Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020)
IEEE Xplore Part Number: CFP20V66-ART; ISBN: 978-1-7281-4108-4

Comparative Analysis of Various Approaches for DoS attack Detection in VANETs

A.Ilavendhan
Research Scholar, Department of CSE
Pondicherry Engineering College
Pondicherry, India
Ilavendhana62@pec.edu

K. Saruladha
Associate Professor, Department of CSE
Pondicherry Engineering College
Pondicherry, India
charuladha@pec.edu

***Abstract*— VANET plays a vital role to optimize the journey between source and destination in the growth of smart cities worldwide. The crucial information shared between vehicles is concerned primarily with safety. VANET is a MANET sub-class network that provides a free movement and communication between the RSU and vehicles. The self organized with high mobility in VANET makes any vehicle can transmit malicious messages to some other vehicle in the network. In the defense horizon of VANETs this is a matter of concern. It is the duty of RSU to ensure the safe transmission of sensitive information across the Network to each node. For this, network access exists as the key safety prerequisite, and several risks or attacks can be experienced. The VANETs is vulnerable to a range of security attacks including masquerading, selfish node attack, Sybil attack etc. One of the main threats to network access is this Denial of Service attack. The most important research in the literature on the prevention of Denial of Service Attack in VANETs was explored in this paper. The limitations of each reviewed paper are also presented and Game theory based security model is defined in this paper.**

Keywords—Attacked Packet Detection Algorithm, Game theory, Best Response

I. INTRODUCTION

VANET is a category of networks where vehicles on the roadside are able to communicate two or more fashion vehicles. A VANET is an auto-organized network which allows communication for exchange of safety messages between vehicles. This network is likely to play an important role in creating a stable road traffic system and in preventing natural traffic malfunctions. In all communicated nodes the limited range radios are mounted. There is a very short transmission range between the car nodes, less than 300 m away. Based on the categorization of the network [1][3], road side units (RSU) are built randomly. RSU can connect with authorities and vehicle nodes. Such networks have no fixed infrastructure and rely on themselves for networking.

For human life, VANET is important while these people move on the road. The drivers and passengers make the traffic system too nice to use non-safety applications. Examples of this application are the transportation map, exterior car parking accessible. The purpose of both applications is usually achieved. Categories must provide users or drivers on the roads with the correct details. However, the data needed to be right in safety applications and moved on from a source to a destination. So, a secure state is an interruption that cannot create problems for users on a continuous basis. This is especially important for communicating the censorial matter of life between a sender and a receiver. Different securities are one of the largest required. Any node wants to work in the network or communications together with the other node.

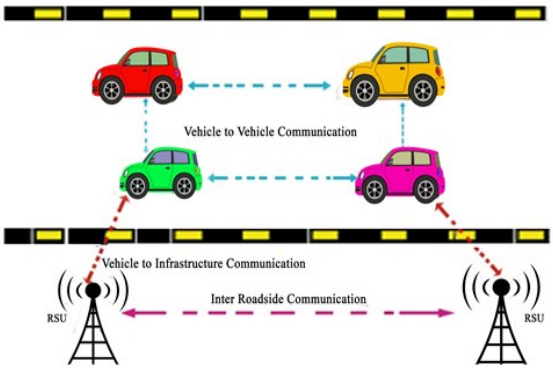

Fig. 1. VANETs Architecture

The network must be available to people those who are in the network. Many researches during the last few years have explored various issues relating to V2I, V2V and Inter Road Side communication represented in Fig.1. They are expected to play intelligently because of their short task. Various companies, governments and institutions around the world were involved in various VANET initiatives over the last decade. Network availability is essential security criteria, not only to ensure the safety prospective but also confidentiality and privacy of data. That can be assured if the network provides even under attack, even if its power metrics are not compromised. This article presents a full overview of the most significant research work on the detection of the VANETs DoS attack and finally introduced the proposed model using game theory for detecting DoS attack.

II. DOS ATTACK

In this attack, the assailant attacks the media for channel jam formation. The channel is no longer available and cannot be reached by the nodes. The basic concept is to

overload the network and make it difficult for legitimate nodes to access networks and means. The vehicle nodes and network infrastructure will be destroyed and overdue. The network cannot run properly and refuses services to authentic nodes and performing several other unnecessary functions. An intruder may target the VANETs by inside or outside. The key goal is to prevent legitimate users from accessing the network. This is achieved by passing a wide number of messages that are unrelated on the control channel. DoS attack[20] mainly affects major bandwidth, CPU and memory resources. The assailants can target the network by jamming, overloading, or losing packets, and causing DoS attacks. The following are the two cases of DoS attacks:

Case 1:- The attacker's main objective is to use network resources so that legitimate users can no longer access resources. This implies that the vehicle nodes in the network cannot carry out all the essential activities, and the information between all the nodes cannot be communicated. In this scenario, an intruder sends a message of warning about accidents in Vehicle to Vehicle architecture shown in Fig.2. The Malicious vehicle intentionally flooding the lane close ahead message to RSU and genuine vehicle V1. In that situation RSU and V1 are busy for receiving the messages from the malicious vehicle.

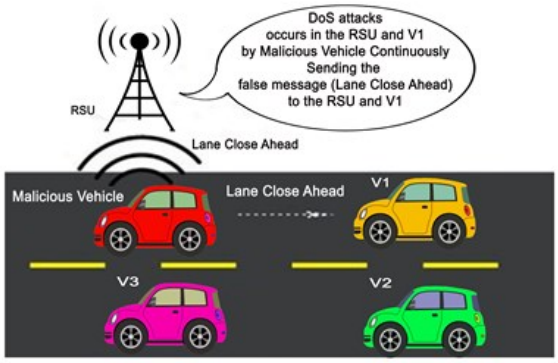

Fig. 2. DoS attacks in V2V and V2I

Case 2:- In this set-up, the attacker vehicle target the Road Side Unit by sending the unwanted message. The RSU is overwhelmed with proofing and does not support the other nodes for communication. The Vehicle Nodes on the network not able to communicate with the RSU due to the overloading of unwanted messages sent by the malicious vehicle.

III. Various Mitigation Methods for DoS Attack

A. Attacked Packet Detection Algorithm

In this method the author used the Attacked Packet Detection Algorithm (APDA)[1][15] to detect the DoS attack. This APDA is incorporated in all RSU, using that the vehicle passing the information to the other vehicle. It helps to detect the location of the vehicle those who sent the messages to other vehicle in the network. The RSU stores the location of the vehicle. Each vehicle stores the information about position, acceleration and frequency of the vehicle. This can be achieved by devices like OBU and TAMPER PROOF. The APDA identify the attacker by tracking the location which is already registered in the RSU.

B. Enhanced Attacked Packet Detection Algorithm

This model uses control packets to communicate through RSU. Using the EAPDA [2][15] algorithm, RSU examine the vehicle packet. After examined the packet in the RSU, the vehicle are allowed for network services. This improves the accessibility to valid nodes for the network resources, thereby increasing the network's performance. During the testing phase, the malicious nodes are detected. RSU measures the time that this request is submitted and received, and the number of vehicles that apply the application in order to assign a time limit to all nodes.

C. MIPDA Method

Malicious and Irrelevant Packet Detection Algorithm (MIPDA)[3] equipped with all RSU in the VANET. Using this algorithm the vehicle communicates with RSU. This algorithm stores and tracks the location information in the RSU. If the malicious vehicle enters in to the network the MIPDA algorithm finds the malicious and irrelevant packets sent by tracking the stored information in the RSU.

D. MMPDA method

In MMPDA[4] method the malicious node detection can be divided into two broad groups called node centeric and data centeric algorithms. Malicious nodes are identified with authentication mechanisms such as security keys, encryption and digital signatures in Node-centered schemes. Instead of data being shared between nodes, the node centric method tracks the nodes. In data centric approach it examines the data for isolating the DoS attack. When the bandwidth of the vehicle reaches the threshold level, the vehicles are labeled as malicious.

When identified as malicious, the node is isolated and a separate path is taken between the source and destination. The multiple malicious and irrelevant nodes in this algorithm are both identified by entropy values. Entropy determines the node intrusion. It is typically used when the network under DoS attack to distinguish between the ordinary and abnormal behavior. For sending packets, MMPDA selects a source node, destination node and RSU. The nodes are clustered where each cluster comprises a single source, target and number of intermediate nodes. Based on the importance of distrust, the cluster head that helps to route packets is selected. The lowest node of mistrust is taken as the center of a cluster. Some of the middle nodes will be used as checking nodes to track the nodes ' behavior. Comparing the node's threshold value with the allocated bandwidth, if it exceeds then isolate the nodes in the attacked area.

E. GDVAN Method

In GDVAN[5] (Greedy Detection for VANETS) the author proposed a Greedy algorithm for identification of

malicious behavior of VANETs The GDVAN is using three newly developed metrics which have been used for greedy behavior identification in high mobility environment in the VANET, due to short span of time and connections it is necessary to adjust backoff parameters adaptively. The report is based respectively upon improved linear regression and fuzzy logic principles, consisting of two suspicion and decision phases. The algorithm can check whether there are greedy nodes by monitoring network traffic tracks. GDVAN is passive, non-resource intensive and needs no modification of the MAC layer. It also has the advantage of being transparent to users and can be done via any network node.

F. Dempster-Shafer method

The author used artificial intelligence based self-organized map and Dempster-Shafer[6] theory to identify the malicious nodes. The author used the trace file to train network, and these trace files serve as input into self-organized maps so that network can be supervised for identify such malicious vehicles. For the identification of malicious behavior the author used SOM classification. The category of malicious nodes generated and Dempster-Shafer theory is used to identify the attacker's node in this classification.

G. Signature Based Authentication(SBA) Method

In this approach, the author proposed a two-stage system to mitigate DoS attackers within and outside VANETs. The first step involves the authentication of a communicating entity with HMAC signatures [7] computed from both private and public key. Since the HMAC can only be determined by authentic users, DoS attack is mitigated by external attackers. The second stage is designed to block the inside attacker if the individual is authentic and subject other vehicle to DoS attack. In this step, it is contrasted with a threshold value to classify the internal attacker based on the number of unworthy signatures inundated by the attacker.

H. IP-CHOCK (filter)-Based Detection Scheme

In this the author utilize the Bloom filter[8] to identify the malicious vehicle, which provides a service for VANET legitimate vehicles, to recognize and protect against IP spoofing of DoS attack. The malicious vehicle has been examined during DoS attack performed in the network. The author defined the detection method into 3 phases. The result of these processes is that the change is sensed through the sensors attached to the vehicle in the first stage. In the second phase, the values of these sensors are analyzed to determine whether these values are able to influence the network. The third phase plays the function of detecting DoS attacks in the facilities once the decision is adopted. This approach provides a safe and bandwidth free communication.

I. Port Hopping Defense Strategy

In this method author introduced the Port Hopping defense strategy[9] to mitigate the DoS attack. Port hopping and a single linear space are implemented in order to implement a simple and elegant defense strategy to adjust the port numbers of the vulnerable networks for V2V and V2I communications in various service slots. A new scheme represented as security strategy matrices to detect the port numbers tested by DoS attackers was implemented to resolve the ambiguity of DoS attacks in complex VANETs.

J. IDMD Method

In IDMD[10] (Improved Detection and Mitigation of DDoS) model the author's main idea is to detect and mitigate the DDoS attack. Two stages consist of attacking topology and congestion of the network. This is initially completed. The second phase consists of the DDoS attack detection and mitigation that will detect an aggressive node performed by vehicular ad-hoc network to refuse the service by checking each node's bandwidth usage on the network, then checking each node's defined threshold and whether the threshold is high then checking the channel at the specified data rate, and then de-allocating the channel.

K. MVSV Method

In order to detect and mitigate the DDoS Attack on VANET, Multivariant stream analysis (MVSA)[11][19] was introduced by the author. MVSA provides V2V communication through RSU. The identification of a DDoS attack begins with reading the trace of the network and decides an average payload rate, frequency at various times and the time to live per vehicle for each strike class. Following this, the method uses traces to measure the stream weight. At last, MVSA classifies the packet as either genuine or malicious. A NS2 simulator was used to test the MVSA performance and the simulation results show the reliability and quality of the MVSA.

L. Machine Learning Method

The author suggested the Anomaly detection based on machine learning [12][13][16] has been introduced on VANET. They have developed a system to detect the DDoS attack in SDVN quickly. Three models have been included in the proposed framework: trigger detector, object selection flow table application, module attack detection. A trigger mechanism based on the message packet was suggested in the first module. They have developed a flow table DDoS attack detection approach in the flow table entry module by combining the DDoS attack and the OpenFlow protocol functionality.

The SVM[17] classification is used in the attack detection module to train and construct a detection model for finding out if the DDoS attacks[14][18] on the network. In addition, the authors generated Scapy and hping3 DDoS attack traffic. DDoS Attack capabilities have also been studied by the UDP, ICMP, and TCP protocols. The results of the simulation show that the classification detection has a lower false alarm rate and the proposed system effectively reduces the start time for attack detection. The Comparative analysis of above methods is listed in Table 1.

TABLE I. COMPARASION OF VARIOUS MITIGATION METHODS

DoS Attack Mitigation method	*Objective*	*Limitations*	*Evaluation metrics*
APDA[1]	To be applied to avoid the delay overhead and enhance the security of VANET	It is difficult to manage the RSU in the networks for tracking the attacker's location.	Packet Delivery Ratio and packet Drop ratio
EAPDA[2]	To check and record the vehicle information for identify the unusual behavior of the vehicle	It takes more time for verification of the nodes.	Throughput, False Positive rate & Delay
MIPDA[3]	To analyze the power of packet generation and reduce delay overhead by detecting the malicious nodes.	Computing the vehicle position in RSU takes maximum time	Delay overhead
MMPDA [4]	To detect the multiple malicious node in the network by entropy and bandwidth	The detection rate of malicious node is minimum due to increase of malicious nodes	Throughput, Packet Drop Ratio, Packet Delivery Ratio, False Positive Rate
GDVAN[5]	To govern the network traffic for analyse the behavior of greedy nodes	If the greedy node increases. The false positive rate is maximum	Minimum Detection Time, connection duration.
Dempster-Shafer[6]	To trace a trace file for providing the self-organized map to supervised learning to the network.	The detection of misbehavior rate is low	Throughput, Packet Delivery Ratio, Routing overhead
SBA[7]	To detect the malicious node by identifying the invalid signature sent by the attacker	If the attacker send Bogus information this method not so successful	Authentication Delay
IP-CHOCK (filter) [8]	To filter the malicious vehice it uses the Bloom filter for giving the services to genuine vehicle	This method not works for high traffic environment.	Detection Delay Time, Percentage of attack, Detection time, Detection probability
Port Hopping Defense[9]	To manage the vulnerable service port number used to V2V and V2I communication at various service slots.	It fails to handle the issue of hopping frequency	Attack Success Rate, Vulnerable service's port, Hopping Frequency
IDMD[10]	To isolate the malicious node when multiple malicious node attack the victim	The bandwidth consumption is high and managing the control packet is difficult	Throughput, Routing overhead, Packet loss
MVSA[11]	To classify the malicious or genuine packet by trace the payload and frequency of each stream class.	The reduce in the packet latency is not extremely guaranteed to detect the malicious node	Packet Delivery Ratio and packet Drop ratio
Machine Learning Method[13]	To analyse the misbehavior node by Support Vector Machine	The false positive rate is maximum	Throughput, Packet Delivery Ratio

IV. GAME THEORY

Game theory offers methods in competitive environments to assess optimal actions. A game formally refers to all situations involving the making of rational decisions by two or more intelligent people. The players make consistent decisions to achieve the assumed goal. When the player knows the rules of the game and can make decisions based on his experience, the player is considered intelligent. Game theory is the mathematical model which will predict the behavior of the vehicles accurately, when compared to other mitigation method discussed in this article. In this paper game based security model is defined by using the characteristics and behavior of the three non-cooperative games is zero-sum game, Bayesian game and stackelberg game. The following Fig.3 illustrates the detection of attacker vehicle in V2V communication.

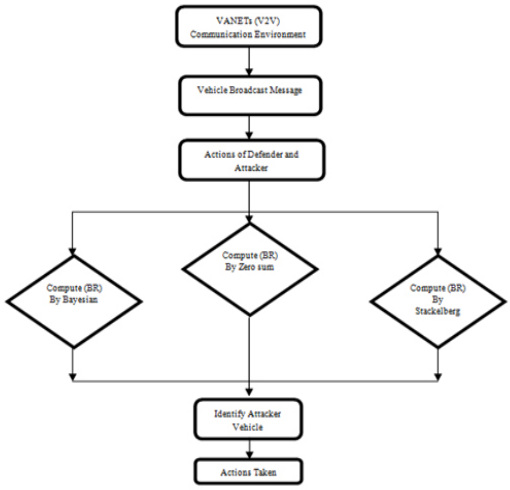

Fig. 3. Game theoretic model

From the above Fig.3 it is observed that vehicle broadcast message is analyzed by the (BR) Best Response is computed between the attacker and defender for each game which is illustrated. According to the Best Response it is easy to analyze the behavior of the malicious vehicle for genuine vehicle communication. Consider attacker and genuine vehicle enter into the V2V communication; the proposed Game model is implemented between the vehicles. The action of each

player is considering for analysis the behavior of the vehicle. This analysis is done by finding the Nash Equilibrium (BR intersection) point in the game. It means that no other player cannot deviate its action. This situation is used for analyze the vehicle behavior for identifying the malicious vehicles.

V. CONCLUSION

In this paper, the different methods of calculating and mitigating DoS attacks have been reviewed. The efficiency and limitations of each of the techniques examined underlines the value measured by the packet delivery rate, packet drop ratio and channel usage rate. This article extracts the limitation of the existing methods and solves those issues by the defined Game theory based security model for defending the DoS attack. The future work is to study and concentrate to mitigate the all possible network attack like Blackhole attack, Wormhole attack, Sinkhole Attack and Sybil Attack which is in-cooperated in the VANETs.

REFERENCES

[1] S.RoselinMary,M. Maheshwari, M.Thamaraiselvan, "Early Detection of DoS Attacks in VANET using Attacked Packet Detection Algorithm (APDA)," In the Proceedings of IEEE International conference on Information Communication and Embedded Systems ISBN :978-1-4673-5788-3, 21-22 Feb. 2013

[2] Amarpreet Singh, Priya Sharma, "A Novel Mechanism for detecting DoS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)," In the Proceedings of IEEE 2nd International conference on Recent Advances in Engineering & Computational Sciences , ISBN: 978-1-4673-8253-3, 21-22 Dec. 2015.

[3] Abdul Quyoom, Harish Sharma "A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)," In the Proceedings of IEEE International Conference on Computing, Communication & Automation, ISBN: 978-1-4799-8890-7, 15-16 May 2015.

[4] Sushil Kamboj, Kulwinder singh, " Detection of Multiple Malicious Nodes using entropy for mitigating the effect of Denial of Service Attack in VANETs," In the Proceedings of IEEE 4th International Conference on Computing Sciences, ISBN: 978-1-5386-8025-4, 30-31 Aug 2018.

[5] Mohamed Nidhal,Jalel Ben-Othman " GDVAN: A New Greedy Behavior Attack Detection Algorithm For VANETs," In the Proceedings of IEEE Transactions on Mobile Computing, ISSN: 1536-1233, pp 759-771, June 2016.

[6] Neha Kushwah, Abhilash Sonker " Malicious Node Detection on Vehicular Ad-Hoc Network Using Dempster Shafer Theory for Denial of Services Attack," In the Proceedings of IEEE 8th International Conference on Computational Intelligence and Communication Networks, ISBN: 978-1-5090-1144-5, 23-23 Dec 2016..

[7] B. Pooja, M. M. Manohara Pai , Radhika M Pai , Nabil Ajam , Joseph Mouzna, " Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," In the Proceedings of IEEE Asia-pacific Conference on Computer Aided System Engineering, ISBN: 978-1-4799-4568-9, 10-12 Feb. 2014.

[8] Karan Verma, Halabi Hasbullah, " IP-CHOCK (filter)-Based detection scheme for Denial of Service (DoS) attacks in VANET," In the Proceedings of IEEE International Conference on Computer and Information Sciences, ISBN: 978-1-4799-4390-6, 3-5 June. 2014.

[9] Yingmo Jie , Mingchu Li , Cheng Guo, Ling Chen, " Dynamic Defense Strategy against DoS Attacks over Vehicular Ad hoc Networks Based on Port Hopping," In the Proceedings of IEEE Access, DOI: 10.1109/ACCESS.2018.2869399, September. 2018.

[10] Charu Guleria ; Harsh Kumar Verma, " Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network," In the Proceedings of IEEE 4th International Conference on Computing Communication and Automation, ISBN: 978-1-5386-6947-1, July 2019.

[11] Raenu Kolandaisamy,Rafidah Md Noor, Ismail Ahmedy, Iftikhar Ahmad,Muhammad Reza, Muhammad Imran and Mohammed Alnuem, "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks," In the Proceedings of Hindawi ,Wireless Communications and Mobile Computing, DOI: 10. https://doi.org/10.1155/2018/2874509, May 2018.

[12] M. Kim, I. Jang, S. Choo, J. Koo, and S. Pack, "Collaborative security attack detection in software-defined vehicular networks," 19th Asia-Pacific Netw. Oper. Manag. Symp. Manag. a World Things, APNOMS 2017, pp. 19–24, 2017.

[13] Alia Mohammed Alrehan , Fahd Abdulsalam Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," In the Proceedings of IEEE 2nd International Conference on Computer Applications and Information, ISBN: 978-1-7281-0108-8, July 2019.

[14] Viswacheda, Ali Chekima and Jamal, "Detection and Mitigation of DoS Attacks in VANET using Secured Minimum Delay Routing Protocol, In Proceedings of International conference on Soft Computing and Pattern Recognition, Advances in Intelligent Systems and Computing, DOI: 10.1007/978-3-319-60618-7_46,Springer, 2018

[15] Sushil Kumar, and Kulwinder, "Detection and Mitigation of Denial of Service Attacks in VANETs using Packet Detection Algorithm," In Proceedings of International Journal for Research in Applied Science & Engineering Technology (IJRASET),ISSN:2321-9653,, Mar. 2018.

[16] S. So and J. Petit, "Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET," 2018 17th IEEE Int. Conf. Mach. Learn. Appl., pp. 564–571, 2018.

[17] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," Veh. Commun., vol. 13, pp. 56–63, 2018.

[18] F. A. Ghaleb and F. Mohammed, "An Effective Misbehavior Detection Model using Artificial Neural Network for Vehicular Ad hoc Network Applications," pp. 13–18, 2017.

[19] A. Haydari, , "Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems," September 2018.

[20] Deeksha, Ajay Kumar, Manu Bansal, , "A Review on VANET Security Attacks and Their Countermeasure," In the Proceedings of IEEE 4th International Conference on Signal Processing, Computing and Control, ISBN: 978-1-5038-5838-9, 21-23 September. 2017.