International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 1, January - February 2017 **ISSN 2278-6856**

A Group Controlled Analysis Model DDOS Attack Detection And Prevention In VANET

Pooja Mittal , Sindhu Grover

Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India,

Abstract

A vehicle network is the critical network with combined features of mobile and sensor network. The heavy traffic and the infrastructure specification increases the chances of DOS attack in the network. In this work, dynamic group based model is provided to generate the DOS prentive communication. At the first stage of this model, the mobility and stability analysis is done to generate the dynamic groups and to identify the virtual controllers. Now, the controller analyzes the communication within group and prioritize the safe and unsafe nodes. As the communication performed the preventive node selection is performed by the controller node. The simulation results shows that the model improved communication throughput and reduce the communication loss.

Keywords : DOS, VANET, Preventive, Group Based, Controller

1.INTRODUCTION

A Vehicle network is the adpatively deployed entwor defined with specification of environment constraints and applied in real time network. The restricted resources and constraints increases the criticality of the network. To optimize the network, there is the requirement to improve the architecture and the communication behaviour of the network. Different factors that affects the network life and the performance are listed hereunder

Topology

The topology is the architectural specificatio of the network that depends on the application and the activity performed in the network. It actually defines the deployment and placement of nodes and the controllers in specific pattern so that the network utilization will be done. In the lower form, the topology is defined in standard form such as ring topology, star topology etc. In the higher form, network scenarios are defined. These scenario includes class room scenario, war-zone scenario etc. The distribution of the resources is also defined by the network.

Application

The requireemnt and communication characterizatio can be adjusted based on the application. According to the application and the process, the roles of Vehicle nodes are defined. The heterogeneous or the homogenous node type, architecture type can be defined for the network. The node criticality, energy left, fault prone features can be defined based on the application specification. The network problems, distortion and attack probability is also defined according to the application specification. The security requirement, optimization requirement can be defined based on the application type. Some constraints at different level can be upgraded or updated based on the application environment.

Routing

After setting up the architecture and the protocol, the final requirement is to perform the communication over the network. According to the application and the process requirements, the communication can be single-cast or multi-cast. To ensure the effective data delivery, there is the requirement of an effective routing approach. The routing must be controlled by some environment specific, domain specific and communication specific constraints. The routing is about to generate the cooperative multihop adaptive path under distance and energy optimization. In more critical network, fault and some other constraints are considered for route optimization. In clustered netwrok, the intra-cluster and inter-cluster routing are the major requirements to optimize the network communication.

To optimize the network communication, the stage specific solution is required. In Vehicle network, the main objective is to achieve the energy adpative and fault prone communication. Different methods and the improvement at various stages are given here under

Deployment

The first level improvement to the network can be achieved by deploying the network adaptively. The arrangement of the nodes and controller is done so that the maximum network coverage and resource utilization will be achieved. The deployment is about to provide the equalized distribution of resources so that the startvation,

bottle neck and congestion situations will not occur. The deployment must be considered in such way, the node degree must be higher so that the alternative node selection will be done on requirement. Deployment must be adaptive to the application, environment, architecture and the routing. The network density, infstructure devices and the service distribution is provided for effective network deployment.

Topology Control

The topogy control is the another architectural constraint defined to provide the effective communication and resource management. The energy consumption over the network can be controlled by controlling the topology. The topology adjustment is required to achieve the communication at node level and network level. The transmission control, communication control can be achieved via topology control.

2. LITERATURE REVIEW

DDOS attack is common attack form that occur in a network because of heavy traffic. In not only slow down the communication but also disrupt the service access. The unavailability like situations can occur in this attack form. The efforts of earlier researchers is provided in this section. Verma et. al.[1] has provided the work on Chock filter based detection scheme against the DOS attack. The malicious node identification was here done using Bloom filter integration. The service availability to the vehicle is analyzed relative to different resources. The defensive mechanism was introduced by the author. Verma et. al.[2] has provided the UDP spoofing for prevention from DOS attack in vehicle network. The method was based on the storage effective tracking by observing the incorporating IPs. The lightweight method was provided with resonable reosuce consumption to defend from flooding attack. The method reduced the storage allocation and the computational cost. Tyagi et. al.[3] has analyzed the threats in vehicle network and provided the authentication preserved solution against the attack. Different suspectible problems were recognized by the model inlcuding protocol tunneling, eavedropping, unauthorized access and DOS attack. The model observed the topological structure of the network and applied the time critical analysis to identify the safe transmission over the network. The security framewokr was provided to reduce the attack impact over the network. Azogu et. al.[4] provided the anti jamming method by applying the carrier sensing. The defensive mechnism was directed by author with specification of security metrics and measures. A channel specific observation and validation was provided to manage the design features in VANET. Author processed the attack model and defensive model with specification of semi dynamic attacks. The channel surfing and hideaway methods were also incorporated to provide the safe communication. A mobility preserved communication model was provided by the author against the mobility and the environment constraints. The resource utilization with integrated security was provided by the author.

Othman et. al.[5] provided the attack modeling and defined the preventive tool against the jamming attack. The markov chain model was provided with security specification under the Automata network. The attack specific observation was taken to regulate the work under attack monitoring. Author observed the greedy behaviour of nodes and provided the automata processing for generating the attack preserved communication. The work ensured the synchronized communication under loss probability analysis. RoslinMary et. al.[6] has provided a new DOS detection algorithm called APDA (Attacked Packet Detetion Algorithm). The method analyzed the packet and the communication pattern before the verification time which itself reduced delay overhead and improved the communication throughput. The vehicle specific mechanism was provided by the author to verify the communication with in session and recognize the misbehaving node. Verma et. al.[7] has proposed a method based on master chock filter and provided the traffic anlaysis from the originator. The preventive flooding algorithm was provided against sniffing attack. The protocol specific evaluation under mobility model observation and interaction was provided by the author. The pair wise synchronization was achieved with reference broadcast scheme to achieve the reliable communication against uncertain conditions. The complementary and cooperative communication was provided by the author to achieve the message validation. Kim et. al.[8] has explored the DOS attack in reference of Vehicle network. The network capability analysis and the impact of DOS attack on these capablities is provided by the author. The traffic sensitive disruption was also handled by the author to provide the secure communication over the network. Singh et. al.[9] has provided an improved DOS detection method called EAPDA (Enhanced Attacked Packet Detection Algorithm) for vehicular network. The algorithmic model provided here is based on the deterioration and provided the performance driven measure to reduce the communication delay. The attack preserved model was provided by the author to generate the adaptive work solution. The algorithm observed the attack criticality and provided the robust solution.

He et. al.[10] has provided a secure signature specific authentication scheme for mitigating the DOS attack. A trust adpative method was provided to recognize the bogus message communication. Author preserved the thread model so that the security evaluation was provided under the attack voilaton so that the communication solution can be obtained. Group rekeying scheme was provided to provide trust adaptive communication. A trust preserved

communication was provided to provide safe network communication. Rajani et. al.[11] defined a swarm based model to achieve the communication security. The message confidentiality, integirty and authorization was provided by the method. Mokdad et. al.[12] used the routing specific solution against DOS attack in sensor network. The transmission was provided on multiple network paths so that the secure routing method was provided. The multipath was generated between the source and destination nodes. The attack preserved communication was provided by the author. The trust based key management model was provided by the author to provide secure and reliable communication. Mohammed et. al.[13] defined a study on different attack forms in vehicular adhoc network.

3.RESEARCH METHODOLOGY

DDOS is the common attack form defined in a wireless network in which the heavy communication traffic flows. This heavy communication not only slow down the communication but also occupy the resources unnecessarily. To provide the effective and safe communication, there is the requirement to identify the attack in earlier stage. In this present work, a group adaptive virtual controller based method is provided for DOS attack detection in the vehicular adhoc network. The work is here defined under the phenomenon of group formation. As the network is infrastructure based and controlled by the placed road side units. Lot of traffic flows in the region of each road side units because of which the communication loss can occur. The provided method has observed the vehicle nodes under physical characterization. This characterization includes the nodes position and the mobility. Based on this observation, the virtual groups are formed by the vehicle nodes. Each of the group is also identified by the controller node. The group formation is here done under the speed, direction and positional specification. Once the groups are formed, the centralized node is considered as the controller node. Now the communication in the region is controlled by this controller and observed the nodes with in this virtual region.

In the second stage, the communication analysis is performed by the controller node within the region. This anlaysis is done under the communication loss, communication delay and response time parameters. Based on these parameters the adaptive effective nodes are identified. The nodes are categorized as the safe and unsafe node by performing the parametric analysis. This parameteric analysis is shown here in figure table 1

Table 1 : Parammetric Analysis

```
If (CommLoss(VehicleNode)=Low And
CommDelay(VehicleNode)=Low And
ReponseTime(VehicleNode)=Low

{

Set VehicleNode.type=safe

}

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

{

Set VehicleNode.type=safe

}

Else if(CommDelay (VehicleNode)=High Or CommLoss
(VehicleNode)=High)

{

Set VehicleNode.type=unsafe

}
```

Here table 1 has showed the rules considered for the detection of the attacker nodes as well as the safe nodes. Now the communication will be performed through these safe nodes so that the improved communication is expected from the work. The work is applied on city scenario. The results obtained from the work are discussed in next section.

4.RESULTS

The provided work is implemented in NS2 environment. The city scenario is composed with 40 vehicle nodes. The infrastructure driven network is composed. The heavy communication traffic is applied to simulate the situatation of DOS attack. The comparative simulation results are here taken in terms of communication delay, packet transmission parameters

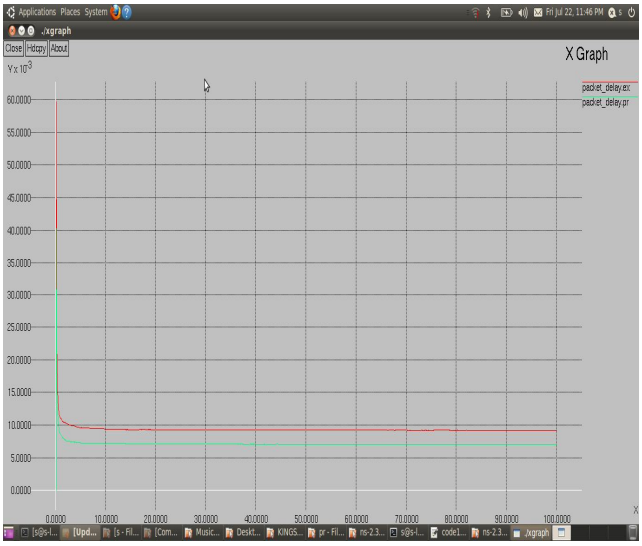

Figure 1 : Communication Delay Analysis

Here figure 1 is hsowing the analysis of work in terms of communication delay. The results shows that the method has reduced the communication delay as the attack preventive solution is obtained.

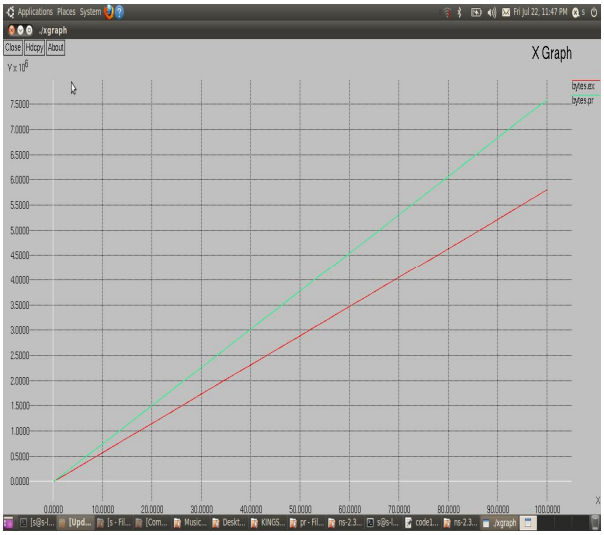

Figure 2 : Packet Communication Analysis

Here figure 2 is hsowing the analysis of work in terms of Packet Communication. The results shows that the method has improved the packet communication as the attack preventive solution is obtained.

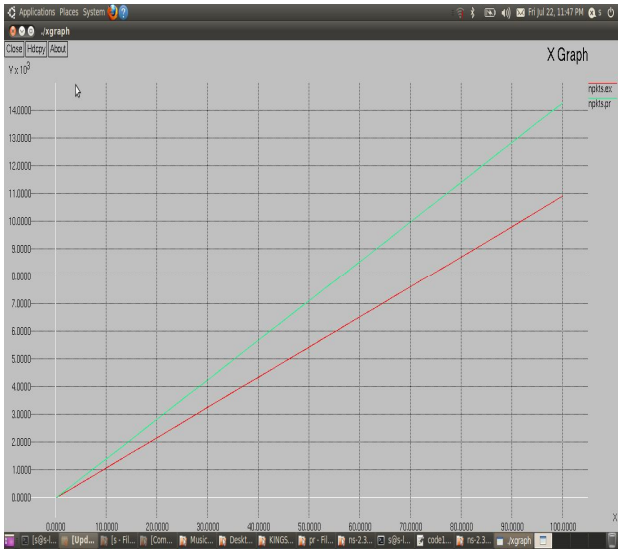

Figure 3 : Bytes Communication Analysis

Here figure 3 is hsowing the analysis of work in terms of bytes Communication. The results shows that the method has improved the bytes communication as the attack preventive solution is obtained.

The comparative analysis is also obtained in terms of communication PDR, communication throughput and Packet Lossrate parameters. The comparative results derivation among these parameters is given here under. Throughput here defines the packet communication per 1000 packets. The numbers of successful communication performed are observed by the throughput. The ratio driven observation in terms of successful packet delivery is represented by PDR (Packet Delivery Ratio). The third parameter is communication loss analysis which is observed in terms of communication failures. These all parameters are shown here in table 1

Table 1: Throughput Analysis

Measures Performance	Existing Techniques	Proposed Model
Throughput	612.13	869.36
PDR	94.29	98.36
Comm Loss	5.71	1.64

Table 1 is showing the showing the analysis in terms of communication throughput, PDR and delay parameters. The figure shows that the proposed approach has improved the communication throughput and PDR whereas the communication loss is decreased. The method overall improved the communication reliability.

5.CONCLUSION

The provided work has defined the group formed method to track the communication at early stage. As the controller is defined to analyze the smaller region. The effective network communication is provided by the method. The simulation results shows that the method improved the communication and reduced the communication delay.

References

[1] K. Verma and H. Hasbullah, "IP-CHOCK (filter)-Based detection scheme for Denial of Service (DoS) attacks in VANET," Computer and Information Sciences (ICCOINS), 2014 International Conference on, Kuala Lumpur, 2014, pp. 1-6.

[2] K. Verma, H. Hasbullah and A. Kumar, "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International, Ghaziabad, 2013, pp. 550-555.

[3] P. Tyagi and D. Dembla, "Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation," Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, New Delhi, 2014, pp. 2084-2090.

[4] I. K. Azogu, M. T. Ferreira, J. A. Larcom and H. Liu, "A new anti-jamming strategy for VANET metrics-directed security defense," 2013 IEEE Globecom Workshops (GC Wkshps), Atlanta, GA, 2013, pp. 1344-1349.

[5] J. Ben-Othman and L. Mokdad, "Modeling and verification tools for jamming attacks in VANETs," 2014 IEEE Global Communications Conference, Austin, TX, 2014, pp. 4562-4567.

[6] S. RoselinMary, M. Maheshwari and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)," Information Communication and Embedded Systems (ICICES), 2013 International Conference on, Chennai, 2013, pp. 237-240.

[7] K. Verma, H. Hasbullah and H. K. Saini, "Reference broadcast synchronization-based prevention to DoS attacks in VANET," Contemporary Computing (IC3), 2014 Seventh International Conference on, Noida, 2014, pp. 270-275.

[8] Yeongkwun Kim, Injoo Kim and C. Y. Shim, "A taxonomy for DOS attacks in VANET," Communications and Information Technologies (ISCIT), 2014 14th International Symposium on, Incheon, 2014, pp. 26-27.

[9] A. Singh and P. Sharma, "A novel mechanism for detecting DOS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)," 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), Chandigarh, 2015, pp. 1-5.

[10] L. He and W. T. Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on, Zhangjiajie, 2012, pp. 261-265.

[11] R. Muraleedharan and L. A. Osadciw, "Cognitive security protocol for sensor based VANET using swarm intelligence," 2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, 2009, pp. 288-290.

[12] L. Mokdad and J. Ben-Othman, "Performance evaluation of security routing strategies to avoid DoS attacks in WSN," Global Communications Conference (GLOBECOM), 2012 IEEE, Anaheim, CA, 2012, pp. 2859-2863.

[13] M. Erritali and B. El Ouahidi, "A review and classification of various VANET Intrusion Detection Systems," Security Days (JNS3), 2013 National, Rabat, 2013, pp. 1-6.