Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 7, July 2016, pg.74 – 84

LOCATION BASE TECHNIQUE FOR EFFICIENT TRANSMISSION UNDER DDOS ATTACK IN VANET

Manpreet Kaur[1], Puneet Kumar[2], Dr. Rachit Gang[3]

[1]Student, M.Tech (CSE), PTU

manu.dhillon1991@gmail.com

[2]Assistant Professor, PTU

puneetsrisai@gmail.com

Abstract— In the interacting systems the flow of information is the most important service. It is clear that a simple self - spreading worm can quickly spread across the Internet and cause severe damage to our society. Facing this great security threats like Distributed Denial-of-Service (DDOS), we need to build an early detection system. We proposed LICBM Approach for efficient data transmission.

Keywords— VANET, AODV, RREP, RREQ, DDOS

I. INTRODUCTION

VANET Vehicular ad-hoc network (VANET) is sub class of mobile ad-hoc network (MANET). MANETS are ad-hoc networks and those types of networks which can alter their location and configure it. They use wireless channel, satellite channel and cellular transmission for communication because these are mobile networks which change their position after every interval. In VANETs vehicles can communicate with road side equipment which is also called as vehicle to roadside communication. In VANETs or MANETs it is not necessary that nodes have

internet connection. Limited Roadside equipment can have wireless connection by which vehicles can send data. Vehicular network give wellbeing, security, and effectiveness to transportation framework and these are new application or services which gave benefit to travelling public to share emergency, security information while travelling. [4].

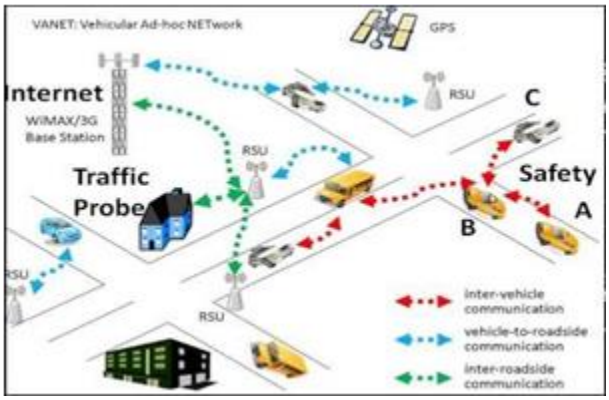


Fig1.VANET ARCHITECTURE

Vehicle-To-Roadside Communication

The vehicle-to-roadside communication configuration represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. [2].

Routing-Based Communication

The routing-based communication configuration is a multi-hop uni - cast where a message is propagated in a multi-hop fashion until the vehicle carrying the desired data is reached. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicles it received the request from, which is then charged with the task of forwarding it towards the query source. [2]

Applications of VANET

According to the DSRC, there are over one hundred recommended applications of VANETs. These applications are of two categories, safety and non-safety related. Moreover, they can be categorized into OBU-to-OBU or OBU-to-RSU applications. Here we list some of these applications.[2]

Co-operative Collision Warning:

Co-operative collision warning is an OBU-to-OBU safety application, that is, in case of any abrupt change in speed or driving direction, the vehicle is considered abnormal and broadcasts a warning message to warn all of the following vehicles of the probable danger. This application requires an efficient broadcasting algorithm with a very small latency.[2]

Lane Change Warning: Lane-change warning is an OBU-to-OBU safety application, that is, a vehicle driver can warn other vehicles of his intention to change the traveling lane and to book an empty room in the approaching lane. Again, this application depends on broadcasting [2].

Intersection Collision Warning:

Intersection collision warning is an OBU-to-RSU safety application. At intersections, a centralized node warns approaching vehicles of possible accidents and assists them determining the suitable approaching speed. This application uses only broadcast messages. In June 2007, General Motors „GM" addressed the previously mentioned applications and announced for the first wireless automated collision avoidance system using vehicle-to vehicle communication [2], as quoted from GM, "If the driver doesn't respond to the alerts, the vehicle can bring itself to a safe stop, avoiding a collision"

Denial of Services (DOS) & Distributed Denial of Services (DDOS)

Denial of Service attack (DOS)

Denial of service attack, attacker takes control over a vehicle's resources or jams the communication channel used by the VANET; by this it can prevent important information from arriving. For example, if a malicious node wants to create a traffic jam on the road, it can make an accident and use the DOS attack to prevent the warning notification from reach of the approaching vehicles.[6]

In VANET environment, usually the attacker attacks the communication medium to cause the channel jam or to make issues for the nodes from accessing the network. The main purpose is to prevent the legitimate nodes from accessing the network services or from using the network resources. Network resources and node will not be able to receive or send important information because of this attack. Finally, the networks are no longer available to authentic users. DOS shall not be allowed to happen in VANET, because life critical information must reach its predestined destination securely and timely. There are 3 ways the offender may achieve DOS attacks, namely communication channel jamming, overloading of network resource, and packets dropping. There are 3 kinds of DOS attacks as described below with their available solutions: [6]

Oppress the Node Resources

In this DOS attack, the attacker's goal is to overwhelm the node resources such that the nodes cannot perform other important and necessary tasks. All the resources of the nodes will continuously busy in message verification, which (messages) is coming from attacker nodes.[3]

a) Case I: V2V Communication suffers by DOS attack in a victim node behind the attacker node receives a warning message "Accident at location Z" which is send by an attacker. Same kind of message send by attacker continuously, keeps the victim node busy and it will completely deny to accessing the network [3]

b) Case II: V2I Communications suffers from DOS Attack; In this case, Road Side Unit (RSU) is suffers from DOS attack; attacker directly attacks. RSU is continuously engage to check the messages, thus RSU is not able to give response to any other nodes, and thus the service is unavailable. Therefore, sending crucial life information in this situation is quite risky.[3]

Physical Layer attack: Channel Jamming

This is a worst level of DOS attack. In this attack, attacker jams the channel, because of that; other users are not able to access the network. The two possible cases are as follows:

a) Case I: In this case high frequencies are sending by an attacker and jam the communication between nodes in a particular domain. Nodes are not able to send or receive messages in that domain thus, services are not available in that particular domain due to attack. Only when a node leaves the domain of attack it can able to send or receive messages. [3]

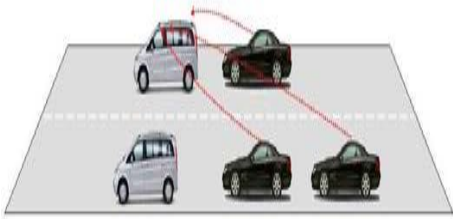
b) Case II: The next level of attack is to jam the communication channel between the nodes and the Roadside unit (RSU). the attacker launches an attack near the RSU to jam out the channel, causing to network breakdown. Thus; nodes and RSU are notable to send or receive messages from each other, this cause network unavailability.[3]

Distributed Denial of Services (DDOS)

DDOS attacks are more severe in the vehicular environment because the mechanism of the attack is in distributed manner where the impact is dispersed in the network. In this kind of attack, the attackers launch attack from different locations. There are two possible cases as follow.[3]

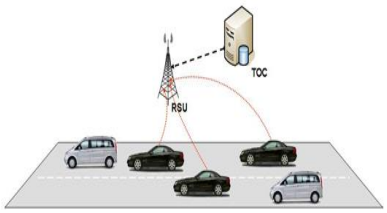
a) Case: Attacks are launch from different locations and each may use different time slots for sending the messages. The nature of the messages and time slots may vary from node to node of the attackers. The aim of the attacks is to achieve network unavailability by bringing the network down at a target node. There are three attackers' nodes (black color cars) send some messages to

a target node in front (grey color car). After some time, the target node cannot communicate with any other nodes in the network [7]



DDOS in vehicle to vehicle

Case: In this case, the target of attack is the VANET infrastructure (RSU). There are three attackers in the network and launch attack on the infrastructure from different locations. When other nodes in the network want to access the network, the infrastructure is overloaded, thus denial of service [8]



DDOS in vehicle to Infrastructure

II. RELATED WORK

The VANET security is an important issue with the rise of the automatically driven vehicle based technologies. The automatically driven vehicle based clusters are programmed for each vehicle to run individually by coordinating with all of the other nodes in the VANET cluster. The proposed model has been designed to detect and mitigate the DoS and DDoS attacks in the VANET clusters to avoid any of the misbehavior or mis - happening in the form of VANET node failure, collision or in any other form. The DDoS attack prevention algorithm works as the real time attack detection and overhead data filtering algorithm in order to protect against the DoS and DDoS attacks. The proposed model result has been obtained on the basis of network load, throughput, packet delivery ratio, etc. The experimental results have proved the efficiency of the proposed model in comparison with the existing models.[1]

VANETs also called as intelligent transportation system (ITS) in which vehicles communicate to provide timely information. Their aim is to provide security, information and management of network. Instead of their many advantages vehicular network is prone to various attacks. In this research removal of Sybil attack in which node creates its multiple identities and it can be affected by various ways. In previous work Sybil attack is prevented by using the timestamp. Every node has some time stamp to communicate with RSU in which identities are verified. If

multiple identities exist then there must be an attacker. On high traffic roads there are number of vehicles for which RSU cannot process all vehicles and also vehicles have high mobility due to which timestamp may be collapse or may miss by vehicle. In previous work three methods were used to find the physical measurement of message that were Time of Arrival (TOA), Angel of Arrival (AOA), and Received Signal Strength (RSSI). In this work, we are using GPSR, Which Reduce the Chances of Attacks.[12]

VANET is a vehicular ad hoc network. This is a part of mobile ad hoc network. VANETs also called as intelligent transportation system (ITS) in which vehicles communicate to provide timely information. Their aim is to provide security, information and management of network. Instead of their many advantages vehicular network is prone to various attacks. Like prankster attack, denial of service attack, blackhole attack, alteration attack, fabrication attack, man in the middle attack, timing attack, illusion attack etc. In this we will use GPSR protocol to remove the Sybil attack. In GPSR protocol physical measurement of vehicle can be verified at any time and GPS coordinates will be compared. If GPS coordinate matched then there is no attack.[14]

Network is collection of nodes that interconnect with each other for exchange the Information. This information is required for that node is kept confidentially. Attacker in the network may capture this confidential information and misused. So security is the major issue. There are many security attacks in network. One of the major threats to internet service is DDOS (Distributed denial of services) attack. DDOS attack is a malicious attempt to suspending or interrupting services to target node. Various schemes are developed defence against to this attack. Main idea of this paper is present basis of DDOS attack. Types of DDOS attack, components of DDOS attack, need for Distributed defense system, comparative study of different defense mechanism.[11]

Vehicular Ad-hoc Network (VANET) is taking more attention in automotive industry due to the safety concern of human lives on roads. Security is one of the safety aspects in VANET. To be secure, network availability must be obtained at all times since availability of the network is critically needed when a node sends any life critical information to other nodes. However, it can be expected that security attacks are likely to increase in the coming future due to more and more wireless applications being developed and deployed onto the well-known expose nature of the wireless medium. In this respect, the network availability is exposed to many types of attacks. Denial of Service (DOS) attack on network availability is presented and its severity level in VANET environment is elaborated. A model to secure the VANET from the DOS attacks has been developed and some possible solutions to overcome the attacks have been discussed.[7]

VANET is an emerging technology; it is a special class of MANET. There are many challenges that must be addressed before it can be successfully deployed. In recent years, not much work is done in the field of security. For security, availability of network is must be obtained at every time since availability of the network is crucially needed when a node sends any important information to other nodes. Nevertheless, it can be expected that security attacks are likely to

increase in the coming future because of more and more wireless applications being developed and deployed onto the well- known expose nature of the wireless medium. In this regard, the network availability is exposed to many types of attack. In this paper, Denial of Service (DOS) attack on network availability is presented with its severity level in VANET environment. A technique to secure the VANET from DOS attack has been introduced and some possible solutions to overcome the attacks have been discussed.[6]

Computing real-time road condition is really tough and it is not achieved using GPS. Initially A vehicle should be authenticated by Trusted Authority (TA) via RSU, only then the navigation query sent to RSU through tamper proof device (in the Vehicle) for identifying best destination route. After authentication, TA generates a re-encryption key to requested vehicle for encrypting the query. Based on vehicle request, contacted RSU identifies the shortest path to reach the destination RSU by passing the vehicle request to neighboring RSU's. After identification of shortest path, it sends the encrypted message to requested vehicle using re-encryption key. Finally it decrypts the message using its own private key. In the modification process, network checks each vehicle speed for avoid accident based on predecessor and successor vehicle's speed using chord algorithm. We also implementing priority based vehicle movement. Network gives high priority in emergency vehicle, it gives medium priority for registered vehicle and it gives low priority for unregistered vehicle.[13]

III. PROPOSED SOLUTION

In the Proposed Technique the DDos attack is detected by counting the no messages sent by node. The Proposed technique find the frequency of message sent by Source node if the count of nodes is more than 3 from the same node id it will be excluded as DDOS Attack . The Secure path is found by the mobile node which towards the intermediate nodes. The LICBM based node move towards the particular destination node by counting the no of messages send by nodes Source node checks the packet frequency towards the destination. If the Frequency is more, than 3 it will exclude as malicious node. Finally the LICBM will find the node which are sending message more than 3 time s it will be excluded from the network Once the Secure route discovery and route maintenance is done, the routing table of the all the nodes in the particular route is updated periodically.

Proposed algorithm:-

The proposed algorithm is for secure data transmission in a VANET

Step 1: Generate Network scenario using NS2

Step 2: Start with some initial elements like „no of nodes", „neighbor node", „Malicious node.

Step 3: Initialize with n no. of nodes.

Step 4: Implement LICBM technique.

Step 5: initially Start LICBM algorithm for finding location and direction of nodes

Step 6: In LICBM finds the location for node is not changing and but is showing fake identity on various location without changing it position the technique will blacklist the and it will isolate the node

Step 7: Then finally With LICBM Algorithm secure transmission will be formed.

Step 8: This process continuation until the efficient and secure transmission is formed.

Step 9: This process continuation until the efficient path is formed in network.

IV. RESULT AND ANALYSIS

End to end delay: The end to end delay is total alive data packets from the sources to the destinations.

Packet Delivery Ratio: It is the ratio of the number .of Packets received successfully and the total number of packets transmitted.

Throughput:
It is defined as the number of packet received at a particular point of time.

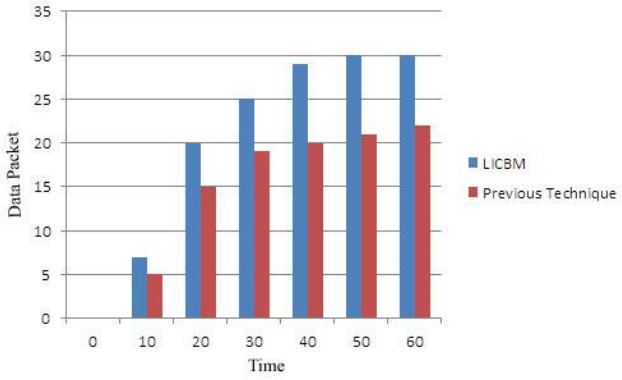


Fig3 packet delivery ratio comparison

The fig4 shows the LICBM has more Packet delivery ratio as compared to previous technique

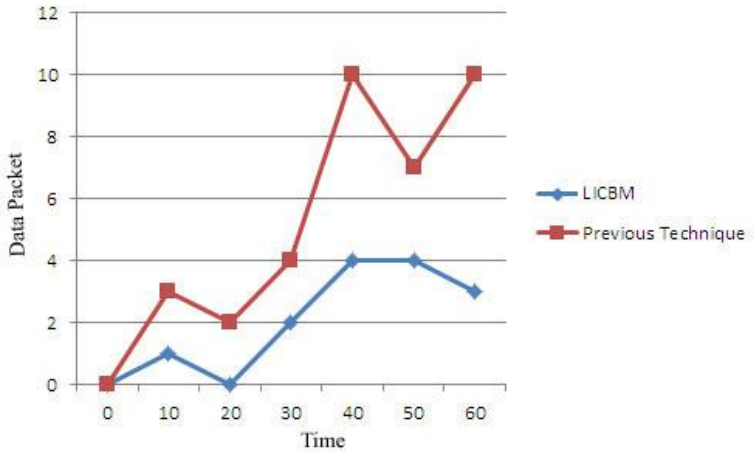
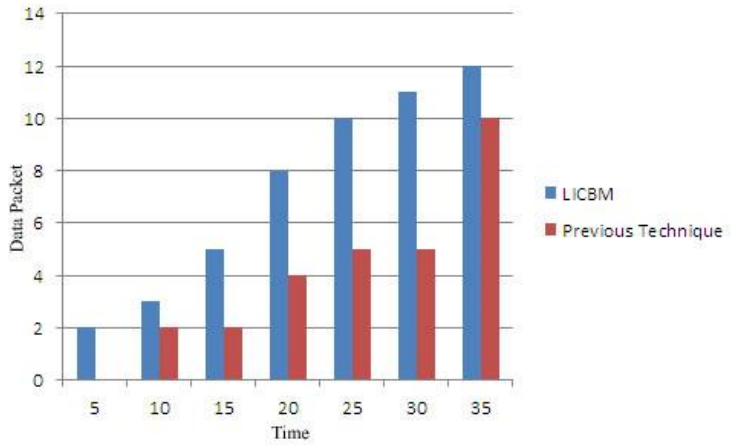


Fig4 end-to-end delay comparison

The fig4 shows the LICBM has less end-to-end delay as compared to previous technique



The fig5 shows the LICBM has high throughput as compared to previous technique

V. CONCLUSION

DOS/DDOS is one of the main security threats in the Internet. Shielding against DOS/DDOS becomes a needed DOS/DDOS detection is regarded to be one of the main phases in overcoming the DOS/DDOS problem. Attacks are discussed in the DoS detection section. Furthermore, a classification of DoS attacks is explained. Network flooding DoS-based. The proposed technique is introduced and reviewed to point out the limitations. Approach has many advantages over more sophisticated statistical instruments

REFERENCES

[1] Mandeep Kaur and Manish Mahajan "A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs", International Journal of Hybrid Information Technology, Vol.8, No.8 2015.

[2] priyanka Soni Abhilash Sharma "Sybil Node Detection and Prevention Approach on Physical Location in VANET" ,International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 7, july 2015.

[3] Varsha Raghuwanshi, Simmi Jain "Denial of Service Attack in VANET: A Survey", International Journal of Engineering Trends and Technology (IJETT) – Volume 28 Number 1 - October 2015.

[4] Priyanka Soni, Abhilash Sharma "A Review of Impact of Sybil Attack in VANET's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, MAY 2015.

[5] Ujwal Parmar, Sharanjit Singh "Overview of Various Attacks in VANET", International Journal of Engineering Research and General Science, Volume 3, Issue 3, May-June, 2015.

[6] Aditya Sinha, Prof. Santosh K. Mishra "Preventing VANET From DOS & DDOS Attack", International Journal of Engineering Trends and Technology (IJETT), Volume 4, Issue 10, Oct 2013.

[7] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan "Denial of Service (DOS) Attack and Its Possible Solutions in VANET" International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol:4, No:5, 2010.

[8] Ayonija Pathre ,Chetan Agrawal, Anurag Jain "IDENTIFICATION OF MALICIOUS VEHICLE IN VANET ENVIRONMENT FROM DDOS ATTACK" , Journal of Global Research in Computer Science, Volume 4, No. 6, June 2013.

[9] Pooja Bansal Shabnam Sharma Aditiya Prakash "A Novel approach for Detection of Distributed Denial of Service attack in VANET", International Journal of Computer Applications, Volume 120 – No.5, June 2015.

[10] Harpreet Kaur, Mrs.SupreetKaur "Security mechanism for Collision Avoidance and Attack Prevention Formants" International Journal of Computer Trends and Technology (IJCTT) – volume 23 Number 2 – May 2015.

[11] Divya Kuriakose V.Praveena "A Survey on DDoS Attacks and Defense Approaches" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 8, October 2013.

[12] Dalbir Singh, Manjot Kaur "Mitigation of Sybil Attack Using Location Aware Nodes in VANET" International Journal of Science and Research (IJSR), Volume 4, Issue 11, November 2015.

[13] C. AROKIA MARY, A.M. ARULRAJ, "ACCIDENT AVOIDENCE BASED ON PREDECESSOR AND SUCCESSOR VEHICLE SPEED WITH PRIVACY PRESERVING NAVIGATION USING CHORD ALGORITHM" International Journal of Innovative Trends and Emerging Technologies, Volume 1, issue 1, March 2015.

[14] Priyanka Soni Abhilash Sharma "Sybil Node Detection and Prevention Approach on Physical Location in VANET" International Journal of Computer Applications Volume 128 – No.16, October 2015.

