Securing Fisheye State Routing Algorithm Against Data Packet Dropping By Malicious Nodes in MANET

A THESIS REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF

Master of Technology
in
Computer Science and Engineering
Specialization: Information Security

By

Sunil Kumar Senapati

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769008 (Orissa), India
2009

Securing Fisheye State Routing Algorithm Against Data Packet Dropping By Malicious Nodes in MANET

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF

Master of Technology

in

Computer Science and Engineering

Specialization: Information Security

By

Sunil Kumar Senapati

Under the Guidance of

Prof. Pabitra Mohan Khilar

Department of Computer Science and Engineering
National Institute of Technology, Rourkela
Orissa-769008, India
2009

To My Parents

National Institute of Technology Rourkela
Rourkela-769008 (Orissa)

Certificate

This is to certify that the work in this Thesis Report entitled "***Securing Fisheye State Routing Algorithm Against Data Packet Dropping by Malicious Nodes in MANET***" by **Mr. Sunil Kumar Senapati** has been carried out under my supervision in partial fulfillment of the requirements for the degree of *Master of Technology* in Computer Science and Engineering, Specialization: Information Security during session 2008-2009 in the Department of Computer Science and Engineering, National Institute of Technology Rourkela, and this work has not been submitted elsewhere for a degree.

Date: 26th May 2009
Place: Rourkela

Prof. Pabitra Mohan Khilar
Dept of Computer Science and Engineering
National Institute of Technology
Rourkela – 769008

Acknowledgements

No thesis is created entirely by an individual, many people have helped to create this thesis and each of their contribution has been valuable. I express my sincere gratitude to my thesis supervisor, *Prof. P. M. Khilar*, *CSE,* for his kind and able guidance for the completion of the thesis work. His consistent support and intellectual guidance made me to energize and innovate new ideas.

I am grateful to *Prof. B. M. Majhi, Professor and Head*, *CSE* for his excellent support during my work. I am thankful to all my classmates for their love and support.

Last, but not least I would like to thank all professors and lecturers, and members of the department of Computer Science and Engineering, N.I.T. Rourkela for their generous help in various ways for the completion of this thesis.

Sunil Kumar Senapati

Dissemination

[1] Sunil Kumar Senapati, Pabitra Mohan Khilar, "Securing FSR Against Data Packet Dropping by Malicious Nodes in MANET", International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), pp.440-442, April, 2009.

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. A performance comparison of different routing protocols has been given here and this research narrows down to security related issues associated with FSR. The attacks on the MANET can be broadly divided into 2 types as active attacks and passive attacks. 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. The actual FSR algorithm considers the link cost between two nodes as 1 if one node comes in the radio range of another. In our proposed scheme the weight has been assigned depending upon the number of times the next node has behaved maliciously or selfishly. Here we have proposed one scheme which uses a two hop time stamp method to detect a malicious node and the Dijkstra's shortest path algorithm has been modified to re compute the optimal paths to destination and hence, to minimize the data packet dropping by malicious nodes in the network.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Chapter 1 Introduction

1.1 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. [1] 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 conditions like topology, traffic, number of nodes etc. This thesis 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 nodes (used synonymously throughout this thesis work) 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 fisheye state routing algorithm against the black hole attack.

1.2 Basic Concepts in MANET

A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links, to form an arbitrary topology. The movement of the nodes in MANET is random. Thus the topology of the wireless network may change unpredictably and rapidly. There is no central governing authority in MANET, so the nodes act as hosts as well as routers. Routing has to be enabled in each node to provide the routing service. Nodes in the MANET are equipped with wireless transmitters and receivers using antennas. The antennas may be omnidirectional or broadcasting, highly directional or point to point which may be steerable or a combination of these. MANETs have many salient features such as dynamic topology, bandwidth constrained applications, energy constrained operations, limited physical security.

1.2.1 Dynamic Topology

The movement of the nodes in MANET is arbitrary and hence the topology of the network may change rapidly and randomly at unpredictable times which in result may contain both unidirectional as well as bidirectional links.

1.2.2 Bandwidth Constrained applications

Nodes in the MANET are having limited bandwidth constrained and have lower link capacity than the traditional wired networks. The maximum transmission rate of a node is always lowered due to various factors in the network like multiple access, fading, noise and interference etc. Some application like multimedia computing and collaborative networking demand more bandwidth which may sometimes exceeds the network capacity.

1.2.3 Energy Constrained Operations

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the operations should have optimized design criteria for conserving energy.

1.2.4 Limited Physical Security

Mobile ad hoc Network is more vulnerable to security threats than the traditional wired network. The attacks such as eavesdropping, spoofing and denial of service are rapidly growing and must be taken into consideration. Some of the security techniques available for the wired network are also applied to the MANET for reducing the threats and the decentralized nature of the network topology in MANET helps the network to be more robust against single point of failure that is in the case of a wired network. The task of making a network scalable and preventing it against the security threats at the same time is very difficult.

1.3 Organization of the Thesis

This thesis is organized as follows. Chapter 1 is the introduction to the MANET and the routing algorithms. Chapter 2 describes various routing strategies in the MANET. Chapter 3 describes the Fish eye state routing algorithm. Chapter 4 explains proposed model i.e. various security issues in FSR and deals with a specific type of attack known as the black hole attack and provides solutions to the security issue. Chapter 5 is the performance evaluation by simulating the proposed method. Chapter 6 is the future enhancements that can be done and concludes the thesis work.

Chapter 2

Classification of Routing Protocols in MANET

Chapter 2 Classification of Routing Algorithms in MANET

2.1 Introduction

Mobile ad hoc Network (MANET) is an emerging field of research in the communication network world. Before MANET the traditional routing algorithms had been used in wired as well as wireless networks. [12] The traditional distance vector and link state routing algorithms don't scale in MANET. [2] This is because of periodic and frequent updates in large networks may consume considerable amount of the available bandwidth, increase channel contention and each node may require recharging their power supply frequently. [3]

To overcome these problems a number of routing protocols have been proposed in MANET. These protocols can be categorized into different categories based on different criteria. [4]

2.1.1 Based on Communication Model

Protocols can be designed based on the communication model such as multichannel or single channel communications. Multichannel protocols are generally used in TDMA or CDMA based networks. They combine routing functionality and channel assignment. Example of such protocols is Clustered-head Gateway Switched Routing (CGSR). Single channel protocols use only one shared media. These types of protocols are generally CSMA/CA oriented.

2.1.2Based on the Structure

Structure of a network depends on the node uniformity. This means some of the protocols consider each node uniformly and others treat nodes differently. In uniform protocols hierarchy is not present. All nodes respond to the routing control message in the same manner.

In non-uniform protocols the routing activity of a node is based on a subset of nodes in the neighborhood or it is topologically partitioned. Hierarchical protocols come under the second category which differentiates the network into different level and sends message for specific level only. Neighbor selection based protocols are ZRP, FSR, and OLSR. Partitioning protocols are CEDAR and CBRP.

2.1.3 Based on State Information

Based on the state information shared between nodes about the network the protocols can be divide into two categories.

(i) Topology based protocols follow the principle that every node in the network maintains large scale topology information as in the case of link state routing algorithm. Topology based protocols are GSR (proactive) and DSR (reactive).

(ii) Destination-based protocols use the principle that each node maintains the information about its neighbors only as in the case of distance vector routing algorithm. Destination based protocols are DSDV, WRP (proactive), AODV, TORA, ABR and WRP (reactive).

2.1.4 Based on type of Cast

Protocols can be unicast, multicast, geocast or broadcast. In unicast protocols one node sends message to a single destination at a time. These are very simple protocols. Unicast protocols are GSR, WRP, OLSR, FSR, CEDAR, CGSR, and Epidemic. [8] Multicast routing protocols send message to multiple destinations by using a routing tree or a mess. Geo-cast protocols deliver data packets for a group of nodes which are geographically separated. In these protocols the routers have location information of the nodes. Broadcast protocols are the protocols which have implemented the basic broadcast operation.

2.1.5 Based on Scheduling

Based on scheduling the routing protocols can be divided into three categories. [3]

(i) Proactive

(ii) Reactive

(iii) Hybrid

In proactive routing protocols the route discovery process is done in start up and maintained using periodic route update process.

In reactive routing protocols the routes are determined as and when required. Hybrid routing protocols combine the basic properties of proactive and reactive routing protocols.

2.2 Proactive Routing Protocols

In proactive routing protocols each node keeps the routing information in a number of tables. These information are exchanged with other nodes periodically and/or when there is a change occurs in the network topology. A number of proactive routing protocols have been proposed. Some of these protocols are DSDV, WRP, GSR, HSR, FSR, OLSR, CGSR, STAR, MMWN etc among which FSR and OLSR scale very well in large and highly mobile network. All these protocols differ in the way they update routing information, the number of tables and the type of information in the tables.

2.2.1 Destination Sequenced Distance Vector (DSDV)

DSDV ensures loop free routes. It provides a single path to the destination which is determined using distance vector shortest path algorithm. This uses two types of packets i.e. full dump and incremental packet. The full dump packet carries all the routing information and the incremental packet which is more frequently exchanged carries the information since the last change or the last full dump. The overhead of this algorithm grow in order of O (N^2) where N is the number of nodes in the network. This is due to the periodic update messages.

2.2.2 Wireless Routing Protocol (WRP)

WRP also guarantees loop free routing by maintaining descendant information. [17] WRP maintains four routing tables which consumes a considerable amount of memory at each node. The connectivity of nodes is ensured by exchanging hello messages by the neighboring nodes which takes considerable amount of bandwidth and also the nodes can’t go to sleep mode to conserve power as they need to be active all the time to respond to the hello message, otherwise the node will be considered as dead. [9]

2.2.3 Global State Routing (GSR)

GSR is based on the traditional link state routing algorithm but it differs in the way it restricts the update messages within neighbors only. [18]

This reduces the number of messages hence, reducing the bandwidth consumption but, the packet size grows as the network grows. So it does not scale well in large networks.

2.2.4 Fisheye State Routing (FSR)

The FSR is a descendant of GSR. FSR scales well in large network as it reduces the frequency of sending the update message to the remote nodes and it sends the messages to the nearby nodes which are in the fish eye scope at a higher frequency. [5] The scalability comes at a price of reduced accuracy. That means the routes to remote destination becomes less accurate as mobility increases. This can be overcome by making the frequency of sending messages to the remote destination according to the mobility.

2.2.5 Cluster-head Gateway Switch Routing (CGSR)

In CGSR the nodes in the network are divided into different clusters. One of the nodes within a cluster is selected as the cluster head which controls the transmission medium as well as the inter-cluster communication. Routing overhead is minimized as the nodes only need to maintain route to the cluster heads. The disadvantage of this protocol is that there exists still some overhead associated with maintaining the clusters information. Each cluster head needs to exchange its cluster member table with other cluster heads. [7]

2.2.6 Optimized Link State Routing (OLSR)

OLSR is a point to point routing protocol based on the traditional link state routing algorithm. [19] It employs MultiPointRelay (MPR) to reduce the number of hello messages. It selects a subset of its neighboring nodes which are at one hop distance those cover all the nodes at a distance of two hops. The set is known as MPR set. The other nodes in the neighborhood don’t rebroadcast the packets; they only receive and process the packets. Then the optimal route is determined by each node and kept in a table so that the destination can be easily available during transmission.

The characteristics and performance comparison of the above proactive protocols is given below in the table – 2.1 adapted from [3].

Protocol	Routing Structure	Number of tables	Frequency of updates	Critical Nodes	Memory Overhead	Control Overhead	Characteristic Feature
DSDV	Flat	2	Periodic and as required	No	O(N)	O(N)	Loop free
WRP	Flat	4	Periodic	No	O(N^2)	O(N)	Loop free using predecessor info
GSR	Flat	3+1list	Periodic and local	No	O(N^2)	O(N)	Localized updates
FSR	Flat	3+1list	Periodic and local	No	O(N^2)	O(N)	Controlled Frequency of updates
CGSR	Hierarchical	2	Periodic	Yes, cluster head	O(2N)	O(N)	Cluster heads exchange info
OLSR	Flat	3	Periodic	No	O(N^2)	O(N^2)	Reduces CO by using MPR

Table – 2.1 Characteristic and performance comparison of proactive routing protocols.

2.3 Reactive Routing Protocols

On demand or reactive routing protocols were designed to reduce the amount of overhead in proactive routing protocols. The routes to destination at each node are discovered and maintained as and when required by broadcasting hello messages. When destination is reached then a route reply is sent to the source using link reversal or piggybacking. The time complexity of route discovery process is O (N+M) where N=number of nodes in the network and M=number of nodes in the reply path for bidirectional links and O (2N) for unidirectional links. [3]

The reactive routing protocols are further divided into two categories.

(i) Source Routing

(ii) Hop by hop Routing

In source routing protocols the data packets carry the entire source to destination address. So, the intermediate nodes do not need to calculate the route. Hence, they don't need to maintain neighbor connectivity check and can go to sleep mode to conserve power. But the disadvantage of this is that the probability of route failure is high if the links in the intermediate nodes fail.

In hop by hop routing the data packet carries only the destination address and the next hop address. So, the nodes need to be active all the time and cannot go to sleep mode to conserve power. A number of reactive routing algorithms have been proposed in the literature among which a few have been discussed in this section.

2.3.1 Ad hoc On-demand Distance Vector (AODV)

It is based on DSDV and DSR protocols. It uses sequence numbering and periodic beaconing procedure of DSDV and similar route discovery process as in DSR. AODV differs from DSR in the way the packet carries information. In DSR the data packet carries all the routing information where in AODV the packets only carry the destination address. In the reply message it carries only the address of the intended recipient and a sequence number. So, AODV can be applied to highly dynamic network. [24] The disadvantage of AODV is that it may consume high bandwidth as any link failure may initiate another route discovery.

2.3.2 Dynamic Source Routing (DSR)

In DSR the data packet carries all the address from the source to the destination. [20] So it cannot perform very well in large networks. In small or moderate sized networks it may perform well. The advantage of this protocol is that it can store multiple routes in the route cache of the nodes. So, no need to discover new routes in case of link failure if another valid route is present in the nodes route cache. The nodes can go to sleep mode to conserve power as it does not require any periodic beaconing.

2.3.3 Light Weight Mobile Routing (LMR)

LMR uses a flooding technique to discover its routes. The nodes maintain multiple routes to destination in each node, hence it is very reliable. It maintains the routing information only to its neighbors hence avoids unnecessary delays and storage. It may introduce temporary invalid routes.

2.3.4 Temporally Ordered Routing Algorithm (TORA)

TORA is same as LMR in link reversal and route repair procedure. The advantage of TORA is that it restricts the control message to a set of neighbors only where a topology change has occurred. [21] It supports multicasting. The disadvantage of TORA is that it may also produce invalid routes.

The characteristic feature and the performance comparison of the above discussed algorithms are given in the table – 2.2 below as adapted from [3].

Protocol	Routing Structure	Multiple Routes	Beacons	Route maintained in	Communication Complexity of Route Discovery	Advantage	Disadvantage
AODV	F	No	Yes, hello message	Routing Table	O(2N)	Adaptable to highly dynamic topology	Scalability problems, large delays, hello message
DSR	F	Yes	No	Route Cache	O(2N)	Multiple routes	Scalability problems due to source routing and flooding, large delays
LMR	F	Yes	No	Routing Table	O(2N)	Multiple Routes	Temporary routing loops
TORA	F	Yes	No	Routing Table	O(2N)	Multiple Routes and send updates to neighbors only when a change occurs in topology	Temporary routing loops

Table – 2.2 Characteristic and performance comparison of reactive routing protocols.

2.4 Hybrid Routing Protocols

Hybrid routing protocols incorporate the basic properties of both proactive and reactive routing protocols. It divides the entire network into zones or some protocols form a tree structure or clusters.

2.4.1 Zone Routing Protocol (ZRP)

The ZRP divides the network into different zones. It implements proactive strategy of route discovery for the nodes inside the zone and it discovers routes to destination for the nodes outside the zone on demand. Hence reduces the overhead. [22] The disadvantage of this protocol is that for a network having large zones it may act like a pure proactive protocol and for a network having low zone values it may act like a pure reactive protocol.

2.4.2 Zone-based Hierarchical Link State (ZHLS)

The ZHLS employs hierarchical structure. The network is divided into non overlapping zones; each node in the network has a zone id and a node id. In the route discovery process the packet needs to carry only two addresses, the node id and the zone id of the destination node. The node needs to broadcast the hello messages containing zone id only, hence reduces considerable amount of overhead. There is no cluster-head or location manager to control the transmission within a zone, it is done statically by a GPS, and hence the overhead is further reduced. The disadvantage of this protocol is that all nodes must have a static zone map in the startup time in order to function well. This may not be feasible where the geographical boundary of the network is dynamic. However, it is highly adaptable to dynamic topology and it may scale well in large network. The characteristic features and performance of the above discussed two protocols [3] have been given in the Table – 2.3.

Protocol	Routing Structure	Multiple Routes	Beacons	Time Complexity	Advantage	Disadvantage
ZRP	F	No	Yes	Intra: O(I) Inter: O(2D)	Reduce transmission	Overlapping Zones
ZHLS	H	Yes, if more than one virtual link exists	No	Intra: O(I) Inter: O(D)	Reduction of single point of failure, low CO	Static zone map required

Table – 2.3 Characteristic and performance comparison of hybrid routing protocols.

2.5 Summary

In MANET various routing algorithms have been proposed and all the algorithms are good in one or the other way depending upon the requirements. The classification of these routing algorithms can be done depending upon different criteria. Based on the scheduling criteria the routing algorithms can be divided into three types. These are proactive or table driven, reactive or event driven and hybrid or both table driven and on demand. In proactive routing protocols the route discovery process is done in start up and maintained using periodic route update process. In reactive routing protocols the routes are determined as and when required. Hybrid routing protocols combine the basic properties of proactive and reactive protocols. Some of the proactive routing protocols are DSDV, WRP, GSR, HSR, FSR, OLSR, CGSR, STAR, MMWN etc among which FSR and OLSR scale very well in large and highly mobile network. The examples of some of the reactive routing algorithms are AODV, DSR, LMR and TORA. The example of the hybrid routing algorithms are ZRP and ZHLS. All the routing algorithms differ from each other in specific ways and can be used to route the data packets to the destination depending upon the requirement of the network.

Chapter 3

Fisheye State Routing Algorithm

Chapter 3 Fisheye State Routing Algorithm

3.1 Introduction

Fisheye State Routing Algorithm (FSR) is a proactive or table driven routing algorithm which has been developed by Wireless Adaptive Mobility Laboratory, University of California, Los Angeles.[13] FSR is based on the traditional link state routing algorithm. Each and every node collects the information about the topology of the network from the neighboring nodes and calculates the routing table. It then disseminates the information locally to the neighboring nodes. The FSR differs from the traditional link state routing algorithm in the way it disseminates the information across the neighboring nodes. It reduces the overhead associated with updating routes by introducing the notion of multi-level fish eye scope. The scope of the fisheye has been given in figure - 3.1. 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]

3.2 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. [5] 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. The topology table contains the most up to date information about the topology of the network from the link state message. The information in the topology table are required while calculating the routing table. The topology table has three fields; destination address, destination sequence number, link state list. Any destination j in TT_i link state list 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]

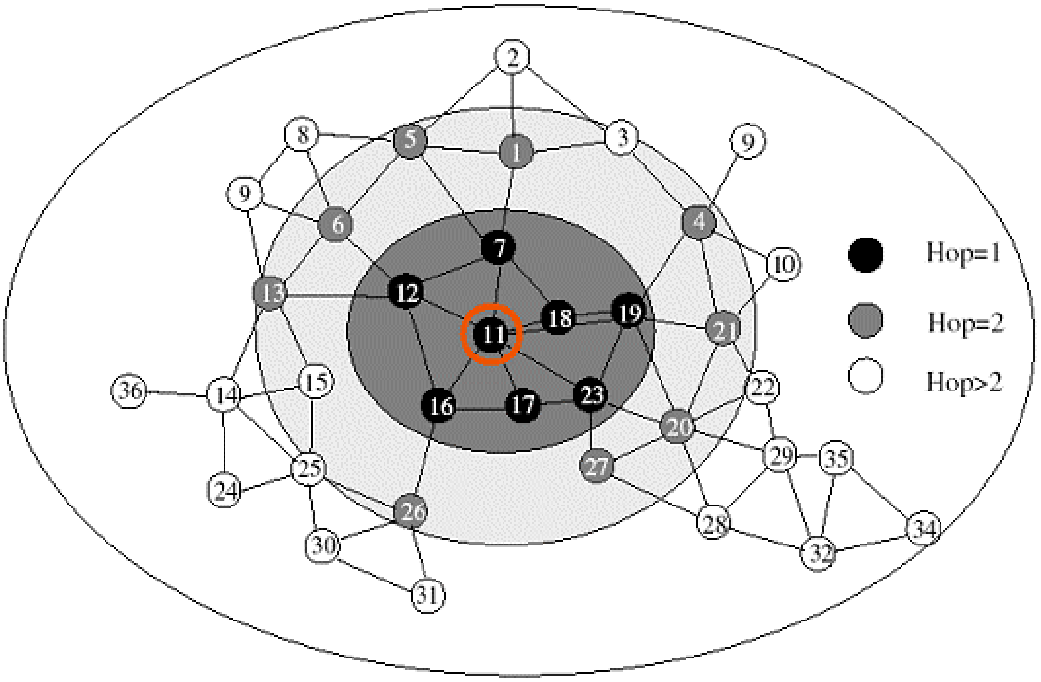

Figure 3.1 – Scope of a Fisheye

3.3 FSR algorithm

The FSR algorithm has been given below in Figure – 3.2 adapted from [5].

```
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 $A_i$;
```

Figure – 3.2 Fisheye State Routing Algorithm

3.4 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 and the scope has been shown in Figure - 3.1. [5] 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.

3.5 Link State Message Processing

When a node receives a link state message, it first checks its neighbor list A_i for the sender's address. If the sender is a new one then it makes an entry in the neighbor's list. Otherwise, it will update the sequence number or the time stamp and the link state information about the sender in the list. Then the node processes the link state information contained the arrived message. While making its own link state packet for sending to the neighbors it copies the most update information from the link state messages to the topology table. In the incoming link state message if the sequence number is larger than the sequence number stored locally in the topology table about the node then only the message is taken into consideration for updating the old one stored in the table. Otherwise, if the sequence number shows an older number then that update message is discarded. Finally, if there are changes in the topology table, the routing table is updated.

3.6 Routing Table Calculation

The routing table of FSR provides the next hop information to forward the packets for the other destinations in the network. Whenever there are changes detected in the topology table of the node the routing table is updated. Based on the latest topology table the Dijkstra's algorithm is performed to find the shortest path from the current node to all the destinations those are in the topology table. The old routing table is replaced with the newly calculated routing table. The routing table has the following fields:

- Destination Address
- Next hop address
- Distance

In the FSR algorithm the weight or the link cost between two nodes has been taken as 1 and the weight function can be changed depending upon the requirement of functionality.

3.7 Data Packet Forwarding

FSR follows hop by hop data forwarding. The source node or any intermediate nodes retrieve the destination address from the data packet, and look at their routing tables. If the route is known, i.e., there is an entry for the destination, the data packet is sent to the next hop node. This procedure repeats until the packet finally reaches the destination. FSR does not provide any security feature for preventing a node's misbehavior for not forwarding the data packet to the next node.

3.8 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.

3.9 Advantages of FSR Protocol

The followings are the advantages of FSR Protocol over most of the other MANET routing protocols. [13]

- Simplicity
- Usage of most up to date shortest routes
- Robustness to host mobility
- Exchanges partial routing updates with the neighbors
- Reduced routing update traffic

Chapter 4

Proposed Model: Security of Fisheye State Routing Algorithm

Chapter 4 Proposed Model : Security of Fisheye State Routing Algorithm

4.1 Introduction

Mobile Ad-hoc Network (MANET) is different from the traditional wired networks due to its mobility, infrastructure less topology and the absence of central authority in the network. These behaviors make the MANET vulnerable to different security threats. The threats on a MANET can be from the unauthorized nodes those are outside the network or from the nodes inside the network. Threats from the nodes outside of the network are likely to be more easily detected than the internal nodes of the network. The threats from the internal nodes are difficult to detect as they are from trusted sources. Threats on the MANET can be broadly divided into 2 categories. [14]

- External Threats
- Internal Threats

4.1.1 External Threats

In the presence of an authentication protocol to protect the upper layers, external threats are dictected at the physical and data link layers. The external threats again can be divided into two categories.

- Passive Threats or threats to confidentiality or Eavesdropping
- Active Threats or threats to the integrity and availability

Passive threats allow unauthorized nodes to listen to and receive messages including routing updates. An unauthorized node can be able to gather data that can be used to infer the network topology and other information such as the identities of the more heavily used nodes which forward or receive data. Hence, techniques may be needed to hide such information. Eavesdropping is also a threat to location privacy. Passive eavesdropping also allows unauthorized nodes to discover that a network actually exists within a geographical location, by just detecting that there is a signal present. Traffic engineering techniques have been developed to combat this.

Active attacks majorly include the denial of service attack which causes the disruption of service of one or more node or the entire network like distortion of the communication. The duration of such attacks and the routing protocol in use defines the effectiveness of such types of attacks. While routing data packets the denial of service attack is viewed as a link break by a reactive protocol so, the participating nodes can be able to find an alternative route. But in the case of a proactive routing algorithm the broken link is timed out and deleted from the list.

4.1.2 Internal Threats

The threats posed by internal nodes are very serious; as internal nodes are have the necessary information to participate in distributed operations. Internal threats also can be divided into two types; active threats and passive threats. Internal nodes can misbehave in a variety of different ways. These can be categorized into three categories - failed nodes, badly failed nodes, selfish nodes or malicious nodes (here in this thesis work the terms selfish and malicious have been used synonymously where in actual context they may differ in some way).

Failed nodes are simply those unable to perform a required operation; this could be for many reasons, including power failure and environmental events. The main problems for an ad hoc routing protocol are failure of updating data structures, or the failure to send or forward data packets, including routing messages. The importance of the preventing such failure is that data packets may contain important information pertaining to security, such as authentication data and routing information. A failure to forward route error messages will mean that originator nodes will not learn of broken links and continue to try to use them, creating bottlenecks. The threat of having failed nodes is most serious if failed nodes are needed as part of an emergency route, or form part of a secure route.

Badly failed nodes are as serious as the failed nodes which exhibit features such as not sending or forwarding data packets or route messages. In addition they can also send false routing messages, which are still correctly formatted, but which may contain false information and are a threat to the integrity of the network.

Selfish nodes exploit the routing protocol to their own advantage, e.g. to enhance performance or save resources. Selfish nodes do not cooperate as the protocol requires whenever there is a personal cost involved, and will exhibit the same behaviors as failed nodes, depending on what operations they decide not to perform. The main attack by selfish nodes is the packet dropping where most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception [14]. Another type of misbehavior by the selfish nodes is partial dropping, which could be difficult to prevent and detect. These selfish nodes comes under the category of passive attacks but sometimes these may also constitute to some of the active attacks like denial of service, integrity of the network. For example, if there is a single route to the destination at a certain time and in that route a selfish node is present, hence, this may cause the network to be divided into two halves. Selfish nodes are very difficult to detect. Most of the selfish nodes behave maliciously due to conserve their battery power which is one of the limited resources in MANET.

4.2 Types of Attacks on FSR

The attacks on FSR protocol 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 and services in MANET. Here the term active attack has been used to mean that if any of the node’s intention in the network to disrupt any of the security goals intended, such types of attack can be termed as active attack. In contrast the passive attack is an attack which is performed by the nodes to benefice itself only. The node has no other intention to disrupt the service of the network.

Passive attacks are done by some of the malicious nodes selfishly to conserve power by not forwarding the packets to the destination. One type of such attacks is known as the black hole attack or the wormhole attack which causes data packet dropping. [6] These nodes are very difficult to detect. No security mechanism has been proposed for FSR protocol previously. [25]

4.3 Black hole attack

The black hole attack comes under the category of passive attacks which is launched by a selfish or malicious node to benefice itself in terms of conserving its energy or battery power. A node which is a black hole has two properties – it participates in the route discovery process and the second property is that, it sometimes does not forward the data packet towards to destination. These nodes create problems in data transmission if they come in the route to destination. The nodes in the MANET are resource constrained; resource may be bandwidth, energy etc. Most of the nodes in MANET rely on batteries as their source of power; so, some of the nodes behave maliciously to conserve their limited battery power. So, when the data packets are forwarded to the destination these selfish nodes 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.

Black hole attack can be launched both on control packets and data packets, but here we have considered the case of data packets, because in fisheye state routing algorithm the number of control packets are very less compared to the number of data packets. 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.

4.4 Proposed Solution to minimize black hole attacks in FSR

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.

In the traditional FSR algorithm each node has one list and three tables. In the modified version that is proposed here 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 as in the case of the FSR algorithm, the actual link cost is taken into consideration. The weight function has been modified to consider the assigned link cost based on the number of malicious behavior instead of number of hop counts. 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.

4.5 Work out Example

In both of the figures given below the network contains 16 nodes. In the Figure - 4.1 the weight of the links or edges between the nodes has been taken as 1 if there is a direct connection between these two. In other words, if a node comes under the radio transmission range of another node then, a direct path is formed between them and link between them is assigned as cost 1. The source is node 'a' and the destination is node 'h'. The cost of sending a packet from 'a' to 'h' is 2.

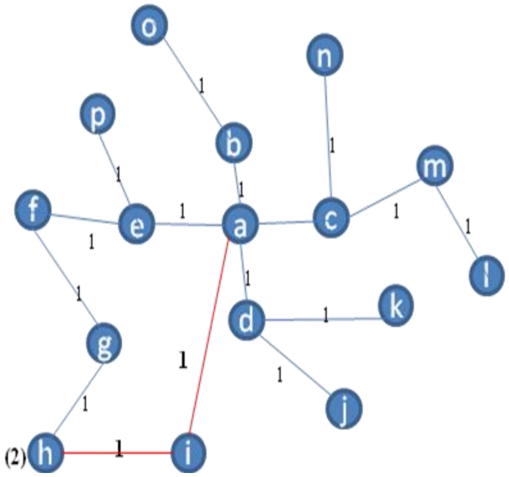

Figure 4.1 – Traditional FSR Scenario

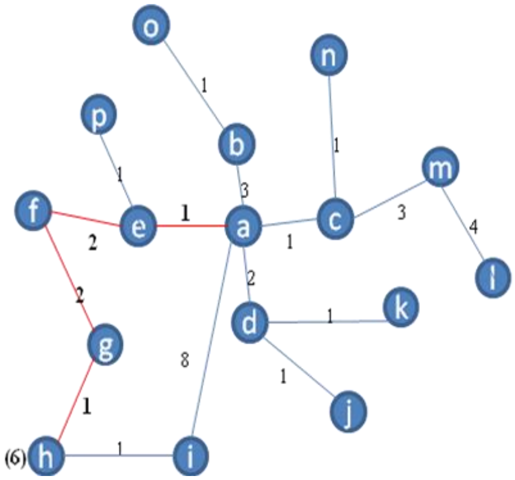

Figure 4.2 – Scenario in the proposed solution

In the case of figure 4.2 the links are assigned different weights based on the number of times the nodes have behaved maliciously. Suppose, initially when node ‘a’ wants to send a data packet to node ‘h’, node ‘a’ checks its own routing table for a valid path from ‘a’ to ‘h’ and node ‘a’ finds the path through ‘i’. So, node ‘a’ sends the data packet to node ‘i’ to forward it to node ‘h’ along with a timestamp for node ‘h’ which is encapsulated in the data packet. If after a certain time interval node ‘h’ does not reply back the time stamp to ‘a’, then, node ‘a’ will come to know that node ‘i’ has not forwarded the data packet to node ‘h’ and it writes 1 to the weight list maintained in the node ‘a’ corresponding to ‘i’. In this process after some time node ‘i’ has behaved maliciously 8 times and the next data packet is to be transmitted or forwarded, so, the optimal route to destination is searched or computed using the Dijkstra’s shortest path algorithm. The edge connecting node ‘a’ and ‘i’ has been assigned weight 8, that means node ‘a’ has sent many data packets out of which node ‘h’ has not received 8 data packets, so, could not reply the time stamp to node ‘a’, hence, ‘i’ has behaved maliciously 8 times. So, after this scenario the computed optimal path from source ‘a’ to destination ‘h’ is a-e-f-g-h whose total path cost is 6. Had it been calculated using the traditional method the path cost would have been 9. In the second scenario the optimal cost has more number of hop counts than the first scenario, but the number of malicious or selfish nodes in the route to destination has been minimized and hence, the number of data packets dropping will be minimum.

4.6 Summary

This chapter presents various security issues and threats present in MANET. Then it classifies different security attacks that can be launched on the fisheye state routing algorithm. Then it discusses in detail about a specific type of attack known as black hole attack which comes under the category of passive attacks. This black hole attack is responsible for the dropping of data packets by malicious nodes in the route to destination. Then a solution has been proposed which uses a two hop timestamp method to detect a node as malicious. Based upon that the links between the nodes have been assigned weights. Then the Dijkstra's shortest path algorithm is performed to compute to optimal route to destination, hence the number of malicious nodes can be minimized and hence, the number of data packet dropping can be minimized.

Chapter 5

Performance Evaluation

Chapter 5 Performance Evaluation

5.1 Introduction

Mobile Ad-hoc Network (MANET) is infrastructure less and there is no central authority to control the routing in the network. So, it is very difficult to design a routing protocol which is scalable as well as secure. There is always a tradeoff between the security and the performance of a routing protocol. A less number of protocols are able to provide security to a routing protocol against various attacks in a MANET without degrading the performance of the routing protocol. Performance itself is a broad term in context of routing algorithm. The set of parameters which are taken into consideration in most of the cases while evaluating the performance of a protocol are throughput, packet delivery ratio, end to end delay etc. Some of the protocols are able to provide secured solution to the routing schemes in MANET without degrading the performance of the protocol in a higher degree. Example of such protocols is secured ad-hoc on demand (SAODV). Fisheye State Routing (FSR) is one of the routing protocols available for MANET which scales well in large network. In FSR no security feature has been implemented previously. Here we have proposed one scheme for minimizing data packet dropping by malicious nodes in FSR. The proposed scheme has been implemented and the performance of the protocol is matched with that of the actual FSR protocol.

5.2 Simulation Environment and parameters

We conducted our experiments using QualNet version 4.5, a scalable simulation environment for wireless network systems developed by Scalable Network Technologies [11]. Our simulated network consists of 25 mobile nodes placed randomly within a 1500 m x 1500 m area. Each node has a transmission range of 150 m and moves at a speed of 10 m/s. The radio transmission range is 150 meters and channel capacity is 2 Mbits/sec. We use IEEE 802.11 MAC protocol with Distributed Coordination Function (DCF) [15] as the MAC layer in our experiments. The random waypoint model [16] was used in the simulation runs. In this model, a node selects a destination randomly within the roaming area and moves towards that destination at a predefined speed uniformly distributed between 0m/s to 10m/s. Once the node arrives at the destination, it pauses at the current position for 30 seconds. The node then selects another destination randomly and moves towards it, pausing there for 30seconds, and so on. Each simulation executed for 300 seconds of simulation time. The traffic used is CBR traffic between random node pairs. The size of data payload is 512 bytes. Multiple runs with different seed numbers were conducted for each scenario and measurements were averaged over those runs.

5.3 Performance Metrics

We use only one metric in our study i.e. packet delivery ratio.

5.3.1 Packet Delivery Ratio: 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. In our experiment the packet delivery ratio is the ratio of total data packets sent by the CBR clients over the total data packets received by the CBR servers.

5.4 Simulation Results

Figure – 5.1 shows the packet delivery ratio in two different scenarios. The dotted 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. The solid line shows the modified version of the FSR algorithm known as secured FSR. In both of the cases the number of malicious nodes is approximately 1/3 of the total number of nodes. The packet delivery ratio is shown as a function of number of nodes. As the number of nodes increases, the packet delivery ratio decreases in the secured FSR graph, but the degradation is graceful as the number of nodes increases so on. But in the case of the traditional FSR as shown in the Figure – 5.1 the packet delivery ratio degrades in a higher degree as the number of nodes increases.

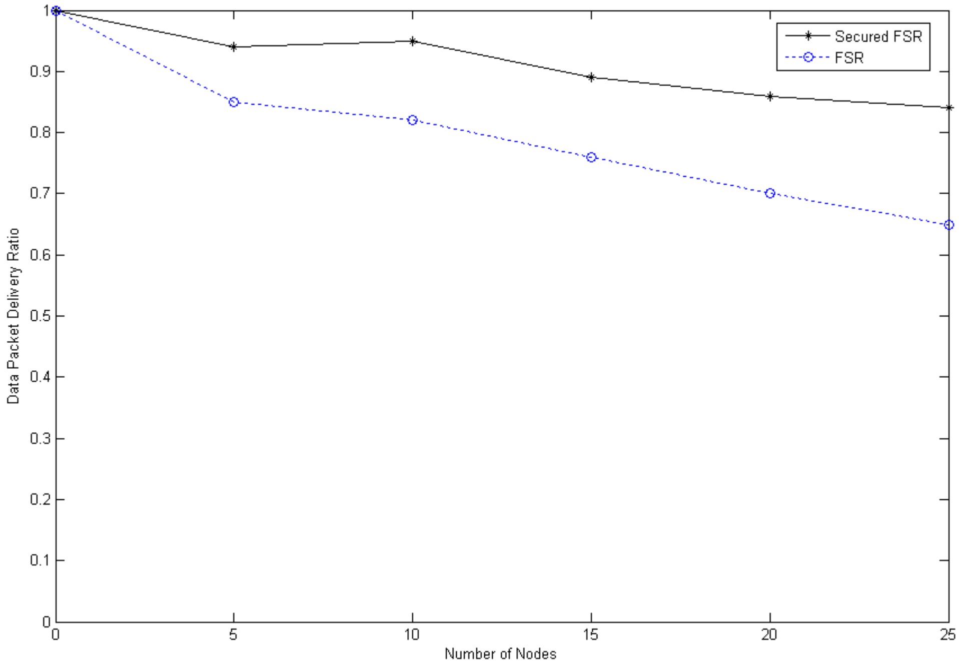

Figure – 5.1 Packet Delivery Ratio

From the graph it is shown that the proposed scheme gives better packet delivery ratio than the traditional FSR protocol in the presence of malicious nodes. Hence, the number of data packets dropping by malicious node has been minimized. The packet delivery ratio never comes below 0.7 in the traditional FSR without the presence of any malicious nodes up to 1000 nodes. [5]

Chapter 6

Conclusion and Future Enhancements

Chapter 6 Conclusion and Future Enhancements

6.1 Summary of the thesis work

Mobile ad hoc network (MANET) is a collection of autonomous systems known as nodes connected in wireless fashion. There is no fixed infrastructure in MANET. Nodes in the MANET can act both as a source or destination or a router. Nodes are resource constraints as well as mobile. Designing an efficient routing algorithm for MANET is a very difficult task. Various routing algorithms have been proposed by different researchers which differ from each other in one or more way. Fisheye State Routing algorithm is one of the few MANET routing algorithms which scales well in highly mobile networks. No security mechanism has been implemented earlier in FSR. Different types of attacks can be launched on FSR out of which the black hole attack is one which comes under the category of passive attacks. The black hole attack causes dropping of data packets by malicious nodes in the path to destination in FSR. 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 QualNet 4.5 simulator 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.

6.2 Future Research Direction

The proposed scheme in this thesis work has been implemented to minimize the number of black holes in the path to destination in the network in FSR algorithm. However, this scheme can be applied to take care of all the proactive routing algorithms in MANET. After simulating the scheme on different proactive algorithms the results can be compared with the actual algorithms for acceptance of this scheme in the corresponding scenarios. The scheme can also be applied to minimize the number of control packets dropping in the proactive routing algorithms available for MANET.

Bibliography

[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, 1-22, ELSEVIER 2004.

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

[5]. Guangyu Pei, Gerla,M, Tsu-WeiChen, "Fisheye state routing: a routing scheme for ad hoc wireless networks" Communications, IEEE International Conference on Volume 1, Issue , Pages: 70-74 vol.1, 2000.

[6]. Djamel Djenouri, Othmane Mahmoudi, Mohamed Bouamama, David Llewellyn-Jones, Madjid Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping", pp.100-108, IEEE International Conference on Pervasive Services, 2007.

[7]. Jieying Zhou, Wenjun Ye, Xiaona Li, Jiajia Zhang "Cluster-based Gateway aided Multicast Routing Protocol in MANET", IEEE 2007.

[8]. Hadi Sargolzaey, Ayyoub Akbari Moghanjoughi and Sabira Khatun, "A Review and Comparison of Reliable Unicast Routing Protocols For Mobile Ad Hoc Networks", JCSNS International Journal of Computer Science and Network Security, VOL.9 No.1, January 2009.

[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, November 1995.

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

[11]. Qualnet Simulator available at : <http://www.qualnet.com>

[12]. Ram ramanathan and Jason redi, “A Brief Overview of Ad hoc Networks: Challenges and Directions”, IEEE Communications Magazine 50th Anniversary Commemorative Issue/May 2002.

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

[14] Po-Wah Yau; Mitchell, C.J., "Reputation methods for routing security for mobile ad hoc networks" Mobile Future and Symposium on Trends in Communications, 2003.

[15] IEEE Computer Society LAN MAN Standards Committee, “Wireless LAN Medium Access Protocol (MAC) and Physical Layer (PHY) Specification”, IEEE Std 802.11, 1997.

[16] Mohammed, A.K., "A modified random way-point model equalized for the node crowding effect," Proceedings of 14th International Conference on Computer Communications and Networks, ICCCN, pp. 49-54, Oct. 2005.

[17] Shree Murthy and J.J.Garcia-Luna-Aceves, “An efficient routing protocol for wireless networks”, Mobile Networks and Applications Volume 1, Issue 2, Pages: 183 – 197, 1996.

[18] Tsu-Wei Chen; Gerla, M., "Global state routing: a new routing scheme for ad-hoc wireless networks," IEEE Communication, Jun 1998.

[19] T.Clausen, A.Qayuum, P.Jacquet, A.Laouitti, L. Viennot, "Optimized Link State Routing Protocol", Proceedings of the IEEE INMIC, 2001.

[20] Cheng Yong; Huang Chuanhe; Shi Wenming, "Trusted Dynamic Source Routing Protocol", International Conference on Wireless Communications, Networking and Mobile Computing, WiCom, pp.1632-1636, 21-25 Sept. 2007

[21] Amer, S. H. and Hamilton, J. A. “Performance evaluation: running DSR and TORA routing protocols concurrently”, in Proceedings of the 2007 Summer Computer Simulation Conference, San Diego, California, July 16 - 19, 2007.

[22] Zygmunt J. Haas, and Marc R. Pearlman, “The Performance of Query Control Schemes for the Zone Routing Protocol”, IEEE/ACM Transactions On Networking, vol. 9, no. 4, August 2001.

[23] Takashi Hamma, Takashi Katoh, Bhed Bahadur Bista, Toyoo Takata, “An Efficient ZHLS Routing Protocol for Mobile Ad Hoc Networks”, Proceedings of the 17th International Conference on Database and Expert Systems Applications (DEXA'06), IEEE, 2006.

[24] Charles E. Perkins and Elizabeth M. Royer. "Ad hoc On-Demand Distance Vector Routing." Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, February 1999.

[25] Sunil Kumar Senapati, Pabitra Mohan Khilar, “Securing FSR Against Data Packet Dropping by Malicious Nodes in MANET”, International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), pp.440-442, April, 2009.