Detection and Prevention of Distributed Denial of Service Attack using Choke Packet: A Review

[1]Mariyam Fatima, [2]Dr. Jameel Ahmad, [3]Dr. Shish Ahmad

[1]Research Scholar, [2,3]Assistant Professor
[1]Department of Computer Science and Engineering,
[1]Integral University, Lucknow, India

***Abstract*: MANET is a collection of various devices that are connected to each other wirelessly. Because of the dynamic nature of MANET, it has become a topmost research topic among scholars. Maintaining security is a major concern in the MANET. So it is important to find out a proper solution in order to secure MANET from various types of attacks.**

Index Terms: Distributed denial of service attack, denial of service attack.

I. INTRODUCTION

MANET is an abbreviation of Mobile Adhoc Network which is also known as ad-hoc network or ad-hoc wireless network that usually consists of various number of moving nodes that are wirelessly connected in a way which is self-configured and self-healing in nature without having a secured foundation. Each node in MANET acts as a router when they send the traffic to another identified node in the network. Each device connects in a MANET can move freely individualistically in any direction in a network and hence will change its link to the other devices frequently. Hence MANET is an autonomous collection in which the devices are connected in a peer to peer and multi-hop fashion without using the central base station or access points. MANET is useful where infrastructure is absent or installation is not possible. MANET can be created either with the help of mobile nodes or by both mobile and fixed nodes.

There are various characteristics of MANET such as- autonomous behavior, dynamic topologies, limited Security, less human intervention, Partitioned operation, multihop routing, Fluctuating link capacity, Lightweight terminals. There are three types of routing protocols in MANET such as- proactive routing protocol, reactive routing protocol and hybrid routing protocol.

II. ATTACKS IN MANET

There are following types of attacks in MANET-

- External attack-

These attacks are fundamentally utilized by the individual who is outside the system and needs to obtain the access to the network. And when they gain access to enter the network. They generally send spoofed packets which eventually results in shutting down of the system.

- Internal attack-

This attack generally occurs inside the network. The node which is added to the network acts as an attacker and is difficult to detect in comparison to the external attack.

- Passive attack-

In this attack, the attacker only listens to the information which is transferred between two parties within the network. The attacker uses this information to hijack the network or to insert the traffic in the future. The attacker does not make the modification in the data .Eavesdropping and traffic analysis is the examples of internal attack.

- Active attack-

In this attack, the attacker tries to modify or alter the data that is being exchanged between two parties in the network in order to disturb the normal functioning of the network. The attacker can drop the packets or inject the packets or modify the packets or can use various other factors of the network to introduce the attack.

III. RELATED WORK

Sandeep Dhende, Sandeep Musale (2017 IEEE), [1] has proposed a secure method to detect and mitigate the attack in MANET. For the detection of a black hole or grey hole attack, an opinion is taken from the neighbor nodes. The nodes in the network demonstrated it honestly. Their system consists of a process that source node sends RREQ message in the network. All the nodes keep the record of their neighbor by using two tables one of which is neighed our List (NL) and neighbor id. When the sender sends the RREP message in the network the neighbor nodes who have the fresh path through them sends the RREP message to the sender. After receiving the RREP message the sender broadcast an opinion message to all the neighbor nodes to get the opinion about the

replied node. The neighbor node replies the sender with the acknowledgment with NO packet or YES packet. If the source receives the No packet it updates the table as opinion table with neighbor id and if it receives YES it set the table as YES.

Ravi Parihar, Ashish Jain, Upendra Singh, (2017 IEEE), [2] has used the SVM technique to identify and detect the packetdropping nodes. SVM classifies the node in two classes either normal or malicious. SVM takes input as a neighbor trust value and calculate that trust value with the data packet and control packets. The SVM machine is generally used to detect the malicious node and to restrict the data transmission between these nodes. In their proposed method SVM receives the set of input data for each specified input. SVM collects the behavior of each node and to validate and classify the nodes based on their behavior. The nodes are termed as either trusted or untrusted with the help of SVM classifier. And finally classifying the nodes into two classes either a normal node or abnormal node.

Mahmoud Reda, Marianne A. Azer, (2017 IEEE), [3] has focused on the comparison between the packet drop attack detection scheme that is between DSR protocol and AODV protocol. Packet delivery fraction is used to calculate the performance to two protocols. The OpNet simulation tool is used. AODV proves to be a better protocol for packet drop attack.

Sachi N. Shah, Rutvij H. Jhaveri, (2016 IEEE), [4] has proposed a trust based routing scheme which combines social and QoS trust. The trust values are calculated on four parameters such as control forward ratio, data forward ratio, residual and intimacy energy. The simulation is carried out on ns 2. Their proposed model consists of adversary model which is used for the packet dropping attack. Packet dropping happens at the time of routing of the data packet. As a result of this, all the neighborhood traffic diverted to the offender node ensuing it to drop the entire packet in the network. For the trust based secure routing model every node in the network broadcast hello message periodically and then monitoring is performed on the promiscuous mode. Each node in this mode listen the packets send by its own neighbor nodes. If node A wants to monitor the packets from node B then it will check whether node B is sending the packets which are sent by A to B or not.

Yugandhara S. Patil, Ashok M. Kanthe, (2016 IEEE), [5] has proposed a false reply count technique to detect the grey hole attack which is a part of a denial of service attack. The false reply count detects the node which sent false replies to the request message to attract traffic during the process of path establishment between the source and destination. TrueLink is used for path authentication. The proposed method contains false reply count which generally runs on every node in the network and the counter is maintained in local RAM to count the number of false replies from the node. And also contain the true link which is used to verify adjacency of nodes that are directly connected within a selected path for the communication between the source and the destination. The verification of the node is executed between every adjacent node within the discovered network.

P. Rathiga, Dr. S. Sathppan (2016 IEEE), [6] has proposed a hybrid approach for grey and the black hole that uses initialized monitor node to collect the packet flow information about the neighboring nodes. Then the information distance metric is calculated using which the detection thresholds are determined. For the detection of trust based black/gray hole attack a trust-based approach is used in which every node monitors the neighbor nodes and calculate the trust value for each node. Based on the trust values the nodes are declared to be malicious or not. The trust value is compared with predefined threshold value. If trust value is below the threshold value it is considered to be a malicious node. For collaborative black/gray hole detection in first stage black hole is discovered by using the RREP packets for the bait RREQ packets. In the second stage gray hole attack is recognized by calculating the packet drop count.

Neha Yadav, Mr. Vivek Parashar (2016 IEEE), [7] has proposed a trust-based technique in which the sender sends the data using encryption and decryption technique. The existing work and methodology are carried out on ns-2.35.

Bhavin Joshi, Nikhil Kumar Singh (2016 IEEE), [8] has proposed a method that uses a packet delivery ratio that is a number of route request per unit time to find whether a node is malicious or not. This method increase the efficiency of the system.

Nadav Schweitzer, Ariel Stulman, Asaf Shabtai ; Roy David Margalit (2016 IEEE), [9] has proposed a novel solution to defend the OLSR protocol. The proposed approach contains protection which prevents more than 95% attacks and the overhead is also decreased drastically as the size of the network increases.

M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti (2014 IEEE), [10] has proposed a statistical approach to defense against RREQ flooding attack. This detection can be applied only on AODV based ad hoc networks. The results show that theses attack can be detected with a low rate of false alerts. Their proposed system composed of notification component and malicious flooding detection mechanism

IV. CONCLUSION

MANETs needs more security as compared to the traditional network because of their dynamic nature. A proper strategy is needed to identity the malicious nodes and a solution to mitigate such attack.

.

REFERENCES

[1] Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar , Anand Najan, *"SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs*," International Conference on Wireless Communications, Signal Processing and Networking WiSPNET), 10.1109/WiSPNET.2017.8300188.

[2] Ravi Parihar, Ashish Jain , Upendra Singh, "*Support vector machine through detecting packet dropping misbehaving nodes in MANET,"* , International conference of Electronics, Communication and Aerospace Technology (ICECA), 10.1109/ICECA.2017.8212711.

[3] Mahmoud Reda, Marianne A. Azer, "*Correlation between protocol selection and packet drop attack severity in ad hoc networks"*, 13th International Computer Engineering Conference (ICENCO), 10.1109/ICENCO.2017.8289819.

[4] Sachi N. Shah, Rutvij H. Jhaveri, "*A trust-based scheme against Packet dropping attacks in MANETs*", 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 10.1109/ICATCCT.2016.7911967.

[5] Yugandhara S. Patil, Ashok M. Kanthe, "*Gray Hole attack detection using false reply count and TrueLink based path authentication in MANET",* International Conference on Computing Communication Control and automation (ICCUBEA), 10.1109/ICCUBEA.2016.7860079.

[6] P. Rathiga, Dr. S. Sathppan , "*Hybrid detection of Black hole and gray hole attacks in MANET",* International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 10.1109/CSITSS.2016.7779411.

[7] Neha Yadav, Vivek Parashar, "*Trust or reputation base encryption decryption technique for preventing network from DOS attack in MANET*", International Conference on Inventive Computation Technologies (ICICT), 10.1109/INVENTIVE.2016.7823211.

[8] Bhavin Joshi, Nikhil Kumar Singh , *"Mitigating dynamic DoS attacks in mobile ad hoc network*", Symposium on Colossal Data Analysis and Networking (CDAN), 10.1109/CDAN.2016.7570941.

[9] Nadav Schweitzer, Ariel Stulman, Asaf Shabtai ; Roy David Margalit, *"Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes",* 10.1109/TMC.2015.2409877.

[10] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, "*Denial of Service (DoS) attacks detection in MANETs through statistical models"*, Global Information Infrastructure and Networking Symposium (GIIS), 10.1109/GIIS.2014.6934261.