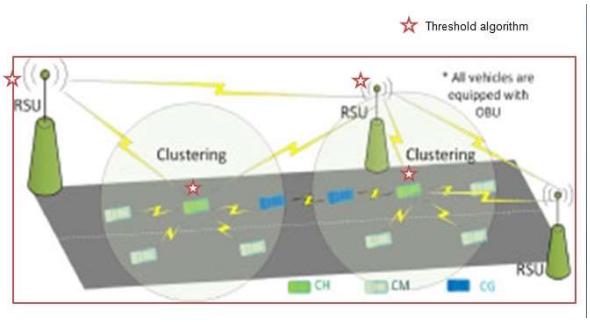

Figure: 3.3 Algorithm Scenario

We have given our proposed algorithm a name, which is the clastrash algorithm. The name clastrash has a meaning. The word ”clas” came from the paper[2] ;They use distance and velocity as independent variables in their method, which interest us. Another word “trash” came from the paper [6]; They used threshold value(in emergency scenarios how much time and data a node need to communicate with RSU). From those 2 papers, we got the idea of clustering and threshold value, which we used in our algorithm with the layer concept. We have created 2 layers of security in our algorithm. The first layer will protect the cluster head node from other member nodes including attackers (who want to perform a ddos attack) and the second layer will protect the RSU from the cluster head if somehow the cluster head got hacked and try to perform a ddos attack on the RSU. Our algorithm takes the number

of nodes, threshold value, and segment length s as input. Where the number of nodes will be counted by a sensor in real life scenario but for our experiment purpose, we will randomly input the number of nodes. After that, we have a threshold value which is the average packet number in the emergency case, which is predefined by performing a ddos attack on the system. Then, segment length denotes the length of the cluster zone of a particular area, which is predefined by the road length. Lastly, the counter will count the number of segments where the cluster head is running. After taking inputs system will create n sized array corresponding to the number of nodes. Then from the array index, randomly a node will be chosen by the system for the role of cluster head. The cluster head then sends a request to all the member nodes for sending the data packet to the cluster head. After receiving the cluster head's request, the member node either accepts and starts sending data packets to the cluster head or rejects the

of receive data with the threshold value. If the threshold value is greater than number of received data the data packets will be sent to RSU. Otherwise, the corresponding node will be ignored by the cluster head. After receiving the member node's data, cluster head will send all the data to the RSU.RSU will first calculate number of total number of received data and compare it with the threshold value. If the threshold value is greater then the calculated total number of received data then RSU will start processing those data, otherwise, RSU ignore those data. Now RSU has all the data from the cluster.RSU process all the data, ignore the attacker's ip, and send all those messages to the cluster head. Cluster head then sends all the data to the corresponding node and increments the value of the counter by 1. Then RSU will again choose a new cluster head and the process will go on like this.

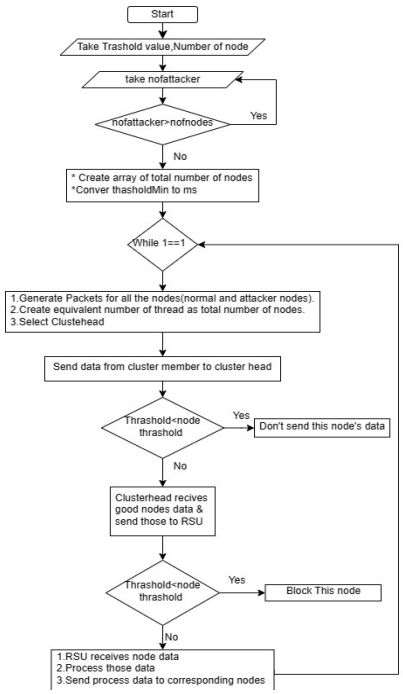

Figure 3.7 Clashtrash Algorithm

4 Result Analysis

All the scenario were simulated in SUMO(Simulation of Urban Mobility) with NS-3(The Network Simulation -3).

We have considered 2 parameter to measure the result of this research. As our aim is create a DDoS prevention algorithm we have to think the basic parameter that is present in the attacked scenario. Time and number of nodes has a relationship with DDoS. Main objective a DDoS attack is to crash the targeted server/node. More faster it can crash the server more deadly it will be for the system, so we can make a relation of time here. A common question will arise that “How much time it will take to crash the system using DDoS attack”. Next, the number or node. The more zombie computer will be more fast the targeted system will crash. Again a question will arise that how many zombie node required to crash the target. So after analyzing those two questions we selected time and number of nodes as our performance matrices.

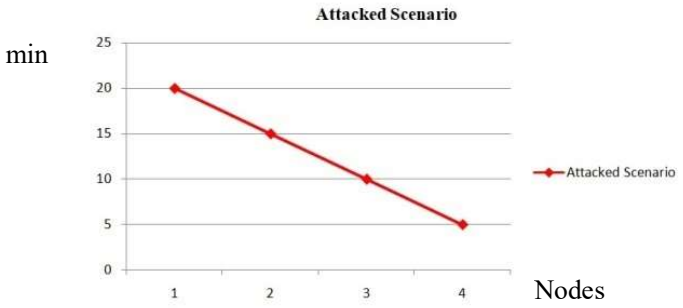

Figure: 4.1 Attacked Scenario

Figure 4.1 shows the System run time while a DDoS attack is performed to the system. We can it the system can run highest 20 with 1 node attack, and stand lowest 5 second with 4 attackers. During the attack when the node number is 1, the system crash after20 min. Then when the node number is 2 the crash time became 15 min. After that node number again increase to 3 and crash time Deceased to 10.lastly when the number of nodes became 4 , system crashes after 5 min.

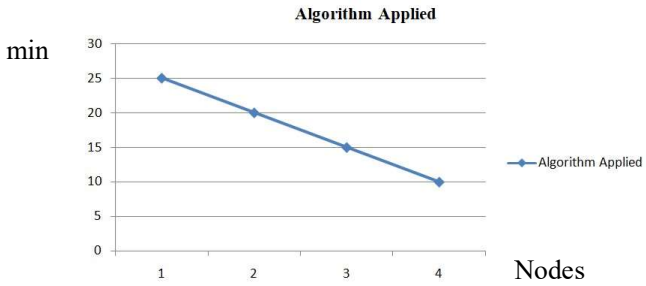

Figure: 4.2 Algorithms Applied

Figure 4.2 shows the System run time of algorithm applied system while a DDoS attack is performed. We can it the system can run highest 25 min with 1 node attack, and stand lowest 10 second with 4 attackers. During the attack when the node number is 1, the system crash after 25 min. Then when the

node number is 2 the crash time became 20 min. After that node number again increase to 3 and crash time Deceased to 15.lastly when the number of nodes became 4 system crashes after 10 min.

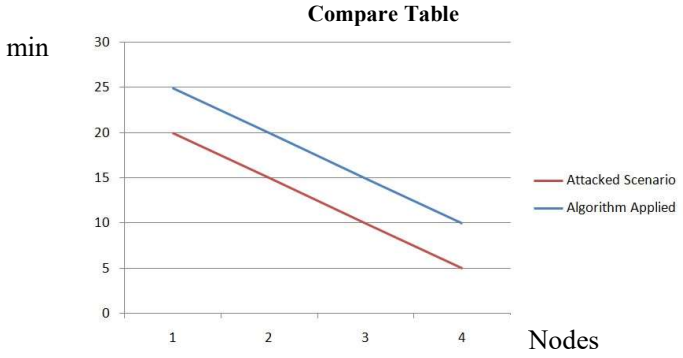

Figure: 4.3 Compare Table

Figure 4.3 shows the comparison between attacked scenario, and algorithm applied scenario. When the number nodes was 1 in attacked scenario systems crashes after 20 min ,and algorithm applied scenario 25 min. When number of nodes is 2 attacked scenario crashes after 15 and

our proposed model will able to defend the DDoS attack for 5 min.

5 Conclusion

Aim of this research is to create a new algorithm which can prevent DDoS attack in VANET. By keeping our Scopes (time, resource and less number of parameter usage.) in mind we proposed and algorithm; which We will conduct our Simulation on SUMO. We expect our proposed algorithm will perform well in the simulation. Whether we or algorithm perform good or bad at the end we will have some important knowledge; which will contribute to the DDoS prevention in VANET sector. In our proposed algorithm we have some voids which we can't avoid due to some circumstances. The first scope that we have in our research is not considering all the scenarios of VANET.Our proposed algorithm was mainly focused on RSU(Road Side Unit) Safety. We have designed the algorithm In a way that all the threats of DDoS attacks could not come to the RSU. We have considered very little about car-to-car DDoS attack safety. The second scope that we have is Lack of knowledge of simulation tools. We had a hard time finding appropriate simulation tools and understanding them. We found the very little amount of resources to learn those tools. Learning those tools took a large portion of our research time. but still, we have a very limited amount of knowledge of those tools, we have implemented our proposed algorithm in basic settings.

References

1. Alrehan, A. M., & Alhaidari, F. A. (2019, May). Machine learning techniques to detect DDoS attacks on VANET system: a survey. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.
2. Cooper, C., Franklin, D., Ros, M., Safaei, F., & Abolhasan, M. (2016). A comparative survey of VANET clustering techniques. *IEEE Communications surveys & tutorials*, *19*(1), 657-681.
3. Haydari, A., & Yilmaz, Y. (2018, November). Real-time detection and mitigation of DDoS attacks in intelligent transportation systems. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)* (pp. 157-163). IEEE.
4. Hossain, M. A., Noor, R. M., Yau, K. L. A., Azzuhri, S. R., Z'aba, M. R., & Ahmedy, I. (2020). Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks. *IEEE Access*, *8*, 78054-78108.
5. Kolandaisamy, R., Md Noor, R., Ahmedy, I., Ahmad, I., Reza Z'aba, M., Imran, M., & Alnuem, M. (2018). A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks. *Wireless communications and mobile computing*, *2018*.
6. Slavik, M., & Mahgoub, I. (2011, July). Applying machine learning to the design of multi-hop broadcast protocols for VANET. In *2011 7th International Wireless Communications and Mobile Computing Conference* (pp. 1742-1747). IEEE.

1. C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna.: Rethinking the Inception Architecture for Computer Vision, In IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp.. 2818–2826, Las Vegas, NV, (2016).
2. B. Zoph, V. Vasudevan, J. Shlens, and Q. V. Le.: Learning Transferable Architectures for Scalable Image Recognition, 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 8697–8710, Salt Lake City, UT, (2018).
3. G. Huang, Z. Liu, L. Van Der Maaten and K. Q. Weinberger.: Densely Connected Convolutional Networks, In IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2261–2269, Honolulu, HI, (2017).
4. Feature scaling, https://en.wikipedia.org/wiki/Feature scaling, last accessed May 2020.
5. Colab, https://research.google.com/colaboratory/faq, last accessed May 2020.
6. Siddiqui, S. A., Salman, A., Malik, M. I., Shafait, F., Mian, A., Shortis, M. R., and Harvey, E. S.: Automatic fish species classification in underwater videos: exploiting pre-trained deep neural network models to compensate for limited labelled data. – ICES Journal of Marine Science, 75(1), pp. 374–389 (2017).
7. Keras, https://keras.io/api/layers/convolution layers/convolution2d, Last accessed May 2020.
8. Understanding AUC-ROC Curve, https://towardsdatascience.com/understandingauc-roccurve-68b2303cc9c5, Last accessed July 30, 2020.