ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Dynamic Profile Based Technique to Detect Flooding Attack in MANET

Sathish.T[1], Sasikala.E[2]

M.Tech, Dept of IT, K.S.R. College of Engineering, Tamilnadu, India[1]

Assistant Professor, Dept of IT, K.S.R. College of Engineering, Tamilnadu, India[2]

ABSTRACT: A MANET is a category of wireless ad hoc network that can change locations and configure itself. These types of networks are without fixed infrastructure and are more prone to attacks that occur in the network. The main challenge in MANET is to design the robust security solution that can protect MANET from various routing attacks. Flooding attack is a kind of Denial of service (DOS) attack which is distributive in nature and can exhaust the victim's network of resources such as bandwidth, energy, computing power etc. In this paper we developed a profile based technique which is used to detect and isolate the flooding attack on MANET using Adhoc on Demand Distance Vector (AODV) routing protocol. A Simulation environment was created by java Simulator.

KEYWORDS: MANET, AODV, RREQ, DPDS

I. INTRODUCTION

A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers connected by wireless links. The routers are free to move randomly and organize themselves capriciously [1]. Thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion. Each of the nodes has a wireless interface and communicates with its neighbors who are all in its coverage range. Source can reach destination through one or multiple hop. The Ad Hoc On-Demand Distance Vector (AODV) routing protocol [2] enables multi-hop routing between participating mobile nodes wishing to establish and maintain an ad-hoc network. AODV is reactive since it does route request only when needed and does not require nodes to maintain routes to destination that are not actively used in communications. Flooding attack in MANET is a more concealed form of DOS attack which is produced by the unintentional failure of nodes in the network or by malicious action. This flooding attack can cause severe degradation in network performance. The main intention of a flooding attack is to interrupt the services given to legitimate users by targeting the resource at the victim node or the network. By consuming the resources like bandwidth, battery power etc attacker can set up the denial of service to the end user. In flooding attack the bogus control packets are flooded into the network targeting the victim or the network as a whole.

AODV is particularly vulnerable to flooding attack because of its route discovery scheme where the RREQ control packets are broadcasted to all one hop neighbors for finding the path to the destination. Bogus RREQ packets can be disseminated targeting the destination or network and consume the network resources thereby degrading the network performance [3].

In the proposed DPDS approach, every node is set with a profile in order to encounter the distributed attack. The proposed DPDS has its profile values set based on the behavior of MANET. It identifies the attack and tries to isolates it whenever the node tries to cross the defined threshold value. This threshold value is made adaptive based on the average request allowed in the network. Furthermore, another distinguishable contribution made by this DPDS is that it can identify

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

the attack impact as early as it gets started. DPDS approach can also isolate the attack traffic by isolating the malicious node from participating in the network.

This paper is organized as follows: Section 2 explains how RREQ flooding attack can be launched and its effects in MANET. Section 3 presents the related work done to detect and prevent the flooding attack in MANET. Section 4 explains the proposed system. Section 5 describes the system flow and the metrics used to calculate the performance of proposed DPDS detection mechanism and its result analysis. Section 6 explains the conclusion and future work.

II. FLOODING ATTACK AND ITS EFFECTS

AODV is a reactive routing protocol and it establishes route on demand. It has limit of how much RREQ can be originated by a node. The default value of RREQ_RATELIMIT [4] is 10 as proposed by RFC 3561.The malicious node can override the limit by increasing or disabling it [5]. It can do so because the node has self-control over this rate limit parameter. By this way the malicious node can flood the network with fake RREQs and lead to a kind of DOS attack. In this type of DOS attack the genuine nodes cannot serve other nodes due to the load imposed by fake RREQs. Bandwidth consumption [6] is increased as more number of RREQs is flooded in the network which would otherwise be used by genuine nodes. RREQ packets have high priority than data packets. As the nodes keep on processing the RREQs in spite of data packets there is an overhead in terms of nodes processing time. The routing table entries are created more by the fake RREQs in order to reach destination. Greater amount of network resources like bandwidth are wasted by trying to find routes to destination which do not exist or the routes which are not going to be used for any data communication. This can have very adverse effects in real time applications.

III. RELATED WORK

In Anonymous communication scheme [7] the traffic from source to destination has to pass through one or more mixes where the Mix reorders and re-encrypts the incoming packet where the incoming and outgoing packet cannot be related so the attacker cannot find the end to end connection and it can also be avoided by using the rate Limitation method which will limit the flow rate of the packets. In support vector machine [8] method the packet is limited by implementing the rreq_ratelimit SVM takes a set of input data and predicts for every given input whether it belong to normal node or malicious node. It collect the behavior of every node and by using those data it find the malicious node. In Trace back scheme [9] any single packet is traced back to its origin with the help of special router in the network which cooperate with each other. However this method is based on assumption that network topology does not change which will not hold good for MANET. Further they require centralized equipment which is not practically feasible in MANET. The behavior based detection [10] defines a profile for the normal behavior and policies which the nodes have to adhere for normal working. Any deviation from the normal statistics is considered to be malicious attempt. It have high false positive rate since no clear line of demarcation. In filtering scheme Public key cryptography and digital signatures are used for authentication of routing messages of nodes [11]. Filter is used to limit the rate of RREQ packets by maintaining the threshold value. Rate-limit and Blacklist-limit are used to avoid RREQ. Blacklist-limit determines the malicious node.

IV. DPDS APPROACH

The proposed DPDS-dynamic profile based detection mechanism for flooding attack in MANET aims at detecting the malicious node and isolating it to enhance the network performance. The dynamic profile based approach has three phases Initialization, detection and isolation phase.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Initialization

In profile initialization phase all the nodes in the network build a table called PT(profile table) and store their profile details. Each node stores all the one hop neighbors profile details [12]. This PT is protected from accessed by the node itself or by the malicious node. The threshold values for RREQ sending and receiving is stored in profile value along with the node identity (Node Id). The threshold value dynamically changes based on the average RREQ flow in the network and the number of users on the network.

Detection

In detection phase each node upon receiving the RREQ packet will check for its profile and records the TS which will help in monitoring the one hop neighbor activity [13]. Any deviation from the profile value is treated as malicious behavior and the node id is added to the isolation list. Further packets from the source are dropped in order to avoid flooding the network, compared to previous approaches where the detection do not have clear line of segmentation. The proposed DPDS distinguishes the attack traffic behavior efficiently as the profile is made adaptive based on network behavior.

Isolation

Once the detection is confirmed, the malicious node id is taken from the isolation list and broadcasted to the neighbors. The neighbor nodes will further restrict receiving the packets from the malicious node. If the entire one hop neighbor nodes refuse to cooperate for forwarding the packets sent by malicious node, then it cannot communicate with other nodes in the network. The node has been isolated from the network in practice even if it is still on the networks in location. The detection mechanism is run at every node. Each node performs the detection and isolation upon the receiving the route request.

V. SYSTEM FLOW

Simulation Study

Java network simulator jist/swans are used for the implementation for the proposed node profile based detection mechanism [14, 15]. The simulator is extended with customized code for generating the flooding attack and the detection mechanism. The profile is initialized based on hello packet interval which is modified for our approach. The PT entry is deleted if the neighbors do not respond with hello packet i.e. if the node moves out of range and no longer act as one hop neighbor. When the malicious behavior is detected, it triggers the hello packet containing the malicious node id to one hop neighbor. This node id is added to isolation list and further RREQ from that node will be discarded by the neighbor nodes. The hello packet interval is modified as per hello interval extension format in RFC 3561.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

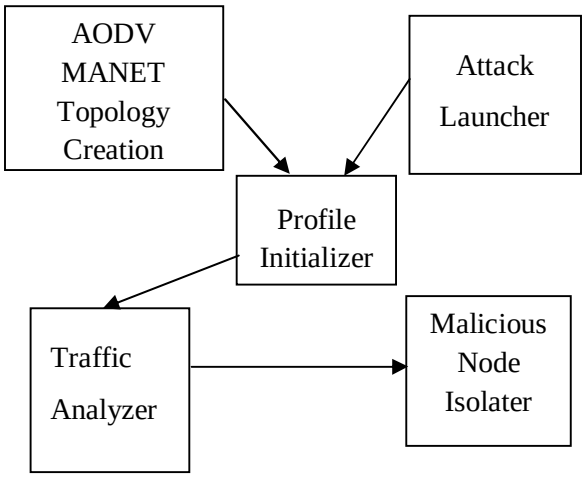

Fig. No. 5.1 Module Diagram

AODV Performance Metrics

The performance of the AODV routing protocol with and without flooding attack is studied in term of the following network parameters and by using these metrics the performance of the profile based technique is studied.

Bandwidth consumption

It is measured as the average number of packets received by the intermediate node (wireless channel) from source to destination over a period of time and expressed in Mbps. The bandwidth consumption is affected by the node mobility, frequent topology change, use of control messages. It is desirable to have less bandwidth consumption to serve the user.

End to end delay

It is the total time taken for the packet to reach from source to destination and it is measured in seconds. It includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges. Due to node mobility, use of control messages and packet retransmissions due to weak signal strengths between nodes, end to end delay increases. Delay should be less for efficient packet transmission.

Packet delivery ratio:

The packet delivery ratio is the ratio of number of packets received at destination node to that of number of packets sent by the source node. It is expressed in percentage. It gives the reliability of the protocol for message deliver. It is affected by node mobility and change in topology. The PDR should be high.

Packet drop rate:

It is the ratio of number of packets dropped during transmission to that of number of packets sent by the source node.It is expressed in percentage.It can occur due to node mobility or buffer overflow.It should be less for efficent routing protocol.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI. CONCLUSION

A new fangled approach based on profile to detect flooding attack in MANET, DPDS is implemented and its effectiveness is evaluated. The main advantage of DPDS is that it detects the malicious nodes at one hop neighbor level as soon as they start exhibiting the attack behavior. DPDS detects and completely isolates the attacker more efficiently as compared to rate limit approach. With DPDS the availability of the resource is assured for the genuine user with better response time and detection rate. Further it also helps in preventing the resource consumption attack and DOS attack which are concealed form of RREQ flooding attack. In future this work can be further extended for other kind of flooding attacks with respect to AODV like hello packets; data packets etc. DPDS can be applied for application involving POS (point of sale) where timely delivery of data is more important in small mobile environment.

REFERENCE

[1] Imrich Chlamtac, Marco conti, Jennifer J,N.Liu,"Mobile ad hoc networking imperatives and challenges" Ad hoc networks I (2003) pages 13-64,Elseiver publications.
[2] C.E Perkins, E.M Royer, "The Ad-hoc on-demand distance vector protocol (AODV)",in Ad-hoc networking, C.E.Perkins (Ed), pp 173-219,Addison-Wesley, 2001.
[3] P.Ning,K.Sun,"How to Misuse AODV:A Case Study of Insider Attacks against Mobile Adhoc RoutingProtocols", Proceedings of the 4th Annual IEEE Information Assurance Workshop,60(2003).
[4] K.Lee Thong. "Performance Analysis of Mobile Adhoc Network Routing Protocols". Thesis Paper submitted to the Department of Computer Science,Naval Post Graduate School, Monterey, CA, 2004.
[5] EU. ZhiAng and Winston Khoon Guan SEAH, "Mitigating Route Request Flooding Attacks in Mobile Ad hoc Networks", Proceedings of International Conferences on Information networking (ICOIN-2006),Sendai,Japan, 2006.
[6] K. Bhuvaneshwari, A. Francis Saviour Devaraj, "Examination of impact of flooding attack on MANET and to accentuate on Performance degradation", International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04 pp. 1652-1656, 2013
[7] Venkat Balakrishnan, Vijay Varadharajan and Uday Tupakula "Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications" International conference on wireless broadband,2007.
[8] Sanjay Sharma and Meenakshi Patel "Detection and Prevention of Flooding Attack Using SVM" International Conference on communication system and Network Technologies,2013.
[9] Yinghua Guo and Sylvie Perreau "Trace Flooding Attack in Mobile Ad Hoc Networks" International conference on wireless broadband,2006.
[10] Neeraj Sharma, B.L. Raina, Prabha Rani et. Al "Attack Prevention Methods For DDOS Attacks In MANETS" AJCSIT 1.1 (2011) pp. 18-21.
[11] Jian-Hua Song, Fan Hong and Yu Zhang "Effective Filtering Scheme against RREQ Flooding Attack in MANET" International Conference on Parallel and Distributed Computing,2009.
[12] S. Kannan, T. Maragatham, S. Karthik and V.P.Arunachalam; "A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols"; International Business Management, 2011.
[13] Y.-A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," In the Proc. Of 1st ACM Workshop on Ad hoc and Sensor Networks, pp. 135-147, 2003.
[14] Java simulator for MANET -Jist/swans
http://jist.ece.cornell.edu/
[15] R. Barr, Z. Haas, and R. van Renesse. JiST: An efficient approach to simulation using virtual machines. Software practice & experience,35(6):539.