International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 7, Issue 3, May - June 2018 ISSN 2278-6856

The DDOS Attack Detection and Prevention in VANET by Group Controlled Analysis Model

VIPIN , Dr.Rajender Singh Chhillar

Department of Computer Science & Application, MaharshiDayanand University, Rohtak, Haryana, India

Abstract :*A Vehicle network is combination of mobile and sensor network features,vehicle network have high chances of DOS attack due to heavy traffic and infrastructure specification. Distributed Denial of Services (DDOS) Attacks in the network affects the communication of network and degrade the network reliability and performance. In Vehicular Ad Hoc Network (VANET) these DOS attack occur because of heavy trafficand slow down the communication. For prevent the DOS attacks, dynamic group based model is implemented. At the dynamic group based model method have mobility and stability analysis for generating the dynamic groups and identifying the virtual controllers. The communication within group analysed by the controller, the safe and unsafe nodes prioritize by the controller. Also the preventive node selection is performed by controller node. After the simulation, the results are comes clearly shows that the model method improves the communication throughput and reduces the communication loss.*

Keywords:-VANET, DDOS, Controller, Group Based,DOS, Communication.

INTRODUCTION

VANET is vehicle network that work with restricted resources and environment constraints, itincreases the criticality of the network. For improving optimization of network, it required improvement in communication behaviour of the network and improvement in the architecture of the network. A vehicle network required to work in real time environment that required time specific communication and work in dynamic manner. Different aspect and factors that affect network performance and life time of network are listed here under

Deployment in VANET

The improvement of network started with the deployment of network adaptively for arranging the nodes and controller in such manner maximum utilization of resources and maximum network coverage area. It will consider the problem of congestion situations and bottle neck did not occur, these problems are solved by deployment of resources distribution in equalized manner. Deployment must have adaptive approach to the architecture, environment, routing and application. Deployment in such manner that alternate node selection for communication will be done on requirement. Effective network deployment required network density, infrastructure devices and the service distribution.

Topology in VANET

Topology of the network is the architectural specification of network which depend on activity performed and the application of the network. Topology defines the utilization of network by specific pattern of placement of nodes and the deployment and the controllers in the network. The topology defined in the form of star topology, ring topology, bus topology in the standard form. Topology in higher form defined as network scenarios. And these scenarios have formation of class room scenario, war-zone scenario and road side scenario etc.

Topology Control in VANET

Topology control provides the transmission control and communication control for a network by its controlling the topology. Topology control is also provides control over energy consumption in the network by controlling the topology. Topology control is the architectural constraint which can provide effective resource management and effective communication. Topology control is required for communication at node level and network level.

Routing in VANET

For effective data delivery, there is requirement of an effective routing approach in the network and routing must be controlled by domain specific, communication specific and environment specific constraints.Communication performed over the network by help of routing according to the application and the process requirement and it can be single-cast or multi-cast. Routing generate the multi-hop adaptive path for energy optimization. Optimization of network communication in clustered network is performed by intra-cluster and inter-cluster routing. Routing in more critical network, fault and some other constraints are considered for route optimization of the network.

In VANET optimization of network communication requires the stage specific solution. Vehicle network objective is to achieve hazel free network communication in adaptive manner of communication between vehicles and devices. Vehicle communication is also requires energy efficient and less congestion.

Application

According to the application of vehicle network, requirements and communications are driven. Role of vehicle nodes are defined according to the application and process. Application specification defines the features of node criticality, fault prone and energy requirements of network. Application specification also defines the network problem and requirements. Architecture type of network and homogenous or heterogeneous node type is also defined by application of network.

LITERATURE REVIEW

In VANET DDOS attack is occur because of heavy traffic in the vehicle network. DDOS attack slow down the network communication and also disrupt the service access in the network. DDOS attack also made unavailability of services like situations in the network. Many researchers made effort provide the identification and solution of these problems [1]. Chock filter based detection also provides the identification and solution of DDOS attack. Bloom filter integration is used for identification of malicious node identification. The availability of services to the vehicle is analysed relative to different resources of network [2]. UDP spoofing defensive mechanism is used for prevention from DDOS attack in vehicle network. Defensive mechanism is based upon storage effective tracking of incorporating IPs. Flooding attack defended by resource utilization given by light weight method. It reduces the computation cost and storage allocation [3].Protocol tunnelling, unauthorised access, DOS attack problem are identified and solution for these problem is provided by model. Model applies the time critical analysis for safe transmission of data over the network and security framework is provided for reducing the effect of attack on network [4].Security measures and metrics specification are considered by defensive mechanism. Design of VANET is implemented by channel specific observation and validation. Mobility constraints and environment constraint with resource utilization and integrated security are considered in mobility preserved communication model. The markov chain model has provided the security under automata network, jamming attack prevented with attack modelling [5]. Attacked Packet Detection Algorithm (APDA) provides the DDOS attack detection and prevention, it analysis the packet and communication pattern [6]. The model reduces delay overhead and improves communication. Sniffing attack is prevented by flooding algorithm. Master chock filter method provides the traffic analysis [7]. Mobility model provides the protocol specific evaluation of nodes in network. Sniffing attack is prevented by flooding algorithm. Reference broadcast scheme is achieved by pair wise synchronization to achieve the reliable communication. Enhanced Attacked Packet Detection Algorithm (EAPDA) provides the improved DDOS detection mechanism for VANET [9]. It is work on performance driven measures to reduce the communication delay and attack preserved model was provided the adaptive work solution. It also observed the problem and attack criticality and provides the robust solution. The trust adaptive method is recognizes the bogus message communication and a secure signature specific authentication technique for prevention of DDOS attack [10].

Thread model is used for security evaluation and attack prevention in the communication network. Safe network communication was achieved by trust preserved network. The message integrity, authorization and confidentiality are provided by swarm based model [11]. Routing specific process provided for solution of DDOS attack in sensor network [12]. Multiple network path used for secure routing method is implemented.

RESEARCH METHODOLOGY AND IMPLEMENTATION

In a wireless network with heavy communication traffic, attacks like DDOS attack are common. Heavy communication traffic in a vehicle network slows down the communication and also occupies the resources of network communication unnecessarily. For a safe and effective communication in VANET, there is need to identify the attack in earlier stages. A group adaptive controller based method is used for detection of DDOS attack in the VANET. All the process in group adaptive controller based method is based on group formation.

In VANE T infrastructure is based on road side units and network of vehicle devices. Heavy traffic flow in road side unit network causes the loss of communication. For solving these problems physical characterization of vehicle nodes is performed including the mobility and position of nodes. From the observations, virtual groups are formed by vehicle nodes. Group formation is done by consideration of direction, position and speed specifications. The centralized node of group is considered as the controller node in VANET. Controller of network is observes the nodes in the network and control the communication in the VANET.

Controller node of network is perform communication analysis and takes the consideration of communication delay, response time and communication loss. On these parameters of the vehicle network the adaptive nodes are identified. Parametric analysis is categorizes the nodes in safe and unsafe node.

Table 1:- Parametric Analysis

```
If ( CommLoss (VehicleNode)=Low,
CommDelay (VehicleNode)=Low And
Response Time(VehicleNode)=Low)

{

Set VehicleNode.Type=safe

}

Else If ( CommDelay (VehicleNode)=Low And
ResponseTime(VehicleNode)=Low)

{

Set VehicleNode.type=safe

}

Else If ( CommDelay (VehicleNode)=High,
CommLoss(VehicleNode)=High)

{

Set VehicleNode.type=unsafe

}
```

Parametric analysis provides the rules for detection of the attacker nodes and safer nodes. Communication in the Vehicle network performed by safe node because it provide

improved communication between devices in vehicle network.

RESEARCH IMPLEMENTATION RESULTS

NS2 Environment is used for implementation and simulation of vehicle network for this research work. A network taken with the 50 Vehicle nodes and heavy communication traffic flows to simulate the DDOS attack. Simulation results are taken with consideration of Packet Transmission Parameters, Bytes Communication Parameters, Bitrate Parameters and Communication Delay Parameters.

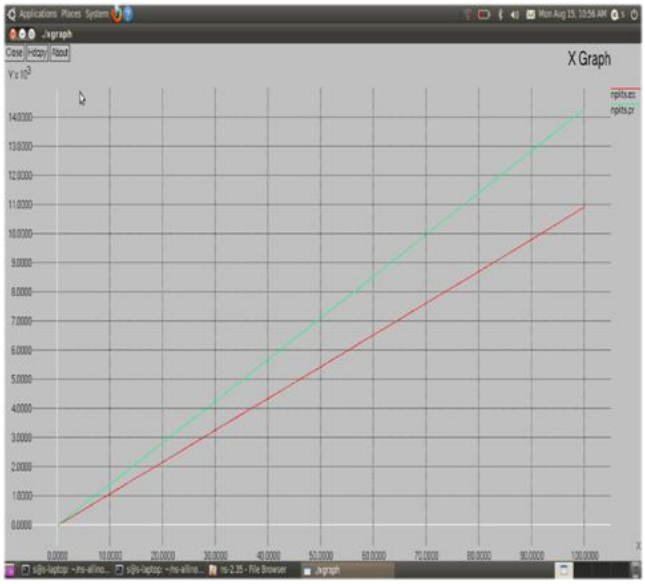

Figure 1:- Packet Communication Analysis

In figure 1 analysis is done for Packet Communication and shows the packet delivery in the network simulation. Outcome shows that this method improves the packet communication in the VANET. And gives attack preventive solution.

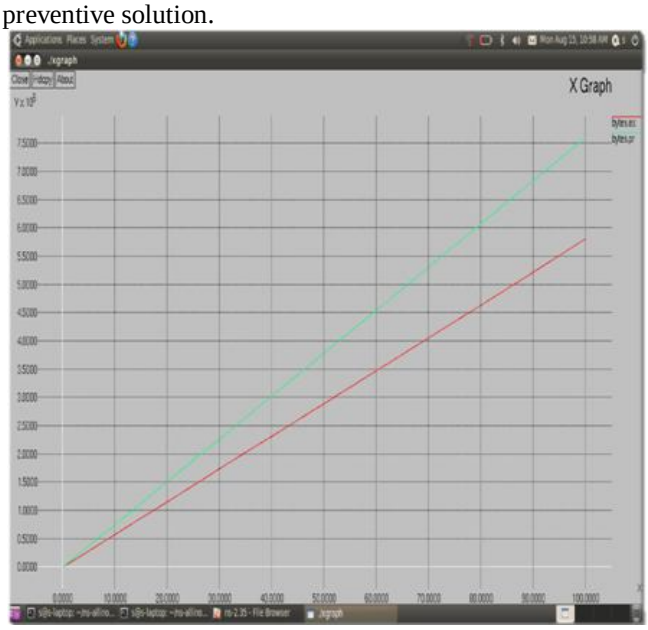

Figure 2:- Bytes Communication Analysis

In figure 2 analysis is performed for bytes communication and it shows that number of bytes communicate in the vehicle network or transmission of data from one node to other nodein more comfortable manner. This method improves the byte communication and prevent from DDOS attack.

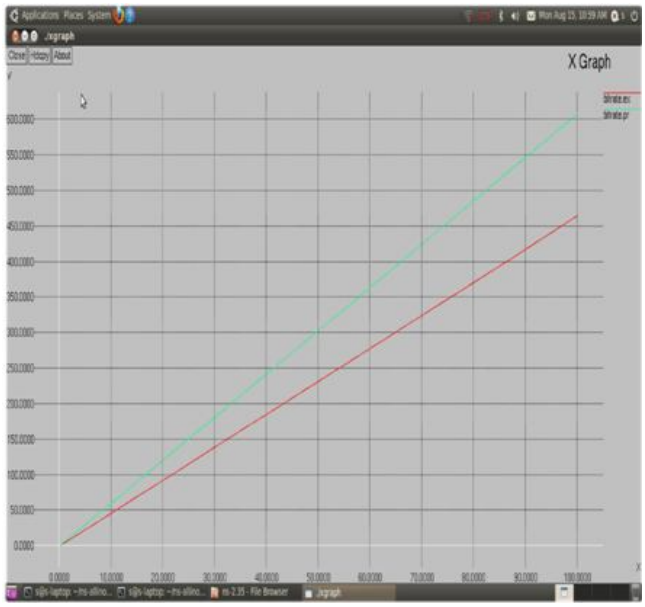

Figure 3:- Bitrate Analysis

In figure 3 Analysis is performed for bitrate communication form one node to other node. It shows improved bitrate communication and provides more convenient transmission of data in secure manner because DDOS attack prevented by this method.

Figure 4:- Communication Delay Analysis

In figure 4 Analysis is performed for communication delay in the vehicle network. It shows clear result that communication delay are prevented by this method and provide better communication in vehicle network by prevention of attack.

Analysis is also performed in comparative manner by Communication Throughput, communication PDR and Packet Lossrate Parameters. Throughput communication parameter provides the packet communication per 900 packets. Throughput is also observes the number of successful communication performed. Packet Delivery Ratio (PDR) is represents the ratio driven observation of successful packet delivery. Communication Loss Analysis is observes the communication failures.

Table 2:- Comparative Analysis

Measures Performance	Existing Techniques	Proposed Model
Throughput	517.48	743.47
PDR	83.16	87.27
Communication Loss	4.87	0.83

Table 2 provide clear result of Comparative Analysis in which communication throughput, Packer Delivery Ratio (PDR) and Communication Loss parameters. The table show clear result, this approach improves the Communication Throughput and Packet Delivery Ratio. On other side it decreased the Communication Loss. This method improves the communication reliability.

CONCLUSION AND FUTURE SCOPES

The group formed method is observes the communication problems and track the communication problems in early stages. The group formed method is provides effective communication. It analyse the network communication and taken consideration of smaller region of vehicle network. It prevents the DDOS attack in the VANET and reduces communication loss. This method proves better and improved communication in VANET.

REFERENCES

[1] HalabiHasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "Distributed Denial of Services (DDOD) Attack and Its possible Solutions in VANET," Word Academy of Science, Engineering and Technology, 67. 2011.

[2] Karan Verma, HalabiHasbullah, Ashok Kumar, "An Efficient Defence Method against UDP Spoofed Flooding Traffic of Denial of Services (DOS) Attacks in VANET" Advance Computing Conference 2012 IEEEDeptt. Of computer & Information Sciences University Petronas, Malaysia.

[3] PathreTyagi and D. Dembla, "Investigating the security threats in VANET Towards security engineering for safer on road transportation," Advances in communications and Informatics conference New Delhi,2014, pp. 2086-2091.

[4] M. Raja and J. P. Hubaux, "Securing Vehicular Ad-Hoc Network", Journal of Computer Security, 2007 pp. 40-65.

[5] J. Ben-Othman and L. Mokdad, "Modeling and Verification tools for Jamming Attacks in VANET," 2014, IEEE Global Communication Conference, Austin, pp. 567-573.

[6] S. RoselinMary, M. Thamaraiselvan and M. Maheshwari, "Early Detection of DDOS attacks in VANET by Attacked Packet Detection Algorithm (APDA)," Information Communications and Embedded Systems (ICICES), 2013 International Conference, Chennai, pp. 230-241.

[7] Qingzi Liu, Qiwu Wu and Li Yong, "A hierarchical security architecture of VANET" International Conference on Cyberspace Technology, Beijing, China, 2013, pp. 6-10.

[8] I. A. Sumra, I. Ahmad, H. Hasbullah and J.I. bin Ab Manan, "Classes of attacks in VANET", International conference on Electronics, Communications and Photonics Conference (SIECPC),Riyadh,2011, pp. 1-5.

[9] A. Singh and P. Sharma, "A novel Mechanism for detecting DDOS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)", 2nd International Conference on Recent Advances in Engineering & Computational Sciences, Chandigarh, 2015, pp. 1-7.

[10] L. Bariah, D. Shehada, E. Salahat and C. Y. Yeun, "Recent Advances in VANET Security: A Survey", IEEE 82nd Vehicular Technology Conference, Boston, 2015, pp. 1-8.

[11] L. Chen, H. Tang and J. Wang, "Analysis of VANET security based on routing protocol Information", Fourth International Conference on Intelligent Control and Information Processing (ICICP), Beijing,2013 pp. 134-138.

[12] L. Mokdad and J. Ben Othman, "Performance evaluation of security routing strategies to avoid DDOS attacks in WSN", Global Communication Conference, IEEE, Anaheim, 2012, pp. 2857-2861.

AUTHOR

VIPIN is a full-time student studying for his M.Tech in Computer Science at Dept. of Computer Science in MaharshiDayanad University, Rohtak, Haryana, India. He received hisB.Tech degree in Computer Science Engineering from MaharshiDyanand University, Rohtak, Haryana, India in 2013. Then he worked in Xerox for 2 years as Data Base Administrator and 1 year in R&D Team for future Researches and Implementation of researches for better Human life in communication and transfer of information, storage of information in secure and reliable form. During 2016-2018, he registered in M.Tech (Computer Science). His current research interests are Mobile Computing and Vehicle Ad Hoc Networking.

Dr.Rajender Singh Chhillar is a senior professor and HOD in the Dept. of Computer Science and Application of MaharshiDayanad University, Rohtak, Haryana, India. He received Ph.D, MBA degree. He has published a large number of International conference papers and journal article on different range of research areas such as software testing, metrics, data mining, data warehousing, oo metrics, software quality and faults.