IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.

www.ijiset.com

ISSN 2348 – 7968

Detection of Route Request Flooding Attack in MANET Using Session Based History Table

Charushila Choube[1], M. Murali[2]

[1] Research Scholar, Computer Science & Engineering, SRM University,
Chennai, Tamil nadu, India

[2] Asst. Professor, Computer Science & Engineering, SRM University,
Chennai, Tamil nadu, India

Abstract

Mobile ad hoc networks are becoming much popular nowadays as a research and network utilities. This network framework is effective but it is surrounded with security related issues. There are a lot of challenges and problems are found like continuously changed topology and changes in resource constrains may form performance and security gaps between MANET arrangement. The data flooding attack causes Denial of Service attacks by flooding of packets. In this paper, an approach is designed and simulated to handle flooding attack and detect the attack by managing the history table and limiting the flooding value.

Keywords: *MANET, RREQ Packets, RREQ Packets, AODV, DoS*

1. Introduction

A mobile ad hoc network (MANET) is infrastructure less network of mobile nodes that can communicate with each other without the use of a centralized administration. The applications of MANET are especially in military services, vehicle networks disaster management and battlefield surveillance. In MANET each node is free to move in any direction hence it does not have any predefined topology, it can change instantly as the node moves and coverage area changes. MANETs are generally formed for short range communication.

The performance of the network depends on the number of devices; it degrades as the number of device increases because all the devices share the available network resources. And so the node may behave as malicious or selfish node to save its own resources and using the other nodes' resources. There are many possible attacks such as black hole attacks, wormhole attacks, malicious flooding attacks, and so on. The malicious flooding attack is one of the fatal attacks on existing on-demand routing protocols. Malicious flooding attacks are performed either by forwarding many Route Request (RREQ) packets or data packets. Hence, they can be categorized into RREQ flooding attacks and data flooding attacks. In on-demand routing protocols like Ad hoc On Demand Vector (AODV), a mobile node sends a RREQ packet to initiate route discovery. Either the destination node, or any intermediate node, which has a recent route to the destination node, sends a Route Reply (RREP) packet back to the source node. When the source node receives the RREP packet then it constructs a path in the direction of receiving RREP and then transmits data packets through this path. If during data transfer, the current path is disconnected then a Route Error (RERR) packet is sent to the source node to notify the path failure and then, the path is reinitiated. Hence, the RREQ packet is an essential packet in mobile ad hoc networks since it is used for establishing a data transmission path. The malicious flooding attacker floods many RREQ packets to its neighbor nodes so that battery power of neighbor node is drain and node is disconnected from the network. If there exist such type of node which (it may be a compromised node). And battery power of legitimate node becomes off so it is not possible to make legal connection between source and destination.

2. Related Study

Mobile ad hoc networks will appear in environments where the nodes of the networks have little or no physical protection. Thus mobile node may be compromised node. This work also works for the security attacks Denial-of-Service (DoS). The attack of initiating / forwarding fake Route Requests (RREQs) can lead to hogging of network resources and hence denial of service to genuine nodes. Interest is emerging in securing MANET because of its mobility factor and limited resources so unnecessary packets which consume battery power should be avoided. The basic attack possible in MANET and ideas to prevent flooding attack are given in Ad Hoc Networks [13]. In this work author explains new DOS attack and its defense in ad hoc networks. The new DOS attack is called Ad Hoc

Flooding Attack (AHFA) in which the intruder broadcasts excessive Route Request packets, all immediate neighbors of the intruder, track the behavior of sender and record it and check its trust by using a trust function. Once the threshold is exceeded, nodes discard any future requests from the intruder. The results of this implementation show FAP can prevent the Ad Hoc Flooding attack efficiently. A way to handle Distributed Denial-of-Service Attack is given in [12] by using policy based networking.

A Filtering Scheme against RREQ flooding attack in Mobile Ad Hoc Networks is proposed [2]. In this paper a new technique is proposed for filtering RREQ flooding. This type of attack is hard to detect since malicious nodes mimic normal nodes in all aspects except that they do route discoveries much more frequently than the other nodes. So the authors propose a distrusted filtering mechanism to mitigate such situations and to stop reduction in throughput. This proposed scheme could prevent this specific kind of DoS attack and does not use any additional network

A Trust Based Security Scheme for RREQ Flooding Attack in MANET [3]. This paper presents a novel technique to mitigate the effect of RREQ flooding attack in MANET using trust estimation function in DSR on demand routing protocol. It maintains a relation table of a neighbour, which categorise a neighbour node as a Friend, Stranger or Acquaintance. If neighbour sends RREQ first time then it is considered as a Stranger, and has the lowest trust value. If node sends previously sent packets then it is considered as Acquaintance. These are the nodes which have the trust level between the Friends and Stranger. Last category is Friends. These are the most trusted nodes and have the highest trust value.

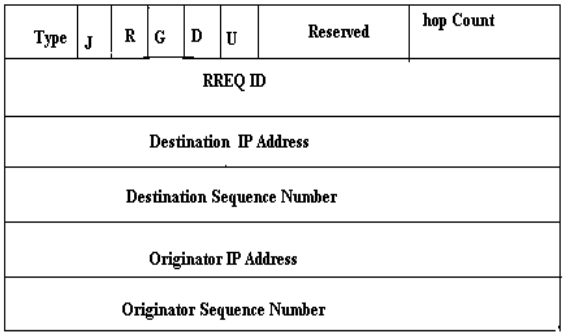
Security Scheme for Distributed DoS in Mobile Ad Hoc Networks [4]. In this paper, a proactive scheme is proposed that could prevent a specific kind of DoS attack and identify the misbehaving node. And to find suitable solution to overcome the attack of initiating / forwarding fake Route Requests (RREQs) that lead to hogging of network resources and hence denial of service to genuine nodes.

Flooding Attack Prevention (FAP) method [5] [7] is defense against the Ad Hoc Flooding Attack in mobile ad hoc networks. When the intruder broadcasts excessive packets of Route Request, then intruder's behavior is recorded by its immediate neighbors and they check its trust by a trust function. Once a node exceeds the threshold value, all the request packets from that node is discarded by other nodes. This implementation shows that FAP can prevent the Ad Hoc Flooding attack efficiently. Another flooding attack prevention method uses neighbor suppression and path cut off method by handling priorities of requests [7]. A defensive mechanism is used against flooding attack by using public key cryptography and digital signatures [6], so that IP address spoofing by malicious node can be prevented.

3. AODV

The Ad hoc On-Demand Distance Vector (AODV) algorithm is a routing protocol which provides dynamic, multi hop routing between mobile nodes of an ad hoc network. As the topology always changes in MANET so AODV provides dynamic routing procedures by finding new routes to destinations, and removes the routing entries for unreachable destinations. Using AODV mobile nodes can respond to link breakages and changes in network topology in a timely manner. AODV operates in a loop-free manner, and it avoids the Bellman-Ford "counting to infinity" problem which provides quick convergence when the topology of ad hoc network changes. When any active link breaks, AODV notifies the affected nodes. Using this notification, nodes remove the entries for those routes by the lost link. Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs) are message types defined by AODV.

Table 1: Format of RREQ Packet



Type	J	R	G	D	U	Reserved	hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							

Type

J Join flag; reserved for multicast.

R Repaired flag; reserved for multicast

G Gratuitous RREP Flag; Indicates whether a gratuitous RREP should be unicast to the node specified in the destination IP address field.

D Destination only flag; indicates only the destination may respond to the RREQ .

U Unknown sequence number; indicates the destination sequence number is unknown.

Reserved Sent as 0; ignored on reception

Hop Count The number of hopes from the originator IP Address to the node handling the request.

RREQ ID A sequence number particularly identifying particular route request when taken in conjunction with the originating node's IP Address.

Destination IP Address IP address of destination for which a route is desired.

Destination Sequence Number The latest sequence number received in the past by the originator for any route towards the destination.

Originator IP Address IP Address of the node which originates the route request.

Originator Sequence Number The current sequence number to be used in the route entry pointing towards the originator of the route request.

4. Proposed Approach

The proposed approach tries to minimize unnecessary RREQ packet flooding and saving the battery power of legitimate node. This approach works on threshold policies of RREQ packets [1]. The Proposed technique is based on history table maintained for previous recorded RREQ packets in certain number of sessions at time of simulation. This approach is based on finding the RREQ packets send and received by each node from their neighbor nodes in sessions maintained in history table. Then average of RREQ packets value in all session is calculated. Discard Limit is also calculated based on this average value. . History table is maintained on each node which contain record the RREQ packets values in the sessions created during simulation and by applying formula for nodes discard limit and average value is calculated.

Assume that if there exists a node which unnecessarily broadcasts the RREQ packets to its neighbor nodes for the intension of battery wastage so that legitimate node gets disconnected from network. Proposed scheme tries to minimize the problem by determining a DISCARD_ LIMIT (D_LIMIT). If a node receives RREQ packet from its neighbor nodes then it maintain the history of RREQ flooding from its neighbor nodes in sessions (a group of five session is maintained).Then it calculates the AVG_VAL of RREQ packets arrived on that node from its neighbors in each session.

This scheme depends on the MAX_VAL, AVG_VAL and DISCARD_LIMIT. If the no. of received RREQ packet is greater than the DISCARD_LIMIT then discard the packets after arriving to that limit and set as UNKNOWN NODE. If the no. of RREQ packet arrived are less than the DISCARD_LIMIT then process the packet, and set as KNOWN NODE. So that average value is known for RREQ packet flooding in sessions.

In fig 1 suppose there are five nodes. N0, N1, N2, N3, N4, N5. N0 initialize route discovery process by sending RREQ packets to its neighbor's node. When N2 or N1 sends RREP packet to N0 then it stops sending packet. These we can say as first session and capture the RREQ packet flooding in all sessions by each node to its neighbors. Now take an average of RREQ packets flooding in sessions by each node to its neighbors. By using this average value calculate

RATE_LIMIT =Max no. of RREQ [S_i] - AVG_VAL

D_LIMIT= (AVG_VAL+RATE_LIMIT)+1

If received RREQ is greater than RREQ DISCARD_LIMIT then Drop the RREQ packets and set the node as UNKNOWN NODE. And if received RREQ less than RREQ DISCARD_LIMIT Process the packet set as KNOWN NODE.

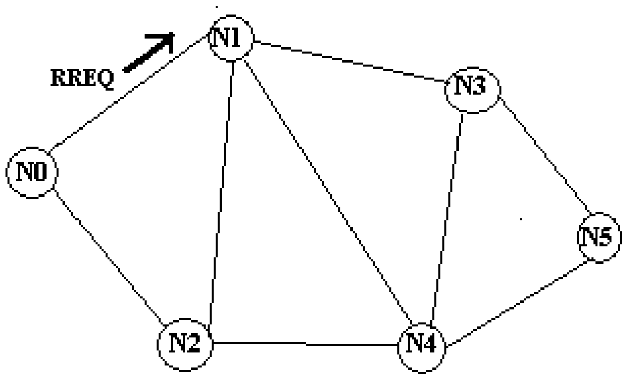


Fig. 1 Setup of Nodes in Network

3.1 Algorithm

1. Begin
If intermediate node k receives RREQ from node i.
2. Determine the RREQ Discard limit (or D_LIMIT) of RREQ receives in all sessions on each node from their neighbors node.
3. AVG_VAL=AVG [S_1, S_2, S_3, S_4, S_5]
4. RATE_LIMIT =max no of RREQ [S_i] - AVG_VAL
5. RREQ Discard limit= (AVG_VAL+RATE_LIMIT) +1
6. If received RREQ >RREQ Discard limit

- Drop the RREQ packet

- Set the node a UNKNOWN NODE.

7. If received RREQ <RREQ Discard limit

- Process the packet
- Set as KNOWN NODE.

In Proposed approach the algorithm is designed to work with AODV protocol. According to the above calculation and steps same process is applied for all Nodes. In this way proposed work detect RREQ flooding attack at node from neighbor nodes and node is malicious or legitimate can be known. .

3.2 Flowchart

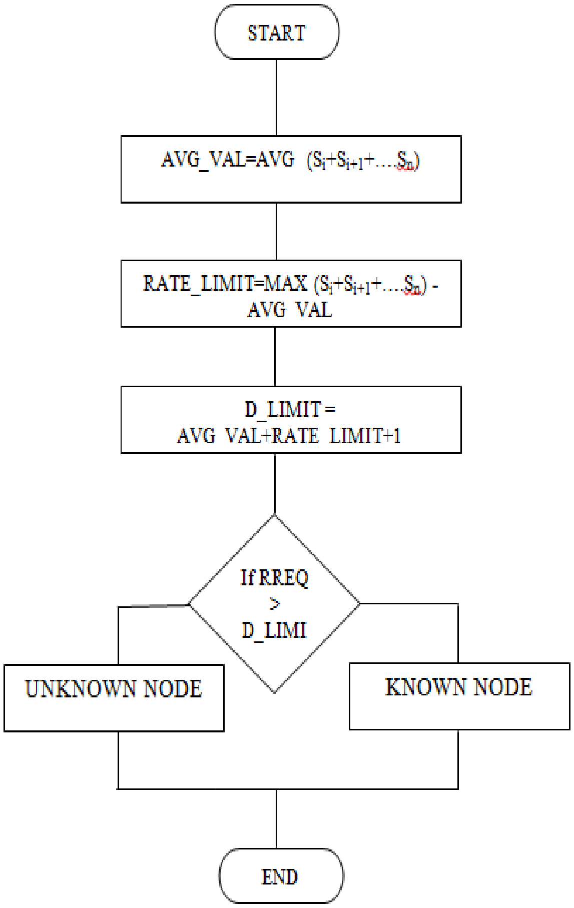

START
AVG_VAL=AVG (S_i+S_i+1+....S_n)
RATE_LIMIT=MAX (S_i+S_i+1+....S_n) - AVG_VAL
D_LIMIT = AVG_VAL+RATE_LIMIT+1
If RREQ > D_LIMI
UNKNOWN NODE
KNOWN NODE
END

Fig. 2 Flowchart of Proposed Method

Fig. 2 shows the working of the proposed approach by a flow chart, which takes average value of all sessions. After calculating average value it is used to calculate threshold values RATE_LIMIT and D_LIMIT discard limit for a node.

Then D_LIMIT is used to decide the status of a node, whether it is known or unknown. So a malicious node can be detected by this approach.

4. Conclusion

In this paper the proposed approach minimizes the problem of battery draining due to unnecessary RREQ packet flooding. Effectiveness of the technique depends on the discard limit and average value of RREQ packet flooding done by its neighbors node which is determine by maintaining history table on each node. These tables capture the RREQ packets flooding value done by its neighbor nodes. If neighbor node always floods RREQ greater then discard limit then it is set as UNKNOWN NODE otherwise in normal flooding it is set as KNOWN NODE. This method helps in saving battery power of legitimate node and to minimize RREQ flooding in route discovery between source and destination

References

[1] Fuu-Cheng Jiang, Chu-Hsing Lin, Hsiang-Wei Wu,“Lifetime Elongation of Ad Hoc Networks under Flooding Attack using Power-Saving Technique”,Science Direct 1570-8705/_ 2014 Elsevier B.V. , pp. 85-89, May 2014.

[2] Jian-Hua Song1, 2, Fan Hong1, Yu Zhang1 “Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks “ Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06)0-7695-2736-1/06 $20.00 © 2006.

[3] Shishir K. Shandilya, Sunita Sahu, “A Trust Based Security Scheme for RREQ Flooding Attack in MANET”. International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010.

[4] Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody “Security Scheme for Distributed DoS in Mobile Ad Hoc Networks” TIFR Mumbai University.

[5] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav “Flooding attack Prevention (FAP) in MANET ” International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.

[6] Zhi Ang EU and Winston Khoon Guan SEAH, “Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks”, Proceedings of International Conference on Information networking (ICOIN-2006), Sendai, Japan, 2006.

[7] P. Yi, Z. Dai, Y. Zhong and S. Zhang, “Resisting Flooding Attacks in Ad Hoc Networks”, Proceedings of International Conference on Information Technology: Coding and Computing (ITCC’05), April 2005, pp.657-662.

[8] Lidong Zhou and Zygmunt J. HaasHappy sankranti/pongalhttp://crackspider.net/ “Securing Ad Hoc

Networks “In Proc IEEE, Special issue on network security, November/December, 1999.

[9] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi” Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes” World Academy of Science, Engineering and Technology 44 2008.

[10] Elizabeth M. Royer, University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology”, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks ”IEEE personal communication, Apr 1999.

[11] Xianjung Geng, Yun Huang, Andrew B. Whinston, “Defending Wireless Infrastructure Against The Challenge of DDoS Attack ”, Mobile Networks and Applications 7, 213–223, 2002,2002 Kluwer Academic Publishers.

[12] Bo-Cang Peng and Chiu-Kuo Liang”Prevention Techniques for Flooding Attack in Ad Hoc Networks”