Intrusion Detectio
In MANET

A Project Work Submitted in Partial
of the requirements for the 8th Semest
BACHELOR OF TECHNOL
in
Information Technol

By

Dipak Basumatary (Roll No. GAU
Sangeeta Mashahary (Roll No. GA
Swmdwn Basumatary (Roll No. GA

Under the supervision
Mr. Kongkon Kal
(HOD, Dept. of IT)

DEPARTMENT OF INFORMATIO

केन्द्रीय प्रौद्योगिकी संस्थान
CENTRAL INSTITUTE OF TECHNO
(A Centrally Funded Institute under Minist
BODOLAND TERRITORIAL AREAS DISTRICTS :: K
Website: www.cit.kokrajhar.in,

May 2015

Intrusion Detection System In MANET

A Project Work Submitted in Partial Fulfilment

of the requirements for the 8th Semester Degree of

BACHELOR OF TECHNOLOGY

in

Information Technology

By

Dipak Basumatary (Roll No. GAU-C-11/141)

Sangeeta Mashahary (Roll No. GAU-C-11/133)

Swmdwn Basumatary (Roll No. GAU-C-11/131)

Under the supervision of

Mr. Kongkon Kalita

(HOD, Dept. of IT)

DEPARTMENT OF INFORMATION TECHNOLOGY

केन्द्रीय प्रौद्योगिकी संस्थान कोकराझार

CENTRAL INSTITUTE OF TECHNOLOGY KOKRAJHAR

(A Centrally Funded Institute under Ministry of HRD, Govt. of India)

BODOLAND TERRITORIAL AREAS DISTRICTS :: KOKRAJHAR :: ASSAM :: 783370

Website: www.cit.kokrajhar. in, www.cit.ac.in

May 2015

DEPARTMENT OF INFORMATION TECHNOLOGY

केन्द्रीय प्रौद्योगिकी संस्थान कोकराझार

CENTRAL INSTITUTE OF TECHNOLOGY, KOKRAJHAR

(An Autonomous Institute under MHRD)

Kokrajhar – 783370, BTAD, Assam, India

CERTIFICATE OF APPROVAL

This is to certify that the work embodied in this project entitled **"Intrusion Detection System In MANET"** submitted by Swmdwn Basumatary, Sangeeta Mashahary, and Dipak Basumatary to the Department of Information Technology, is carried out under our direct supervisions and guidance.

The project work has been prepared as per the regulations of Central Institute of Technology and I strongly recommend that this project work be accepted in partial fulfilment of the requirement for the degree of B.Tech.

26-5-2015

Supervisor

Mr. Kongkon Kalita

(HOD, Dept. of IT)

Head
Dept. of Information Technology
CIT, Kokrajhar

DEPARTMENT OF INFORMATION TECHNOLOGY

केन्द्रीय प्रौद्योगिकी संस्थान कोकराझार

CENTRAL INSTITUTE OF TECHNOLOGY, KOKRAJHAR

(An Autonomous Institute under MHRD)

Kokrajhar – 783370, BTAD, Assam, India

Certificate by the Board of Examiners

This is to certify that the project work entitled **"Intrusion Detection System In MANET"** submitted by Dipak Basumatary, Sangeeta Mashahary and Swmdwn Basumatary to the Department of Information Technology of Central Institute of Technology, Kokrajhar has been examined and evaluated.

The project work has been prepared as per the regulations of Central Institute of Technology, Kokrajhar and qualifies to be accepted in partial fulfilment of the requirement for the degree of B.Tech.

Ranjan Patowary 26/05/15

Project Co-ordinator

Mr. Ranjan Patowary

(Asst.Professor, Dept. of IT)

Assistant Professor
Dept. of Information Technology
Central Institute of Technology
Kokrajhar

26/5/15

Board of Examiners

EXTERNAL EXAMINER

Dept. Of Information Technology
CIT, Kokrajhar

DECLARATION

We hereby declare that the work entitled **"Intrusion Detection System In MANET"** is an authentic record of our own work carried out at Central Institute of Technology, Kokrajhar for the award of the Degree of Bachelor of Technology in Information Technology. The work presented for assessment in this Project Report has not been previously been submitted for another assessment and that our debts (for words, data, arguments, and ideas) have been appropriately acknowledged.

Date: 26th May, 2015

Place: Kokrajhar

Dipak Basumatary

Dipak Basumatary (GAU-C-11/141)

Sangeeta Mashahary

Sangeeta Mashahary (GAU-C-11/133)

Swmdwn Basumatary

Swmdwn Basumatary (GAU-C-11/131)

ACKNOWLEDGEMENT

We take this opportunity to express our profound gratitude and deep regards to our guide ***Mr. Kangkan Kalita*** for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. We are thankful for his aspiring guidance, invaluably constructive criticism, friendly advice and suggestions during the project work. We are sincerely grateful to him for sharing his truthful and illuminating views on a number of issues related to project work. The blessing, help and guidance given by him time to time shall carry us a long way in the journey of life on which we are about to embark.

We would also like to thank to all our faculty members for giving their precious time and relevant information and experience, we required, without which the Project would have been incomplete.

Our thanks and appreciations also goes to our colleagues in developing the project and people who have willingly helped us out with their abilities.

Lastly, we thank almighty, our parents, and our group members for their constant encouragement without which this assignment would not be possible.

Date: 26th May, 2015
Place: Kokrajhar

Dipak Basumatary
(Dipak Basumatary)
University Roll: GAU-C-11/141
University Registration No: 015199 2011-12

Sangeeta Mashahary
(Sangeeta Mashahary)
University Roll: GAU-C-11/133
University Registration No: 015142 2011-12

Swmdwn Basumatary
(Swmdwn Basumatary)
University Roll: GAU-C-11/131
University Registration No: 015179 2011-12

ABSTRACT

Mobile Ad-hoc Network (MANET) is an infrastructure less, temporary, wireless network that is composed of mobile devices which can arrange themselves in various way and operates without the supervision of any central co-ordinator. In Mobile Ad-hoc Networks, data transmission is performed within an untrusted wireless environment. As the nodes are free to move, so any node can enter or leave the network at any time creating suitable conditions for the malicious nodes to enter the network and perform several attacks. In this attacks, the malicious node records the data packets at one location in the network and tunnels them into the network locally. Our aim in this project is to provide various methods for mitigating the attack by detecting, identifying the malicious nodes and then nullifying their capabilities for further damage.

Keywords: 1.Communication, 2.Network, 3.Wireless, 4.AODV, 5.Mobile-nodes, 6.Attacks.

Table of Contents

List of figures

Page No.

List of Table

Page No

Chapter 1

MANET(Mobile Ad-hoc Network)

1.1 Introduction to MANET (Mobile Ad-hoc Network)

A MANET is a collection of wireless mobile computers (or nodes) forming a temporary network without using any centralized access point, infrastructure or centralized administration. It is a self-starting dynamic network comprising of mobile nodes, where each and every participation node voluntary transmit the packet defined to some remote node using wireless (radio transmission) transmission. MANETs, possess certain characteristics like bandwidth-constrained, variable capacity links, Energy-constrained operations, Limited Physical Security, Dynamic network topology, Frequent routing updates. In this kind of network each and every network does participate voluntarily in transit packet that flow to and from different nodes. Each node do follow the same routing algorithm to route different packets[3].

Mobile Ad-hoc networks are demonstrating the possibility of achievements in solving many real world problems, for example communication in emergency response system, military and police networks, oil drilling, personal area networking, conferences and mining operation. However, MANET uses an untrusted environment for data communication and therefore, it can be subjected to many sorts of attacks[3].

1.2 Applications of MANET

Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad-hoc networking allows us to maintain connections to the network as well as easily adding and removing devices to and from the network. MANET can be applied to a large variety of use cases where conventional networking cannot be applied. MANET is used in some of the following areas:

- **Military battlefield:** The modern digital battlefield demands robust and reliable communication in many forms. In the battlefield it is needed by soldiers for relaying information related to situational awareness.
- **Disaster Area Network:** Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld.
- **Personal Area Network:** Personal Area Networks (PANs) are formed between various mobile devices mainly in an ad-hoc manner, e.g. for creating a home network. They can remain an autonomous network, interconnecting various devices, at home, for example, but PANs will become more meaningful when connected to a larger network.

1.3 Features of MANET

Mobile Ad-hoc network is a collection of autonomous and mobile elements such as laptop, smart phone, tablets PC, etc. The mobile nodes can dynamically self-organise in arbitrary temporary network topology. There is no preset infrastructure thus it does not have the clear boundary. Some of the main features of MANET are discussed below:

- **Infrastructure less:** MANET is an infrastructure less system which has no central server, or specialized hardware and fixed routers. All communications between nodes are provided only by wireless connectivity.
- **Node Movement:** It follows dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network.
- **Limited Physical Security:** Mobile wireless network are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing and denial-of-service attacks should be carefully considered. The characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed internet.

- **Power Limitation:** The mobile host are small and light weight. They are supplied by limited power resources such as small batteries. This limitation vulnerability namely when attackers may target some node batteries to disconnect them, which may lead to network partition. Some attacks may try to engage the mobile nodes un-necessarily, so that they keep on using their battery for early drainage.
- Nodes can perform the role of both the hosts and routers.
- Frequent routing updates.

1.4 Advantages of MANET

- **Mobility:** These networks can be set up at any place and time. The wireless mobile nodes can move at the same time in different directions. Although the routing algorithm can deal with this issue, the performance simulations show that there is a threshold level of node mobility such that protocol operation begins to fail.
- **Speed:** Creating an ad hoc network from scratch requires a few settings changes and no additional hardware or software. If you need to connect multiple computers quickly and easily, then an ad hoc network is an ideal solution.
- **Connectivity:** The use of centralized points or gateways is not necessary for the communication within the MANET, due to the collaboration between nodes in the task of delivering packets.
- **Fast Installation:** The level of flexibility for setting up MANET is high, since they do not require any previous installation or infrastructure and, thus, they can be brought up and torn down in a very short time.
- **Cost:** MANET could be more economical in some cases as they eliminate fixed infrastructure costs and reduce power consumptions at mobile nodes.
- They provide access to information and services regardless of geographic position.

1.5 Disadvantages of MANET

- **Security:** Analyses some of the vulnerabilities and attacks MANET can suffer. The authors divide the possible attacks in passive ones, when the attacker only attempts to discover valuable information by listening to the routing traffic; and active

attacks, which occur when the attacker injects arbitrary packets into the network with some proposal like disabling the network.

- **Location:** The addressing is the another problem for the network layer in MANET, since the information about the location the IP addressing used in the fixed networks offers some facilities for routing that cannot be applied in MANET. The way of addressing in MANET has nothing to do with the position of the node.
- **High Latency:** In an energy conserving design nodes are sleeping or idle when they do not have to transmit any data. When the data exchange between two nodes goes through nodes that are sleeping, the delay may be higher if the routing algorithm decides that these nodes have to wake up.
- **Bandwidth constraints:** The capacity of the wireless links is always much lower than in wired counterparts. Indeed, several Gbps are available for wired LAN, while, nowadays, the commercial applications for wireless LANs work typically around 2 Mbps.
- **Energy Constraints:** The power of the batteries is limited in all the devices, which does not allow infinitive operation time for the nodes. Therefore, energy should not be wasted and that is why some energy conserving algorithms have been implemented (COMPOW, PARO and MBCR are some examples).
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.

1.6 Routing in MANET

A MANET is an infrastructure-less, self-organised and multi-hop network with rapidly changing topology causing the wireless links to be broken and re-established. A key issue is the necessity that the routing protocols must be able to respond rapidly to the topological changes in the network. In this networks, each node must be capable of acting as a router. As a result of limited bandwidth of nodes, the source and the destination may have to communicate via intermediate nodes. Major problems in routing are Asymmetric links, Routing overhead, interference and Dynamic topology[3].

Routing in MANETs has been an active area of research and in recent years numerous protocol have been introduced for addressing the problem of routing, reviewed in later sections. This protocols are divided into two broad classes – ***Reactive and Proactive.***

Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engaging themselves in multi-hop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets; so there is need of a routing procedure. This is always ready to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

Chapter 2

Protocols of MANET

Classification of routing protocols in Mobile Ad-hoc Network can be done in many ways, but most of these are done depending on routing strategy ad network structure. The routing protocols can be categorized as flat routing, hierarchical routing and geographic position assisted routing while depending on the network structure. According to routing strategy, routing protocols can be classified as table-driven and source initiated [7].

The classification of routing protocol is shown in figure below:

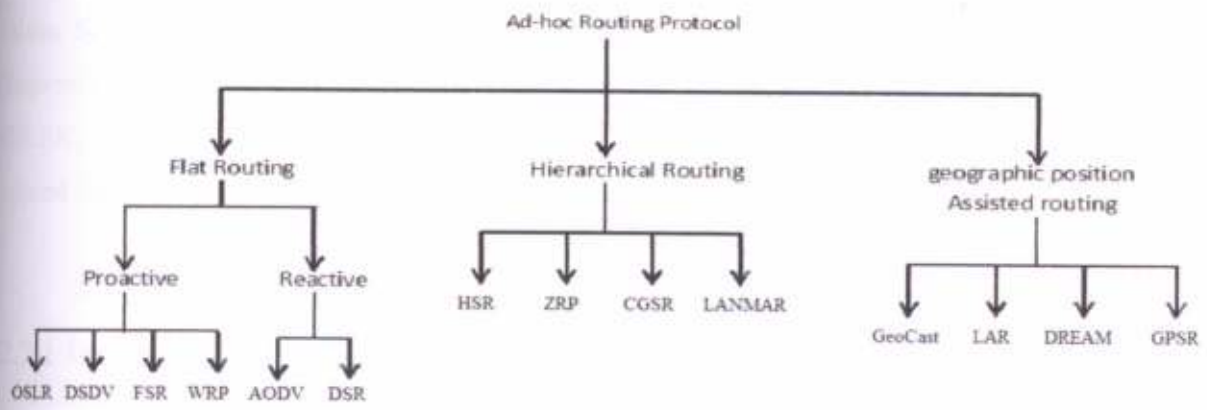

Fig. 2.1 Classification of routing protocols in Mobile Ad-hoc Network.

2.1 Flat Routing Protocols

Flat routing protocols are divided into two classes; the first one is proactive routing protocols and the other is reactive routing protocols. One thing is general for both protocol classes is that every node participating in routing play an equal role. They have further been classified after their design principles; proactive routing is mostly based on Link-State while on-demand routing is based on Distance-Vector [7].

2.2 Proactive Protocol

This protocol rely upon maintaining routing tables of known destination, this reduces the amount of control traffic overhead that Proactive routing generates because packets are forwarded immediately using known routes, However, routing tables must be kept up-to-date; this uses memory and nodes periodically sent update message to neighbours, even when no traffic is present, wasting bandwidth. Proactive routing is unsuitable for highly dynamic networks because routing table must be updated with each topology change, this leads to increased control message overheads which can degrade network performance at high loads.

As such this protocols are often referred to as table-driven. These protocols try to maintain valid routes to all communication mobile nodes all the time, which means before a route is actually needed. Periodic route updates are exchanged in order to synchronize the tables. Some examples of table-driven ad-hoc routing protocols include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV), Optimised Link State Routing Protocol (OLSR) and Wireless Routing Protocol (WRP). These protocols differ in the number of routing related tables and how changes are broadcasted in the network structure.

2.2.1 Distance-Vector Routing Protocol (DSDV)

The first MANET algorithm that we implemented as part of this work is called the Destination-Sequenced Distance Vector (DSDV) routing algorithm. It is a proactive routing algorithm. The DSDV algorithm is a Distance Vector (DV) based routing algorithm designed for use in MANETs, which are defined as the cooperative engagement of a collection of Mobile Hosts without the required intervention of any centralised Access Point (AP). It operates each node as a specialised router which periodically advertises its knowledge of the network with the other nodes in the network. It makes modifications to the basic Bellman-Ford routing algorithms, thereby doing away with the count-to-infinity problem. The algorithm is designed for portable computing devices such as laptops who have energy and processing capabilities.

2.2.2 Optimized Link State Routing Protocol (OSLR)

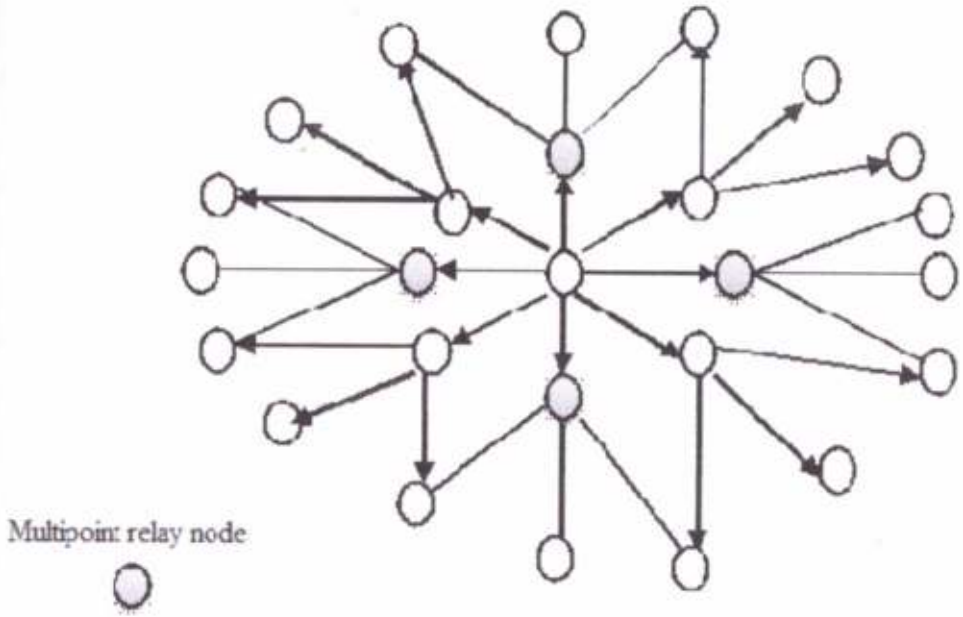

Fig. 2.2 Multipoint Relay

OLSR is a point-to-point routing protocol based on the traditional link-state algorithm. In this strategy, each node maintains topology information about the network by periodically exchanging link-state messages. The novelty of OLSR is that it minimizes the size of each control message and the number of rebroadcasting nodes during each route update by employing multipoint replaying (MPR) strategy. To do this, during each topology update, each node in the network selects a set of neighbouring nodes to retransmit its packets. This set of nodes is called the multipoint relays of that node. Any node which is not in the set can read and process each packet but do not retransmit. To select the MPRs, each node periodically broadcasts a list of its one hop neighbours using hello messages. From the list of nodes in the hello messages, each node selects a subset of one hop neighbours, which covers all of its two hop neighbours. For example, in the above figure, node at the centre can select the blue coloured nodes to be the MPR nodes. Since these nodes cover all the nodes, which are two hops away. Each node determines an optimal route (in terms of hops) to every known destination using its topology information (from the topology table and neighbouring table), and stores this information.

2.2.3 Wireless Routing Protocol

Wireless routing protocols (WRP) is a loop free routing protocol. WRP is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbours. Each node in the network uses a set of four tables to maintain more accurate information: Distance table (DT), Routing table (RT), Link-cost table (LCT), Message retransmission list (MRL) table. In case of link failure between two nodes, the nodes send update messages to their neighbours. WRP belongs to the class of path-finding algorithms with an important exception. It counters the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbours. This eliminates looping situations and enables faster route convergence when a link failure occurs.

2.3 Reactive Protocol

In Reactive protocols, a node initiates a route discovery throughout the network, only when it wants to send a packet to its destination. For this purpose a node initiates a route discovery process through the network. This process is complete a route is determined or all possible permutations have been examined. Once the route has been established, it is maintained by a route maintenance process until either the destination becomes in accessible along every part from the source or until the router is no longer desired. In Reactive schemes nodes maintain the routes to active destinations. A route search is needed for every unknown destinations. Therefore, theoretically the communication overload is reduced at expense of delay due to research. Some of the Reactive protocols are Dynamic Source Routing (DSR), Ad-Hoc On-demand Distance Vector (AODV), and Secure AODV (SAODV).

2.3.1 Ad-hoc On-Demand Distance Vector (AODV)

The AODV routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. It is an on-demand and distance-vector routing protocol which is established by AODV from a destination only on demand. AODV finds a route only when required and hence is reactive in nature. However, once established a route is maintained as long as it is needed. Reactive routing protocols find a path between the source and the destination only when the path is needed, i.e., if there are data to be exchanged between the

source and the destination. An advantages of this approach is that the routing overhead is greatly reduced. A disadvantage is a possible large delay from the moment the route is needed until the time the route is actually required. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. The unused entries in the routing tables are recycled after a time. When a link fails, a route error is passed back to a transmitting node and the process repeats.

AODV is used for unicast, multicast and broadcast communication. It adopts the basic on-demand mechanism of route discovery and route maintenance from DSR and the use of hop by hop routing sequence number. When a source code tries to send information to destination node and it does node have a route to destination, it starts the route discovery process it broadcast router request to neighbours and then forward to the neighbours so on till the route destination is located. It also send a router reply packet to the neighbours which first receives the RREQ. RREP is routed along the reverse path. Each own maintain own sequence number and id. To maintain route the node survey the link status of their next hop neighbour in active route. If the nodes or some immediate node move, the node upstream of the break remove the routing entry and send RERR message to affect the active route up stream neighbours. This continue till the source node is reached[5].

- **RREQ (Route Request):** A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ). Every node maintains two separate counters: a node sequence number and a broadcast_id. The RREQ contains the following fields:-

Source address	Broadcast ID	Source sequence no.	Destination Address	Destination sequence no.	Hop count

Table 2.1 RREQ field

The pair <source address, broadcast ID> uniquely identifies a RREQ. Broadcast id is incremented whenever the source issues a new RREQ.

- **RREP (Route Reply):** A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

Source Address	Destination Address	Destination Sequence	Hop Count	Lifetime

Table 2.2 RREP field

- **RERR (Route Error):-** Nodes monitor the link status of next hops in active routes. When a link break again an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbours that are likely to use it as a next hop towards each destination.

2.3.1.1 Routing table in AODV

- Destination IP address.
- Destination sequence number.
- Valid destination sequence number.
- Other state and routing flag.
- Hop count.
- Next hop.
- List of precursors.
- Lifetime

2.3.1.2 Route discovery in AODV

When a source node desires to send a message to a certain destination node to which it does not have a valid route, it initiates a route discovery process. The source node broadcasts an RREQ (Route Request) message to its neighbours, which then forward the request to their neighbours, and so on, until either the destination or an intermediate node with a route to the destination in its routing table is reached. During the process of forwarding the RREQ, an intermediate node record in its routing table the address of the neighbour from which the first copy of the broadcast packet is received, thereby establishing a reverse path. Additional copies of the same RREQ received later are discarded. Once the RREQ reaches the destination or an intermediate node with a route, the respective node responds by unicasting an RREP (Route Reply) message back to the neighbour from which it first received the RREQ, which relays the RREP backward via the precursor nodes to the source node.

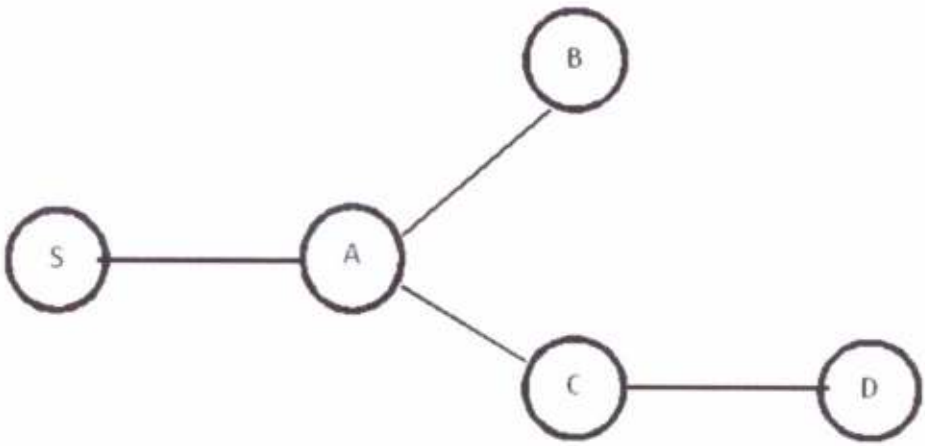

Fig. 2.3 Route discovery process

From the above fig 2 (b), let us consider that "S" needs to route to "D". Therefore, the various steps that need to be carried out while route discovery process are explained with the following steps:

Step 1:

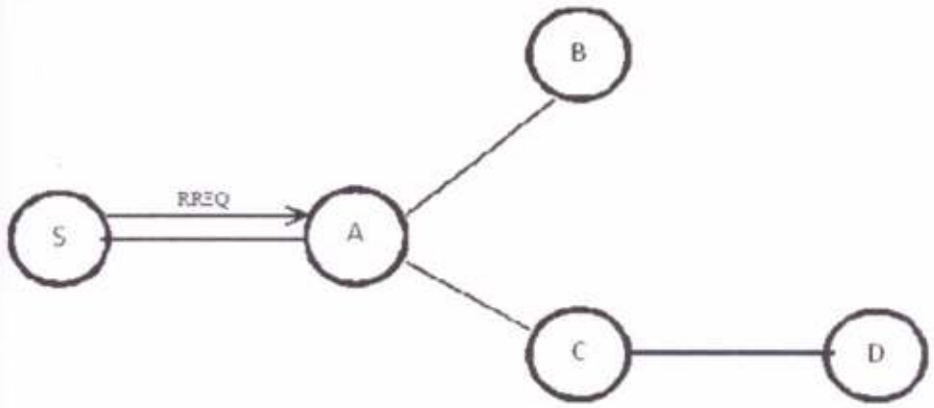

Fig.2.4 Route discovery 1

The above fig. 2(c) shows that the node "S" creates a Route Request(RREQ) entering D's IP address, sequence number, "S's" IP address, sequence number, hop-count (=0) and broadcast to its neighbours.

Step 2:

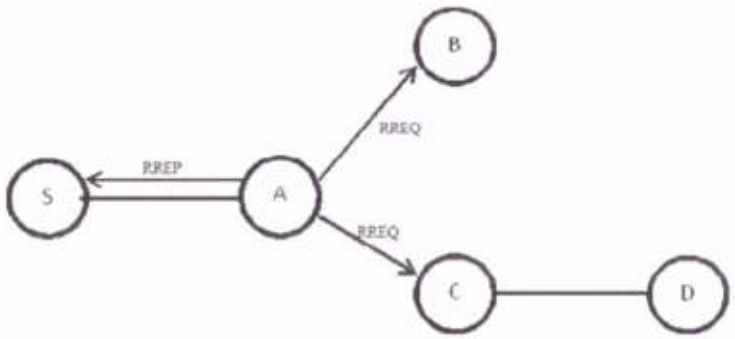

Fig. 2.5 Route discovery 2

The above fig. 2.5 shows that node "A" receives RREQ and makes a reverse route entry for "S" where destination=S, next-hop=S, hop-count=1. It has no routes to "D", so it rebroadcasts RREQ to its neighbours.

Step 3:

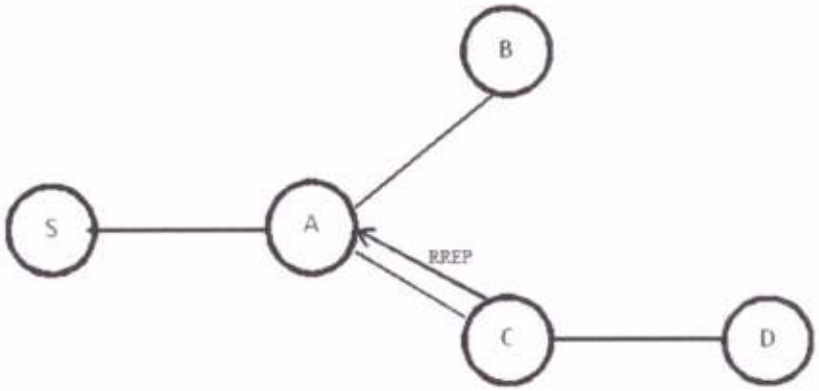

Fig 2.6 Forward path setup 1

The above fig.2.6 shows how that node "C" receives RREQ and creates a Route Reply (RREP) entering "Ds" IP address, sequence number, "Ss" IP address, hop-count to D(=1). Node "C" then unicasts RREP to "A".

Step 4:

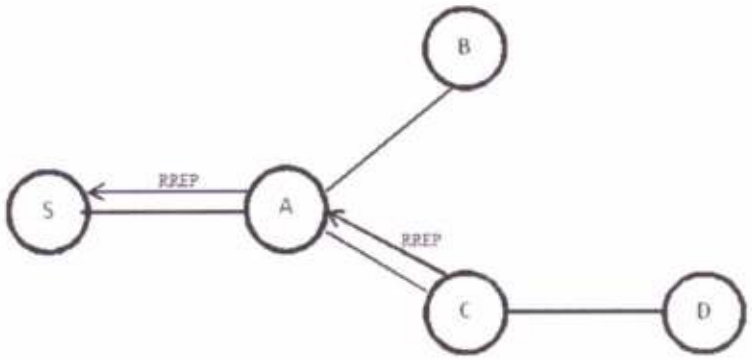

Fig. 2.7 Forward path setup 2

The above fig.2.7 shows that node "A" receives RREP and makes a forward route entry to "D" where destination = D, next-hop = C, hop-count=2. "A" then unicasts RREP to "S".

Step 5:

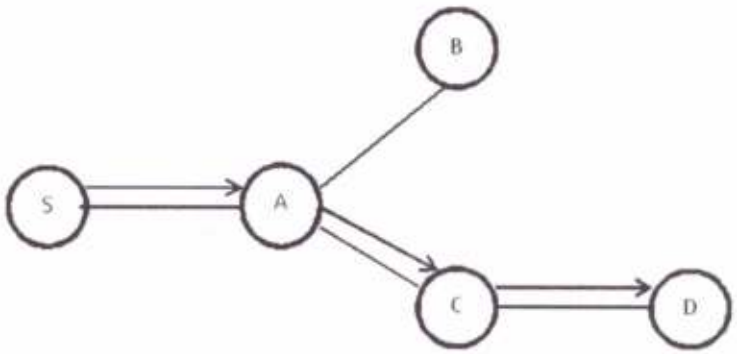

Fig. 2.8 Data delivery path

The above fig.2.8 shows that node "S" receives RREP and makes a forward route entry to D where destination = D, next-hop = A, hop-count = 3. Node "S" at last sends data packet on route to "D".

2.3.1.3 Route maintenance in AODV

Routes are maintained as follows: HELLO messages are sent periodically via broadcast to the neighbouring nodes. When a source node moves, it has to re-initiate the route discovery protocol to find a new route to the destination. On the other hand, when an intermediate node along the route moves, its upstream neighbour will notice route breakage due to the movement and propagate an RERR (Route-Error) message to each of its active upstream neighbours. These nodes in turn propagate the RERR packet to their upstream neighbours, and so on until the source node is reached. The source node may then choose to re- initiate the route discovery for that destination if a route is still desired. Every routing table entry at every node must include the latest information available about the sequence number for the IP address of the destination node for which the route table entry is maintained. This sequence number is called the destination sequence number. It is updated whenever a node receives new information about the sequence number from RREQ, RREP or RERR messages that may be received related to that destination. AODV depends on each node in the network to own and maintain its destination sequence number to guarantee the loop-freedom of all the routes towards that node.

A destination node increments its own sequence number under two circumstances:

- Immediately before a node originates a route discovery; it must increment its own sequence number.
- Immediately before a destination node originates a RREP in response to a RREQ, it must update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet.
- Example of route maintenance:

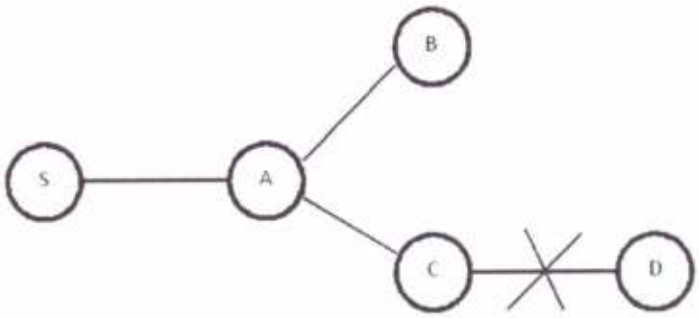

Fig. 2.9 Route maintenance process

Let us consider the above fig. 2.9 in such a way that the link between node "C" and node "D" breaks. The various steps that need to be carried out while route maintenance process are explained with the help of following steps:

Step 1:

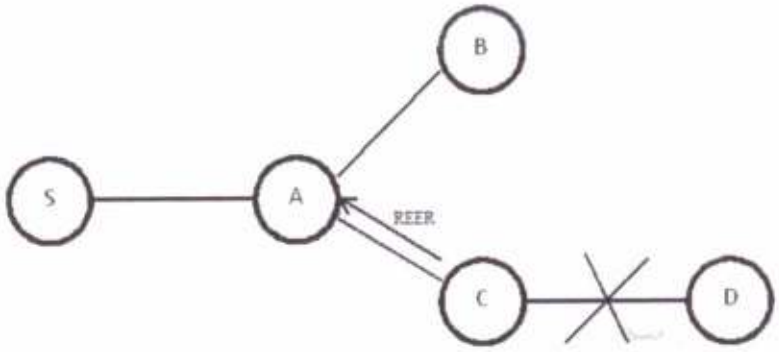

Fig. 2.10. Link breaks between "C" and "D".

The above fig.2.10 shows that the link between "C "and "D" breaks and node "C" invalidates route to "D" in route table creating Route Error message listing all destinations that are now unreachable. It then sends the RERR to its neighbours.

Step 2:

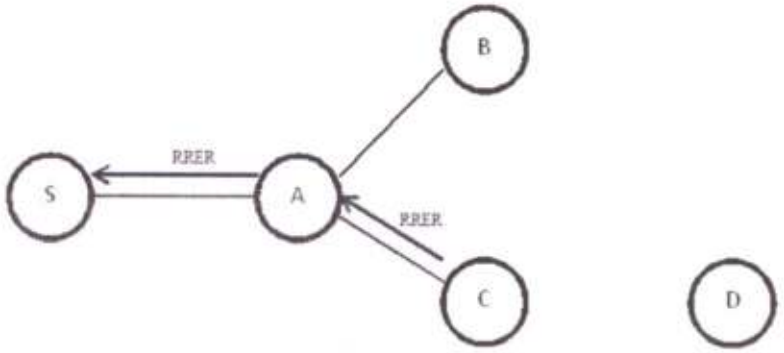

Fig 2.11 Node "A" receives Route-Error (RERR)

The above fig.2.11 shows that after receiving RERR the node "A" checks whether node "C "is its next hop on route to "D" and then deletes route to "D" (making distance -> infinity). Node "A" then forwards RERR to "S".

Step 3:

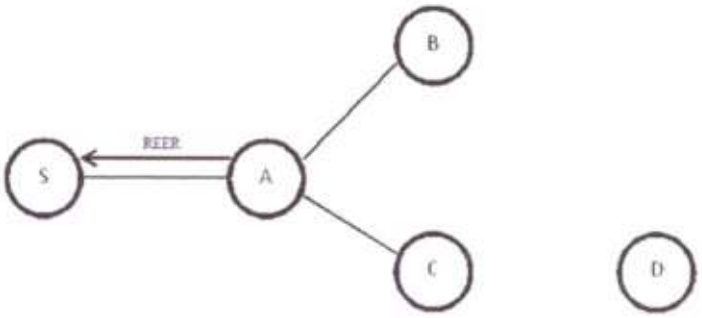

Fig 2.12 Node "S" receives RERR

The above fig.2.12 shows that after receiving RERR node "S" checks whether "A" is its next hop on route to "D" and deletes route to "D". Node "S" then rediscovers route if still needed.

2.3.2 Dynamic Source Routing (DSR):

This is an On-Demand routing protocol. In DSR, the route path are discovered after a packet is sent by a source to a destination node in the Ad-hoc network. The source node initially does not have a path to the destination when the first packet is sent. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing

network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad-hoc network.

An optimum path for a communication between a source node and target node is determined by Route Discovery process. Route Maintenance ensures that the communication path remains optimum and loop-free according the change in network conditions, even if this requires altering the route during a transmission. Route Reply would only be generated if the message has reached the projected destination node (route record which is firstly contained in Route Request would be inserted into the Route Reply).

To return the Route Reply, the destination node must have a route to the source node. If the route is in the route cache of target node, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Reply message header (symmetric links). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The incorrect hop will be detached from the node's route cache; all routes containing the hop are reduced at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

Example of DSR:

Let, x, y, z, v and w form Ad-hoc network. Where "x" is the source node and "z" is the destination node.

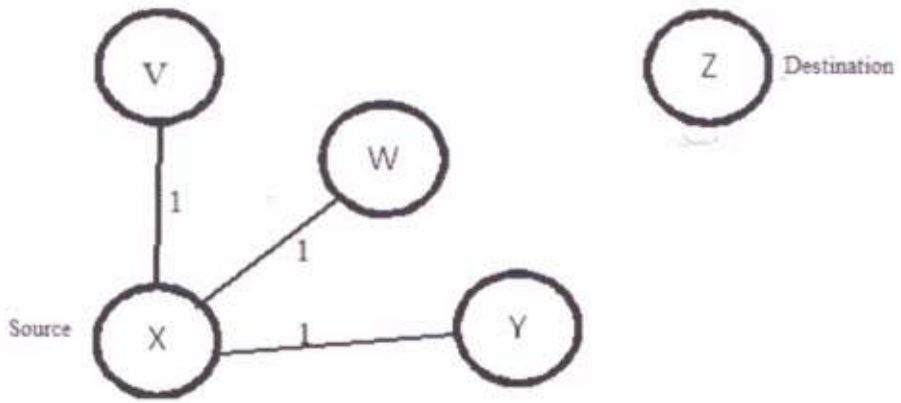

Fig.2.13 DSR algorithm routing protocol

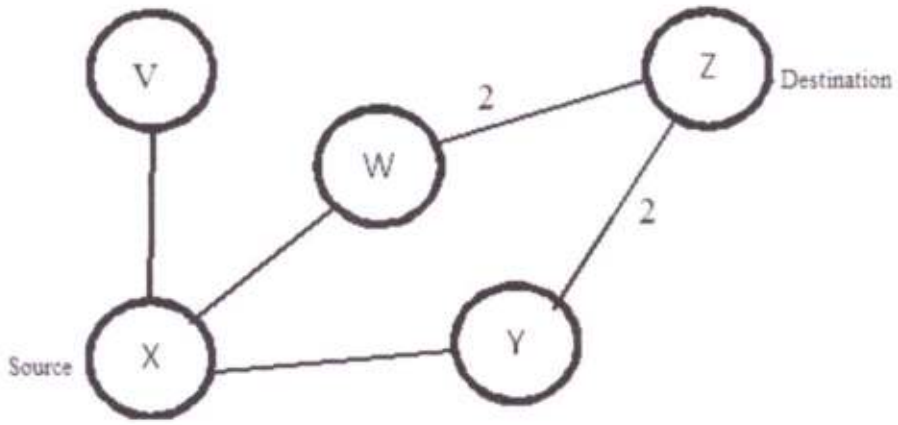

Fig.2.14 Showing re-broadcasting by nodes V, W, Y.

2.3.2.1. Route Discovery Algorithm

a) X broadcast a Route Request Packet with the address of destination Z.

b) The neighboring nodes V, W, Z receive the Route Request Packet from X, as shown in fig.2.13.

c) The receiving nodes V, W, Y each append their own address to the Router packet and broadcast the packet further as shown in fig.2.14.

d) The destination node Z receives the Route Request Packet. The Router Reply Packet now contains information of all the addresses of nodes on the path from the source node X to the destination node Z.

e) On receiving the Reply Request Packet the destination node Z sends a reply called the Router Reply Packet to the source node X by travelling a path of address it has got from the Route Request Packet.

2.3.2.2. Route Maintenance Algorithm

a) In DSR algorithm a link break is detected by a node along the path from node X to node Z, in this case node W.

b) The node W send a message to source node X indicating a link break.

c) In this case, node X can use another path like X-Y-Z or it must initiate another route discovery packet to the same destination node, in this case Z.

2.3.2.3. Advantages and disadvantages of DSR

DSR uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

The disadvantage of DSR is that the route maintenance mechanism does not locally repair a broken down link. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

2.4. Hierarchical Routing

These protocols try to incorporate various aspects of proactive and reactive routing protocols. They are generally used to provide hierarchical routing; routing in general can be either flat or hierarchical. The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption. Some examples of Hybrid Routing Protocols include Zone Routing Protocol (ZRP) and Cluster Head Gateway Switch Routing Protocol (CGSR). In what follows, we present a few of the proposed routing protocols from each class developed for the ad hoc networks. The most important protocols and those which dominate recent literature are AODV, DSR, SRP, ZRP and DSDV [6].

2.4.1. Zone Routing Protocol (ZRP)

Zone routing protocol is a hybrid protocol. It combines the advantages of both proactive and reactive routing protocols. A routing zone is defined for every node. Each node specifies a

zone radius in terms of hops. Zones can be overlapped and size of a zone affects the network performance. The large routing zones are appropriate in situations where route demand is high or the network consists of many slowly moving nodes. On the other hand, the smaller routing zones are preferred where demand for routes is less and /or the network consists of a small number of nodes that move fast relative to one another. Proactive routing protocol works with in the zone whereas; reactive routing protocol works between the zones.

ZRP consists of three components:

- The proactive Intra zone routing protocol (IARP)
- The reactive Inter zone routing protocol (IERP)
- Bordercast resolution protocol (BRP).

Each component works independently of the other and they may use different technologies in order to maximize efficiency in their particular area. The main role of IARP is to ensure that every node with in the zone has a consistent updated routing table that has the information of route to all the destination nodes within the network. The work of IERP gets started when destination is not available with in the zone. It relies on bordercast resolution protocol in the sense that border nodes will perform on-demand routing to search for routing information to nodes residing outside the source node zone [6].

2.4.2. Cluster-head Gateway Switch Routing Protocol (CGSR)

Cluster-head Gateway Switch Routing Protocol is a multichannel operation capable protocol. It enables code operation among clusters. The clusters are formed by cluster head election procedure, which is quite intensive process. On that reason the protocol uses so called Least Cluster Change (LCC) algorithm for that election. By using LCC can cluster heads only changed when two cluster heads come into contact with each other or when a node moves out of contact of all other cluster heads. CGSR is not an autonomous protocol. It uses DSDV as the underlying routing scheme. The DSDV approach is modified to use a hierarchical cluster head-to-gateway routing. A packet sent by a node is first routed to its cluster head, and then the packet is routed from the cluster head to a gateway to another cluster head, until the destination node's cluster head is reached. That destination cluster head then transmits the packet to the destination node [6].

2.4.3 Fisheye Secure Routing (FSR)

Fisheye Source Routing (FSR) is based on a method to divide each information details and accuracy is better for nodes to be near. The name's basis is on the phenomenon of fish eye's ability to see objects the better the nearer they are. In FSR zones are classified according to the distance, measured by hops, from the node. FSR is a protocol to be built on top of another protocol. It can be applied to work together with some link-state protocols as GSR. In GSR link state packets are not flooded but nodes maintain a link state table based on the up-to-date information received from neighboring nodes and periodically exchange it with their local neighbors. The drawbacks of GSR are the large size update messages and the latency of the link state change propagation. FSR is applied to eliminate that situation by reducing the size of update messages without seriously affecting routing accuracy. The reduction of update message size is obtained by using different exchange periods for different entries in the table. The entries corresponding to nodes within the smaller scope are propagated to the neighbors with the highest frequency. As a result, a considerable fraction of link state entries are suppressed, thus reducing the message size. The imprecise knowledge of best path to a distant destination is compensated by the fact that the route becomes progressively more accurate as the packet gets closer to its destination [6].

Chapter 3

Threats of AODV

Wireless Mobile Ad hoc Networks (MANET) are vulnerable to many security attacks because of shared channel, insecure operating environment, lack of central authority, limited resource availability, dynamically changing network topology, resource constraints. MANETs open issues like security problem, finite transmission bandwidth, abusive broadcasting messages, reliable data delivery, dynamic link establishment and restricted hardware caused processing capabilities emerges into new horizon of different research areas[3].

The multi-layer attacks are comprises of DoS, impersonation, replay, man-in-the-middle. Various attacks at Data Link/MAC layer include malicious behaviour, selfish behaviour, active, passive, internal external, WEP weakness, disruption MAC (802.11).

Physical layer comprises interference, traffic jamming, eavesdropping. The active attacks at network layer comprises of wormhole attack, blackhole attack, byzantine attack, information disclosure, resource consumption attack, routing attack. The blackhole node exploits the ad hoc routing protocol (AODV) to advertise itself as having a valid route to a destination node with the intention of intercepting packets, even though the route is spurious. The packets are consumed by the blackhole node and these nodes can conduct coordinated attacks. Greyhole is a node that can switch from normal behaviour to behaviour like a blackhole node. Wormhole attacks depend on a node misrepresenting its location, therefore, location based routing protocols have the potential to prevent wormhole attacks. Session hijacking is the transport layer attack which is a critical error and gives an opportunity to the malicious node to behave as a legitimate system. This layer also includes SYN flooding. Repudiation and data corruption are specific to application layer[3].

3.1 Categories of attacks

- **Passive attack:** These types of attacks are not disrupting the network. A passive attack does not alter the data transmitted within the network. Bit it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attackers does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Detection of such type of attacks is difficult since the operation of network itself does not get affected. In order to overcome this type of

attacks powerful encryption algorithms are used to encrypt the data being transmitted. Some examples of Passive attack are:

- Eavesdropping Attack.
- Traffic Analysis.

- **Active Attack:** These types of attacks are disrupted the network, to alter or destroy data being exchanged in the network. These attacks can be internal or external. Wormhole attack is one of the major security threats that can cause major disruption in network communication where a malicious node captures packet from one location in the network, tunnels it to another malicious node at distant point, when then replays it locally Once the wormhole link is established malicious nodes can either drop the packet, perform eavesdropping Denial Service Attack.

  - Dropping Attack
  - Modification Attack
  - Black Hole Attack
  - Grey Hole Attack
  - Wormhole Attack

- **Other Attacks:**
  - Timing Attack
  - Route Table Poisoning Attack
  - Location Disclosure Attack
  - Rushing Attack

3.2 Blackhole Attack

Blackhole attack is one such attack and a kind of Daniel-of-service in which a malicious node make use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the route discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes responds immediately to the source node as the nodes do not refer to routing

table. The source node assumes that the route discovery process complete, ignores other RREP message from other nodes and select the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received message instead of replaying them as the protocol requires.

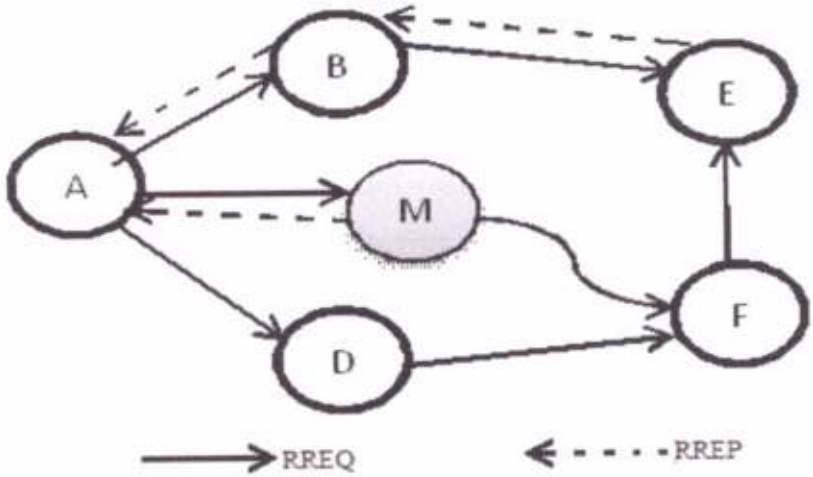

Fig 3.1 Blackhole Attack in AODV

In the fig 3(a), a malicious node "M", when node "A" broadcast a RREQ packet, node "B", "D" and "M" receive it. Node "M", being a malicious node does not check up with its routing table for the requested route to note "E". Hence, it immediately change back a RREP packet, claiming a route to the destination. Node "A" receives the RREP from "M" ahead of the RREP from "B" and "D". Node "A" assumes that the route through "M" is the shortest route and sends any packet to the destination through it. When the node "A" sends data to "M", it absorbs all the data and thus behaves like a blackhole.

3.2.1 Mitigating of Blackhole Attack

It can be made an additional route to the intemediate node that replies the RREQ message to check whether the route from the intermediate node to the destination node exists or not. When the source node receives the furthur reply from the next hop, it extracts the check result from the reply packets. If the result is yes, we establisha route to the destination and begin to send out data packets. If the next hop has no route to the inqiured intermediate node, but has a

route to the destination node, we discard the reply packet from the inquired intermediate and use the new route through the next hop to the destination.

3.3 Greyhole Attack

The greyhole attack has two phases. In the first phase, a malicious node exploids the AODV protocol to adverse itself as having a valid route to adestination node, with the intention of intercepted packets with a certain probability. This is more difficult to detect than the blackhole attack where the malicious node drops the received data packet with certainity. A grehole attack may exihibit its malicious behaviour in different ways. It may drop packets coming from(or destined to) certain specied nodes. Another type of greyhole node may behave maliciously for some time duration by dropping packets but may switch to normal behaviour later.

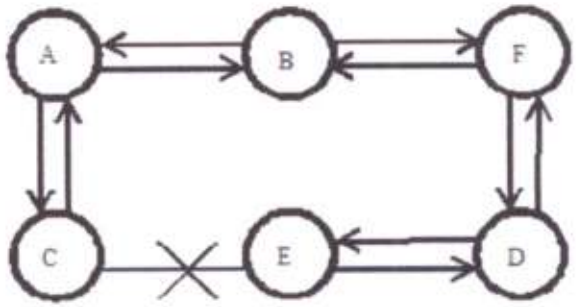

Fig.3.2 Greyhole atack in AODV

In the fig.3(b), "A" node wants send packets to node "D". The route that it has is "AECD". When the packet comes to node "C", which is malicious node, it will start dropping packets and the communication will fail.

3.3.1 Mitigation of Greyhole Attack

Every single node must sense its neighbouring nodes using "Hello" message with a fixed interval. Here, time has to be defined earlier to the communication process. Apart from this the Route Discovery and Route maintenance process must be carried out as the malicious node will take part in the Route Disc1overy process. The node that are added to the blacklist must not be considered for routing process.

3.4. Sinkhole Attack

The Sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack, a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric. As a result, the adversary manages to attract all traffic that is destined to the base station. By taking part in the routing process, she can then launch more severe attacks, like selective forwarding, modifying or even dropping the packets coming through.

3.5. Wormhole Attack

These multi-hop wireless networks are especially suited for scenarios where it is infeasible or expensive to deploy significant networking infrastructure. However, the open nature of the wireless communication channels, the lack of infrastructure and the hostile environment where they may be deployed, make them vulnerable to a wide range of security attacks. This attacks could involve eavesdropping, message tampering, or identity spoofing, which have been addressed by customised cryptographic primitives. Many attacks are targeted directly at the data traffic by dropping all data packets (blackhole attack), selectively dropping data packets and performing statistical analysis on the data packets to obtain critical information, such as the location of primary entities in the network. For an attacker to be able to launch damaging the data attacks, one option is to have a large number of powerful adversary nodes, distributed over the network and processing cryptographic keys. Alternately, the attacker can achieve such attacks by having a few powerful adversary nodes that need not authenticate themselves to the network. The attacker can achieve by targeting specific control traffic in the network. A particularly severe control attack on the routing functionality of wireless networks, called the Wormhole attack has been introduced in the context of Ad-hoc network. In this attack, two colluding node that are far apart are connected by a tunnel giving an illusion that they are neighbours. Each of these nodes receive route request and topology control message from the network and sends it to the other colluding nodes via tunnel which will then reply it into the network from there. By using this additional tunnel, this nodes are able to advertise that they have the shortest through them. Once these link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange

of some topology control (TC) messages and data packets through the wormhole tunnel. Since these MRPs forward flawed (imperfection) topology information, it results in spreading of incorrect topology information throughout the network. On receiving these false information, other nodes may send these message through for fast delivery. Thus it prevents honest intermediate nodes from establishing links between source and destination.

During the attack, a malicious node captures packets from one location in the network, and "tunnels" them to another malicious node at a distant point, which replace them locally. The tunnel can be established in many different ways, such as through an out-of-band hidden channel, packet encapsulation, or high power transmission. This tunnel makes the tunnelled packets arrived either sooner or with lesser number of hops compared to the packets transmitted over normal multi-hop routes. This creates the illusion that the two end points of the tunnel are very close to each other. A wormhole tunnel can actually be useful if used for forwarding all the packets. However, in its malicious incarnation, it can be used by the two malicious end point of the tunnel to pass routing traffic to attract routes through them. The malicious end points can then launch a variety of attacks against the data traffic flowing on the wormhole, such as the greyhole attack or statistical flow analysis of the traffic. Also the wormhole attack can affect route establishment by preventing any two nodes in the network that are greater than two hopes away from discovering routes to each other. The wormhole attack affect many applications and utilities in the ad-hoc network, such as network routing, data aggregation and clustering protocols, and location based wireless security systems. Finally the wormwhole attack is considered particularly insidious since it can be launched without having access to any cryptographic keys or compromising any legitimate node in the network.

The wormhole attack is possible even if the attacker has not compromised any host and even if all communication provides authentication and confidentiality. Here, an attacker records all the packet at one location in the networks, tunnels them to another location, and retransmit them into the network. Since the content of the packets are not modified, wormhole cannot be detected b cryptographic techniques. These malicious nodes can be directly connected or many hops away through tunnelling.

The tunnel can be categorized in many ways e.g Out-of-Band and In-Band channel. These channels tunnelled arrived packets either sooner or lesser number of hops compared to the packets transmitted over normal multi-hop paths. These makes the illusion that the two end points of a tunnel are very close to each other. These process is used by the attacker to disrupt the correct operation of Mobile Ad-hoc routing protocol.

A malicious node can be formed using, first, In-Band channel where one malicious node forward the route request packet to another malicious node via one or more nodes in the network. Second is the Out-Of Band channel where one malicious node directly connected with another malicious node by either weird link or long range wireless link. The main purpose of both the wormhole attacks is to gain sensitive information from the network.

When two malicious node form a wormhole if they hide themselves in the routing path is a hidden wormhole attack. In the fig 3.3, the receiver "R" notice that "S" 'is the directly neighbour of it but actually packet is delivered via node Z1-A-B-Z2.

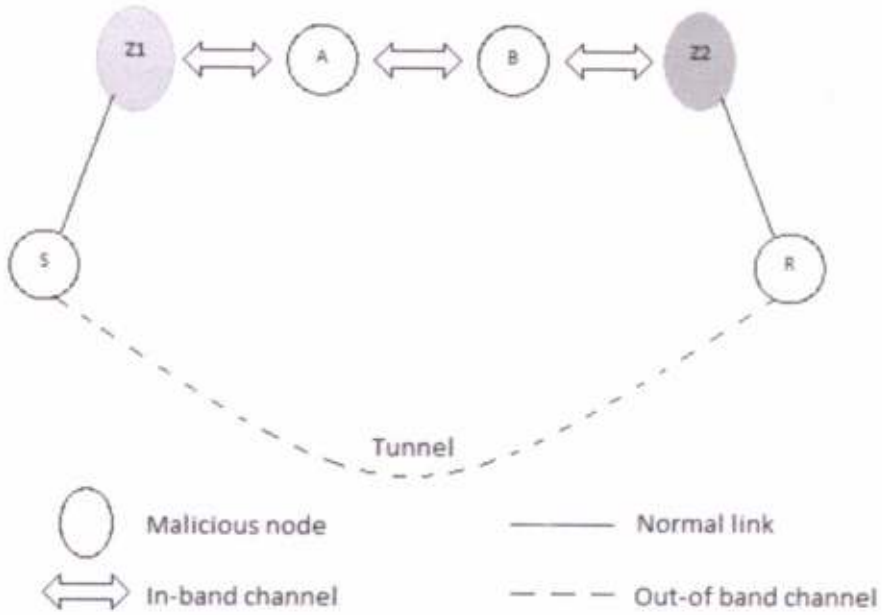

Fig. 3.3 Wormhole attack

If malicious nodes do not hide themselves in the routing path is an exposed or open wormhole attack. In this type of attack, legitimate nodes are aware of the existence of malicious nodes; but do not know that these are malicious nodes.

3.5.1. Types of Wormhole attack

- In-Band wormhole:
  a) Self-Contained wormhole
  b) Extended in-band wormhole

- Out-band wormhole
  a) Hidden wormhole
  b) Exposed wormhole

3.5.2 In-Band wormhole

An in-band wormhole does not use an external communication medium to develop the link between the colluding nodes. An in-band wormhole instead develops a covert overlay tunnel over the existing wireless medium. An in-band wormhole can be a preferred choice of attackers and can be potentially more harmful as it does not require any additional hardware infrastructure and consumes existing communication medium capacity for routing the tunneled traffic. An in-band wormhole developed over a wireless network using false OLSR messages. Nodes create an illusion of being neighbors by sending false routing advertisements of hop symmetric link between the two nodes without the actual exchange of "HELLO" messages. This false link information is propagated to other nodes across the network via a broadcast of OLSR Topology Control (TC) messages. This false link information thus undermines the shortest path routing calculations attracting many end-to-end flows by advertising incorrect shortest paths. The attracted traffic is then forwarded through a tunnel with the help of a third colluder node. This colluder node acts as an application-layer relay for wormhole traffic between the wormhole endpoints.

3.5.3 Out-Band wormhole attack

In an out-of-band wormhole, the colluder nodes establish a direct link between the two end-points of the wormhole tunnel in the network. This link is established using a wired link or a long-range wireless transmission. The wormhole attacker receives packets at one end and directs the packets to be forwarded to the other end through the established link. The attacker can thus analyze and tamper a large amount of traffic through this link.

3.5.4 Wormhole attack analysis

The placement of compromised nodes to launch a wormhole attack plays an important role in the effectiveness of a wormhole.

Let us consider an example to prove the above statement:

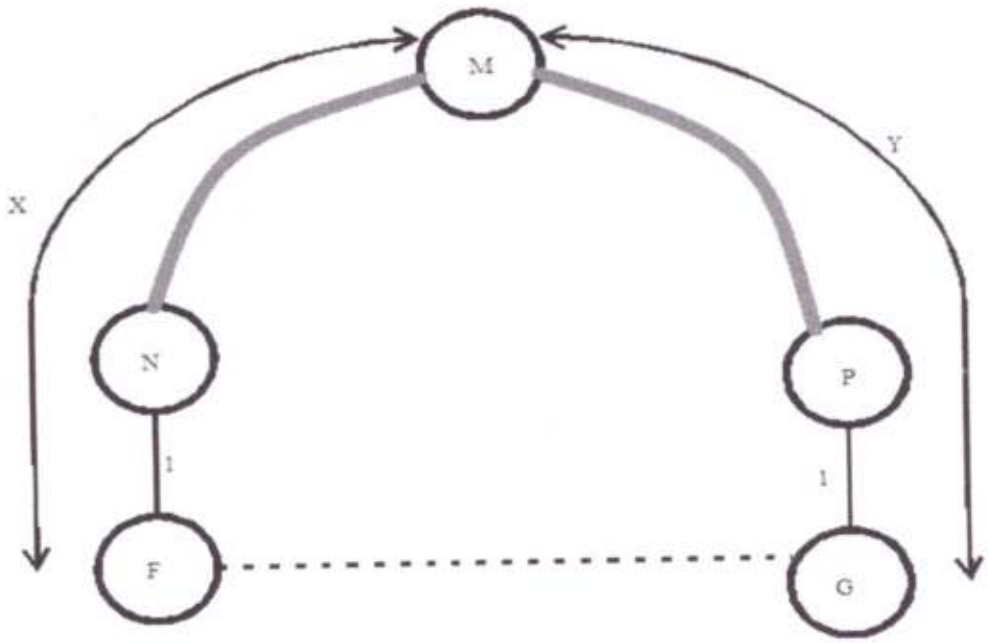

Fig 3.4. Representation of wormhole constructed by attacker nodes "E1" and "E2".

Let F and G represent the tunnel end points and node M represent the intermediate relay node as shown in the above figure (fig 3.4). Let N and P be the first uncompromised nodes on the paths from F and P to M respectively that do not pass through the wormhole link. Let the path from F to M that does not pass through the wormhole link be of length X hops, and that from G to M be of length *Y* hops. To prevent nodes N and P from getting attracted to the wormhole link to route traffic to node M, the length of the paths from N and P to M should be less than that offered by the path passing through the wormhole link. The length of the path from N to M via the wormhole link is *Y+2* hops. Thus the actual path from N to M should be less than *Y+2* hops. As N is a neighbour of F, the length of the path from F to M should be less than *Y+3* hops.

Thus, $x < y + 3$.....(1) The path from P to M is *Y-1* hops. To prevent P from getting attracted by the wormhole link N-P, the path from P to M offered by the wormhole link should be greater than Y-1 hops. The path from P to M passing through the wormhole link is of length X+2 hops.

Thus, $X + 2 > Y - 1$ .....(2)

From equations 1 and 2, it then follows that:

$$Y - 3 < X < Y + 3$$

So we see that only those three node combinations can be used to create a wormhole where X lies between Y - 3 and Y + 3.

Chapter 4

The Network Simulator

The network simulator is discrete event packet level simulator. The network simulator covers a very large number of application of different kind of protocols of different network types consisting of different network elements and traffic models. Network simulator is a package of tools that simulates behaviour of networks such as creating network topologies, log events that happen under any load, analyse the events and understand the network. Well the main aim is to learn how to use network simulator and to get acquainted with the simulated objects and understand the operations of network simulation and we also need to analyse the behaviour of the simulation object using network simulation.[9]

4.1. Features of Network Simulator

Network Simulator is mainly based on two languages. They are C++ and OTcl. OTcl is the object oriented version of Tool Command language. The network simulator is a bank of different network and protocol objects.

C++ helps in the following way:

- It helps to increase the efficiency of simulation.
- It is used to provide details of the protocols and their operation.
- It is used to reduce packet and event processing time.

OTcl helps in the following way:

- With the help of OTcl we can describe different network topologies.
- It helps us to specify the protocols and their applications.
- It allows fast development.
- Tcl is compatible with many platforms and it is flexible for integration.
- Tcl is very easy to use and it is available in free.

4.2. NS2 (Network Simulator-2)

One of the most popular simulator among networking researchers. This simulator simulates both wired and wireless networks. Simulation scripts are written in the OTcl language, an extension of the Tcl scripting language. The core of ns-2 is also written in C++, but the C++ simulation objects are linked to shadow objects in OTcl and variables can be linked between both language realms.[9]

4.3. Network Animator (NAM)

When we will run the program in ns2 we can visualize the network in the NAM. But instead of giving random positions to the nodes, we can give suitable initial positions to the nodes and can form a suitable topology.[9] So, in the program we can give positions to the nodes in NAM in the following way:

1. Give position to the nodes in NAM.
2. $ns duplex-link-op $n0 $n2 orient-right-down
3. $ns duplex-link-op $n1 $n2 orient-right-up
4. $ns simplex-link-op $n2 $n3 orient-right
5. $ns simplex-link-op $n3 $n2 orient-left
6. $ns duplex-link-op $n3 $n4 orient-right-up
7. $ns duplex-link-op $n3 $n5 orient-right-down

4.4. The Trace File

NS simulation can produce visualization trace as well as ASCII file corresponding to the events that are registered at the network. While tracing ns inserts four objects: EnqT, DeqT, RecvT & DrpT. EnqT registers information regarding the arrival of packet and is queued at the input queue of the link. When overflow of a packet occurs, then the information of the dropped packet is registered in DrpT.DeqT holds the information about the packet that is de-queued instantly. RecvT hold the information about the packet that has been received instantly.[9]

Event	Time	From Node	To Node	Pkt Type	Pkt Size	Flags	Fid	Src Addr	Dst Addr	Seq No.	Pkt Id

Table. 4.1 Structure of Trace file

1. The first field is event. It gives four possible symbols '+' '-' 'r' 'd'. These four symbols correspond respectively to en-queued, de-queued, received and dropped.
2. The second field gives the time at which the event occurs.
3. The third field gives the input node of the link at which the event occurs.
4. The fourth field gives the output node at which the event occurs.
5. The fifth field shows the information about the packet type. i.e., whether the packet is UDP or TCP.
6. The sixth field gives the packet size.
7. The seventh field give information about some flags.
8. The eight field is the flow id(fid) for IPv6 that a user can set for each flow in a tcl script. It is also used for specifying the color of flow in NAM display.
9. The ninth field is the source address.
10. The tenth field is the destination address.
11. The eleventh field is the network layer protocol's packet sequence number.
12. The last field shows the unique id of packet.

Following the two trace files:

r 1.84471 2 1 cbr 210 ------- 1 3.0 1.0 195 600

r 1.84566 2 0 ack 40 -------- 2 3.2 0.1 82 602

Chapter 5

Related work

The wormhole attack in wireless network was independently introduced by Dahill, Papadimitratos, and Hu. Hu et al., introduced the concept of geographical and temporal packet leashes for detecting wormholes. The solution requires either that each mode has accurate location information and loose clock synchronization (geographical leash) or accurate clock synchronization (temporal leash). An implicit assumption in the approach is that packet processing, sending and receiving delays are negligible. Both geographical and temporal leashes need to add authentication data to each packet to protect the leash use the large amount of storage for the Merkle hash tree based authentication scheme, and do not isolate malicious node. Capkun et al. present SECTOR, which can detect wormhole attacks without requiring any clock synchronization but using special hardware for a challenge request-response and for accurate time measurements. Hu and Evans use directional antennas to prevent a sub-class of wormhole attack. They provide a method for secure neighbour discovery using the directionality of the antennas and under the assumption that all the nodes are aligned. The requirements of the directional antennas on all nodes may be infeasible for some deployments. Another approach is sending acknowledgement to packets to discover wormhole in the path. This approach introduces overhead of control messages and thus not isolate the malicious nodes. Wang et al. present a method for graphically visualizing the occurrence of wormhole in static sensor networks by reconstructing the layout of the sensor using multidimensional scaling.

A fundamental building block for detecting the wormhole attack in mobile network is a protocol for secure neighbour discovery. Neighbour discovery can be looked upon as a subset of the problem of location determination under the condition that the location of a node can be determined by other nodes. Several physical properties of the received signals are used for one hop location estimation-signal strength, time of flight, and angle of arrival. The time of flight approach is similar to the temporal leash and suffers from the same drawbacks. Typically the location determination protocols have an explicit localization phase when beacon message are exchanged after which each node determines its relative location with respect to its neighbours. However, this is not secure since a powerful adversary can increase its transmission power for just this phase. The plethora of existing protocols for a node to determine its own location,

sometimes in the presence of malicious beacon nodes, are asymmetric to our problem where the determination has to be done securely by the neighbours of a node.

There are a few solutions proposed in the literature for secure neighbour discovery. The approach by Evans uses directional antennas on each node with precise alignment of nodes. The approach by Perrig is presented in context of designing a route discovery component that is secure to rushing attack. The approach relies on the time of flight and thus assumes very accurate time measurement and disregards all sources of delay other than the propagation delay. The MAC delay in networks of even moderate density can make this assumption dubious. Many schemes use beacons sent by powerful nodes to enable location determination by other nodes. Satry et al. tackle the problem of a nodes securely verifying the location of possibly malicious beacon nodes that send spurious information about their own location. Their approach uses a very fast (e.g., radio frequency) and a relatively slow (e.g., ultrasound) signal to derive distance from the time delay. While this kind of capability can be mounted on a limited set of beacon nodes, it is infeasible to do this on all the nodes in the network[2].

Chapter 6

Proposed work

This project has proposed a detection technique by modifying the aodv.cc using AODV protocol. In this technique the attack is detected by taking two things into account i.e. the number of hop count and delay per hop information for different paths from source to destination. Here no external hardware is required for wormhole detection. This technique also uses the same technique as the AODV protocol and also has two message types- RREQ and RREP. The only difference that is present between them is that the RREQ packet send by the sender for the route discovery process contains an extra timestamp field which includes the time when the data is send. The RREP packet includes the same field as the RREP packet in the AODV protocol. The time stamp field used in RREQ packet cannot be processed by the intermediate nodes as the sender protects the field by sending a message authentication code of the timestamp to the destination.

According to this technique, the receiver gathers information of each path from source to destination. The source sends RREQ packet to initiate the route discovery process and the RREP packet is send by the destination node to the sender node after the wormhole detection process. The RREP packet is only send through those routes that are found to be free from malicious attacks. When the sender starts the route discovery process it broadcasts the RREQ packet. The RREQ packet includes the previous hop field, hop count field and the time stamp field. The previous hop field is occupied with the sender's node id, the hop count field is set to 1 and the timestamp field is filled with the time when the packet is send. Here only previous hop information are used excluding the whole routing information to save network resources. RREQ is processed by each of the intermediate nodes before reaching the destination node. When an intermediate node receives an RREQ packet, it reads the previous hop field and makes a reverse route to the sender and then replaces its node id into the previous hop field and increases the hop count field by 1 and broadcast the modified RREQ packet to its neighbours. If a RREQ is received with different id then the reverse route is set up otherwise if same id RREQ is received the packet is dropped. When the destination node gets RREQ from its neighbour it does not immediately reply to the requested node but collects the information on each route from source to destination by observing the time stamp.

6.1. Objective

As the nodes are free to move in an Ad-hoc network, so any node can enter or leave the network at any time creating suitable conditions for the malicious nodes to enter the network and perform several attacks. The main objective in this report is to provide various methods for mitigating the attack by detecting, identifying the malicious nodes and then nullifying their capabilities so that there exist no packet loss in the transmission of data packet from a source to its destination.

6.2. Implementation

Here we have introduced a new packet called ACK. The ACK packet is sent to the sender by the receiver when it receives a packet. At first the sender will broadcast RREQ packet. When the sender receives the RREP packet from the neighbour node it set its timer and sends the data packet through the path which is found to be shorter. After that it silently keeps on waiting for the ACK packet from the destination. If the ACK packet is not received then the timer becomes 0, then it is assumed that a malicious node is present and the route through which the data packet was sent is deleted and the data packet is sent to the next shorter path in the routing table.

Software requirements:

Programming languages: TCL, C++, OTCL

Simulator: NS2 2.35

User Interface: NAM

Operating System Environment: Ubuntu 11.34

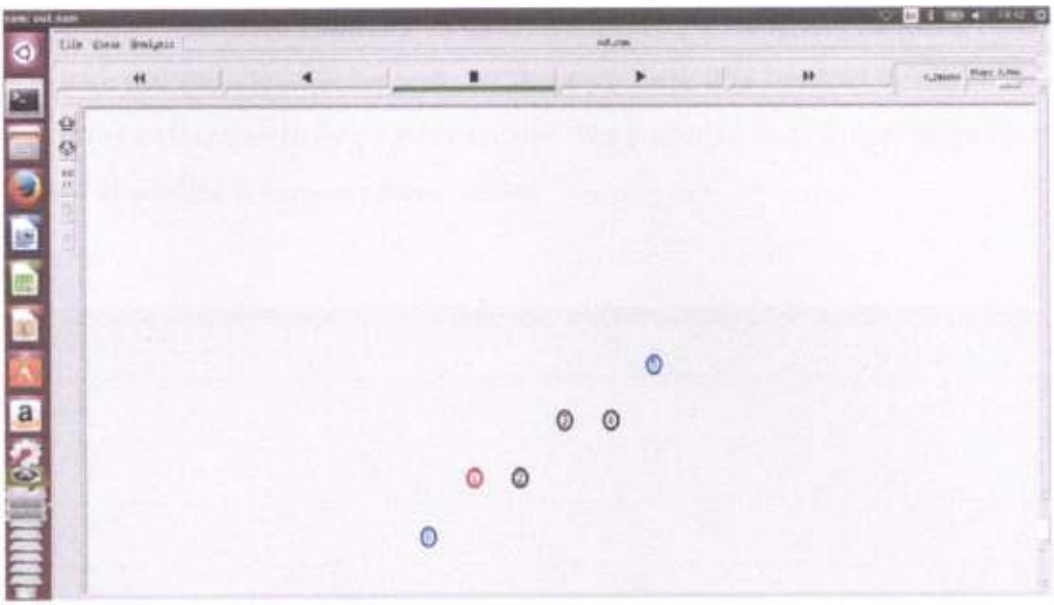

Fig. 6.1. Simulated Network

The designed network with six nodes is shown in fig.6.1, where, node 0 is the source node and the node 5. After simulating the above network using the protocol AODV the trace files are acquired. With the help of these trace file we can calculate the performance parameters like Packet Delivery Ratio (PDR), Packet loss.

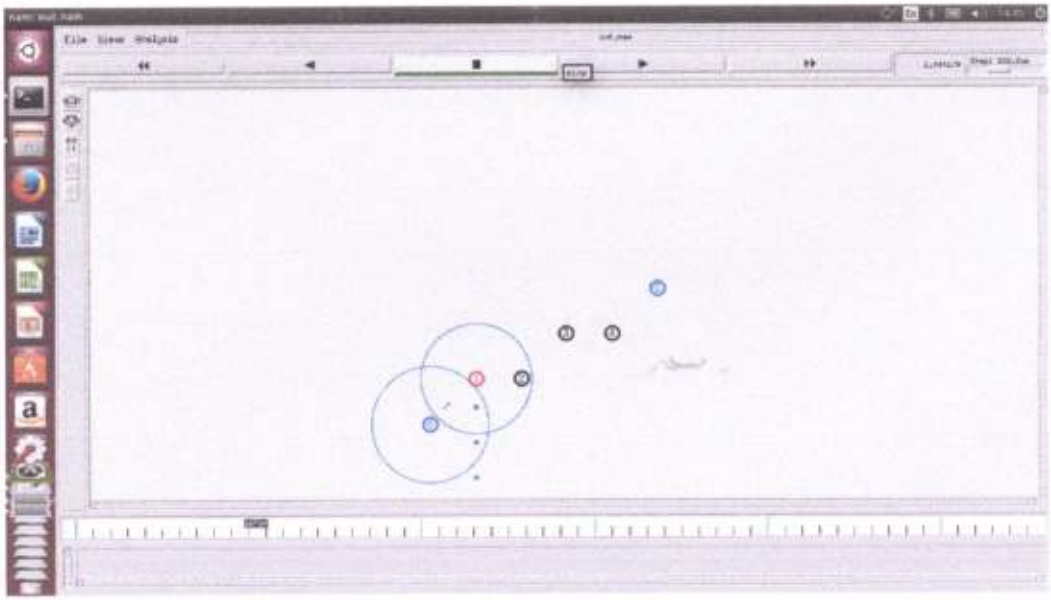

Fig.6.2 Simulated Network with malicious node

The simulated network in the above fig.6.2 generates a malicious node (node 1). Here, the data packets sent from the source node are dropped, since it is attacked by the malicious node which is not further sent to its neighbour nodes. The malicious node simply drops the data packet instead of sending it to its neighbour nodes.

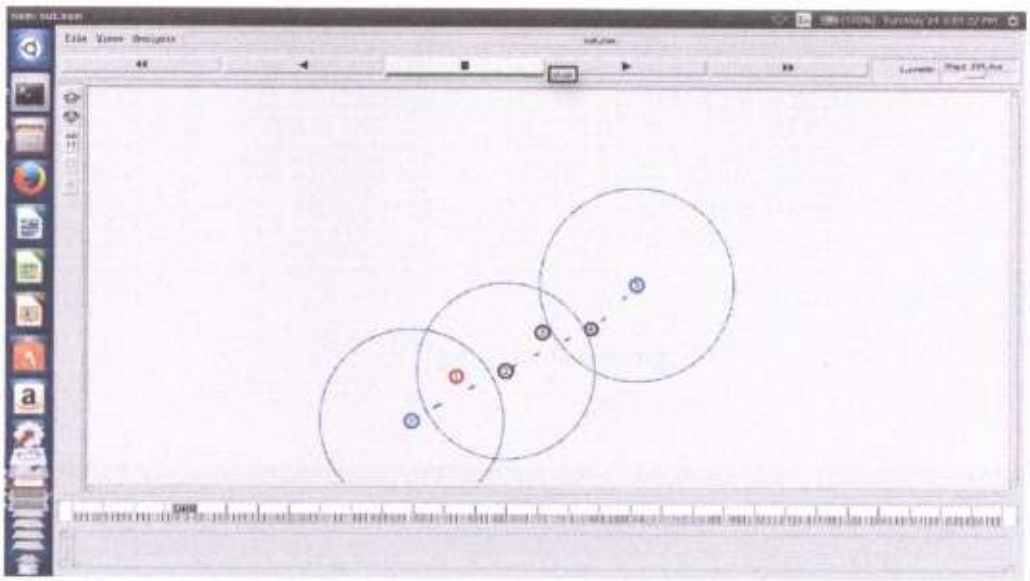

Fig.6.3. Modified Simulated Network with packet transmission.

The simulated network in the above fig.6.3 shows that the data packet sent from the source node is delivered to its neighbour nodes and so on till the destination(node 5) is reached. This results that the packet sent from the source node is successfully received by the destination node without dropping of the data packets.

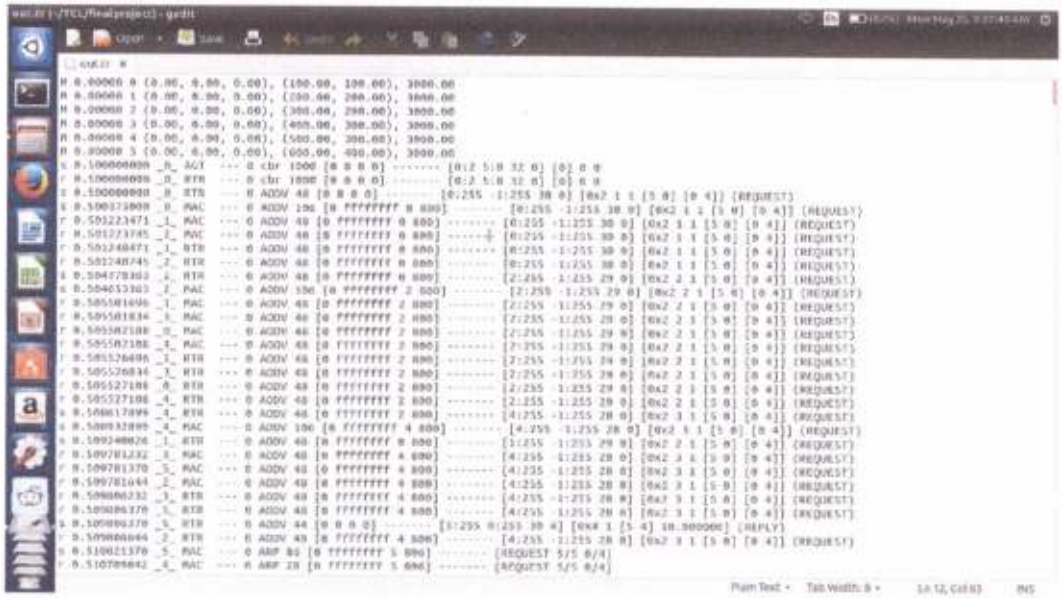

Fig.6.4 The trace format

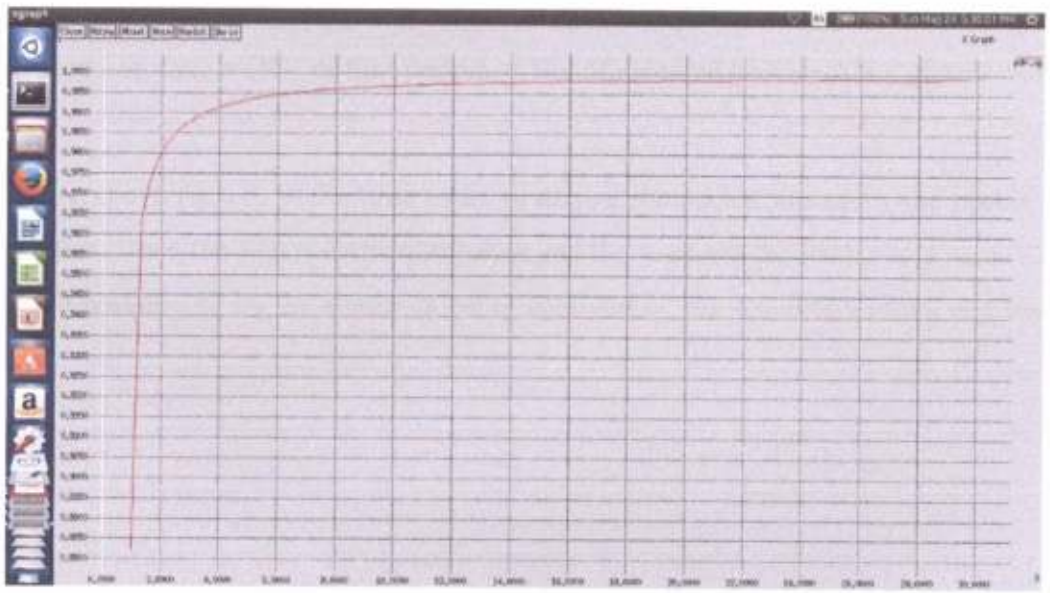

Fig.6.5 Packet delivery ratio.

Packet delivery ratio can be calculated as:

Packet delivery ratio = (Total packet received by all destination node / total packet sent by source node)

In the above fig.6.5, the x-axis is considered as time taken to deliver the packet and the y-axis is the Packet delivery ratio. Thus, we can say that the more time taken to deliver the data packet the higher is the packet delivery ratio.

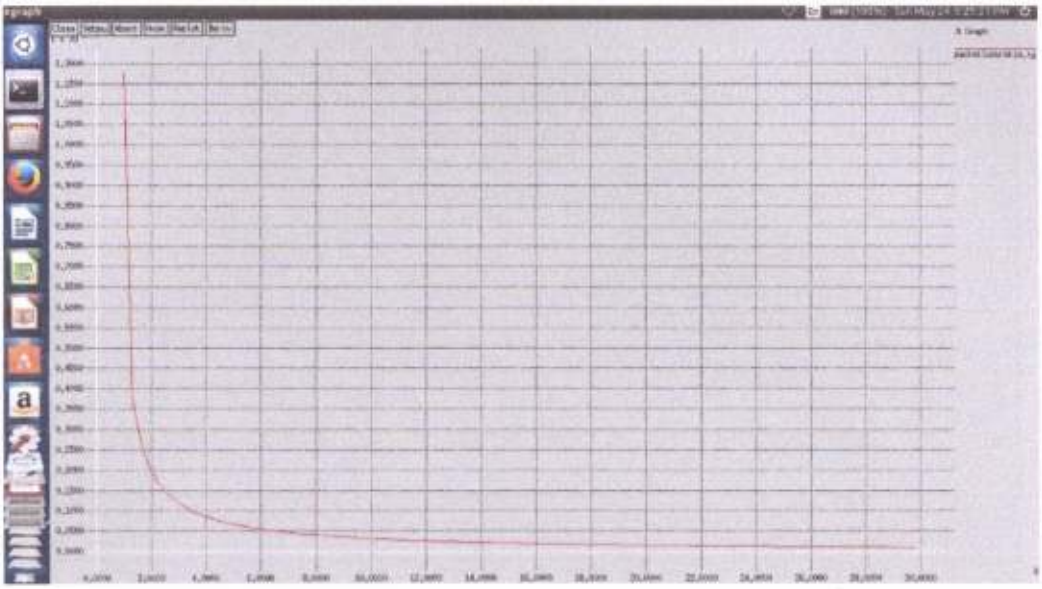

Fig.6.6 packet loss ratio

Packet loss is calculated as,

Packet loss ratio = (No. of sent packets – No. of received packets)/(No. of sent packets * 100)

In the above fig.6.6, as the time taken to deliver the packet increases, the packet loss ratio decreases. Here, the x-axis is the time taken and the y-axis is the Packet loss ratio. Thus, that the data packet sent by the sender is being received by the receiver without any loss of packets.

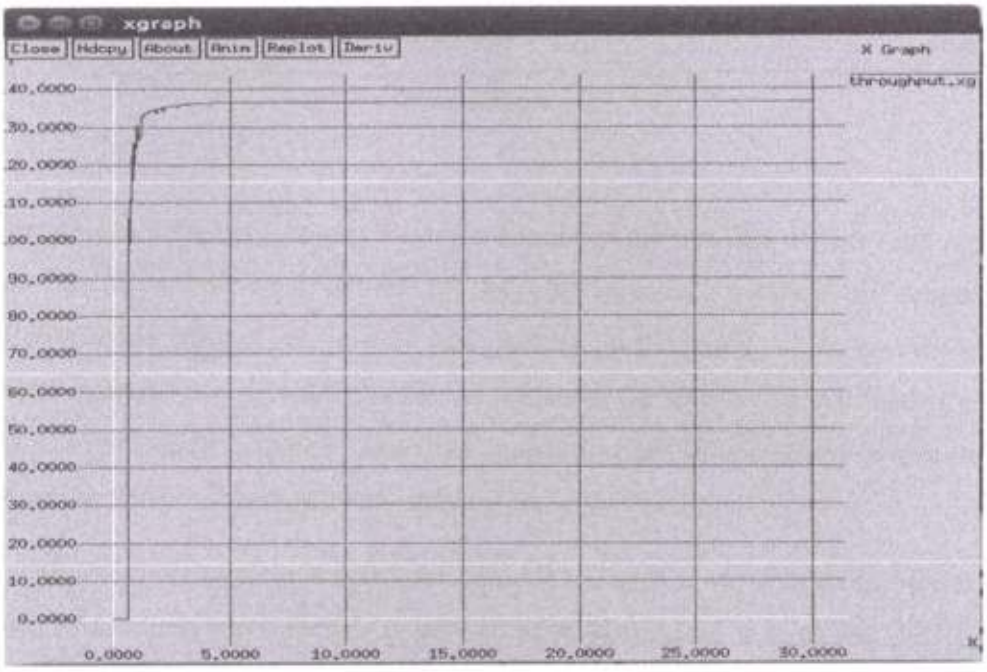

Fig.6.7 Simulated Throughput

Throughput is the ratio of the total amount of data that a receiver receives from sender to a time it takes for receiver to get the last packet. In the above fig.6.7, x-axis represents the time and y-axis represents the throughput. So, the throughput increases as the time increases.

6.3. Advantages of Proposed Work

- It does not require any special hardware such as directional antenna.
- It does not require clock synchronization and positioning system.

Chapter 7

Conclusion

After analysing the performance from the simulated data, packet delivery ratio, packet loss ratio, and the throughput we found that the data packet sent from a particular source node to its destination node without any loss of data packets. In this paper we have analysed the security threats in an Ad-hoc network phases and presented the security objectives that need to be achieved. On one hand the security sensitive applications of ad-hoc networks require high degree of security, and are inherently vulnerable to security attacks.

The attacks by the malicious nodes are powerful in such a way that it can be easily set up in mobile ad-hoc networks. In this paper we have introduced a modified detection of malicious nodes using AODV protocol in wireless ad-hoc networks. The performance of this method is simulated using Ns2-Simulator.

Chapter 8

Future Scope

There are certain different attacks in Mobile Ad-hoc Network that can generate a multiple malicious nodes and attack the network. The attacks can be Wormhole attack, Blackhole attack, Greyhole attack and Sinkhole attack. Our detection method is mainly based on the delay per hop values between normal paths and the paths under attack. For this reason, since the modified detection method does not work well when all the paths are attack affected.

So, our future work is to detect the attacks generated with multiple malicious nodes, such as wormhole attacks and enhance our modified detection method to remove this situation.

References:-

[1] L. Hu and D. Evans, "Using Directional Antennas To Prevent Wormhole Attacks" in Network and Distributed System Security Symposium, pp. 131-141, 2004

[2] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multi-hop Wireless networks".

[3] Y Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks": MobiCom'2000, Boston, Massachusetts, Aug. 6-11, 2000, pp. 275 - 283.

[4] I Khalil, S Bagchi, and NB Shroff," LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multi-hop Wireless Networks", in the International Conference on Dependable System and Networks (DSN), pp. 612-621, 2005.

[5] C. E. Perkins, E. M. Royer, I. D. Chakeres, "Ad hoc On-Demand Distance Vector (AODV) Routing Protocol", draft-perkins-manet-aodvbis-00.txt, October 2003.

[6] S. R. Das, R. Castaneda, J. Yan, R. Sengupta, "Comparative Performance Evaluation of Routing Protocols for Mobile Ad hoc Networks", Proceedings of the International Conference on Computer Communications and Networks, pp.153-161, 1998.

[7] Md. Mahbubul Alam, and Tanmoon Taz Shetu, "Congestion control in Mobile Ad-hoc Networks (MANET)".

[8] A.Agarwal, A.Bar-noy, D.Coppersmith, R.Ramaswami, B.Schierber, and M.Sudan., "Efficient routing in optical networks," Journal of the ACM, 43(6).

[9] L. Breslau et al., "Advances in network simulation," IEEE Computer, 33(5):59-67, May 2000.

[10] Aditya Bakshi, A.K.Sharma, Atul Mishra, "Significance of Mobile Ad-Hoc Networks (MANET)"

[11] Mehdi Medadian, M.H. Yektaie and A.M.Rahmani, " Combat with Black Hole Atta in AODV routing protocol in MANET", First Asian Himalayas International Conference on Internet (AH-IC12009), 3-5th Nov, 2009.

[12] NS-2 tutorials on Youtube.

[13] Google forums on NS-2.