Detection and Prevention of Malicious Flooding - A DoS Attack in Adhoc Network

Malvika Bahl, Ritesh Kushwaha, Sameena Zafar

Abstract- The operations in Mobile Ad-hoc Networks (MANETs) are still not very resistant to RREQ flooding attack because of its mechanism of discovering route and transmitting packets. For controlling congestion problems, the protocol has already defined a limit of RREQ packets that can be originated by a node. Attacker node exploits this weakness and initiates many more RREQ packets which may be futile and abundant enough to waste precious resources of the network. The threshold parameter is set at each node which checks the number of RREQ packets which it receives per unit time. The threshold value helps in determining whether a node is malicious or normal. If the RREQs generated by a node per unit time exceeds allowable limit, assumption can be made that the sender is a malicious node.

Keywords—Wireless Adhoc Network, malicious nodes, Flooding.

I. INTRODUCTION

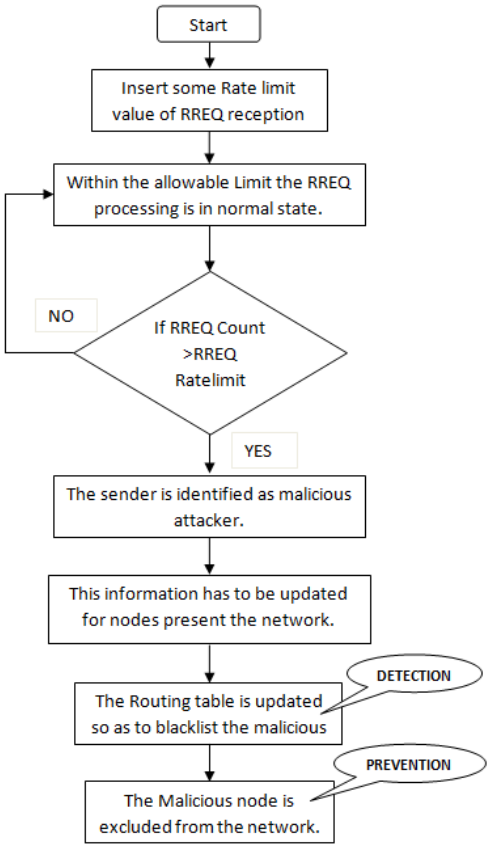
A mobile ad-hoc network is a self organized autonomous network that consists of mobile nodes; each equipped with a transmitter and a receiver, which interact with each other over wireless links. Such networks are suitable in battlefield with no existing infrastructure; emergency workers at an earthquake that destroyed the infrastructure and others. In all such cases, and others, each node consists of a router and a host, usually on the same computer/node. Wireless channel is used by these networks and such channel is considered highly vulnerable against malicious attacks because of limited battery, no fixed infrastructure, dynamic topology and memory usage etc. Security is a key feature in any network and hence its implementation here too differs from the fixed wired networks.

Nodes with malicious intent can easily setup various kinds of attacks. Black hole Attack is done by a type of malicious node that would take part in route discovery mechanism and try to become part of a route which is active. Gray hole Attack is conducted by a type of malicious node that would not participate in route discovery mechanism initiated by other nodes and thus it would not be a part of active route. [2] A black hole drops all the packets which are supposed to be forwarded by it. [1]Jellyfish attack is a type of selective black hole attack. JF node starts delaying/dropping data packets for certain amount of time before forwarding normally. [4]There are various types of attacks in Mobile Adhoc networks (MANET) [5] The denial of service (DoS) attack is launched by the intruder inserting packets into the network to devour network resources. For example, if a doubtful node floods the MANET by generating route request packets and seizes the bandwidth.

Flooding Attack- It is a denial of service attack in which malicious node sends the futile packets to devour the precious network resources.

II. PROPOSED FLOWCHART

The proposed methodology and approach is shown in the form of a flowchart as below.



III. PROPOSED METHOD

AODV routing protocol is not very resistant to RREQ flooding attack because of its mechanism of route discovery and packet broadcasting scheme. To handle congestion, the protocol has already implemented some methods. AODV has a predefined limit of how many RREQ packets can be originated by a node. According to RFC 3561 the default value of RREQ_RATELIMIT is 10.

Also, after a RREQ packet is broadcasted, the initiator has to wait for a ROUTE REPLY. If a reply is not received within round-trip time in milliseconds, the node will retry again in order to discover a route by broadcasting another RREQ, until it attains a maximum of retry times at the maximum TTL value. When the source node broadcasts a RREQ for the first time, it will wait for RREP PACKET.

Malicious/attacker node exploits this weakness and initiates many more RREQ packets which may be fake or futile than the normal node in order to consume the network resources or the affected node's valuable resource.

The RREQ packets are prioritized over the data packets; the nodes take more time in the processing of the RREQ packets and thereby cause a delay.

A malicious node can override the restriction put by RREQ_RATELIMIT by increasing it or changing it to disable mode. A node can do the same as it has self-control over its parameters. A compromised node may set the value of parameter RREQ_RATELIMIT to a value of large magnitude. This permits it to flood the network with futile RREQs and leads to a kind of DoS attack.

In this type of DoS attack a non-malicious node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs. It causes loss of bandwidth, processing time, throughput etc.

So in our work the proposed algorithm uses a filter to detect malicious node and reduces their impact on performance of the network. The filter has to limit the rate of RREQ packets. Each node has a pre-assigned threshold value.

The threshold parameter denotes the number of RREQs that can be accepted and processed as normal per unit time by a node. Every node monitors the route request packets it receives and maintains a count of RREQs received for each RREQ originator during a time period which is preset. On receiving a RREQ, a check is performed. If the rate of this RREQ sender is within the limits, then the RREQ packet is processed as non malicious packet.

The threshold value is instrumental in determining whether a node is acting in a maliciously manner or not. If the number of RREQs originated by a node per unit time exceeds the value of threshold, it can be assumed that the corresponding node is trying to flood the network with fake/futile RREQ packets. On identifying a sender node as malicious will prevent further flooding of the fake RREQs in the network. The neighboring nodes of the malicious node are therefore free to entertain the RREQs from other genuine nodes. In this way we can increase throughput, end to end delay and packet delivery ratio of AODV over MANET.

IV. SIMULATION RESULTS

For the proof of our methodology we have used NS-2.35 simulator in order to analyze the performance of proposed scheme. In our simulation we used network layer protocol AODV as a base protocol. Our simulation has taken into consideration both single and well as multiple malicious node scenarios.

Different sets of simulations have been carried out taking 10, 20, 30, 40, 50 nodes. (Fig 1 and 2).

A 500 x 500 meter square area is taken as network area. We compare the performance of original AODV protocol with proposed scheme in presence of RREQ Flooding attack.

Fig 3 represents the behavior of AODV, AODV under attack and AODV under proposed algorithm.

V. CONCLUSION

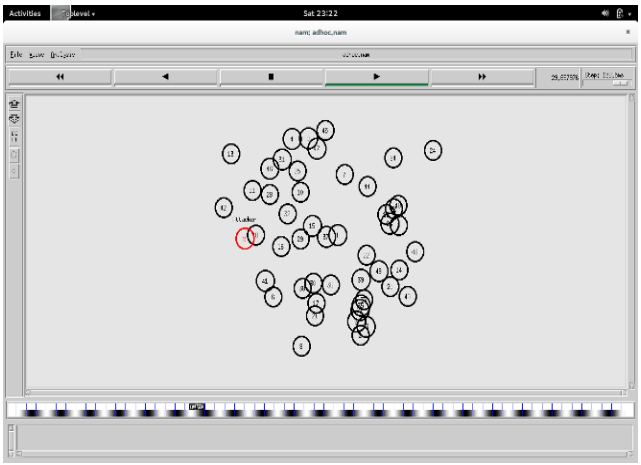


Fig.1

This research paper proposes the new scheme for mitigating flooding attack, which is a Denial of service attack in MANET, by excess transmission of Route request packets using AODV protocol. The results show that this method can easily detect the attacker node and protect the network resources from RREQ flooding attack.

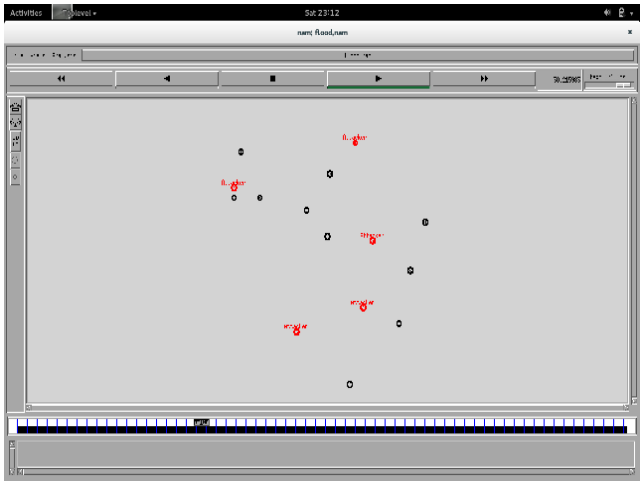


Fig. 2

Fig 3

REFERENCES

[1] Htoo Maung Nyo, Piboonlit Viriyaphol, “Detecting and Eliminating Black Hole in AODV Routing Detecting and Eliminating Black Hole in AODV ,IEEE 2011

[2] Mohammed Saeed Alkatheiri, Jianwei Liu, Abdur Rashid Sangi ,”AODV Routing Protocol Under Several Routing Attacks in MANETs” 2011, IEEE

[3] Mohammad Taqi Soleimani Secure AODV against Maliciously Packet Dropping ,IEEE

[4] Meenakshi Patel , “Detection of malicious attack in MANET-a behavioral approach, 2012

[5] Ankur mishra1, Ranjeet jaiswal,”A novel approach for Detecting and eliminating cooperative black hole attack using advanced dri table in ad hoc network .”978-1-4673-4529-3/12/$31.00_c 2012 IEEE.

[6] hizbullah khattak, nizamuddin, fahad khurshid, noor ul amin preventing black and gray hole attacks in aodv using optimal path routing and Hash 978-1-4673-5200-0/13/$31.00 ©2013 IEEE

[7] Tsung-Chuan Huang, Sheng-Chieh Chen, Lung Tang Energy-Aware Gossip Routing for Mobile Ad Hoc Networks, 2011 IEEE International Conference on High Performance Computing and Communications.

[8] J.Premalatha Enhancing Quality of Service in MANETS by Effective Routing 978-1-4244-5137-1/10/$26.00 ©2010 IEEE

[9] Kashif Laeeq, RFAP, A Preventive Measure against Route Request Flooding Attack in MANETS, 978-1-4673-2252-2/12/$31.00 ©2012 IEEE