A Trust Based Security Scheme for RREQ Flooding Attack in MANET

Shishir K. Shandilya
Head, PG Dept. of Computer Science & Engineering
NRI Institute of Information Science and Technology
Bhopal, India

Sunita Sahu
PG Dept. of Computer Science & Engineering
NRI Institute of Information Science and Technology
Bhopal, India

ABSTRACT

Mobile ad hoc are gaining popularity because of availability of low cost mobile devices and its ability to provide instant wireless networking capabilities where implementation of wired network is not possible or costly. MANETs are vulnerable to various types of attack because of its features like continuous changing topology, resource constraints and unavailability of any centralized infrastructure. Many denial of service type of attacks are possible in the MANET and one of these type attack is flooding attack in which malicious node sends the useless packets to consume the valuable network resources. Flooding attack is possible in all most all on demand routing protocol. In this paper we present a novel technique to mitigate the effect of RREQ flooding attack in MANET using trust estimation function in DSR on demand routing protocol.

Keywords

Mobile Ad-hoc Networks ,Denial of service, Flooding Attack.

1. INTRODUCTION

Mobile ad hoc networks have been gaining popularity because of availability of low cost mobile devices and its ability to provide instant wireless networking capabilities where implementation of wired network is not possible or costly. MANET is a collection of mobile node with routing capabilities and connected with wireless link. Mobile node can directly communicate to each other if they fall in the radio coverage range of each other [1]. In order to forward the packet to the node which are beyond the coverage range, MANET uses the concept of multi hop communication. Nodes in the MANET are free to move, which dynamically changes the topology of the network. It does not require any expensive infrastructure to support the mobility [2]. Creating the Ad hoc networks is possible where implementation of infrastructure is not possible or expensive.

MANET are generally formed for short range communication. The performance/speed of the network depends on the number of devices; it degrades as the number of device increases because all the devices shares the available network resources.

Like conventional wired network MANET also uses routing protocols to route the packets to its destination. Ad hoc networks routing protocols are divided into two categories: Proactive and reactive [3].

Proactive routing protocols are also known as "table driven" routing .In this, all the nodes store the routing information about other node present in the networks and routing updates are propagated in the network whenever network topology changes. The advantage of proactive routing protocol is that node experiences minimal delay when route is needed and unexpired route is available in the routing table but the disadvantage of proactive routing is that these are not scalable and maintenance of routing table requires substantial network resources. In the case of reactive routing protocol, route between the nodes is searched only when node wants to communicate with other node. To discover the routes they use route discovery procedure which in turns uses the flooding method. In this, initiator forwards the RREQ packet to all of its neighbor's. If neighbor has the route for destination they reply otherwise forward the RREQ to the next node. In this way RREQ packet reaches to the destination which sends the reply to RREQ. But the method which is used to facilitate route discovery are used by the Intruders or the malicious node to consume the network resources which may lead to flooding attack.

In this paper, we propose a novel technique which uses the DSR on demand routing protocol to reduce the effect of RREQ flooding attack in the networks with high node mobility.

The organization of this paper is as follows. Section 2 provides the overview of related work. Section 3 described the Flooding attacks and its types. Section 4 presents the DSR routing protocol. Section 5 presents our proposal to prevent the RREQ flooding attack. Section 6 shows the result of the proposed technique, and finally, the section 7 concludes the paper.

2. RELATED WORK

Significant works have been done in securing the ad hoc network. Some researches defined the method for secure routing but secure routing also can not able to handle the flooding attack.

The first flooding attack prevention(FAP) method was proposed in [4]. In their paper, first they described RREQ flooding and data flooding. This was the first paper that addressed the prevention of flooding attack in ad hoc network. The authors proposed the separate approach for RREQ flooding and data flooding. To resist the RREQ flooding, they defined the neighbor suppression method which prioritizes the node based on the number of RREQ received. A node gets higher priority if it sends less numbers of RREQ packets and defined the threshold value. To deal with data flooding they used path cutoff method. In this method when node identifies that sender is originating data flooding then it cutoff the path and sends the route error message. In this way attack is prevented up to some extent but the disadvantage of this method is flooding packet still exists in the network.

This limitation of FAP is eliminated by [5] presented threshold prevention. In this method they defined the fixed threshold value for every node in the network. If any node receives the RREQ flooding packet more than the threshold value then the sender is

assumed as a attacker and all the packets from attacker is discarded by the receiver node. This method eliminates the flooding packet but if the intruder has the idea about the threshold value then it can bypass the TP mechanism. Normal node with high mobility is treated as the malicious node.

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.

To prevent the flooding attack in MANET that can work well in higher node mobility situation, we proposed a novel technique which uses the trust estimation function and delay queue in basic DSR routing protocol.

3. 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.

4. FLOODING ATTACK

Flooding attack is a denial of service type of attack in which the malicious node broadcast the excessive false packet in the network to consume the available resources so that valid or legitimated user can not able to use the network resources for valid communication. Because of the limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network.

The flooding attack is possible in all most all the on demand routing, even in the secure on demand routing SRP, SAODV, ARAN, Ariadne etc. Depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

- RREQ flooding
- DATA flooding

4.1 RREQ FLOODING

In the RREQ flooding attack, the attacker broadcast the many RREQ packets per time interval to the IP address which does not exist in the network and disable the limited flooding feature.

On demand routing protocols uses the route discovery process to obtain the route between the two nodes. In the route discovery the source node broadcast the RREQ packets in the network. Because the priority of the RREQ control packet is higher then data packet then at the high load also RREQ packet are transmitted. A malicious node exploits this feature of on demand routing to launch the RREQ flooding attack.

4.2 DATA FLOODING

In the data flooding, malicious node flood the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of bogus data packets. These useless data packet exhausts the network resources and hence legitimated user can not able to use the resources for valid communication.

5. PROPOSED APPROACH

The proposed flooding attack detection and prevention model is distributed cooperative model in which all the node locally run the intrusion detection code and cooperate with each other to detect and prevent flooding attack in the network.

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.

- Stranger,
- Acquaintance and
- Friend.

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.

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.

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 and 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.

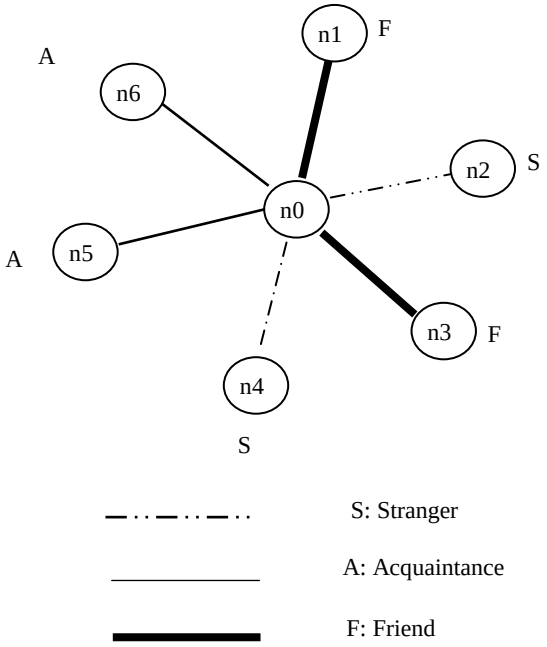

Figure 1. Nodes in a MANET with F-S-A relationship

Table 1. Friendship table of node n0

Neighbors	Relationship status
n1	Friend
n2	Stranger
n3	Friend
n4	Stranger
n5	Acquaintance
n6	Acquaintance

In our scheme, to detect the flooding attack, when any node receives the RREQ from its neighbors then it performs the following steps:

1. It increments the R[i] by one which is a counter maintained by every node for its neighbor which indicates how many RREQ packets it has received from its neighbor.

2. It checks the friendship table to check what type of relationship it is having with this neighbor. It could be friend, acquaintance or stranger.

3. Compares the R[i] with the corresponding threshold values which is a node maximum number of RREQ packets that can be allowed from its neighbor.

3.1 If the neighbor is friend node then it compares whether the R[i] is below the threshold value Xtf then it forwards the packet to next hop otherwise discard the packet and blacklist the node.

3.2 If the neighbor is acquaintance and the R[i] is less than Xta then it forwards the packet otherwise put the node in to the delay queue and allow the node to forward the some packets and analyze its behavior continuously, if still it is misbehaving then declare as a intruder and blacklist the node otherwise treat a normal node.

3.3 If the neighbor is stranger and R[i] is less than Xts then forward otherwise discard the packet and blacklist the node.

6. SIMULATION RESULTS

We used the NS-2 simulator to analyze the performance of proposed scheme. The DSR routing protocol is used for all simulation and the other simulation parameters are shown in the table 2. The topology of the MANET depends on the pause time and mobility speed. It changes frequently when pause time is less and mobility speed is more.

We compare the performance of original DSR protocol in presence of malicious node and the performance of proposed technique in presence of malicious node. To evaluate the performance of the system, we used total number of RREQ sent and RREQ received in the network as a performance matrix.

Table 2. Simulation Parameters

No. of nodes	50
Simulation time	300 sec
Mobility speed	20 ms
Pause time	0 to 150 ms
Routing algorithm	DSR
Mobility model	Random waypoint
Simulation area	1500 X 300
Packets Rate	4/sec
Packet size	512
Traffic type	CBR(UDP)
No. of malicious node	1 to 10

The figure shows the graph of total RREQ sent/receives versus malicious node with mobility speed 20 and pause time zero(0). It is clear from the graph that total number of RREQ packet in the network increases with malicious node because malicious node floods the RREQ packet in the network.

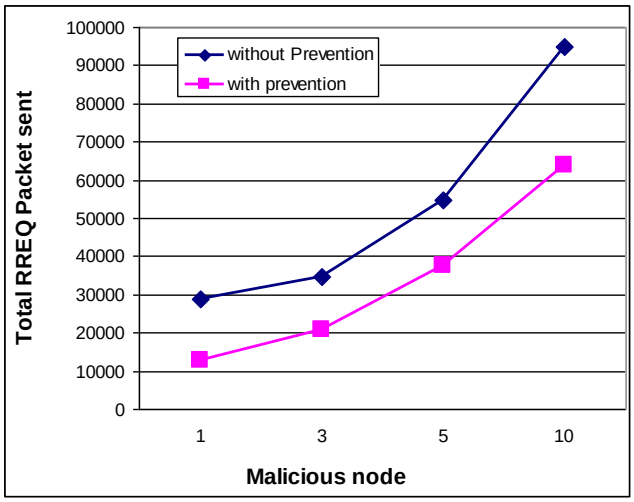

Figure 2. Analysis of RREQ sent

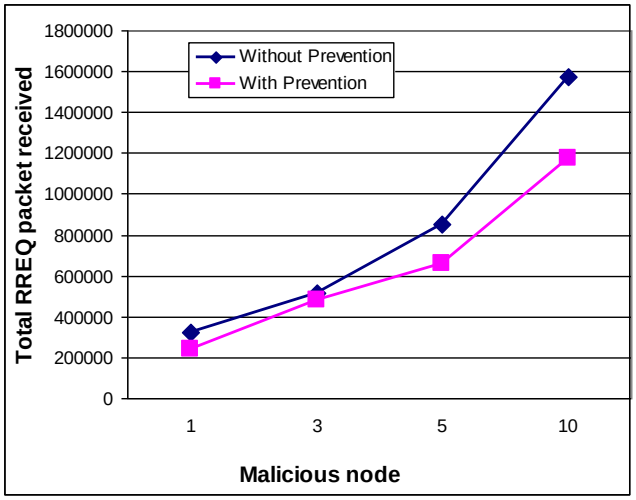

Figure 3. Analysis of RREQ received

The above figure shows that the proposed approach can able to prevent attack up to great extent.

The Figure 4 shows the graph of total RREQ sent in the network with varying mobility speed and pause time which uses the above simulation parameter with 10 malicious node. It also compares the basic DSR routing with proposed method in the presence of malicious node and it is clear that our propose approach efficiently reduces the flooded RREQ packets from the network

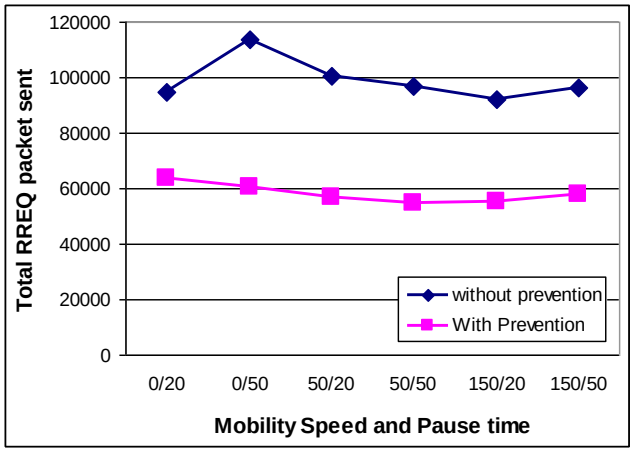

Figure 4. Performance on different mobility speed and pause time

7. CONCLUSION

In this paper, we present a distributive approach to detect and prevent the RREQ flooding attack. The effectiveness of the proposed technique depends on the selection of threshold values. Although, the concept of delay queue reduces the probability of accidental blacklisting of the node but it also delays the detection of misbehaving node by allowing him sends more packet until delay queue time out occurs. Further the proposed method can be extended to prevent data flooding also.

8. REFERENCES

[1] 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.

[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] 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

[4] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang "Resisting Flooding Attacks in Ad Hoc Networks" Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) 0-7695-2315-3/05 $ 20.00 IEEE

[5] Bo-Cang Peng and Chiu-Kuo Liang"Prevention techniques for flooding attack in Ad Hoc Networks"

[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 "http://www.monarch.cs.cmu.edu/

[10] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari" Real-time Intrusion Detection for Ad hoc Networks" Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05) 0-7695-2342-0/05 $20.00 © 2005 IEEE

[11] V. Madhu Viswanatham and A.A. Chari"An Approach for Detecting Attacks in Mobile Adhoc Networks" Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications

[12] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad hoc Networks", In Proc. ACM/IEEE Int'l. Conf. on Mobile Computing and Networking, pp 275-283, 2000.

[13] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad hoc Networks", In Proc. ACM/IEEE Int'l Conf. on Mobile Computing and Networking, pp. 255-265, 2000.

[14] R.Ranjana and M.Rajaram, "Detecting Intrusion Attacks in Ad-hoc Networks," Asian journal in information technology 6(7) 758-761,2007

[15] Dorothy E. Denning" AN INTRUSION-DETECTION MODEL" IEEE transaction on software engineering, vol. 13, no. 7,pp 222-232, Feb 1987.