INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS IN ENGINEERING,
TECHNOLOGY AND SCIENCES (IJ-CA-ETS)

SECURING FSR AGAINST DATA PACKET DROPPING BY MALICIOUS NODES

[1]Sunil Kumar Senapati, [2]Pabitra Mohan Khilar

[1,2] NIT Rourkela/CSE, Rourkela, India.
[1]*senapati.sunil@gmail.com*, [2]*pmkhilar@nitrkl.ac.in*

ABSTRACT:
Mobile Ad Hoc Network (MANET) is an emerging area of research in the communication network world. As the MANET is infrastructure less, it is having dynamic nature of arbitrary network topology. So it needs set of new networking strategies to be implemented in order to provide efficient end to end communication. These (MANET) networks have immense application in various fields like disaster management, sensor networks, battle field etc.. Many routing protocols have been proposed in MANET among which Fisheye State Routing (FSR) protocol scales well in large network. Security in MANET is a very difficult problem to incorporate without degrading the performance of the protocol. There are various security issues associated with the FSR algorithm among which is the black hole attack which causes data packet dropping by malicious node. Here we have proposed one scheme to minimize the data packet dropping by malicious nodes in the network.

Keywords: *Manet, FSR, Routing, Security, Black hole attack, data packet dropping.*

1. INTRODUCTION

Mobile Ad hoc network is an emerging field in the communication network world which has received a tremendous amount of attentions from various researchers. The MANET is infrastructure less, unlike the traditional network. The nodes are mobile as well as resource constraint. In MANET every node acts as the source or destination as well as a router [3]. The routing must be enabled in every node to forward the incoming packet to the destination. The information shared between two nodes in the MANET needs to be accurate in order to discover a path from the source to the destination. Various routing algorithms have been proposed by different researchers and all the routing strategies are efficient in one way or the other depending upon the size of the network. Designing an efficient routing algorithm has become difficult due to the limited resources in MANET. An efficient routing algorithm is required to be designed for the limited resources in the MANET and at the same time it should be adaptable to changing network condition like topology, traffic, number of nodes etc. Security is one of the aspect of the routing algorithms in MANET. The FSR suffers from various security threats among which the black hole attack is one. No security mechanism has been implemented yet in FSR. Here we have discussed one solution which can minimize black hole attack hence reducing the number of data packets dropped by the malicious nodes.

The remainder of this paper is organized as follows. Section 2 describes the FSR routing protocol in detail in the MANET. Section 3 explains various security issues in FSR and provides some solutions to the security issues. The next section is the future work to be done. Section 4 concludes the paper.

2. RELATED WORK

Fish Eye State Routing (FSR) algorithm is based on the traditional link state routing algorithm. It reduces the overhead associated with updating routes by introducing the notion of multi-level fish eye scope. The frequency of exchanging the routing information with neighbors depends on the distance between the source and the destination. From the link state entries the node calculates the optimal shortest routes to other nodes. FSR is simple, scalable and efficient in mobile ad hoc network **[5]**.

2.1 Representation of Network Topology in FSR

The network is represented as a undirected graph G=(V,E) where V=number of vertices or nodes in the network and E= number of edges or undirected links in the network. Each node has a unique identifier which represents a mobile host with a wireless communication device with transmission range R, and an infinite storage space. **[3]** A link between two nodes i and j is formed when the distance between i and j becomes less than R. The link (i,j) is moved if distance between i and j exceeds the range R. In FSR, for each node i, one list and three tables are maintained.

(i) A neighbor list A_i
(ii) A topology table TT_i
(iii) A next hop table $NEXT_i$
(iv) A distance table D_i

A_i stores all the nodes those are neighbors to the node i. Any destination j in TT_i has two parts TT_i.LS(j) which denotes the link state information reported by node j and TT_i.SEQ(j) indicates the time stamp at which j has generated the link state information. For each destination j, $NEXT_i$(j) denotes the next hop to forward packets destined to j. $D_i(j)$ denotes the distance of the shortest path from i to j. A weight function can be used measure the distance of a link and is denoted by E-> Z_0^+, which returns 1 if there is a direct link between two nodes , else, it returns ∞. **[5]**

2.2 FSR algorithm

```
Step i : Initialize $A_i$, $TT_i$, $NEXT_i$, $D_i$

Step ii : if (pkt.Queue≠empty)
          for each pkt Є pkt.Queue
          $A_i$← $A_i$ U {pkt.source}
          source ← pkt.source
          $TT_i$.LS(j) ← $TT_i$.LS(j) U {source}
          for each j Є V
          do
            if ( j≠i) ^ (pkt.SEQ(j)) > $TT_i$.SEQ(j))
          then $TT_i$.SEQ(j) ← pkt.SEQ(j);
                 $TT_i$.LS(j) ← pkt.LS(j);
Step iii : for each j Є $A_i$ do
           if weight(i,j) = ∞
           $A_i$ = $A_i$ – {j};
Step iv : for each x Є $A_i$ do
         $TT_i$.LS(i) ← $TT_i$.LS(i) U {x};
          message.senderid ← i;
          for each x Є N do
          for ScopeLevel l:= 1 to L do
          if ((Clock() mod $UpdateInterval_l$ = 0)
             ^ ($D_i$(x) Є $FisheyeScope_l$))       // $D_i$(x) is calculated using

//Disjkstra's Shortest path algorithm
          then message.TT ← message.TT U {$TT_i$.LS(x)};
step v : broadcast(j,message) to all j Є $A_i$;
```

2.3 FSR Protocol Description

FSR is based on the link state routing protocol but it differs in the way it disseminates routing update information or the link state information. In LS each node sends the link state packet by flooding whenever a topology change is detected by a node. But in FSR the nodes maintain a link state table and periodically exchange this table with the neighbors only. The selection of the frequency at which the LS table will be sent to the neighboring nodes depend on the distance between the two nodes. This is based on the fisheye technique. The eye of a fish captures with high details the pixels near the focal point of the fish eye. The detail decreases as the distance of the object increases from the focal point.

In FSR a full topology map is maintained at each node and shortest path is calculated using Dijkstra's algorithm. The scope of the fisheye is defined as a set of nodes that can be reached within a given number of hops. The number of levels and the size of the scope depends on the size of the network. GSR can be viewed as a special case of FSR with only one level and radius of the scope be ∞. FSR retains a routing entry for each destination, hence, it maintains low single packet transmission latency.

2.4 Complexity of FSR

Memory complexity at each node is $O(N^2)$ as all the nodes are represented in terms of connection matrix. Computation complexity is same as of the Dijkstra's algorithm which is $O(N^{2)}$. Control overhead (CO) can be defined as the number of control packets forwarded per unit time and for FSR the CO is O(1). Convergence time is the time required to detect a change and the CT for FSR is same as that of LS which is O(D.I) where D is the maximum hop distance i.e. the network diameter and I is the routing update interval.

3. SECURITY ISSUES IN FSR

The attacks on MANET protocols can be divided into 2 categories.

(i) active attacks
(ii) passive attacks

Active attacks are attacks which are lunched intended to disrupt the service of a network. Such attacks produce threats to confidentiality, integrity and availability of data. *Passive attacks* are done by some of the malicious nodes selfishly to conserve power by not forwarding the packets to the destination. These nodes are very difficult to detect. No security mechanism has been proposed for FSR protocol previously.

3.1 Black hole attack in FSR

Some of the malicious nodes in FSR don't forward the packets towards the destination. So the packets move up to that node and are dropped. This acts as a type of black hole, so these kind of attacks are known as black hole attacks. The types of packets dropped can be both control packet and data packet. The control packets are very few compared to the data packets. FSR need not bother about the control packet dropping as it pre computes the routes to destination by flooding, so if one node does not take part in the route discovery process, other nodes can be taken for route discovery. But, when forwarding data packets if some of the packets are dropped, then alternate route is searched to forward the packets even if that route is the shortest one. This increases the time complexity of the protocol.

3.2 Solution to minimize black holes

This problem can be minimized by selecting the appropriate route where the number of malicious nodes will be minimum. This can be done in a two step process.

(i) By detecting the malicious nodes

(ii) By avoiding the malicious node while computing optimal path

To detect the malicious node we have proposed one method which uses a time stamp along with the data packets. If a node forwards a packet to the next hop then the next to next hop can acknowledge the source by replying the time stamp to the source which is at a distance of two hops.

A weight list is maintained in each node in addition to the previous list and the three tables. The weight list stores the weight assigned to each link in the network. The weight is assigned on the basis of the number of times a node has behaved maliciously. A threshold is maintained depending on the requirement of level of security of the network. If any link cost exceeds the threshold value then that link is moved from the table in the next route discovery process. While calculating the shortest distance to each destination using the traditional Dijkstra's algorithm used in FSR it has been modified slightly. Instead of taking the number of intermediate hop counts for calculation, the actual link cost is taken into consideration. The route calculated using this algorithm may not be the shortest one, but it provides the optimal route all the time which contains least number of malicious nodes. So the amount of data packet dropping can be minimized.

4. CONCLUSION

In this paper we have discussed a specific type of proposed routing algorithm i.e. Fisheye State Routing algorithm. We have classified different types of attacks that can be lunched on FSR. Then we have defined the problem as one type of attack known as the black hole attack which causes dropping of packets by the malicious nodes. Then we have proposed one strategy to minimize the number of black holes or malicious nodes in the optimal path in the phase of route discovery process, hence the number of data packets dropped can be minimized.

In the future work we will formulate the proposed idea in algorithm. We will simulate the modified FSR algorithm using NS2 and compare the results with the existing FSR algorithm. We will analyze the proposed algorithm and the simulation results and provide roadmap for future research in this area.

.

5. REFERENCES

1. *Chapter 5 Internetworking hand book, users.teilam.gr/~skontos/tei_site/html/pdf_cisco/Routing/routing_basic.pdf*
2. *http://www.inetdaemon.com/tutorials/internet/ip/routing/dv_vs_ls.shtml*
3. *Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, A review of routing protocols for mobile ad hoc network, Ad Hoc Networks 2 (2004) 1-22, ELSEVIER*
4. *Xukai Zou, Byrav Ramamurthy and Spyros Magliveras, Routing Techniques in Wireless Ad Hoc Networks – Classification and Comparion, 20 Dec 2005* **...** *[Zou2002]*
5. *Guangyu Pei, Mario Gerla, Tsu Wei Chen , Fisheye state Routing in Mobile Ad Hoc Networks , citeseer.ist.psu.edu/299444.html*
6. *On Securing MANET Routing Protocols Against Control Packet Dropping by Djamel Djenouri, 1-4244-1325-7, July 2007, IEEE.*
7. *Jieying Zhou, Wenjun Ye, Xiaona Li, Jiajia Zhang Cluster-based Gateway aided Multicast Routing Protocol in MANET 1-4244-1312-5/07/, 2007 IEEE.*
8. *Thomas Heide Clausen, Classification of MANET unicast routing rotocols,http://www.soi.wide.ad.jp/class/20030000/slides/05/33.html, #05 10/30/2003*
9. *Shree Murthy , J. J. Garcia-Luna Aceves, A Routing Protocol for Packet Radio Networks, ACM International Conference on Mobile Computing and Networking, MOBICOM'95 pp. 86-95 13.-15., November 1995*
10. *L. Zhou and Z.J. Haas, "Securing Ad hoc Networks", IEEE Networks, 13(6): 24-30, Nov/Dec 1999*