Research Article Impact Factor: 0.621 ISSN: 2319-507X
Roshan Helonde, IJPRET, 2014; Volume 2 (9): 337-343 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURING FSR AGAINST BLACKHOLE ATTACK IN MOBILE AD HOC NETWORK (MANET)

ROSHAN P. HELONDE[1], ATHAR HUSSAIN[2], GAURAO DAREKAR[3]

M.E Student, Department of Computer Science and Information Technology, H.V.P.M's College of Engineering & Technology, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: This paper puts lights on the various proposed routing algorithms in MANET and it narrows down to a special type of routing strategy known as Fisheye State Routing (FSR) which scales well in large network and it describes various security issues in FSR and some solutions to overcome those security problems. This work specifically deals with a special type of attack known as black hole attack which causes data packet dropping by malicious nodes or selfish and provides a solution to minimize the number of malicious nodes in the path to destination and hence minimizes number of data packet dropping by these selfish nodes hence, it secures the FSR algorithm against the black hole attack. The proposed scheme deals with minimizing passive attacks, which causes dropping of data packets by the selfish nodes or malicious nodes. The idea is based on modifying the traditional Dijkstra's Algorithm, which computes shortest route to all destinations from a source. So one scheme has been proposed which uses a two hop time stamp method to detect a malicious node and the Dijkstra's shortest path algorithm has been modified to recomputed the optimal paths to destination and hence, to minimize the data packet dropping by malicious nodes in the network.

Keywords: Manet, Fisheye State Routing, Black hole attack, Ad hoc Network.

Corresponding Author: MR. ROSHAN P. HELONDE

Access Online On:

www.ijpret.com

How to Cite This Article:

Roshan Helonde, IJPRET, 2014; Volume 2 (9): 337-343

PAPER-QR CODE

INTRODUCTION

MANET is one of the recent active fields and has received spectacular consideration because of their self-configuration and self-maintenance. Early research assumed a friendly and cooperative environment of wireless network. As a result they focused on problems such as wireless channel access and multihop routing [6]. But security has become a primary concern to provide protected communication between mobile nodes in a hostile environment. Although mobile ad hoc networks have several advantages over wired networks, on the other side they pose a number of non-trivial challenges to the security design as they are more vulnerable than wired networks.

RELATED WORK

FSR routes each data packet according to locally computed routing table. The routing table uses most recent topology information. The fisheye scope [2] message updating scheme will not lose routing accuracy for inner scope nodes. For outer scope nodes, information in routing entries may blur due to longer exchange interval, but the extra work of "finding" the destination is not necessary. Thus low single packet transmission latency can be maintained. At a mobile environment, this inaccuracy for remote nodes will increase. However, when a packet approaches its destination, it finds increasingly accurate routing instructions as it enters sectors with a higher refresh rate.

FISHEYE SCOPE

The fisheye scope [2] is defined as the set of nodes that can be reached within a given number of hops. An example of a fisheye scope (at node A) of hop 2 is shown below.

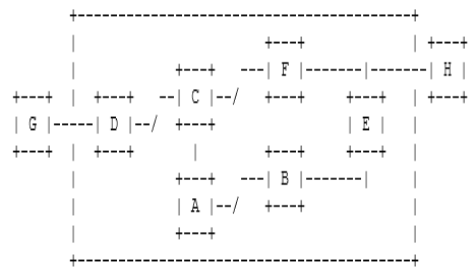

Figure1: Fisheye Scope at Node A of Hop2

Note that in this example node E can be reached through B from A with 2 hops and through F with 3 hops. Since the minimum path length is 2, E is within the fisheye scope of node A. By setting multiple hop radius, multiple level of scopes will cover the entire network.

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 [2]. 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. 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 [5], for each node i, one list and three tables are maintained.

(i) A neighbor list Ai

(ii) A topology table TTi

(iii) A next hop table NEXTi

(iv) A distance table Di

Ai stores all the nodes those are neighbors to the node i. Any destination j in TTi has two parts TTi.LS(j) which denotes the link state information reported by node j and TTi.SEQ(j) indicates the time stamp at which j has generated the link state information. For each destination j, NEXTi(j) denotes the next hop to forward packets destined to j. Di(j) denotes the distance of the shortest path from i to j.

FSR ALGORITHM

```
Step i : Initialize Ai, TTi, NEXTi, Di

Step ii : if (pkt.Queue≠empty)
          for each pkt ∈ pkt.Queue
          Ai← Ai U {pkt.source}
          source ← pkt.source
          TTi.LS(j) ← TTi.LS(j) U {source}
          for each j ∈ V
          do
            if ( j≠i) ^ (pkt.SEQ(j)) >
TTi.SEQ(j))
          then TTi.SEQ(j) ← pkt.SEQ(j);
               TTi.LS(j) ← pkt.LS(j);
Step iii : for each j ∈ Ai do
          if weight(i,j) = ∞
          Ai = Ai – {j};
Step iv : for each x ∈ Ai do
          TTi.LS(i) ← TTi.LS(i) U {x};
           message.senderid ← i;
           for each x ∈ N do
           for ScopeLevel l:= 1 to L do
           if ((Clock() mod UpdateIntervall = 0)
             ^ (Di(x) ∈ FisheyeScopel))      //
Di(x) is calculated using

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

Figure2: Fisheye State Routing Algorithm

FISHEYE TECHNIQUE

Fisheye State Routing (FSR) uses the "fisheye" technique proposed by Kleinrock and Stevens, where the technique was used to reduce the size of information required to represent graphical data. The eye of a fish captures with high detail the pixels near the focal point. The detail decreases as the distance from the focal point increases. In routing, the fisheye [2] approach translates to maintaining accurate distance and path quality information about the immediate neighborhood of a node, with progressively less detail as the distance increases.

ATTACKS ON FSR

(i) Active attacks

(ii) Passive attacks

Active attacks [1] are attacks, which are lunched, intended to disrupt the service of a network. Such attacks produce threats to confidentiality, integrity and availability of data and services in Mobile Ad hoc Network [10].

Passive attacks are done by some of the malicious nodes selfishly to conserve power by not forwarding the packets to the destination or loss those packets called as packet loss.

BLACK HOLE ATTACK

The black hole attack comes under the category of passive attacks which is launched by a selfish or malicious node. A node, which is a black hole [3], has two properties it participates in the route discovery [9] process and the second property is that, it sometimes does not forward the data packet towards to destination. When the data packets are forwarded to the destination these selfish nodes [5] simply do not forward the data packets towards the destination. So all the packets move up to that node and disappear. Hence, these nodes act as a black hole, which causes data packet dropping.

SOLUTION TO MINIMIZE BLACK HOLES

This problem can be minimized by selecting the appropriate route where the number of malicious nodes [3] 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. We use only one performance metric in this study i.e. packet delivery ratio [8]. The packet delivery ratio (PDR) is defined as the ratio of the total number of data packets received by the destinations over the total number of data packets transmitted by the sources. The green line graph shows the data packet delivery ratio if the route to destination is calculated using the traditional FSR algorithm in the presence of malicious nodes.

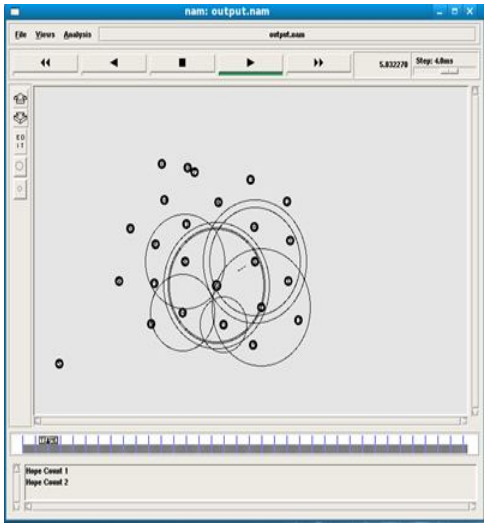

Figure 3: Communication between nodes in Network

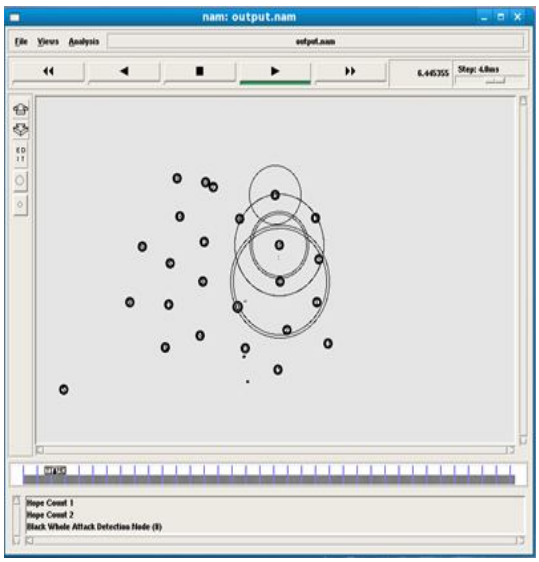

Figure 4: Data Packet Dropping while communication between nodes in Network

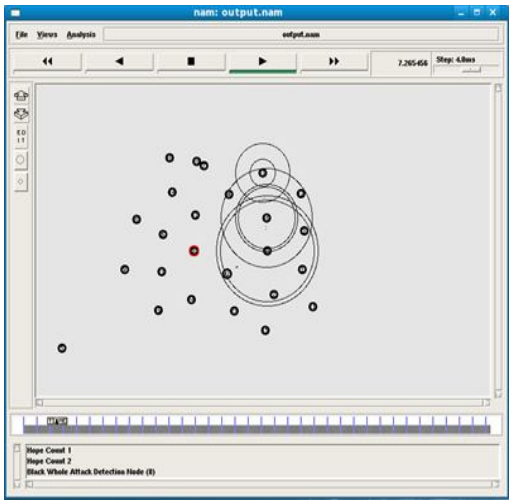

Figure 5: Black hole Attack Detection at Node 8 due to Data Packet Dropping

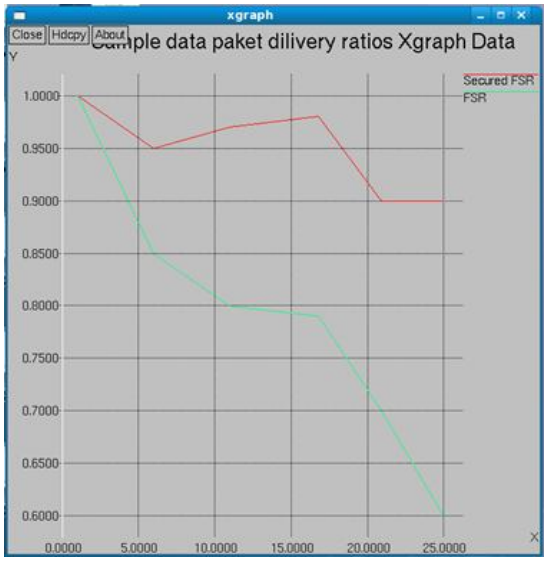

Figure 6: Graphical Result of Performance Metric like PDR in between Secured FSR and Traditional FSR

The red line shows the modified version of the FSR algorithm known as secured FSR [8].

CONCLUSION

In our paper, one scheme is proposed to minimize the number of black holes or malicious nodes or selfish nodes in the path to destination, hence, the number of data packet dropping can be minimized. The simulation of the proposed scheme is conducted using Network Simulator 2 and the packet delivery ratio graph as a function of number of nodes shows that

the proposed scheme has a better packet delivery ratio than the traditional FSR protocol. The proposed scheme gives better packet delivery ratio than the traditional FSR protocol in the presence of malicious nodes.

REFERENCES

1. Zaiba Ishrat, "Security issues, challenges & Solution in MANET", (IJCST), Vol- 2, Iss ue- 4, Oct - Dec 2011.

2. Guangyu Pei, Gerla, M, Tsu-WeiChen, "Fisheye state routing: a routing scheme for ad hoc wireless networks" IEEE Vol 1, Issue, Pages: 70-74 vol.1, 2000.

3. Ekta Kamboj and Harish Rohil, "Detection of Black Hole Attack on AODV in MANET Using Fuzzy Logic", (IJCST), Vol. 1, Issue 6 [2011], pp 316-318.

4. L. Zhou and Z.J. Haas, "Securing Ad hoc Networks", IEEE Networks, pp. 24-30, Nov/Dec 1999.

5. Pei, Gerla, Hong, and Chen [Page 3], Internet-Draft, Fisheye State Routing Protocol November 17, 2000.

6. Xukai Zou, Byrav Ramamurthy and Spyros Magliveras, "Routing Techniques in Wireless Ad Hoc Networks – Classification and Comparion", 20 Dec 2005.

7. Djamel Djenouri, On Securing MANET Routing Protocols Against Control Packet Dropping, July 2007, IEEE.

8. Guangyu Pei, Mario Gerla, Tsu Wei Chen, Fisheye state Routing in Mobile Ad Hoc Networks.

9. Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, "A review of routing protocols for mobile ad hoc network", Ad Hoc Networks 2, 1-22, ELSEVIER 2004.

10. Thomas Heide Clausen, Classification of MANET unicast routing protocols, 2003.