Route Request Flooding Attack Using Trust based Security Scheme in Manet

Ujwala D. Khartad & R. K. Krishna

Rajiv Gandhi College of Enginnering Research & Technolgy, Chandrapur, India
E-mail : ujwala2011.pazare@gmail.com, rkrishna40@rediif.com

Abstract **-** In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications, including some mission critical applications, and as such security has become one of the major concerns in MANETs. A mobile ad hoc network is set up with a group of mobile wireless nodes without the use of any dedicated routers or base stations. Each node acts as an end node as well as a router for other nodes. A Mobile Ad-hoc Network (MANET) is based on self organizing, dynamic structure and freedom of mobility idea. The characteristics like dynamic structure, limited power, restricted bandwidth and continuously changing network routes makes MANET more vulnerable to the attacks and providing the security to it proves to be a challenging area.In this paper,we describe that how the flooding attack occur and the effect of flooding attack. Finally, we present simulation results to show the detrimental effects of Flooding Attack.

Keywords **-** *mobile ad hoc network, security, flooding attack, Defense.*

I. INTRODUCTION

A mobile ad-hoc network (MANET) is autonomous, infrastructure less network of mobile nodes that can communicate with each other without the use of a centralized administration. The applicative areas of manet are specially emerging operations, military services, vehicle networks,disaster management, battlefield surveillance. The manet system can be viewed as a random graph due to the movement of the nodes, their transmitter/receiver coverage patterns , the transmission power levels and the co-channel interference levels. Hence the network topology keeps on changing with time as the nodes move or adjusts their transmission and reception parameters. Thus the salient characteristics of a manet are dynamic structure, continuously changing topologies and router restricted bandwidth, resource constraints, limited physical security and no infrastructure [7]. A mobile ad hoc network (MANET) consists of a group of mobile wireless nodes that allow data communications beyond direct radio transmission through the use of intermediate nodes that will help to forward data packets. In MANETs, there is no central entity to coordinate the operations of the network, therefore there are more security challenges as compared to wired networks. Due to the nature of the wireless medium, malicious nodes or trusted nodes infected by viruses or worms can disrupt the operations of ad hoc networks by injecting wrong routing information or forging data packets.

MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omnidirectional (broadcast), highly- directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

This article is structured as follows: We describe the Route request flooding attack in MANET and messase format and damages caused by it.Then describe the how occur the flooding attack in manet.Then what effects of flooding attack.

II. RELATED WORK

The flooding attack is the most common attack found in manet. The aim of the flooding attack is to exhaust the network resources such as bandwidth and to consume a node’s resources or to disrupt the routing operation to degrade the network performance. This leads to a kind of Denial-of- Service (DoS) attack,

wastage of bandwidth, wastage of node's processing power and exhaustion of node's battery power as well as a degraded performance. Most of the network resources are wasted in trying to generate the routes to the destination that do not exist. The Route Request Flooding Attack (RRFA) is a denial-of service attack which aims to flood the network with a large number of RREQs to non-existent destinations in the network. In this attack, the malicious node will generate a large number of RREQs, possibly in the region of hundreds or thousands of RREQs, into the network until the network is saturated with RREQs and unable to transmit data packets. In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network.

III. HOW OCCUR FLOODING ATTACK

The flooding attack occuration was proposed in [13]. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the hosts memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

Flooding packets in the whole network will consume a lot of network resources. To reduce congestion, the protocol has already adopted some methods which are briefly described as follows. Firstly, the number of RREQ that can be originated per second is limited. Secondly, after broadcasting a RREQ, the initiator will wait for a ROUTE REPLY.-If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, until it reaches a maximum of retry times at the maximum TTL value. Time intervals between repeated attempts by a source node at route discovery for a single destination must satisfy a binary exponential backoff. The first time a source node broadcasts a RREQ, it waits round-trip time for the reception of a ROUTE REPLY [15].

But for the second RREQ, the time to wait for the ROUTE REPLY should be calculated according to a binary exponential backoff, by which the waiting time now becomes 2 * round-trip time. Thirdly, The RREQ packets are broadcasted in an incremental ring to reduce the overhead caused by flooding the whole network. At first, the packets are flooded in a small area (a ring) confined by a small starting time-to-live (TTL) in the IP headers. After RING TRAVERSAL TIME, if no ROUTE REPLY is received, the forwarding area is enlarged by increasing the TTL by a fixed value. The procedure is repeated until a ROUTE REPLY is received which means that a route has been found.

In the flooding attack, the attack node violates the above rules to exhaust the network resources. Firstly, the attacker will produce many IP addresses which do not exist in the networks if he knows the scope of the IP addresses in the networks. As no node can return ROUTE REPLY packets for these ROUTE REQUEST, the reverse route in the nodes' route table will be conserved longer than normal. If the attacker cannot get the scope of IP addresses in the network, he can just choose random IP addresses. Secondly, the attacker successively originates mass RREQ messages with these void IP addresses as destination and tries to send excessive RREQ without considering the RREQ RATELIMIT, that is, without waiting for the ROUTE REPLY or waiting a round-trip time. Besides, the TTL of RREQ is set up to a maximum at the beginning without using an expanding ring search method. Under such attack, the whole network will be full of RREQ packets from the attacker. The communication bandwidth and other node resources will be exhausted by the flooded RREQ packets. For example, the storage of route table is limited. If the large amounts of RREQ packets are arriving in a very short time, the storage of the route table in the node will be used up soon so that the node can not receive new RREQ packets any more.

IV. EFFECT OF FLOODING ATTACK

Flooding Attack can seriously degrade the performance of reactive routing protocols and affect a node in the following ways.This was proposed in [15].

A. Degrade the performance in buffer:

The buffer used by the routing protocol may overflow since a reactive protocol has to buffer data packets during the route discovery process. Furthermore, if a large number of data packets originating from the application layer are actually unreachable, genuine data packets in the buffer may be replaced by these unreachable data packets, depending onthe buffer management scheme used.

B. Degrade the performance in wireless interface :

Depending on the design of the wireless interface, the buffer used by the wireless network interface card may overflow due to the large number of RREQs to be sent.Similarly, genuine data packets may be dropped if routing packets have priority over data packets.

C. Degrade the performance in RREQ packets :

Since RREQ packets are broadcast into the entire network, the increased number of RREQ packets in the network results in more MAC layer collisions and

consequently, congestion in the network as well as delays for the data packets. Higher level protocols like TCP whichis sensitive to round trip times and congestion in the network will be affected.

D. Degrade the performance in lifetime of Manet:

Since MANET nodes are likely to be power and bandwidth constrained, RRFA can reduce the lifetime of the network through useless RREQ transmissions as well as additional overheads of authenticating a large number of RREQs, if used.

a. Abbreviations and Acronyms

To study the effect of flooding attack in mobile ad hoc networks, The wireless networks simulation software we use is NS2[13].

The following metrics is used to evaluate the performance of flooding attack.

- *Packet loss rate:*

The ratio of the number of packets dropped by the nodes divided by the number of packets originated by the application layer continuous bit rate (CBR) sources. The packet loss ratio is important as it describes the loss rate that can be seen by the transport protocols,which in turn affects the maximum throughput that the network can support. The metric characterizes both the completeness and correctness of the routing protocol.

- *Average delay:*

Average of delays incurred by all the packets which are successfully transmitted.

- *Throughput:*

Average number of packets per second× packet size.

- *Average number of hops:*

Total length of all routes divided by the total number of routes. although behave legally, can not set up paths to send data.

B. Under different number of attack nodes

There are 50 nodes, including 0–5 attack nodes. The MAC bandwidth is set to 11 M. The frequency of flooding attack is set to 100 packets/ s. During simulation, the number of flooding nodes increases from 0 to 5.The packet loss rate starts from 3.5% under no attack and increases to 54% with one attack node, 75%with two attack nodes, and more than 82 % with three attack nodes. When the number of attack nodes is greater than two, the network becomes considerably congested. Throughput starts from 8 255 byte under no attack and decreases to 2 324 byte with one attack node, 1 287 byte with two attack nodes, 1 287 byte with two attack nodes, and 589 byte with four attack nodes. For the packet size is 512 byte, it shows that all nodes in the network can only receive a packet in one second. Flooding nodes have exhausted the communication bandwidth and node resource so that the valid ommunication can not be kept any more. With the increase of the number of attack nodes, the packet average delay extends from 0.59 s to 9.6 s and then remained at around 10 s. The average number of hops decreases from 2.3 to 1.5 hops. It shows that most packets which are more than two hops can not get to the destination nodes because of the network congestion.

C. Under different flooding Frequencies

The packet loss rate starts from 3.5% under no attack and increases to 16% under 20 packets/s flooding, and 42% under 40 packets/s.

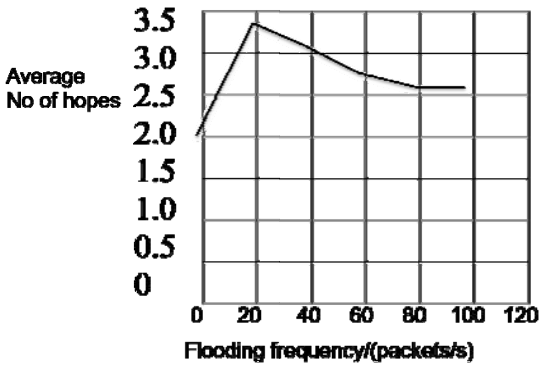
When the flooding frequency is higher than 40 packets/s, the curve becomes flat.It shows that 40 packets/s is a turning point, and if the flooding frequency is greater than 40, it would be difficult to obtain apparent results. Similarly, throughput starts from 8 227 byte under no attack and decreases to 4 153 byte under 20 packets/s flooding, 2 837 byte under 40 packets/s flooding, and 2 461 byte under 60 packets/s. When the flooding frequency is greater than 40, the throughput decline would be not obvious any more. Average delay is similar to the above parameters, which sharply increases from 0.19 s to 12 s when the flooding frequency increases from 0 to 40 packets/s. The average number of hops goes up to a peak 3.2 and then declines to a stable value 2.5 in the end. This phenomenon can be explained as, before the communication bandwidth and node sources are exhausted, the average number of hops increases in direct proportion to the increasing frequency of flooding attacks due to more congestion. However, when network resources have been exhausted, with the increasing frequency of flooding attacks, nodes begin to discard the congestion packets, especially those which have a long route. It results in the loss of packets with long routes and the remaining of packets with very short routes.

D. Under different bandwidths

The packet loss rate is about 3% under no attack. When the frequency of flooding attack is low (e.g., 20 packets/s), the packet loss rate decreases from 42 % to 16 % as network bandwidth increases from 1 M to 5.5M. However, when the flooding frequency goes greater than 40 packets/s, the influence of bandwidth on the network performance is not obvious. Throughput and average delay are similar. This phenomenon can be explained as the number of flooding packets is over NIC's network interface card's (NIC'S) processing power, and most of the packets in the queue are discarded. Therefore, simply increasing the network bandwidth can not improve network performance.

E. Under different numbers of nodes

The packet loss rate increases from 42% to 70% as the number of nodes increases from 25 to 100 under one node's attacking. Throughput is similar, which-decreases from 3 665 byte to 743 byte as the number of nodes increases from 25 to 100 under one node's attacking. With the increase of attack nodes, two above parameters get closer and closer. Throughput nearly drops to 0 under 5 nodes' attacking. It shows that flooding nodes have exhausted . the communication bandwidth and node resources so that the valid communication can not be kept.



Average delay increases with the increase of attack nodes, but it seems nothing to do with the number of nodes. Similarly, the average number of hops decreases with the increase of attack nodes and it has nothing to do with the number of nodes.

V. PROPOSED APPROACH

In [6], the author proposed the distributive approach to resist the flooding attack. In this method they have used the two threshold value; RATE_LIMIT and BLACKLIST_LIMIT. If RREQ count of any node is less then RATE_LIMIT then the request is processed otherwise check whether it is less then BLACKLIST_LIMIT, if yes then black list the node but if the count is greater than RREQ_LIMIT and less than BLACKLIST_LIMIT then put the RREQ in the delay queue and process after queue time out occurs. This method can Handel the network with high mobility.

In [7], the author analyzed the flooding attack in anonymous communication. They used the threshold tuple which consist of three components: transmission threshold, blacklist threshold and white listing threshold. if any node generates RREQ packet more than transmission threshold then its neighbor discards the packet if it crosses the transmission threshold more than blacklist threshold then it black list the node. But to deal with accidental blacklisting they defined white listing threshold. If any node performs good for number of intervals equal to white listing threshold then it again start treating as a normal node.

In [8], the author used the extended DSR protocol based on the trust function to mitigate the effects of flooding attack. In this work, based on the trust value they categorized the nodes in three categories: Friends, acquaintance and stranger. Stranger are the non trusted node, friends are the trusted node and acquaintance has the trust values more than stranger and less than friends. Based on relationship they defines the three threshold value. If any node receives the RREQ packets then checks the relationship and based on that it checks for the threshold value if it is less than the threshold then forward the packet otherwise discard the packet and blacklist the neighbor node. The main problem with this method was it does not work well with higher node mobility.

DSR

The Dynamic Source Routing (DSR) protocol is a on-demand routing protocol.[2,9]. DSR protocol maintains the route cache to store the route to the mobile node it is aware. This protocol composed of two major phases : route discovery and route maintenance. Whenever any node has the data to send, first it checks the route cache for the route to the destination .if it has the unexpired route, then it use it otherwise initiate a route discovery process by broadcasting the RREQ packet which contains the source address and the destination address. Whenever any intermediate node receives the RREQ, and it does not have the route to the destination it adds its own address in the route record and forward to its neighbor. RREP is generated whenever RREQ reaches to destination node or intermediate node which has the route to destination in its route cache. Route maintenance mechanism is used to detect whether the path to the destination exist or not. Route maintenance uses the route error message and acknowledgement Route error message is initiated whenever the destination's data link layer recognize any transmission error. DSR is suited for small to medium sized networks as its packet overhead (not packet data overhead) can scale all the way down to zero when all nodes are relatively stationary. The packet data overhead will increase significantly for networks with larger hop diameters as more routing information will need to be contained in the packet headers.

In our work we have used the Dynamic Source Routing (DSR) routing protocol along with the trust estimation function. Because the communication between the node in the MANET depends on the cooperation and the trust level on its neighbors so to calculate the trust level we have used the trust estimation function in the Route discovery phase of the basic DSR routing protocol which will calculate the trust level of each neighboring node. Various parameters which are used for trust estimation are:

- Total number of RREQ packet sent by the neighbor per unit time
- total number of packet successfully transmitted by the neighbor
- Ratio of number of packet received correctly from the neighbor to the total number of received packet.

In our scheme based on their relationship with the neighboring node, we have categorized the node in three categories that are given below.

A. STRANGER:

The strangers are the non trusted node means a stranger node is a node with minimum trust level. Initially when any node joins the network, then this trust relationship with its all the neighbors are low or negligible this that node is treated as stranger.

B. ACQUANTANCE:

These are the nodes which have the trust level between the friends and stranger. Means a node is acquaintance to its neighbor means it has received some packets through that node.

C. FRIEND:

Friends are most trusted nodes or the nodes with highest trust level can be treated as friends. Here the higher trust level means neighbors had received or transfer many packets successfully through this particular node.

During the route discovery phase of the DSR Routing protocol, the trust value is also computed for all the neighbors of any node. The result of trust estimation function is the relationship status of all of neighbors as friend, acquaintance or stranger.

Consider a MANET of figure 1 with seven nodes.(n0 – n6) where node n1,n2,n3,n4,n5,n6 are the neighbors node of node n0. Node n1 and n3 has a friend relationship with n0, node n2 and n4 are stranger to n0 and n5 and n6 are acquaintance to node n0. These relationships are shown in the friendship table 1.

To detect the intrusion, in our scheme each node stores a friendship table. Friendship table is used to store the relationship status of any node with its neighbors. The friendship table has two columns.

- First the identifier or name of all of its neighboring node
- Second its relationship status with the neighbor node that could be either friend, Acquaintance or stranger.

This table is referred every time when any node receives the packets. Initially when node joins the networks they are considered as a stranger. A node is considered as a stranger if nodes have never sent or receive message to or from the neighbor. A node is considered as an acquaintance if its trust level is neither very neither low nor too high means node receives some packet through this neighbor. If node receives many packets to or from any node successfully, then trust level is very high the node is considered as a friend. There is very high probability of attack from stranger but very low probability from friend. Different threshold values are defined for different types of neighbors to become friend, Acquaintance and stranger. Tracq and Trfri are the threshold values for the acquaintance and the friend respectively. Along with this every node maintains a local counter to count RREQ that is compared with threshold value of neighbors. If RREQ count is greater than Trfri then neighbor is considered as a friend and if it is greater than Tracq and less than Trfri then neighbor is acquaintance otherwise considered as a stranger.

To extend the method proposed in [5] for higher node mobility, we added the concept of delay queue. Consider the situation where the node mobility is very higher so all most all the nodes relationship status can be stranger or acquaintance because to become a friend to its neighbor, node has to forward many packets successfully to its neighbor. But because of the higher mobility nodes changes its position frequently so possibility of friend relationship is very low. As we know that the threshold value of the stranger or acquaintance is lower than the friends so if any node sends many RREQ packets per unit time because of the mobility this is considered as misbehavior because its count exceeds threshold limits. Then according to method proposed in [5], the neighbor node discards the packets and declare the node as a intruder or malicious node, which is not true. So to deal with such kind of situations we have added the concept of delay queue here.

VI. CONCLUSION AND FUTURE WORK

In this paper, the influence of flooding attack on the entire network performance is analyzed under the circumstances of different parameters including the number of attack nodes, flooding frequency, network bandwidth, and the number of normal nodes. The future work is that how the flooding attack is detected and prevented using core node. The expected outcomes of the implementation are Comparative of defenses

available for attacks ,Metrics will be achieved through the simulator, Simulated output of proposed method , Calculated metrics, Comparative with existing methods.

REFERENCES

[1] S. Corson University of Maryland, J. Macke Naval Research Laboratory "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations" January 1999.

[2] 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 .

[3] C. Perkins Nokia Research Center,E. Belding-Royer University of California, Santa Barbara, S. Das University of Cincinnati "Ad hoc On-Demand Distance Vector (AODV) Routing" July 2003.

[4] Tiranuch Anantvalee Department of Computer Science and Engineering Florida Atlantic University, Boca Raton,, Jie Wu Department of Computer Science and Engineering Florida Atlantic University, Boca Raton, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" 2006

[5] D. Johnson Rice University,Y. Hu UIUC D. Maltz Microsoft Research" The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4" February 2007.

[6] 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.

[7] Venkat Balakrishnan, Vijay Varadharajan,and Uday Tupakula" Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications" The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) 0- 7695-2842-2/07 $25.00 © 2007.

[8] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka and T. Rama Rao "prevention of flooding attack in mobile ad hoc network". International Conference on Advances in Computing, Communication and Control (ICAC3'09).

[9] David B. Johnson David A. Maltz Josh Broch "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks .

[10] Zhi Ang EU and Winston Khoon Guan SEAH," Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks"2009 IEEE.

[11] T. Clausen LIX, Ecole Polytechnique C. Dearlove BAE Systems ATC Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs)" March 2009.

[12] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao , " Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", World Academy of Science, Engineering and Technology 2009.

[13] Chakeres CenGen "IANA Allocations for Mobile Ad Hoc Network (MANET) Protocols " March 2009.

[14] K.URMILA VIDHYA , M. MOHANA PRIYA Sri Krishna College of Engineering & Technology, Coimbatore, India "A NOVEL TECHNIQUE FOR DEFENDING ROUTING ATTACKS IN OLSR MANET" 2010 IEEE International Conference on Computational Intelligence and Computing Research.

[15] Manish B. Guddhe, Dr. M. U. Kharat,"Core Assisted Defense against Flooding Attacks In MANET "January 10 , 2009.

[16] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, Department of Computer Science and Engineering, MANIT Bhopal, M.P., India, Department of Computer Science and Engineering, MANIT Bhopal, M.P., India, Department of Electronic and Telecommunication, MANIT Bhopal, M.P., India," Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.

[17] Ping Yi , Futai Zou, Yan Zou, and Zhiyang Wang," Performance analysis of mobile ad hoc networks under flooding attacks " Journal of Systems Engineering and Electronics Vol. 22, No. 2, April 2011, pp. 334–339

[18] HyoJin Kim, Ramachandra Bhargav Chitti and JooSeok Song " Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks " , Journal of Information Processing Systems, Vol.7, No.1, March 2011.

◈◈◈