Indian Journal of Science and Technology, *Vol 9(36), DOI: 10.17485/ijst/2016/v9i36/97141, September 2016*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Novel Model based on Group Controlled Observation for DDOS Attack Detection and Prevention in VANET

Sindhu Grover* and Pooja Mittal

Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak - 124001, Haryana, India; sindhugrover@gmail.com, mpoojamdu@gmail.com

Abstract

Objectives: To identify the Distributed Denial Of service (DDOS) attack in the network and generate a preventive path while performing the V2V communication. The objective of work is to reduce the communication delay and communication loss. **Methods/Statistical Analysis:** In this work a group controlled method is provided for vehicular network to observe the attack within the group. The parameter driven analysis is applied within the group and identified the attacker node. Once the attacker is identified, the preventive path is generated. The paper has presented the algorithmic model for preventive route formulation. **Findings:** In Vehicular Ad Hoc Network (VANET), the large node traffic exist which results heavy network communication. DDOS in this attack degrades overall network reliability. In this paper, a group controlled analysis model is proposed to identify the DDOS attacked node and to generate the preventive communication path. At the early stage, the Road Side Unit (RSU) region is processed under mobility parameters to generate the node groups. Each group is also defined with an established controller. Finally, the group communication is observed under communication parameters to identify the attacker node. The paper has explored the model and the associated work stages in detail. **Application/ Improvements:** The work is defined specifically for vehicular network and to identify the DDOS attack. The group specific restricted region analysis is provided to recognize the attacker node and to generate the preventive path.

Keywords: DDOS, Group Based, Infrastructure Driven, VANET

1. Introduction

Congestion is the foremost problem in a network that represents the heavy network communication. As the number of nodes in a geographical area increases, the bulk communication occurs and generates the congestion situation. Congestion can occur in a network either intentionally or unintentionally. Because of this, it is difficult to identify the actual cause of congestion. Some intelligent observations are required to identify the congestion situation and source in network. In ad hoc network such as VANET, the congestion situation and its identification is more critical. As the network is public and new nodes introduced in the particular geographical region continuously, it becomes very difficult to identify the congestion source. In more critical form, the congestion is identified as DOS (Denial of Service) Attack. To improve the communication reliability, there is the requirement of some congestion control algorithm at different stages of communication. According to this control method, at first the observation is applied based parameter specific communication analysis. The channel status, load vector, network feed are the basic criteria to observe the congestion situation in a network. The parameter setup with specification of communication delay and reactive control mechanism is defined to identify the explicit feed in the network. The communication load with condition adaptive analysis is defined to generate the congestion limit. The mobility and the high communication also affect the congestion vector and its analysis process. Congestion in a network can affect the synchronized communication, co-ordinated communication and the channel based

*Author for correspondence

communication. It increases the network latency and increases the communication drop. The drop in case of jamming of DDOS attack is shown in Figure 1.

The Figure 2 shows that the node M is the attached node which increased the network traffic because of communication loss occurs as selecting this node as cooperative communication node.

In this paper, a group assisted analysis model is presented to identify the DDOS attack and provide the preventive communication solution. The work model first generated the controlled groups and later on applied the multiple parameters based analysis to identify the attack.

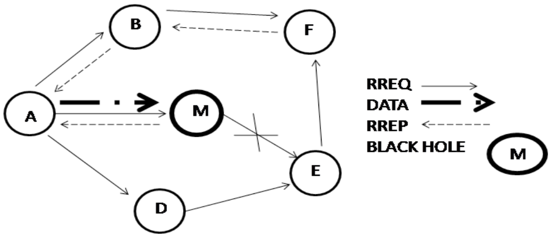

Figure 1. DDOS attack.

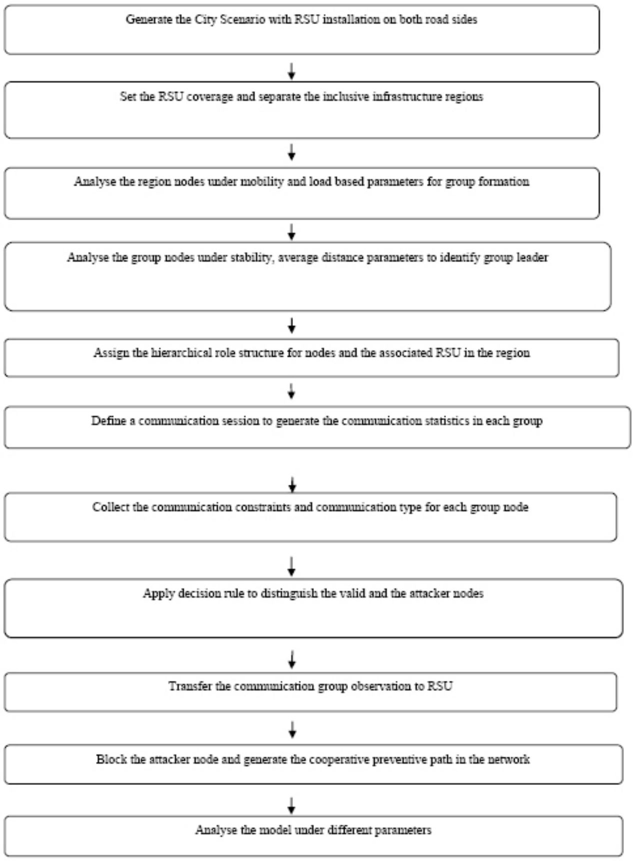
Generate the City Scenario with RSU installation on both road sides
Set the RSU coverage and separate the inclusive infrastructure regions
Analyse the region nodes under mobility and load based parameters for group formation
Analyse the group nodes under stability, average distance parameters to identify group leader
Assign the hierarchical role structure for nodes and the associated RSU in the region
Define a communication session to generate the communication statistics in each group
Collect the communication constraints and communication type for each group node
Apply decision rule to distinguish the valid and the attacker nodes
Transfer the communication group observation to RSU
Block the attacker node and generate the cooperative preventive path in the network
Analyse the model under different parameters

Figure 2. Proposed model.

In this section, the congestion problem and the effect of VANET is discussed. The characterization of this attack is defined in this section. In section 2, the work defined by earlier researchers is discussed. In section 3, comparative analysis table is discussed. In section 4, the proposed work model is discussed. In section 5, the conclusion of the work is presented.

DDOS attack disturbs the network transmission and slow down the communication. It not only increases the communication delay but also increases the communication failure cases. In VANET, where already heavy traffic and communication exist, the criticality of DDOS attack increases. To improve the effectiveness of VANET communication under DDOS attack, different researchers included their contribution. In this section, some of earlier work of different researchers is discussed. A study on DDOS attack for VANET was defined by[1] Author identified the capabilities, responsibilities and challenges of VANET and observed the attack impact for this busy network.

A novel congestion detection and removal method was proposed by[2] Author observed the attacker behaviour in broadcast communication and identifies the false packet communication in the network. The traffic observation is applied for vehicle nodes as well as for RSUs. In proposed scheme, the nodes with false communication are executed and generate the routing information for effective network communication. Author applied work on routing protocol to generate the preventive communication. A study work on different types of DDOS attack in vehicular network was provided by[3] Author explored the functioning of these attacks and the impact on the vehicular network. In[4] proposed an algorithm to identify the malicious and irrelevant packet identification in VANET as DDOS attack occur in the network. An eventual observation in case of false information, jamming attack and selfish node behaviour was predicted by the author. Author provided the infrastructure based analysis to identify the attack causes for the network. In[5] provided request-response detection based algorithm for identification of DDOS. A limit specific observation is applied to separate the valid and the attack communication between node pairs. The validation and the hop count parameters are also considered to generate more effective results. In[6] defined a master chock filter concept to identify the busy network situation and to reduce the blocking situation for the network. Author identified the originator and applied a sniffing attack observation to provide effective bandwidth utilization. The node mobility and the transportation conditions are analysed to provide effective packet delivery in the network. In[7] defined a light weight traffic monitoring method to identify the intrusion attack in the network. Author identified the cases of DOS attack, integrity target attack and false alert generation for the network. Author framed some rules to identify three different attacks and ensured the accurate communication against these attacks.

Authentication and cryptography models are also adopted by different researchers to verify the node authenticity and provided the safe communication in network. A featured authenticated method for signature verification was defined to prevent the DDOS attack. In[8] defined an analytical concept for attack reward analysis to provide secure communication against DDOS attack. Author used the automata theory to observe the communication behaviour and identified the abnormal transition. Finally, the greedy rule is applied to distinguish the attacked and normal communication. In [9]used the hash chain based pre-authentication process in group verification to reduce the attack probability in network. The key pool based security modelling has provided the secure and reliable communication in network. In[10] designed a new version of TESLA protocol to provide authenticated communication in network and provide tolerance against DOS attack. A power estimation based reliable protocol design was proposed. The method reduced the power consumption while communicating with trust nodes which decreased the overall power consumption and improved the reliability of network.in[11] applied the existence of privacy preserved communication to generate safe message communication in hybrid vehicle network. Author tracked the unauthorized network communication under vehicle revocation scheme and provided a clear observation on network attacks. Author defined a comparative observation to detect the attack and provided the safe and reliable communication. In[12] defined an improvement to UDP protocol to identify the storage data structure and map it with bloom filter to provide effective network communication. Author applied the resource requirement analysis to improve the detection rate and reduce the computational cost. In[13] used the elliptic curve based signature verification algorithm to provide the authenticated and reliable communication. Author defined the solution using integer factoring and discrete logarithmic problem to identify the key communication areas and provided the safe communication in the network. In[14] also used same elliptic curve cryptography method to verify the node trust and provided the hash valued based key distribution. Author defined the light weight algorithm to reduce the computational delay and improve the communication strength for the network. In[15] applied the improvement to MAC 802.11p protocol to identify solution for jamming attack. Author applied the periodic position analysis for earlier prediction of nodes and reduced the packet drop during mobility. In[16] has provided a performance analysis framework for collision avoidance in vehicular network. Author applied different routing methods for different network configuration including the topology change, geographic change and clustered routing method. Author defined the analysis under multiple parameters including congestion, delay and jitter. In[17] has defined an analytical study on different routing methods. A study on routing method was provided under V2V and V2I communication. Author identified the routing issues and characterizes them under different protocols. in[18] has proposed an intelligent authentication method for generating the dynamic communication path. Author defined the effective data collection scheme for communication over the moving vehicles. A destination driven secure communication scheme was provided by the author to improve the communication reliability. Another systematic survey on routing method was provided by[19]. A routing method was provided by the author using Point to Point routing and broadcast routing method. Author discussed overall tree different type of routing methods and identified the hidden challenges. The traffic adaptive classification of these protocols was also provided by the author.

From this section, it is identified that different researchers provided the work on DDOS attack using preventive and authentication based approaches. The existing work is based on infrastructure specification and the communication on a node is defined based on authentication and authorization method. Different cryptographic methods were suggested by different researchers to provide encoded communication in the network. Some of the work is defined based on MAC improvement where the contention window control was suggested by the author. From this work observation, it is concluded that the existing methods applied the work on fix infrastructure derivation.

2. Comparative Analysis

Different researchers have provided different preventive methods to provide safe and reliable communication against congestion. In this section, some of the common approaches of DDOS prevention and congestion resolvement is discussed in detail Table 1.

In this section, some of the common approaches are discussed for DDOS detection and prevention. Some of the approaches are node directed and some are RSU directed. The implementation of these approaches is done either on MAC layer or for routing layer. Based on this analysis, a more intelligent group specific method is provided to provide segmented network analysis. This proposed model is described in next section.

Table 1. Congestion preventive methods

Approach	Methodology Used	Features
RSU Monitored Method[1]	• RSUs monitor the communication between vehicles and infrastructure. False information traffic is recognized and based on analysis safety message is generated. • RSU observe the communication continuity to observe the wrong packets or node activity.	• Node-to-RSU communication is observed. • Diversion Activities for real time communication is identified.
Synchronization Method[2]	• Mathematical formulation was applied to ensure synchronized communication for attack mitigation. • MAC layer protocol is improved. • Jitter and Back off periods are observed for attack analysis.	• Contention window control was suggested for safe communication. • EDCA parameters are configured for communication improvement.
MIPDA[4]	• Nodes positions are detected to identify the abnormal communication activities. • Velocity and frequency measures are applied for irrelevant communication observation.	• RSU Driven method • Delay overhead and communication strength are key vectors. • Verification time analysis was implied for ensuring the safe communication.
RRDA[5]	• Transition range was set by RSU for abnormality identification. • Vehicle parameter map for service access was compared over the database.	• RSU Driven Method. • Threshold Limit for abnormality Identification. • Change Observation.
RBS[6]	• The broadcast communication control is provided using time synchronization method. • Chock Filters are applied for Communication control • Frequency change observation is implied.	• MAC Integrated Method. • Propagation time, sending time criteria are observed. • Frequency filter is applied.
BFICR[7]	• Bloom filter is applied on master node for signature map and Reliable communication filtration.	• Hash function controlled method. • Density driven communication analysis.
Greedy[8]	• Behaviour Packet Analysis. • Transition rate observation. • Poisson process integration for attack formulation.	• Attack discovery was provided for reliable and safe communication. • Threshold limits are applied for abnormality observation.
PPSCP[11]	• CA authority based authentication measures are applied for reliable VANET communication • V2V and V2I control communication is provided.	• Shared keysetup is implied. • Handshaking for reliable communication is drawn.

3. Group Controlled DDOS Attack Detection and Preventive Model

In this paper, a dynamic clustered framed model is provided to identify the DDOS attack and provided a preventive network communication after node blocking. The model is defined specially for city scenario in which the network is controlled by the infrastructure devices. But if the attack observation will be applied by individual nodes, it's almost impossible to apply self-assessment and represent itself as attack node. Another possibility is to assign RSU to observe the coverage nodes, but the heavy communication in the region can increase the load on these infrastructure devices. In this paper, the conceptual grouping is suggested in RSU region to achieve the analysis work distribution. In this proposed DDOS identification model, each RSU will first observe the communication for a particular short term session and generate the group based on multiple parameters. The parameters considered here are node speed, direction and load limit. The grouping must ensure the inclusion of each node in specific group. After forming the group, the next work is to identify the group leader in each group to control the group communication. The leader identification is based on average distance with group node, ratio of inter-group and intra-group communication and probability of group stay. After forming the groups, the communication mechanism will be modified by assigning the observer role. The group leader will observe the group nodes and send the collected information statistics to RSU. The session adaptive group node analysis will be applied by the group leader. The analysis will be in terms of session communication, maximum paired communication, average delay, communication type etc. Based on these parameters, a decision will be formed to identify the node quality. Here the observation will be applied to distinguish the valid communication node, critical nodes and the attack node. After generating the communication information, the information will be transmitted to RSU. RSU will take the decision to block the attacked node. After blocking the node, the preventive communication will be applied as cooperative communication between network nodes. The communication model is shown here in Figure 2.

3.1 Proposed Model based on Group Formation

To provide the optimized communication and to avoid the overload communication situation in the RSU region, the group formation method is defined. The group generation is the primary activity defined in this work. The group formation is here critical because of node mobility as well as lesser coverage of vehicle nodes. The major requirement of group formation is to maintain the group for longer time. Because of which, the multiple nodes are observed simultaneously to obtain the connectivity probability in limit time. The mobility parameters including node speed, direction are considered in Figure 2 to identify the eligibility of a node to a group. The degree of node is also identified to verify the number of groups that can have same vehicle node. While generating the group, the overload condition of group is also avoided by restricting the number of members in a group. The upper and lower limit is defined to control the overload and under load conditions. Based on these parameters the group formation is done. After identifying the groups, the group leader is identified based on the group node observation. The average connectivity, mobility and load parameters are considered to identify the group leader.

3.2 DDOS Identification

After generating the groups and group leader, the next work is to use the group leader characterization for DDOS identification in the RSU region. The group leader will setup a communication session to analyse the communication in the network. In this session, the analysis will be done under following parameters

- The average data communication performed by a node.
- The communication frequency between each node pair.
- The communication is broadcast, multicast or unicast.
- Average Communication delay of each node.

After collecting the statistics, the decision will be formed to distinguish the valid, critical and attack nodes. To derive the conclusion, the statistics information will be transmitted to RSU. Here RSU will apply the analysis under collected parameters and identify the valid node and the attacker.

4. Conclusion

In this paper, a group fame model is defined to identify the DDOS attack node and to provide the reliable communication over the network. The Proposed model is based on the effective group formation. At the earlier stage of this model, the group leader is elected under speed and loss parameters. Later on the group leader based group communication analysis is applied for identification of attacker. Finally, the safe communication is drawn over the network. The paper also explored the requirement observation of DDOS attack detection and the associated communication issues. In this paper, the work model is presented. In future, the work will be simulated in NS2 environment and the parameter specific results derivation will be obtained.

5. References

1. Pathre A, Agrawal C, Jain A. A novel defense scheme against DDOS attack in VANET. 10th International Conference on Wireless and Optical Communications Networks (WOCN); Bhopal. 2013. p. 1–5.
2. BiswasS J, Misic M, Misic M. DDoS attack on WAVE-enabled VANET through synchronization. IEEE 2nd Global Communications Conference (GLOBECOM); Anaheim, CA. 2012. p. 1079–84.
3. Kim Y, Kim I, Shim CY. A taxonomy for DOS attacks in VANET. 14th International Symposium on Communications and Information Technologies (ISCIT); Incheon. 2014. p. 26–7.
4. Quyoom A, Ali R, Gouttam DN, Sharma H. A novel mechanism of detection of denial of service attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA). International Conference on Computing, Communication and Automation (ICCCA); Noida. 2015. p. 414–9.
5. Gandhi UD, Keerthana RVSM. Request response detection algorithm for detecting DoS attack in VANET. International Conference on Optimization, Reliabilty, and Information Technology (ICROIT); Faridabad. 2014. p. 192–4.
6. Verma K, Hasbullah H, Saini HK. Reference broadcast synchronization-based prevention to DoS attacks in VANET. 7th International Conference on Contemporary Computing (IC3); Noida. 2014. p. 270–5.
7. Verma K, Hasbullah H, Kumar A. An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. IEEE 3rd International Advance Computing Conference (IACC); Ghaziabad. 2013. p. 550–5.
8. Ben-Othman J, Mokdad L. Modeling and verification tools for jamming attacks in VANETs. IEEE Global Communications Conference (GLOBECOM); Austin, TX. 2014. p. 4562–7.
9. He L, Zhu WT. Mitigating DoS attacks against signature-based authentication in VANETs. IEEE International Conference on Computer Science and Automation Engineering (CSAE); Zhangjiajie. 2012. p. 261–5.
10. Ruan N, Hori Y. DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things. International Conference on Selected Topics in Mobile and Wireless Networking (iCOST); Avignon. 2012. p. 60–5.
11. Mikki M, Mansour YM, Yim K. Privacy preserving secure communication protocol for vehicular Ad Hoc networks. 7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS); Taichung. 2013. p. 188–95.
12. Sedjelmaci H, Senouci SM, Abu-Rgheff MA. An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet of Things Journal. 2014; 1(6):570–7.
13. Mishra B, Panigrahy SK, Charan T, Tripathy D, Jena J, Jena SK. A secure and efficient message authentication protocol for VANETs with privacy preservation. World Congress on Information and Communication Technologies (WICT); Mumbai. 2011. p. 880–5.
14. Smitha A, Pai MMN, Ajam J, Mouzna M. An optimized adaptive algorithm for authentication of safety critical messages in VANET. 8th International ICST Conference on Communications and Networking in China (CHINACOM); Guilin. 2013. p. 149–54.
15. Lyamin N, Vinel A, Jonsson M, Loo J. Real-time detection of denial-of-service attacks in IEEE vehicular networks. IEEE Communications Letters. 2014; 18(1):110–3.
16. Jaiganesh S, Jarina S, Amudhavel J, Premkumar K, Sampathkumar S, Vengattaraman T. Performance analysis of collision avoidance frame works in VANETS. Indian Journal of Science and Technology. 2016 Mar; 9(11):1–7.
17. Saravanan D, Agalya V, Amudhavel J, Janakiraman S. A brief survey on performance analysis and routing strategies on VANETS. Indian Journal of Science and Technology. 2016 Mar; 9(11):1–6.
18. Malik A, Pandey B. An intelligent authentication based vehicle initiated broadcast-dynamic path data collection scheme in VANET. Indian Journal of Science and Technology. 2016 Apr; 9(16):1–9.
19. Valantina GM, Jayashri S. A systematic survey of vanet routing protocols based on transmission strategies. Indian Journal of Science and Technology. 2016 June; 9(22):1–4.