A
Dissertation
On

Generic Framework and Mitigation Algorithm against Black hole attack for AODV Routing Protocol in MANET

Submitted in Partial Fulfillment of the Requirement

For the Award of the Degree of

Master of Technology

In

Computer Science & Engineering

Submitted By

Anishi Gupta

University Roll No. 2K12/CSE/03

Under the Esteemed Guidance of

Prof. Daya Gupta

Professor and Former HoD, Computer Engineering Department,

DTU, Delhi

2012-2014

DELHI TECHNOLOGICAL UNIVERSITY

DELHI – 110042

Department of Computer Engineering
Delhi Technological University
Delhi-110042
www.dce.edu

CERTIFICATE

This is to certify that the dissertation titled "**Generic Framework and Mitigation Algorithm against Black hole attack for AODV Routing Protocol in MANET**" is a bonafide record of work done at **Delhi Technological University** by **Anishi Gupta, Roll No. 2K12/CSE/03** for partial fulfillment of the requirements for the degree of Master of Technology in Computer Science & Engineering. This project was carried out under my supervision and has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma to the best of my knowledge and belief.

Dr.(Mrs.) Daya Gupta
Professor and Former HoD
Department of Computer Engineering
Delhi Technological University

Date: _____

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to all the people who have supported and encouraged me during the course of this project without which, this work could not have been accomplished.

First of all, I am very grateful to my project supervisor Prof. Daya Gupta for providing the opportunity of carrying out this project under her guidance. I am deeply indebted to her for the support, advice and encouragement she provided without which the project could not have been a success. I am also grateful to Dr. Rajeev Kapoor, HoD, Computer Science, Delhi Technological University for his immense support. I am also thankful to my parents for being there for me at all times. Last but not the least; I am grateful to Delhi Technological University for providing the right resources and environment for this work to be carried out.

Anishi Gupta
University Roll no: 2K12/CSE/03
M.Tech (Computer Science & Engineering)
Department of Computer Engineering
Delhi Technological University
Delhi – 110042

ABSTRACT

Ad hoc On Demand Vector (AODV) is a demand driven route protocol in Mobile Ad hoc Network (MANET). Adhoc Network is always constraint about resources and threat from malicious nodes and hence light solution is preferably needed. Moreover AODV is susceptible to many attacks such as black hole, gray hole, worm hole and so on. There is always a security threat in adhoc network.

For this reason**,** in this thesis, we propose a new method **Extended Modified Enhanced AODV (EMEAODV)** which is an extended work of our previous work **Modified Enhanced AODV (MEAODV).** The new proposed method is effective for multiple sessions unlike our previous method. Moreover detection and prevention of black hole attack is done by real time monitoring suspected node by its neighbor node.

The method uses the concept of broadcasting. Monitoring of node which replies to RouteRequest (RREQ) by source is done in promiscuous mode. Malicious node is actually detected by neighbor node of RouteReply (RREP) sender node.

In simulation, new method has shown outstanding results as compared to MEAODV (Modified Enhanced AODV), EAODV (Enhanced AODV), and IAODV (Improved AODV) mitigation methods of AODV routing protocol. We have simulated our proposed method by using different mobility models such as Random Way Point, Manhattan Grid, Random Walk and Gauss Markov model. We have compared our mitigating scheme with different other mitigating schemes and proved that our algorithm is best in term of packet delivery ratio and end to end delay by varying number of nodes, number of malicious nodes, number of TCP connections and mobility speed.

Table of Contents

List of Figures

List of Tables

CHAPTER 1

Introduction

1.1 General Concept

Wireless network provides flexibility to users as, there is no need of a wired connection to extend the network from point A to point B. Traditionally wireless networks have been divided into two categories based on central management unit [1]:

1. infrastructure networks.
2. ad hoc networks.

Infrastructure networks need an access point (AP) for communication. In addition, the connection between the Basic Set Services (BSSs) are organized by the AP (access point) for the use of route when the need arises. However, one main drawback of usage of infrastructure network is the huge amount of overhead for maintaining the routing tables.

A wireless ad hoc network on the other hand, does not support any centralized management facility. The network is named ad hoc because it does not depend on any preexisting infrastructure. Ad Hoc networks do not have a fixed topology or a central management point. Therefore, sending and receiving packets sending and receiving are more complicated to handle than that of infrastructure networks. One such wireless ad hoc network is the mobile ad hoc network.

1.1.1 Mobile ad hoc network (MANET)

A MANET (mobile adhoc network) is a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration [2]. The wireless mobile nodes are not regulated by any centralized control like base stations or mobile switching centers. Communication in the network by nodes can be done using multi hop transmission. Further, since MANET is formed in ad hoc manner, all nodes are not in a same communication range. In order to establish communication link, it is necessary to have cooperation amongst the nodes.

Characteristics of Manets are:

1. It has dynamic topology.
2. The links formed and broken with mobility.
3. It has uni-directional links.
4. Resources are constraint such as battery power, wireless transmitter range, and Network partitions.
5. Nodes can perform the roles of both hosts and routers.
6. There is constraint in bandwidth along with variable link capacity.
7. There is energy-constrained Operation.
8. Threats to physical security.
9. Routing updates are quite frequent.

Numerous routing protocols are used for communication between nodes in the mobile adhoc network. The routing protocols are classified as follows:

1) Proactive Routing Protocols.

2) Reactive Routing Protocols

3) Hybrid Routing Protocols

Proactive routing protocols are also known as table driven routing protocols. In this every node has to maintain routing table in which information about the network topology is being contained even without requiring it. This feature although useful for datagram traffic, incurs substantial signaling traffic and power consumption [3].

Reactive routing protocol is also named as demand routing protocol. In this protocol whenever there is a need of route between source and destination, source node initiates route discovery on demand basis.

A hybrid protocol is developed for overcoming the shortcomings of both proactive and reactive routing protocols. There is a trade-off between proactive and reactive protocols. There is a large amount of overhead and less latency in proactive protocols while more

latency and less overhead is being occurred in reactive protocols. Hybrid protocol uses the route discovery approach of reactive protocol and the mechanism of table maintenance in proactive protocol so that latency and overhead problems can be avoided in the network. Hybrid protocol is best suitable for large networks having a large numbers of nodes.

Mobile ad hoc networks are more vulnerable to threats than the traditional wired networks [4].Thus maintaining security is very tedious in mobile ad hoc network when compared to wired network. Some vulnerabilities that exist in the wireless ad hoc networks are lack of secure boundaries, threats from compromised nodes inside the network, lack of centralized management facility, restricted power supply and scalability.

Wireless adhoc networks are also susceptible to various attacks such as:

1. *Passive Eavesdropping* - An attacker can judge the activity of the network by listening into the network. In order to draw inference about the network topology, nodes first listens to control messages in order to understand the topology of nodes and how they are communicating with each other. Therefore, it can gather useful information about the network before attacking into the network.

2. *Selective Existence (Selfish Nodes)* - This malicious node due to its selfishness characteristics gets the name of *selfish node* where it does not participate in the operations related to the network, moreover it uses the network for its benefits in order to enhance its performance and save its own resource for example power. Therefore these selfish node behaviors are known as *selective existence attacks* [5].

3. *Gray hole attack (Routing Misbehavior)* - Gray hole attack is an active type of attack, which lead to dropping of messages. Victim node initially agrees to forward packets and after that fails to do so. Initially the node behaves correctly and after that it takes control over the route between source and destination by sending false reply to node which initiates RREQ message. Afterwards, the node drops the packets in order to perform a (DoS) denial of service attack.

4. *Black hole attack* – In order to carry out a Black hole attack, malicious node needs to wait for neighboring nodes to send RREQ messages. Whenever the malicious node receiver the RREQ packet, it simply sends a false RREP message without checking its routing table and

giving the illusion of route from source to destination. The malicious node sends the RREP message with high sequence number to settle in the routing table of source node.

5. *Impersonation* – Impersonation is achieved by malicious node by changing the IP address of source node in the control message. Another utility for impersonation is to persuade nodes to change the routing entries in routing tables in order to be pretending as a friendly node, for example attacks against routing table.

6. *Modification Attack* – Modification means that the original message is being altered and does not perform normal functions. Modifying the fields such as hop count, sequence number and time to live in the control messages, malicious node can do the activity of its own attacks.

7. *Attack against the Routing Tables* – This type of attack is attempted by creating a lot of false routing entries for non-existent nodes by using RREQ messages. As a result of which, routing table of the victim node becomes full and does not have enough space to create a new entry.

8. *Sleep Deprivation Torture Attack (Battery Exhaustion)* - Sleep Deprivation Torture is one of the highly damaging denial of service attacks, which adversely affects only nodes which are having highly limited resource. Attacker can cause harm by propagating some control messages through the adhoc network, where other nodes are also interested to take participation. As a result of which other nodes turn into the operation mode from the sleep mode as soon as they get control messages in the network and start processing these useless control packets until their batteries completely dies out.

1.2 Motivation

Mobile ad hoc networks are more vulnerable to threats than the traditional wired networks because the medium of communication is radio waves, and packets are easily trapped. Hence there is always a high possibility of a security threat in wireless adhoc networks. Thus maintaining security is a crucial task in such networks. There are various types of attacks which adversely affect the network. Some of the attacks are black hole, worm hole and so on.

Since black hole attack is easily performed by malicious node, so frequency of occurrences of black hole attack is more as compare to other attacks in adhoc network. Hence it is important to develop protocol and mitigate black hole attack.

Researchers have proposed various protocols such as EAODV, IAODV and OAODV to mitigate against black hole attack. But all of them have some merits and demerits. These protocols are subjected to environment constraints. There is a need to analyze which protocol is best suited one. In order to analyze this, there is a need of generic framework of these protocols. Thesis aims to develop efficient protocols to mitigate Black hole attack in order to choose appropriate protocol for given environment.

1.3 Related Work

H.Weerasinghe and H. Fu [6], in order to keep track of black hole attack use DRI (Data Routing Information) for past routing experience among mobile nodes in the network. The **main drawback** of this technique is that there is need of maintaining an extra database of past routing experiences along with a routine work of maintaining their routing table. It is obvious that by maintaining past routing information there is a lot of wastage of memory space as well as a large amount of processing time is consumed which contributes towards slow data transfer.

The **second drawback** is over consumption of limited bandwidth. Validity of routes is being cross checked which is contained in RREP message by an intermediate node whose implementation is done by sending a FREQ (Further Request) message to the next-hop neighbor of the corresponding intermediate node. The process of sending additional FREQ messages again consumes a large amount of bandwidth from a given limited and valuable resource.

P. Raj and P. Swadas [7], proposed a sufficient solution in which we need to check RREP messages from immediate nodes for various intrusion activities. The main drawback of this technique is that this process takes a significant amount of time in notifying all nodes in a large network along with network overhead that could be caused by ALARM broadcast

message. Moreover it has an advantage of multiple session usage instead of single session usage.

E.A Mary [8] proposed certificate based authentication to mitigate the effect of black hole attack. The drawback of this approach is over consumption of limited bandwidth. In order to maintain certificates of other nodes received by an issuer node an extra database is needed in addition to certificates that is being issued by an issuer node.

Enhance AODV [9] is one of the methods for mitigating black hole attack. It uses Route Discovery Process. The Drawback of this approach is that if multiple reply messages come from the same malicious node, then every time we are using detection method to check for malicious reply. This increases end to end delay.

Intrusion Detection System (IDS) [10] Method uses IDSAODV protocol. The IDSAODV Protocol will check for minimum path to destination having maximum destination sequence number in the RREP packet. The drawback of this approach is that if multiple reply comes again from the same malicious node, then Reply is not discarded, moreover it is being accepted and hence there is no mitigation of black hole effect. This algorithm does not run if multiple reply comes from the same malicious node.

The proposed algorithm Opinion AODV [11] uses two extra field-request weight and reply weight. Request weight in routing table indicates the total number of RREQs that are forwarded by the particular node. In the similar way Reply weight indicates the number of RREPs forwarded. Main drawback of this approach is high control packet overhead due to extra control packets in addition to network overhead because of broadcasting OREQ control packets. Second drawback is that if multiple reply packet come from the same malicious node then every time we are checking for malicious reply. This increases end to end delay. In order to redetect it requires to save the malicious id in the black list.

An inquisition based Detection and Mitigating Techniques of AODV Protocol [12] - The drawback of this method is that this process takes an adequate amount of time in notifying all

nodes for a network having large number of nodes in addition to the network overhead. Moreover extra space is required for maintaining observation table along with black hole table in addition with new fields in the routing table.

The algorithm named IAODV [13] uses the concept of shortest path to destination having less number of hop counts. The main drawback of this approach is that it has large space storage for mitigating black hole effect. It uses Routing table of source node to store id of malicious node. Moreover every time when reply from same or different malicious node comes, then size of routing table of source node gets increases.

1.4 Problem Statement

Normally, wireless communication is susceptible to several attacks more severely as compare to wire line communication. Since some sort of radio frequencies on air is used for communication and packets are easily trapped in wireless networks, hence there is always a security threat in such networks.

Researchers have proposed numerous adaption of AODV protocol suitable for environment. However they suffer from a number of disadvantages listed below.

- In P. Raj and P. Swadas [7] the process increases time for notifying all nodes and cause overhead to network because of ALARM broadcast message
- Enhance AODV [9] increases end to end delay.
- Opinion AODV [11] has high control packet overhead and network overhead because of broadcasting OREQ control Packets.
- IAODV [13] has problem of large space storage for storing id of malicious node.

To overcome some of the problems, there is a need to develop a protocol which works in multiple session and a framework which will guide the user to choose appropriate protocol.

Therefore the problem statement of the thesis is

"**A Generic Framework for mitigating against black hole attack that is efficient in terms of packet delivery ratio, delay and space usage for AODV routing protocol**".

1.5 Scope of thesis

This thesis develops a mitigating framework against black hole attack for safe and guaranteed transfer of data packets between source and destination node. To achieve efficiency following sub problems are attempted.

It emphasizes on the following goals for proposing mitigating framework against black hole attack:

1. A Modified Enhanced AODV (MEAODV) [14] is developed to mitigate black hole effect that is more efficient in terms of packet delivery fraction and end to end delay as compare to EAODV.
2. Further improvement of MEAODV, called EMEAODV to incorporate multiple session.
3. Comparison of protocols mentioned in point 1 and 2 with EAODV and IAODV to prove that Packet Delivery Ratio is high, End-to-end delay is low and it is highly suitable in multiple session environment.
4. A generic framework is drawn for guiding the user to select appropriate aforesaid protocols according to environment.

1.6 Thesis Organization

The rest of thesis is organized into seven chapters as follows:

Chapter 2 which is titled as 'Related work and literature survey' contains classification of routing protocols, introduction of Mobility models for MANETs, Security Issues in MANET, Types of attacks, AODV Routing Protocol, similar work done in the past by different researchers.

Chapter 3 which is titled as '**Modified Enhanced AODV Routing Protocol (MEAODV) against Black hole attack**' presents the mitigation algorithm for mitigating against Black hole effect in aodv routing protocol and this work has been **published in IEEE Conference, 2013**.

Chapter 4 which is titled as '**Extended Modified Enhanced AODV Routing Protocol (EMEAODV) against Black hole attack'** presents the detection and mitigation algorithm in order to counter Black hole attack for multiple session.

Chapter 5 which is being entitled as 'Simulation work and result analysis' shows the comparison of our mitigating scheme with few already proposed mitigating schemes against Black hole attack.

Chapter 6 entitled as 'Generic Framework of Black hole attack on Network layer with different Mobility Models' portraits the general framework use for guiding the user to select appropriate protocol according to application.

Chapter 7 deals with 'Conclusion and future work'.

Lastly 'Publications from the Thesis' is being dealt in chapter 8. This chapter enlists the published and communicated papers. The final conclusion of thesis is drawn by enlisting references throughout our thesis.

CHAPTER 2

Related work and Literature survey

2.1 Classification of routing protocols

Routing protocols define a set of standard which governs the path of data packets from source node to destination node in a network. In MANET, there are various types of routing protocols which are being applied according to the network conditions. Figure 2.1 below shows the general classification of the routing protocols in MANETs [15] and the family tree of adhoc network is shown below in figure 2.2.

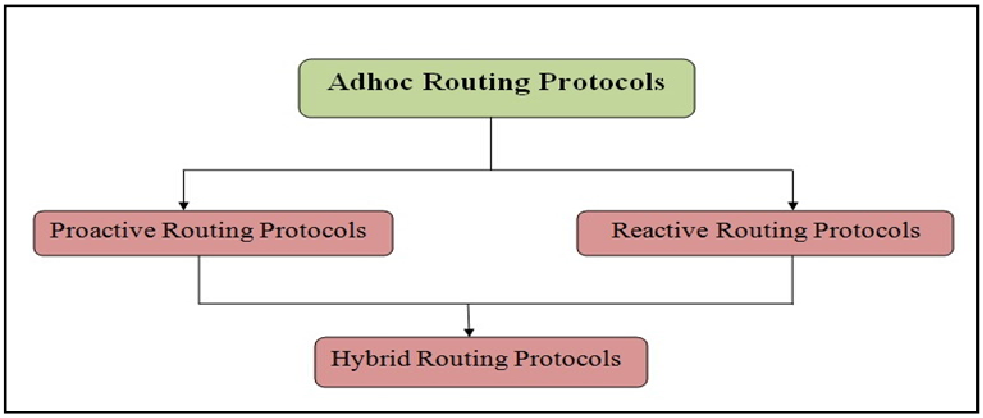

Figure 2.1 Classification of routing protocols

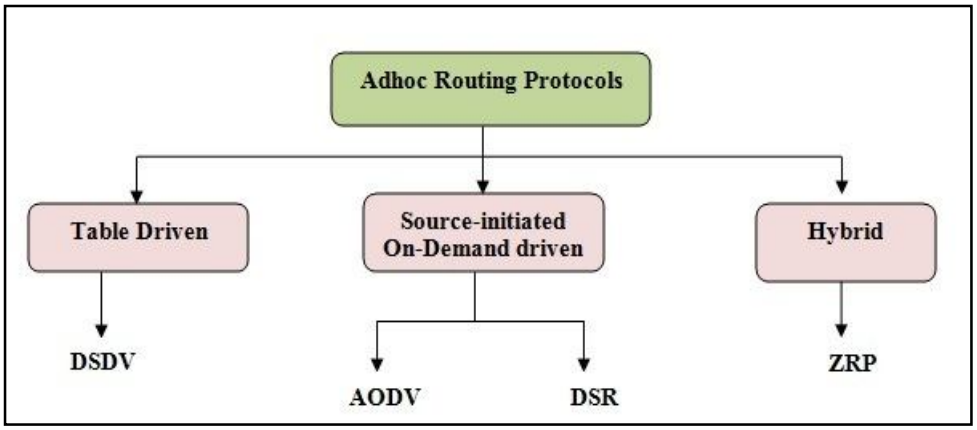

Figure 2.2 Family Tree

2.1.1 Proactive Routing Protocols: Proactive routing protocols are also known as table driven routing protocols. In this every node has to maintain routing table in which information about the network topology is being contained even without requiring it. This feature although useful for datagram traffic, incurs substantial signaling traffic and power consumption [3]. Whenever dynamic topology of network changes, the routing tables are required to update periodically. Proactive protocols are badly suitable for large networks as they require to maintain routing entries for each and every node in the table of every node which are preset in the network. According to different protocols, different number of routing tables are maintained. There are numerous well known proactive routing protocols for example: DSDV, OLSR, WRP etc.

i) Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV) - DSDV is generated by using the concept of Bellman–Ford routing algorithm [16] with few modifications. In this routing protocol, every node in the adhoc network has a routing table. The routing table of each node maintains the list of all present destinations and the number of hops to each of the destination. Each routing entry in the table is tagged with a destination sequence number, which is being produced by the destination node. The routing tables are being updated by periodic transmissions which helps in maintaining the information of dynamic topology of the adhoc network. If any prominent change is found regarding routing information, the updates are immediately transmitted. So, the updates regarding routing information can be either periodic or event driven. DSDV protocol requires that each mobile node in the network must do the advertisement of its own routing table to its current immediate neighbors. Broadcasting or multicasting, both perform advertisement. Due the advertisements, the intermediate nodes come to know about the change which has occurred due to node movement in the adhoc network.

2.1.2 Reactive Routing Protocols: Reactive routing protocol is also named as on demand routing protocol. In this protocol whenever there is a need of route between source and destination, source node initiates route discovery on demand basis. Source node first checks its route cache whether route from source to destination is available or not, if the desired

route is not present then route discovery process is being initiated. For example DSR and AODV.

i) Dynamic Source Routing (DSR)

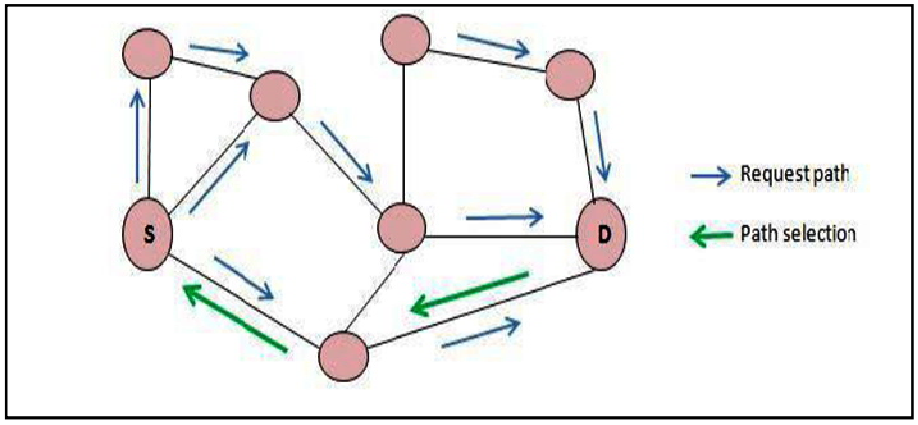

Figure 2.3[17] Dynamic source routing

Dynamic Source Routing (DSR) is a reactive protocol based on the on-demand route discovery process. Dynamic Source Routing (DSR) protocol is based on link state routing. The route from source to destination is being determined by the source node and the address of intermediate nodes which are present in the given route are included in the packet. DSR was designed for multi hop networks for small Diameters as shown in above figure 2.3[17]. It is a beaconless protocol in which no HELLO messages are exchanged between nodes to notify them of their neighbors in the network [18].

ii) Ad Hoc On-Demand Distance Vector Routing (AODV) - AODV is generally an improvement of DSDV. But, AODV is rather a reactive routing protocol instead of proactive. It reduces the number of broadcasts by generating routes on demand process, which is not applicable in DSDV. Whenever a source node wants to communicate with any node present in the network, provided the given source node has no information in its routing table, route discovery process is initiated for packet transmission as shown in figure 2.4. Every node keep track of two values: sequence number of node and a broadcast id. The source node initiates path discovery by broadcasting a route request (RREQ) packet to its neighbors. The neighbor sends a route reply (RREP) back to the source by satisfying the RREQ, or re- broadcasts the

RREQ to its own immediate neighbors after incrementing the hop count. On receiving multiple copies of the same route broadcast packet from various neighbors i.e. when a neighbor node receives a RREQ packet, that is already being received with same broadcast id and source address, it rather drops the redundant RREQ instead of rebroadcasting it. If a node is not able to satisfy the RREQ, it implements the reverse path setup, in addition with forward path setup by keeping track of the following information for the transmission of the RREP.

When the next hop is out of reach, the node upstream of the break broadcasts a RREP with a fresh sequence number (i.e., a sequence number that is one larger than the previously known sequence number) and hop count of one to its active upstream neighboring nodes. These nodes subsequently broadcasts that message to their active immediate neighbors and so on. This process continues until all active source nodes are being notified; it definitely terminates because there are finite number of nodes in the wireless network plus AODV maintains only loop-free routes. Source nodes can restart the route discovery process as soon as they are being notified of a broken link if they still need a route to the same destination.

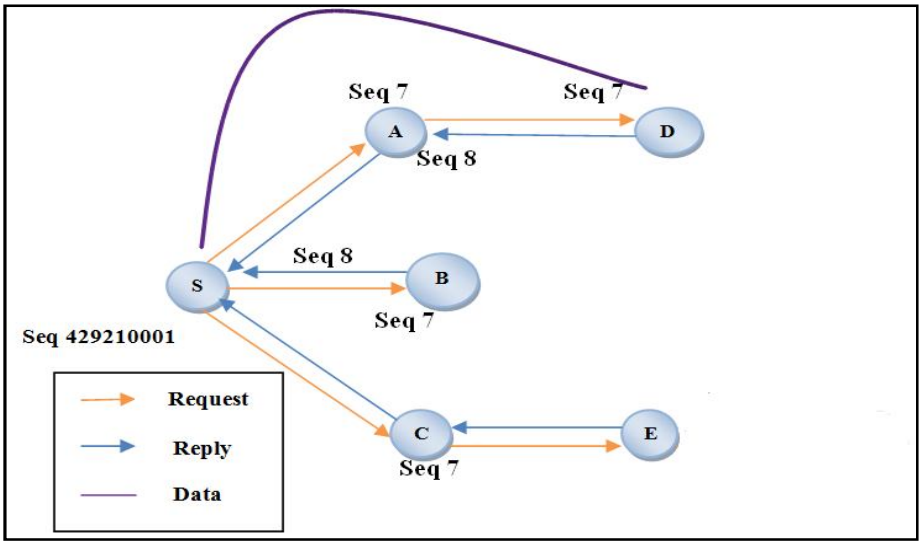

Figure 2.4 Route Discovery Process

2.1.3 Hybrid Routing Protocol: There is a trade-off between proactive and reactive protocols. There is a large amount of overhead and less latency in proactive protocols while more latency and less overhead is being occurred in reactive protocols. So a hybrid protocol is developed for overcoming the shortcomings of both proactive and reactive routing protocols. Hybrid routing protocol combines the concept of both proactive and reactive routing protocol. It uses the route discovery approach of reactive protocol and the mechanism of table maintenance in proactive protocol so that latency and overhead problems can be avoided in the network. Hybrid protocol is best suitable for large networks having a large numbers of nodes. This large network is categorized into set of zones where inside the zone routing is being performed by using reactive approach and reactive approach is used for routing outside the zone. There are numerous of famous hybrid routing protocols in MANET for example ZRP.

i) Zone Routing Protocol (ZRP): ZRP [19] is suitable for wide utility in MANETs, especially for the networks having diversity in mobility patterns. In this protocol, there is maintenance of routes by each node within a local region, which is termed as routing zone. By using a concept of query-reply mechanism, route creation is being done. A node must be aware of its neighbor nodes for creating different zones in the network. A neighbor node is the one which establishes a direct communication from a given node, and that is, it lies within one hop transmission range of a node. Rather than blind broadcasting, query control mechanism is being used by ZRP in order to reduce route query traffic with the help of query source. Query source directs query messages outward and away from covered routing zones. A covered node is a node which lies within the routing zone of a node where that node has received a route query. When the query packet is being forwarded, a node recognizes whether query packet is coming from its intermediate node or not. If yes, then all the known neighboring nodes of that particular node which lies within its same zone as covered are being marked. The query is broadcasted until it reaches the destination node. The destination node sets the reverse path and a reply message is send back and hence the route is being created.

2.2 Mobility models in MANET

The movement pattern of mobile users is being described by mobility model in adhoc network, and it also indicates how the location, velocity and acceleration of mobile users change over time. Since performance of protocol is highly determined by mobility patterns, it is required that the movement pattern of real life applications must be imitated by mobility models in a reasonable way.

There are various models in MANET. Some of them are as follows:

2.2.1 RANDOM-BASED MOBILITY MODELS

In random-based mobility models, there is random and free movement of the mobile nodes without restrictions. To be more precise, we randomly and independently choose the destination, speed and direction of other nodes. This kind of model is widely used for studying many simulations.

The Random Waypoint model is frequently used mobility model, which is being discussed in section 2.1 and then, one variant of the Random Waypoint model, namely the Random Walk model is described in section 2.3

2.2.1.1 Random Waypoint Model

The Random Waypoint Model was first proposed by Johnson and Maltz [20]. Its simplicity and availability characteristics make it as a 'benchmark' for evaluating routing protocols. In order to generate the mobility pattern of the Random Waypoint model the setdest tool can be used. This tool is incorporated in the widely used network simulator ns-2.Moreover the movement of nodes is strongly random as shown in figure 2.5 [21].

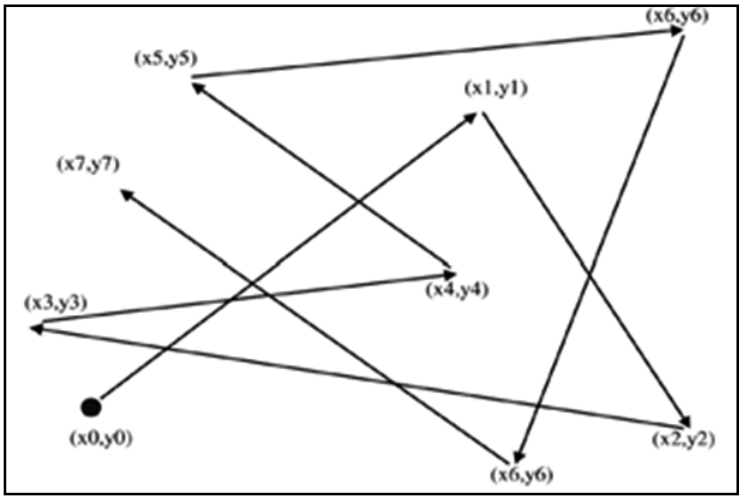

Figure 2.5[21] Example of node movement in the Random Waypoint Model

2.2.1.2 Random Walk Model

The Random Walk model was originally proposed for imitating the unpredictable movement of particles in Physics. Some of the mobile nodes are assumed to have unexpected move, Random Walk mobility model is proposed to mimic their movement behavior [22]. The Random Walk model is quite similar with the Random Waypoint model because the movement of nodes is strongly random in both models. Random Walk model is the specific case of Random Waypoint model having zero pause time.

However, in the Random Walk model, the speed and direction of mobile nodes get change at each time interval.

The Random Walk model is a memory less mobility model where the previous status information is not used for the future reference. In other words we can say, the current velocity is not dependent on its previous velocity and the future velocity is also independent of its current velocity.

2.2.2 MOBILITY MODELS WITH TEMPORAL DEPENDENCY

There is constraint and limitation on the node mobility by the physical laws of acceleration, velocity and rate of change of direction. Therefore, the current velocity of a mobile node may depend on its previous velocity. Thus there is correlation in velocities of single node at

different time slots. We call this type of characteristic of mobile nodes as the Temporal Dependency of velocity.

However, the memory less behavior of Random Walk model, Random Waypoint model and other variants prevents them to capture this temporal dependency behavior. As a result of which, various mobility models possessing temporal dependency are proposed. In Section 3.1 Gauss-Markov Mobility Model is described in details.

2.2.2.1 Gauss-Markov Mobility Model

The Gauss-Markov Mobility Model was first introduced by Liang and Haas [23] and widely utilized [24][22]. In this model, there is correlation between velocity of mobile node over time and modeled as a Gauss-Markov stochastic process.

The relation between the current speed and direction with the previous speed and direction is related in the following equation.

$$s_n = \alpha s_{n-1} + (1-\alpha)\bar{s} + (1-\alpha^2)\sqrt{s}_{Xn-1} \quad (1)$$

$$d_n = \alpha d_{n-1} + (1-\alpha)\bar{d} + (1-\alpha^2)\sqrt{d}_{Xn-1} \quad (2)$$

As sn and dn indicates the speed value and direction value for movement in the period time n. sn-1 and dn- 1 indicates speed value and direction value for movement in the period time n-1. α denotes the constant value in the range [0, 1]. s and d are constant values denoting the mean speed and direction. sX and dX are variables from a Gaussian distribution. The different levels of randomness or degree of random is being represented by single parameter α. The moving behavior of mobile nodes are being effected by degree of random. When we set the value of α to zero, then we get the maximum speed and direction as Sn = S + SX and dn = d + dX. The current speed and direction of each mobile node now becomes independent of its previous speed and direction with a Brownian motion [25]. In the similar way, when we set the value of α to one, we get the minimum speed and direction as sn = Sn-1 and

dn = dn- 1. Therefore, the movement of every mobile node now becomes a linear motion.
The calculation is made regarding destination position of the motion from the following equations.

$$x_n = x_{n-1} + s_{n-1}\cos d_{n-1} \quad (3)$$

$$y_n = y_{n-1} + s_{n-1}\sin d_{n-1} \quad (4)$$

While (xn,yn) and (xn-1,yn-1) indicates the positions of their destinations for the period time n and n- 1, respectively.

2.2.3 MOBILITY MODELS WITH GEOGRAPHIC RESTRICTION

In this section, another limitation of Random Waypoint model is being dealt, it is the unconstraint motion of mobile node. There is free and random movement of mobile nodes in the Random Waypoint model. However, in most real life applications, it is being observed that a movement of node is subject to the environment. In particular, there is always a bound in the motions of vehicles to the freeways and the buildings and other obstacles block pedestrian on the road. Therefore, the Pseudo-random way is defined for nodes to move on specified pathways in the simulation field. This kind of characteristics is being addressed by some recent works and integrate the obstacles into mobility models. We call this kind of mobility model is named as a mobility model with geographic restriction.
We describe one such mobility model, Pathway Mobility Model in the following Section.

2.2.3.1 Pathway Mobility Model

We need to restrict the node movement to the pathways in order to integrate geographic constraints into the mobility model. The map is specified in the simulation field. Tian, Hahner and Becker et al. [26] utilize a random graph to model the map of city. We can either generate this graph randomly or accurately on the basis of certain map of a real city. The buildings of the city are being represented by the vertices of the graph and the streets and freeways between those buildings are being indicated by edges of the graphs.

Initially, there is random placement of the nodes on the edges of the graph. Then destination is chosen randomly for each particular node and by opting shortest path along the edges, the node moves towards this destination node. By arriving at that particular destination, the node pauses there for T time and again a new destination is chosen for the next movement. This procedure is repeated till we reach the end of simulation.

Unlike the Random Waypoint model where there is free movement of nodes, here only pathways are allowed for mobile nodes to travel. However, the choice of the destination node is done randomly, to some extend certain level of randomness still exists in this model. So, in this graph based mobility model, the nodes are meant to travel in a pseudo-random fashion on the pathways.

Similarly, in the Freeway mobility model and Manhattan mobility model, there is restriction in the movement of mobile node to the pathway in the simulation field.
Figure 2.6-2.8[21] illustrates the maps used for Freeway, Manhattan and Pathway models.

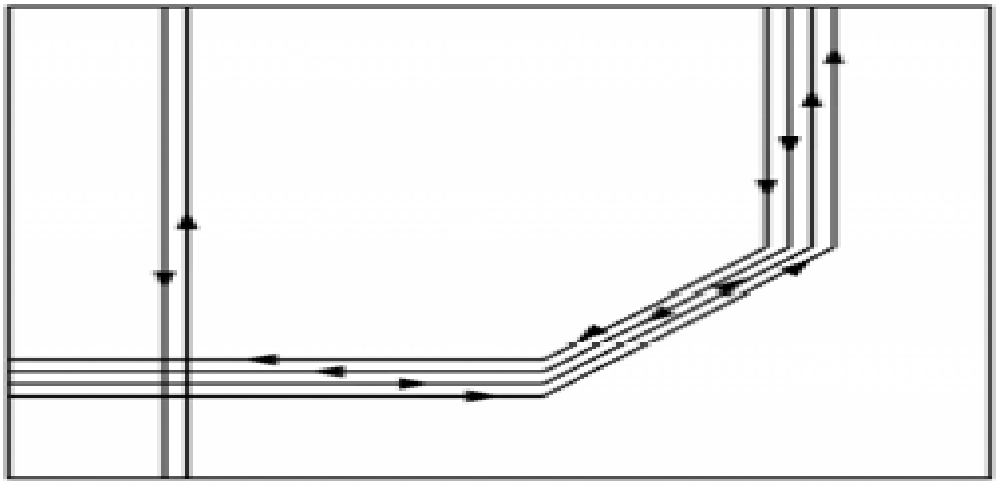

Figure 2.6[21] Freeway Model

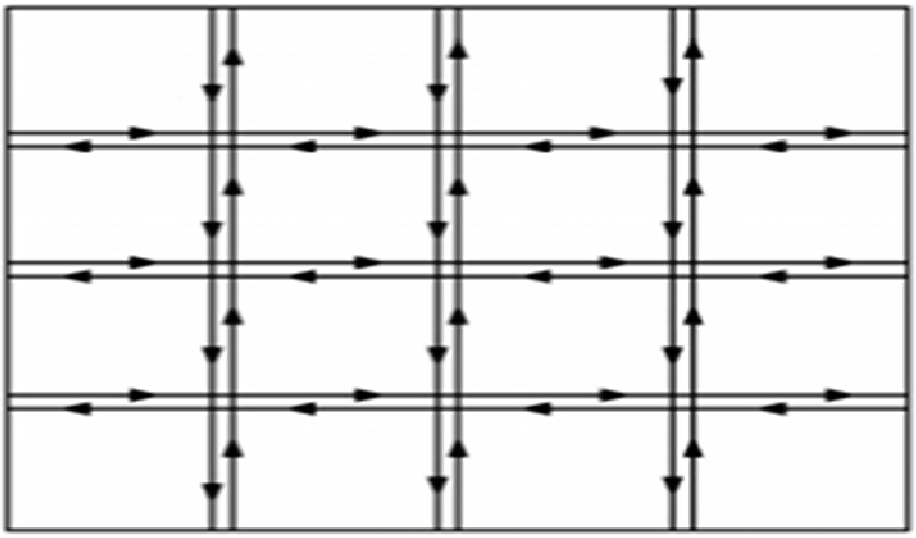

Figure 2.7[21] Manhattan Model

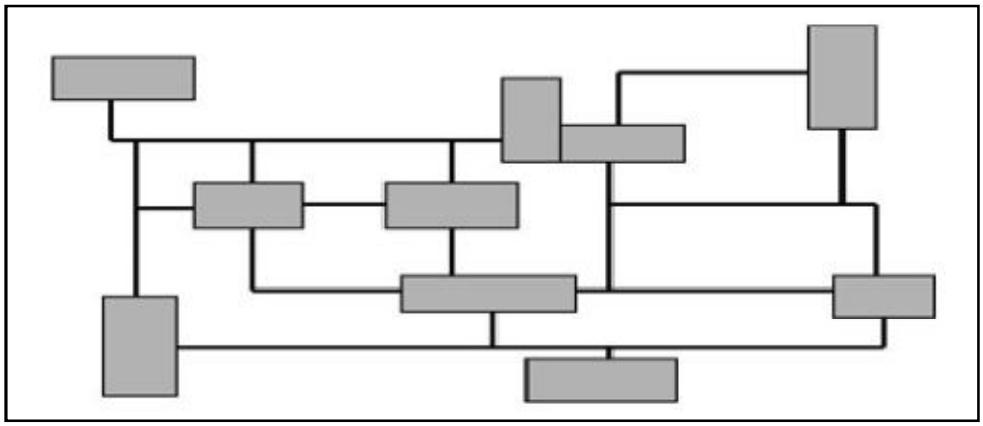

Figure 2.8[21] The pathway graphs used in the Freeway, Manhattan and Pathway Model

2.3 Securities issues in Mobile Ad Hoc Networks

Since mobile ad hoc networks are more vulnerable to threats than the traditional wired networks [4], maintaining security is very tedious task in mobile ad hoc network than in the wired network. In this following section, we discuss the various vulnerabilities that exist in the wireless ad hoc networks.

2.3.1 Lack of Secure *Boundaries*

No clear secure boundary is there in the mobile adhoc network. This vulnerability got its origin from the nature of the wireless network: freedom of joining, leaving and moving inside the network.

In the traditional wired network, opponent must have access to the medium of network physically, or it needs to pass through several defense lines for example firewall and gateway before they can perform intruder behavior to the target nodes. However, in wireless ad hoc network, there is nothing to do with physical access, only opponent is supposed to be in the radio range of other nodes in the wireless network.

By coming into their range, it can easily perform communication with any other nodes in the given range and hence it can join the network automatically. So finally a conclusion is drawn regarding mobile adhoc network that it does not have secure boundaries. Mobile adhoc network is susceptible to various attacks due to lack of secure boundaries.

2.3.2 Threats from Compromised nodes Inside the Network

In the previous subsection, we discuss about the susceptibility that there is lack of secure boundaries in the wireless ad hoc network, which is the basic cause of various link attacks. The main emphasis of these link attacks is on the links between the nodes, and they perform some malicious activity for the destruction of these links.

This vulnerability can be seen as the threats from the compromised nodes inside the wireless network. Since mobile nodes are autonomous devices, they can freely join or leave the network, it is difficult for the mobile nodes to form some effective policy in order to get rid of malicious behavior from all nodes with which it communicate.

Since mobile adhoc network has dynamic topology so a compromised node frequently change its victim node and perform intruder behavior to some other nodes and hence it is difficult to track the intruder activity of compromised node in the adhoc network. Therefore,

threats inside the network from the compromised node are more dangerous than attacks from outside world.

2.3.3 Lack of Centralized Management Facility

There is no centralized facility of management in wireless network which leads to many vulnerable. Lets have a look at this problem in detailed manner.

Firstly it is very difficult to monitor the traffic in highly dynamic topology of adhoc network because of absence of central management unit. Breakage of path, transmission impairments and many more such things happen frequently in the wireless network. Therefore, on changing the attack pattern and victim nodes in different periods of time, detection of malicious failure becomes more difficult task. In case of each victim node which suffers from high failure, it cannot be guaranteed proved that it is because of malicious nodes. However, a system point of view gives a clear picture that the opponent has performed such a high misbehavior though these all illegal actions occur on different nodes at different time. From the above example it is clear that lack of centralized management facility will leads to various problems when it comes for the detection of various attacks in the ad hoc network.

Second, lack of centralized management machinery will impede the trust management for the nodes in the ad hoc network [4].

Third, some algorithms in the wireless ad hoc network depends on the cooperative participation of nodes and the infrastructure. Because of lack of centralized authority the adversary can get benefit from this vulnerability and perform attacks for breaking the cooperative algorithm.

2.3.4 Restricted Power Supply

Due to mobility characteristics of mobile nodes, it is so common that nodes depend on battery as their power supply. While in the wired network, nodes get infinite power supply

from outlets, there is no constraint of power supply in the network.; the nodes in the wireless ad hoc network suffers from the problem of restricted battery power.

The first problem that may be caused by the restricted power supply is denial-of-service attacks. Since the opponent knows that the victim node is power-restricted, so either it sends additional useless packets to victim node or ask victim node to forward those packets to some other nodes or trap victim node in some time-consuming activity. The main aim of these activity is to consume the limited power of nodes in the network.

Moreover, a node in wireless ad hoc network may behave as a selfish node for preserving its own power for its own usage. Selfish node also perform denial of service attack and creates problem when a node needs to cooperate with this selfish node for packet transmission.
Moreover, we should not consider all of the selfish nodes as intruder nodes: some nodes may suffer from restricted power supply problem and thus act in a selfish manner, this activity can be tolerated; however, there may be some node who intentionally pretend that it runs out of power and thus do not willing for cooperation with other nodes for performing some operation, but in actual this node has sufficient battery power for cooperative operation.

Lastly, selfish behaviors should not be regarded as malicious behaviors, but this thing we should know whether selfishness is actually caused by the limited battery power, or intentionally for non-cooperation.

2.3.5 Scalability

Finally, while discussing the vulnerability problem in the adhoc network, we must address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network. Like in the traditional wired network where scale is generally predefined during designing time and will not change much during its usage, the scale of the wireless network keeps changing all the time, the reason being mobile characteristics of the nodes in the mobile ad hoc network, where you can hardly predict how many nodes will be in the network in the future. As a result of which, the protocols and services which are being applied to the ad hoc

network for example routing protocol and key management service, it should have compatibility with the scalability of the ad hoc network. In other words protocols and services have to manage its scalability up and down efficiently.

2.4 Types of Attacks [27, 28]

2.4.1 Passive Eavesdropping

An attacker can judge the activity of the network by listening into the network. In order to draw inference about the network topology, nodes first listens to control messages in order to understand the topology of nodes and how they are communicating with each other. Therefore, it can gather useful information about the network before attacking into the network. Information transmitted in encrypted form can also be listened by a attacker though it must be confidential for upper layer applications.

Eavesdropping is also a threat to location privacy [29]. An intruder node can keep track of adhoc network which exists within an area with the help of detecting the signals. To combat this, various traffic engineering techniques have been proposed.

2.4.2 Selective Existence (Selfish Nodes)

This malicious node due to its selfishness characteristics gets the name of *selfish node* where it does not participate in the operations related to the network, moreover it uses the network for its benefits in order to enhance its performance and save its own resource for example power. Therefore these selfish node behaviors are known as *selective existence attacks* [5].

Selfish nodes do not even send any HELLO messages in the network and drop all packets which are being transmitted to them as along as it is not benefitted from that packets. Whenever a selfish node needs to communicate with other nodes, it initiates a route discovery process and then transmit the desired packets.

When the node feels no need to use the network, it turn back to the “silent mode”. After a while, intermediate nodes invalidate their entries in the routing table to this selfish node and selfish node does not get visible in the network.

Actually packet dropping activity is divided into two category. First category involves the selective dropping of packets and second category involves dropping of packet without looking into their content. In first category, the attacker drop packets of selected nodes. To do this activity, it must look into the content of packet whether it comes from that node or not. This activity involves CPU resource and battery life. Obviously, this is not the desired behavior for selfish nodes because it involves battery life. These types of attackers are not interested in content of the packets if it involves its own resources. So selfish nodes perform second category of attacks. Thus selectively dropping messages is not a selfish node behavior mentioned in [30].

2.4.3 Gray hole attack (Routing Misbehavior)

Gray hole attack is an active type of attack, which lead to dropping of messages. Victim node initially agrees to forward packets and after that fails to do so. Initially the node behaves correctly and after that it takes control over the route between source and destination by sending false reply to node which initiates RREQ message. Afterwards, the node drops the packets in order to perform a (DoS) denial of service attack.

If a neighbor node tries to send packets over victim node which looses the connection to destination node, then they need to discover a route again by broadcasting RREQ messages. Malicious node establishes a route by sending RREP messages. The process goes on until malicious node succeeds in its goal.

2.4.4 Black hole attack

In order to carry out a Black hole attack, malicious node needs to wait for neighboring nodes to send RREQ messages. Whenever the malicious node receiver the RREQ packet, it simply sends a false RREP message without checking its routing table and giving the illusion of

route from source to destination. The malicious node sends the RREP message with high sequence number to settle in the routing table of source node. Source node assumes that route discovery process is completed and it ignore the reply (RREP) messages from other nodes. In this way, malicious get control over the network .On receiving the data packet from source node, instead of forwarding, it simply drops all packets. This is a Black hole attack behavior.

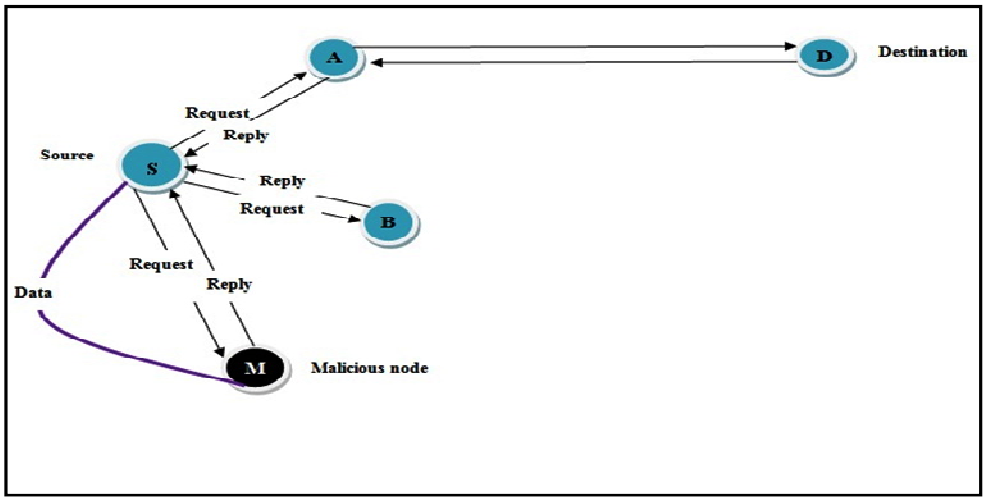

Figure 2.9 Black hole attack

As shown in figure 2.9, a source node S will broadcast the RREQ message to its immediate nodes for route discovery process between node S to the destination node D. A malicious node M is the first node to send a RREP message to the source node S, so it will not check for a fresh route to a destination node D, instead it will send RREP packet to the source node. The source node will accept the RREP message from malicious node and will discard any RREP message from other intermediate node .Moreover the source node will update its routing table for the new route to the destination node S.

Then, the source node will start sending buffered data packets to a malicious node M by getting assured that it will forward to the destination node S. Nevertheless, the malicious node instead of forwarding, will drop all the data packets.

2.4.5 Impersonation

MAC or IP address uniquely identify hosts in the network, the reason being lack of authentication in wireless networks.

These addresses are not sufficient to authenticate the source node. Hence non-repudiation activity is not considered for ad-hoc network protocols. MAC and IP spoofing are the most simplest methods where a node can pretend as another node or node gets hidden in the network. Impersonation is achieved by malicious node by changing the IP address of source node in the control message. Another utility for impersonation is to persuade nodes to change the routing entries in routing tables in order to be pretending as a friendly node, for example attacks against routing table.

One of the interesting impersonations is Man-in-the-middle attack [5]. This attack is performed by combining spoofing and dropping attacks by intruder node. As far as the location of malicious node is considered, it must be placed within the transmission range for destination node, at the centre of the route or victim node must not be notified of any route information to the destination.

With the help of attacks against the routing table, malicious node may also change the routing entries of table of the victim node for redirecting its own packets. At this particular point, malicious node waits for a sender node to send RREQ message to the destination node. When a sender node sends an RREQ message, intruder node instead of forwarding RREQ message to intermediate nodes, simply drops the RREQ and a spoofed RREP message is being replayed to source node pretending to make it come from the destination node. At the same time, malicious node sends a RREQ message to the destination node and the RREP message which comes from the destination node is being dropped. By doing this type of activity; malicious node gets complete control over the communication between source and destination node.

2.4.6 Modification attack

Utility of control messages is to establish the shortest path between two nodes. But by altering the content of control messages (e.g. RREQ, RREP and RERR), malicious nodes can route packets to the desired direction. Modification means that the original message is being altered and does not perform normal functions. Modifying the fields such as hop count, sequence number and time to live in the control messages, malicious node can do the activity of its own attacks.

Impersonation does not come into the category of such kind of attacks; impersonation is only being achieved by modifying source address in order to pretend as other node in the adhoc network. But altering route information in control messages is enacted to misguide the victim or neighbor node and this kind of modification attack is generally performed against the replay messages.

Another attack is enacted by altering destination IP address field in the control message. Hence, messages are not forwarded to desired node and the communication link is broken. Simultaneously the malicious node can forward all messages to the victim node for denial of service (DoS) attack.

2.4.7 Attack against the Routing Tables

In order to find different nodes in the network, every node maintains its own routing table, simultaneously network topology for each and every node is drawn by this routing table for a period of maximum 3 seconds. If this table is being attacked by malicious node, victim nodes are not able to find any route to other nodes with which they want to connect. A new control message is being fabricated for performing attack. Therefore it is also named fabricating attack. There are numerous attacks against routing tables. A false control messages is being fabricated for each kind of attack. For example; to order to attempt for a black hole attack, malicious node sends false RREP message and get control over the path from source to destination.

Another type of attack is attempted by creating a lots of false routing entries for non-existent nodes by using RREQ messages. As a result of which, routing table of the victim node becomes full and does not have enough space to create a new entry. This type of attack is called as routing table overflow.
Network integrity and network topology are being adversely affected by attacks against the routing tables.

2.4.8 Sleep Deprivation Torture attack (Battery Exhaustion)

Most of the techniques are used for maximizing battery life and mobile nodes are willing to retained in sleep mode when they do not perform any action. Sleep Deprivation Torture is one of the highly damaging denial of service attacks, which adversely affects only nodes which are having highly limited resource. Attacker can cause harm by propagating some control messages through the adhoc network, where other nodes are also interested to take participation. As a result of which other nodes turn into the operation mode from the sleep mode as soon as they get control messages in the network and start processing these useless control packets until their batteries completely dies out.

2.5 Adhoc On demand Routing Protocol

AODV, a reactive routing protocol uses a broadcast route discovery mechanism. The protocol operates in two phases: route discovery and route maintenance [17].

2.5.1 Route Discovery

Whenever a source node wants to communicate with any node present in the network, provided the given source node has no information in its routing table, route discovery process is initiated for packet transmission. Every node keep track of two values: sequence number of node and a broadcast id. A route request (RREQ) packet is being broadcasted to its neighbors by a source node, when a route discovery is being initiated by a source node.

The RREQ packet contains the following fields:

< src address; src sequence number; broadcast id; dest address; dest sequence number; hop count> as reflected in table 2.1. The pair < src address; broadcast id > uniquely identifies a RREQ. Every time when the source issues a new RREQ, broadcast id is incremented. The neighbor sends a route reply (RREP) back to the source by satisfying the RREQ, or re-broadcasts the RREQ to its own immediate neighbors after incrementing the hop count. On receiving multiple copies of the same route broadcast packet from various neighbors i.e. when a neighbor node receives a RREQ packet, that is already being received with same broadcast id and source address, it rather drops the redundant RREQ instead of rebroadcasting it. If a node is not able to satisfy the RREQ, it implements the reverse path setup, in addition with forward path setup by keeping track of the following information for the transmission of the RREP

Destination IP address
Source IP address
Broadcast ID
Expiration time for reverse path route entry
Source node's sequence number

Table 2.1 The route request packet

2.5.1.1 Reverse Path Setup

Every RREQ packet contains two sequence numbers (in addition to broadcast id): the sequence number of source and the last known destination sequence number to the source node. The source sequence number maintains freshness information about the re-verse route which comes to the source, and sequence number of destination node signifies the freshness a route to the destination node before that route is accepted by the source node. As the RREQ propagates from a source node to various destination nodes, reverse path from all nodes back to the source node is automatically being set. In setting up the reverse path, when a node receives the copy of the RREQ, it records the address of the neighbor. These entries of reverse path route are maintained for at least sufficient time for the RREQ to propagate the network and generate a reply to the sender.

2.5.1.2 Forward Path Setup

Finally, a RREQ will arrive at a node (most probably the destination itself) that inhibits a current route to the destination. On receiving RREQ, receiving node checks that RREQ over a bi-directional link. If a neighbor node has a route entry for the destined destination, it compares the sequence number of destination in its own route entry table to the destination sequence number in the RREQ. If the RREQ's sequence number for the destination is greater than that present in routing table of intermediate node, the intermediate node must not use its present entry in table to respond to the RREQ. Instead, the neighbor node rebroadcasts the RREQ. The intermediate node can send RREP packet only when sequence number present in the routing table is greater than or equal to that present in RREQ packet. A RREP contains the following information:

<source addr; dest addr; dest sequence #; hop cnt; lifetime >

2.5.2 Route Table Management

The Routing Table entry is shown in table 2.2. The Route table entries also stores useful information in addition with the source and destination sequence numbers, and is called the soft-state associated with the entry. The route request expiration timer is associated with reverse path routing entries. The utility of this timer is to purge reverse path routing entries from those neighbor nodes which do not exist on the path that starts from the source node and ends with destination node. The expiration time totally depends upon the size of the ad- hoc or wireless network. Another important parameter which is associated with routing entries is the route caching timeout, or the time after which the route between source to destination is considered to be invalid. In each routing table entry, the active intermediate nodes which propagate packets for the given destination node and those packets are received by the particular node, address of these active nodes is also maintained. An intermediate node is considered to be active (for that particular destination) if it originates or relays at least one packet for that particular destination node within the most current active timeout period.

A route entry is considered active if it is in use by any active neighbors. (The path from a source node to a destination node having packets propagate through active entries of routing table, is

called an active path). Each time the timeout for the route entry is reset to the current time plus active route timeout, whenever data is transmitted from a source node toward a destination node using route entry.

Destination
Next Hop
Number of hops(metric)
Sequence number for the destination
Active neighbors for this route
Expiration time for the route table entry

Table 2.2 Routing table entry

2.5.3 Route Maintenance

Periodic hello messages detect link failures as well as ensure symmetric links. When the next hop is out of reach, the node upstream of the break broadcasts a RREP with a fresh sequence number (i.e., a sequence number that is one larger than the previously known sequence number) and hop count of one to its active upstream neighboring nodes. These nodes subsequently broadcasts that message to their active immediate neighbors and so on. This process continues until all active source nodes are being notified; it definitely terminates because there are finite number of nodes in the wireless network plus AODV maintains only loop-free routes. Source nodes can restart the route discovery process as soon as they are being notified of a broken link if they still need a route to the same destination as shown in figure 2.10 [17].

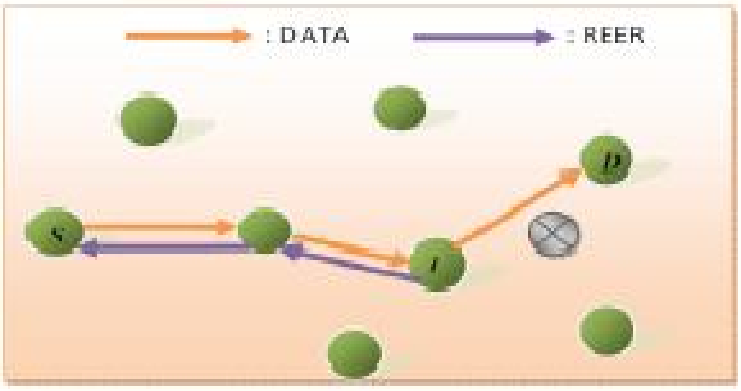

Figure 2.10[17] Route Maintenance Process

2.5.4 Local Connectivity Management

Nodes learn of their neighbors in one of two ways. On receiving a broadcast from a neighbor node, a node updates its local connectivity information to make sure that it includes this neighbor node. In the process that a node was not able to send packets to all of its active downstream intermediate nodes within hello interval, it broadcasts a hello message to its neighbors containing its identity and sequence number.

The sequence number of node is not changed during hello message transmissions. This hello message is retained from rebroadcast out- side the neighborhood of the node because its time to live (TTL) value of 1. Neighbor nodes which receive this packet update their local connectivity information to that particular node. Receiving a broadcast message or a hello message from a new neighbor node, or failing to receive consecutive hello messages from a node which was previously in the neighborhood, is an indication that the local connectivity has changed. No protocol action is triggered when hello messages from inactive neighbor is failed to received.

One of the utility of the local connectivity management with hello messages is that only nodes with bidirectional connectivity are considered to be neighbors. For this purpose, whenever a node sent hello message, it lists the nodes from which it has heard the hello messages. Each node checks to ensure that it uses only routes to neighbor nodes which have heard that particular node's hello message. To save local bandwidth, such type of checking should be performed only if it is being explicitly configured into the nodes.

2.5.5 Working of AODV Protocol

The route from source to destination is found by following method shown in figure as follows:

Step by step explanations of figure 2.11[17] is as follows:

1. Source node ’S’ needs to send data to destination.
2. Node S sends RREQ packet to its neighbors A, B, C.

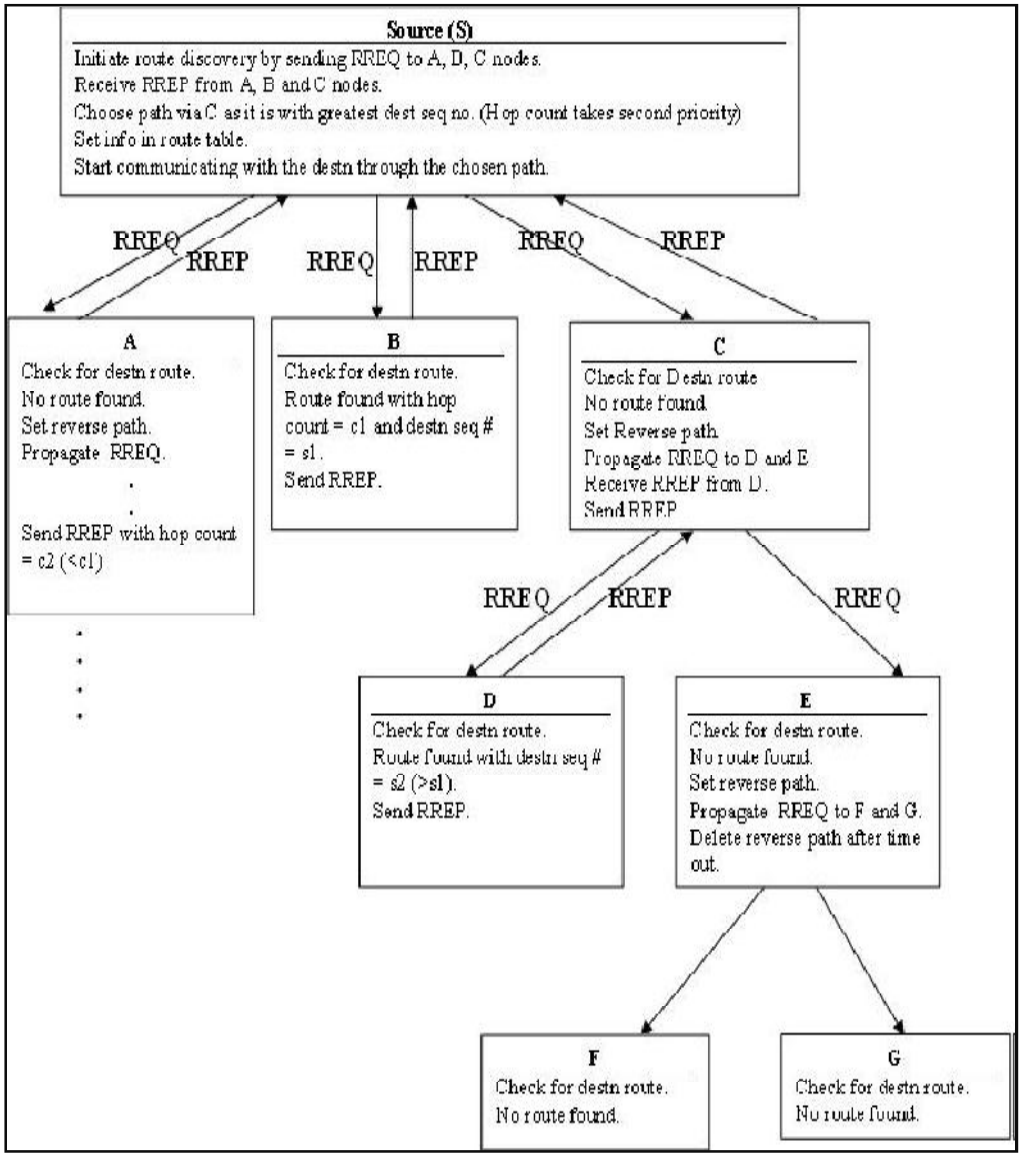

Figure 2.11[17] Working of AODV Protocol

3. On finding the path in its routing table (with destination seq-number s1 and hop count c1) node B sends RREP to S.
4. Node C sets up reverse path.
5. Node C forwards RREQ packet to its neighbor nodes node D and node E.
6. Node E sets up reverse path.
7. Node E forwards RREQ to its neighbors nodes node F and node G.

8. After a time out period E deletes the reverse path when it does not receive any RREPs from node F and node G.
9. On finding the path (with dest seq-number s2 which is greater than s1 and hop count c1) again in its routing table, node D sends RREP to node C.
10. Node C receives RREP from node D and sets up forward path and forwards RREP to node S.
11. Node A by looking into its routing table finds that it has no route to destination, sets its reverse path and forwards RREQ packets to its neighbors; receives RREP (with path having hop count c2 which is greater than c1); again sets forward path on receiving RREP; and forwards this RREP to S.
12. Node S receives multiple RREP packets as one RREP from node C (with destn seq-number s2 and hop count c1), another RREP from node B (with destn seq-number s1 and hop count c1), and another RREP from node A (with destn seq-number x which is less than s1 and s2 and hop count c2 which is less than c1).
13. Node S chooses RREP from node C (which was originated from node D), because it provides first priority of highest destination sequence number and then second priority of smallest hop count. Though RREP from node A has smallest hop count, it is neglected because the sequence number of destination node is greater than RREP from node C.

2.6 Literature survey

Many techniques have been proposed by researcher to prevent black hole attack.

H.Weerasinghe and H. Fu [6], use DRI (Data Routing Information) in order to keep track of past routing experience among mobile nodes in the network .The crosschecking of RREP messages is also done from intermediate nodes by source nodes. The **main drawback** of this technique is that there is need of maintaining an extra database of past routing experiences along with a routine work of maintaining their routing table. It is obvious that by maintaining past routing information there is a lot of wastage of memory space as well as a large amount of processing time is consumed which contributes towards slow data transfer.

The **second drawback** is over consumption of limited bandwidth. Validity of routes is being cross checked which is contained in RREP message by an intermediate node whose implementation is done by sending a FREQ (Further Request) message to the next-hop neighbor of the corresponding intermediate node. The process of sending additional FREQ messages again consumes a large amount of bandwidth from a given limited and valuable resource.

P. Raj and P. Swadas [7], proposed a sufficient solution in which we need to check RREP messages from immediate nodes for various intrusion activities. This technique uses the concept of cooperation between intermediate nodes. If a node discovers a packet drop activity by an intruder, the discovering node notifies all other immediate nodes which are in transmission range of each other about the presence of an attack by broadcasting an ALARM message. The main drawback of this technique is that this process takes a significant amount of time in notifying all nodes in a large network along with network overhead that could be caused by ALARM broadcast message. Moreover it has an advantage of multiple session usage instead of single session usage.

E.A Mary [8] proposed certificate based authentication to mitigate the effect of black hole attack. Every node which is coming in the vicinity of network has to prove its identity and need to fetch a certificate from its neighboring node. Each issuing certificate has a limited validity period and contains the time of issue and expiration time as certificate fields. Before an expiration of the issued certificate, the issuer issues same certificate with an updated version having extended time of expiry if the issuer node is still satisfied with the security level of the concerned node. All intermediate nodes in the network are trusted through the previous certificates in the path of network. The public key of the destination is being contained in the last certificate. If certificates are found to be wrong which is issued by a node, then that node is assumed to be malicious. The drawback of this approach is over consumption of limited bandwidth. In order to maintain certificates of other nodes received by an issuer node an extra database is needed in addition to certificates that is being issued by an issuer node.

Enhance AODV (EAODV) Method [9] - Enhance AODV is one of the methods for mitigating black hole attack. It uses Route Discovery Process. In this method reply table is used to store source IP address of reply packet. Then, detection for malicious reply is being checked and node id of malicious node is saved in malicious list. rt-update parameter provides control over the packets. This method provides better Performance Delivery Ratio as compare to ERDA method. The Drawback of this approach is that if multiple reply messages come from the same malicious node, then every time we are using detection method to check for malicious reply. This increases end to end delay.

Intrusion Detection System (IDS) Method [10] - In this approach, it is assumed that first reply comes from the malicious node itself. When RREQ packet is being received by a malicious node, it immediately sends RREP packet pretending to have fresh enough path to the destination. The IDSAODV Protocol will check for minimum path to destination having maximum destination sequence number in the RREP packet. It will discard the first RREP packet from malicious node and will choose second RREP packet from destination node. The IDSAODV Protocol will initiate route discovery process for another path to destination, other than intruder path.

Advantage of this method is Performance Delivery Ratio of IDSAODV method is much better than that of AODV method. The drawback of this approach is that if multiple reply comes again from the same malicious node, then Reply is not discarded, moreover it is being accepted and hence there is no mitigation of black hole effect. This algorithm does not run if multiple reply comes from the same malicious node.

Opinion AODV (OAODV) Method [11] - The proposed algorithm (Opinion AODV) uses two extra field-request weight and reply weight. Request weight in routing table indicates the total number of RREQs that are forwarded by the particular node. In the similar way Reply weight indicates the number of RREPs forwarded. Proposed method has two modules-updating request/reply weights and collecting feedback. Moreover two extra control packets are used such as OREQ (opinion request) and OREP (opinion reply) for mitigating black hole effect. Each time when reply is received, ratio of request weight and reply weight is

calculated. When the ratio is very less, node from which reply comes is considered to be malicious. Main drawback of this approach is high control packet overhead due to extra control packets in addition to network overhead because of broadcasting OREQ control packets. Second drawback is that if multiple reply packet come from the same malicious node then every time we are checking for malicious reply. This increases end to end delay. Instead of detecting again, we should save the malicious id in the black list. Advantage of this approach is that it does not use any extra space for maintaining blacklist.

An inquisition based Detection and Mitigating Techniques of AODV Protocol [12] - In normal AODV protocol, the node on receiving the RREP packet, checks the value of sequence number of packet in the routing table and accepts if it has a higher seq_no of RREP packet than the one present in the routing table. Extra technique has been added for checking whether the seq_no of RREP packet is higher than the threshold value (A value that is dynamically updated in time intervals) or not. The moment the value of RREP seq_no is found to be higher than the calculated threshold value, the node is suspected to be malicious and it is added to the Observation List with the status field Su. The threshold value is keep on dynamically updating using the data collected in the time interval. This case will detect black hole attack only if it is in form of Single black hole attack rather than multiple black hole attack. It provides better PDF as compare to that of AODV under black hole attack. The drawback of this method is that this process takes an adequate amount of time in notifying all nodes for a network having large number of nodes in addition to the network overhead. Moreover extra space is required for maintaining observation table along with black hole table in addition with new fields in the routing table.

Improved AODV method [13] - The algorithm named IAODV uses the concept of shortest and next shortest path based on the number of hops to destination having less number of hop counts. The main drawback of this approach is that it has large space storage for mitigating black hole effect. It uses Routing table of source node to store id of malicious node. Moreover every time when reply from same or different malicious node comes, then size of routing table of source node gets tremendously increase.

The tabular representation of similar work contribution by few authors is portrayed below in table 2.3.

Algorithms	Author/Authors	Technique used	Merits	Demerits	Session Usage
Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks [6]	Hesiri Weerasinghe and Huirong Fu	Including the address of the next hop node in RREP Packet ,use the concept of DRI(Data routing information)	better throughput rate and minimum packet loss percentage	wastage of memory space as well as a large amount of processing time. Network overhead	Single session
DPRAODV (Detection, Prevention and Reactive AODV) [7]	P. Raj and P. Swedes	Packet drop activity	Multiple session usage	Network overhead by broadcasting ALARM message	Multiple session
Black Hole Attack Prevention in Multicast Routing Protocols [8]	E. A .Mary Anita, V. Vasudevan	certificate based authentication	Authentication is also being checked	over consumption of limited bandwidth in addition of maintaining extra database for certificates	Single session
EAODV(Enhanced AODV) algorithm [9]	Zaid Ahmad, Kamarularifin Abd., and JalilJamalul-lail Ab Manan	Mitigation during Route Discovery Process by using rt_upd parameter	Low network overhead	Single connection/session usage	Single session
IDSAODV(Intrusion Detection Sytem)AODV [10]	Ranjeet Suryawanshi, Sunil Tamhankar	Highest Destination Sequence number	Low network overhead	Single session usage in addition to work for only single reply from malicious node. Fails to work for multiple reply from malicious node.	Single session
OAODV(Opinion AODV) [11]	Rajesh Yerneni, and Anil k. Sarje	Extra control packets-OREQ and OREP along with two extra fields as request weight and reply weight in the routing protocol	Efficient in terms of Packet delivery ratio as compare to normal AODV susceptible to attack	High control packet overhead, high network overhead in addition to single session usage.	Single session
An inquisition based Detection and Mitigating Techniques [12]	Vrutik Shah, and Nilesh Modi	Threshold based detection and mitigation	Efficient in terms of Packet delivery ratio as compare to normal AODV susceptible to attack	Network overhead along with maintenance of extra space for making observation table	Single session
Improved AODV [13]	Jaspal Kumar, M. Kulkarni, Daya Gupta	shortest and next shortest path based on the number of hops	Efficient to work in multiple session environment	Extra space is required to mitigate against Black hole effect	Multiple session

Table 2.3 Representation of similar work contribution by few authors

CHAPTER 3

Modified Enhanced AODV (MEAODV) against Black hole attack

The MEAODV [14] is an enhancement of EAODV [9] routing protocol, which provides better Packet Delivery Ratio and low end to end delay as compare to EAODV method against black hole attack.

In MEAODV, there is a revision of logic as described in EAODV but with few different condition parameters for checking the RREP message for better route discovery mechanism.

The MEAODV method works similar to EAODV method except redundancy in the process of detecting malicious node is prevented. The MEAODV, by getting rt-modify parameter "false" exhibits a detection of malicious node only when malicious node has not previously send the RREP message (malicious node is not already present in intrud_list). If malicious node is already present in intrud_list, there is no need to detect for malicious node, simply a packet of malicious node is dropped. Moreover, in the previous EAODV work, when rt-modify parameter is "false", there is always a check on malicious node. This is done by detecting malicious node, even if it is already present on intrud_list. So this kind of redundancy is also prevented in the propose work named MEAODV.

As there is a need of an improved and efficient protocol in terms of packet delivery ratio, so in order to achieve this goal we adopt a strategy for detecting and mitigating against black hole attack which is stated below:

3.1 Approach for detecting against Black hole effect

In order for detection against black hole attack, packet drop ratio is used. If packet drop ratio is found to be 1 then node is considered to be malicious and it is being discarded from the network.

3.2 Approach for mitigation against Black hole effect

In order to mitigate against Black hole attack, *rt_modify* variable is used. Depending on the value of rt_modify variable, detection process takes place. If rt_modify parameter is set to false then node sending packets is being checked for malicious activity and finally if node comes out to be malicious then its id is saved intruder list and that particular node is discarded from the network.

3.3 Mitigating Algorithm against Black hole attack

The code of MEAODV method is as follows:

```
Modified Enhance AODV
1. RecvReply(Packet P){
2. Save P.srcIPadd and P.ds_seqno to rreply_table
3.  if(rt_modify is false){
4.          if(P.srcIPadd in intrud_list){
5.                          Drop packet P
6.                          flush rreply_table
7.                                  return}
8.          else{
9.                   if(0<packet drop ratio<1){
10.                          set rt_modify to true}
11.                 else{
12.                     save P.srcIPadd in intrud_list;
13.                     Drop packet P
14.                     flush rreply_table
15.                     return}
16.             }
17.                         }
18.  if(P.dsIPadd not in RT routing table entry)
19.  {
20.     Add P.dsIPadd to RT entry}
```

```
21. Select ds_seqno from RT
22. if(rt_modify and((P is from destination node)
23.     or (P.ds_seqno > RT.ds_seqno)
24.     or(P.ds_seqno= RT.ds_seqno and
25.     P.hopcount < RT.hopcount)))
26.     {
27.         if (P is from destination node)
28.               { set rt_modify to false;
29.                update RT entry with P;
30.             send out data packets in buffer}
31.  else if (intermediate node){forward packet}
32.  else { discard packet}
33.     }
```

The working of MEAODV is as follows:

1. At the beginning, rt_modify parameter is set to “false”.
2. Since malicious node is the first node to reply, so it (M1) will send a RREP message to a sender node S.
3. The ip_address and destination sequence number will be stored in reply table.
4. Since rt_modify parameter is “false”, so detection for malicious node gets started.
5. Since the node is the malicious one, its id is being saved in a intruder list, the RREP packet is dropped, reply table is flushed and recvReply function is returned.
6. Again when a RREP packet is received from destination node D, then also a detection process for malicious node gets started.
7. In the process of detection, Packet Drop Ratio comes out to be less than one, so rt-modify parameter is set to “true”.
8. Now since rt_modify parameter is “true” and a node is destination, we make rt_modify “false”. RT Entry is updated with packet ‘P’ of destination

node and packets are send out in buffer. Hence sender node S updates its routing table with new route information.

9. Now, rt_modify becomes false, any reply message that comes after reply of destination node, will be ignored until the process of isolating malicious node is completed.
Thus this method prevents malicious node from entering routing table.

The MEAODV method behaves differently from EAODV in the following ways:

1. In EAODV method, logic begins with rt_modify parameter initially set to “true”, where as in MEAODV method, rt_modify is initially set to “false”.
2. EAODV initially stored the value of “srcIPadd” and “DSN seq no.” of packet of malicious node which is being overwritten by packet information of destination node; where as, in MEAODV method, packet information of only destination node is stored as shown in figure 3.1 [9] and figure 3.2.

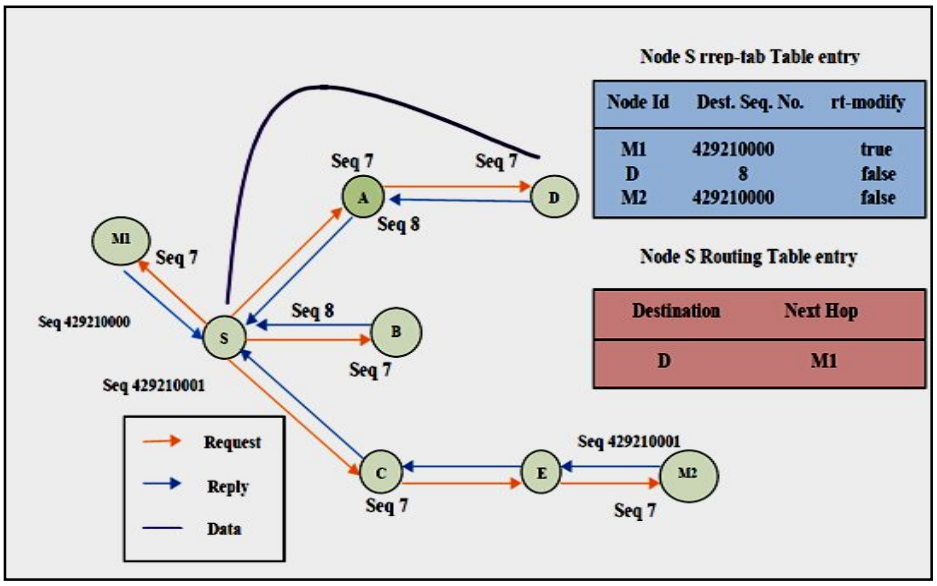

Figure 3.1[9] Route Discovery in the EAODV

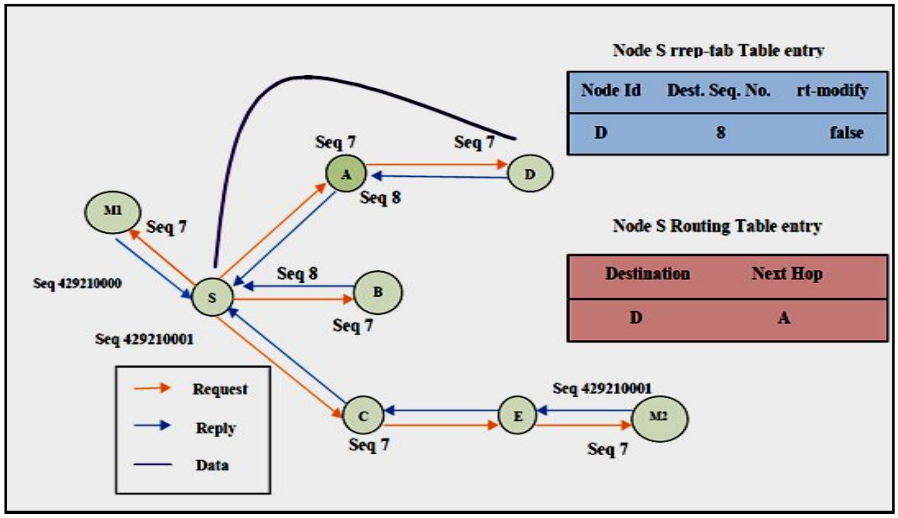

Figure 3.2 Route Discovery in the MEAODV

3.4 Graphs

NS-2.35 is used for simulating purpose. AWK files are used to generate data after analyzing trace files. The results were analyzed by using following three conditions:

1) Normal AODV protocol (without attack)

2) AODV protocol with EAODV method

3) AODV protocol with MEAODV method

Performance Delivery Ratio (PDR) and End-to-End Delay are used as an evaluation metric to measure the performance between MEAODV and EAODV.

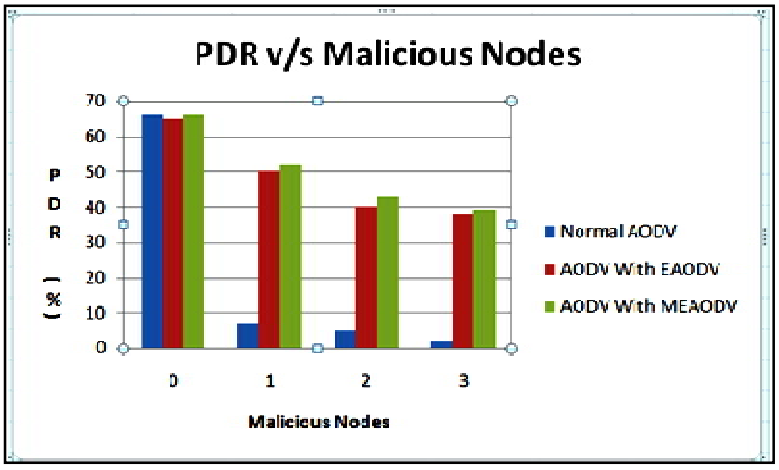

Figure 3.3 Performance Delivery Ratio versus number of malicious nodes

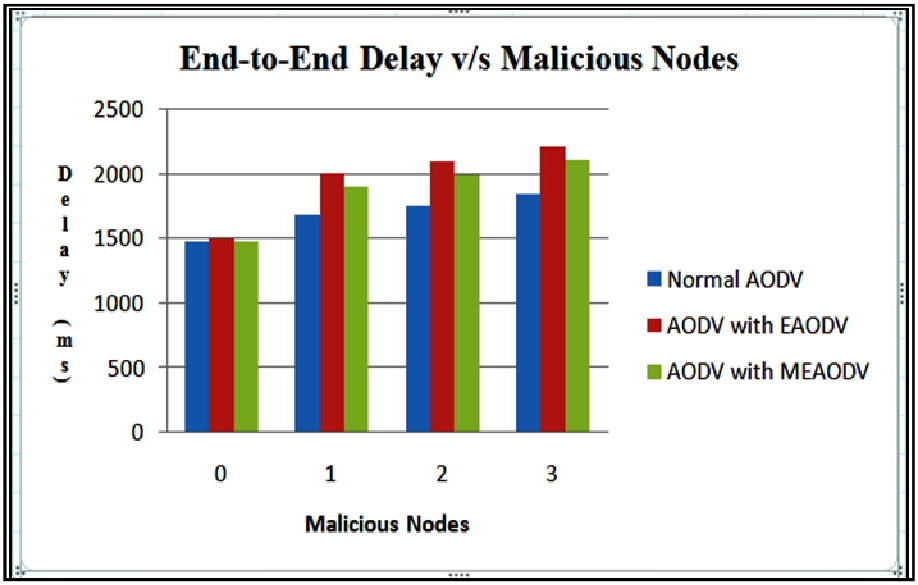

Figure 3.4 End-to-End Delay versus number of malicious nodes

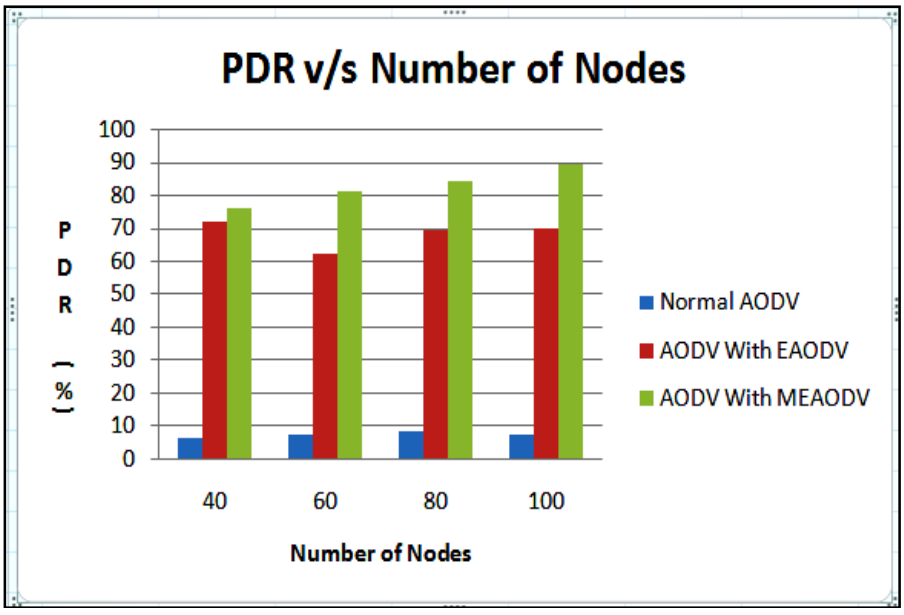

Figure 3.5 Performance Delivery Ratio versus number of nodes

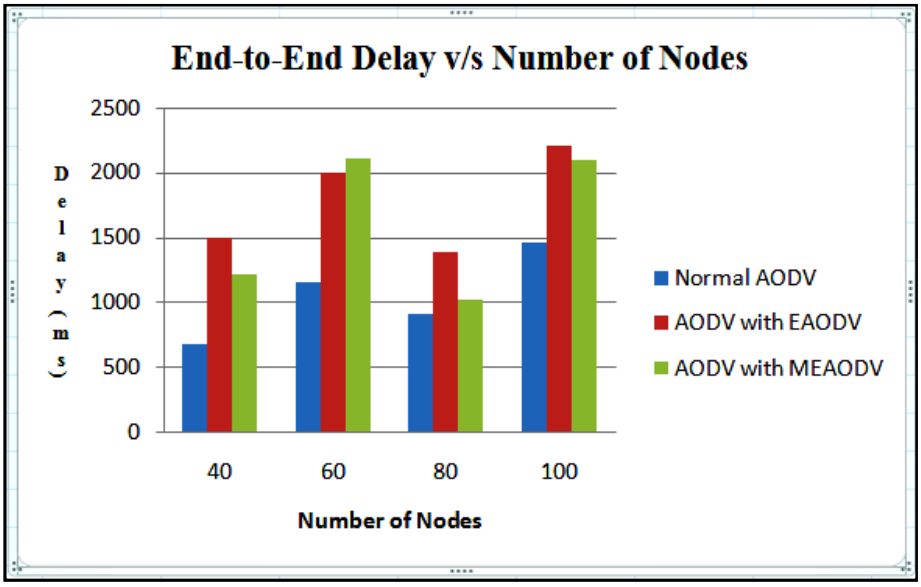

Figure 3.6 End-to-End Delay versus number of nodes

CHAPTER 4

Extended Modified Enhanced AODV (EMEAODV) against Black hole attack

From the previous chapter it is clear that MEAODV protocol proves efficient in terms of packet delivery ratio but it gets fail for multiple session usage. As there is a need of an efficient protocol which works in multiple session environment, so our objective is multiple session usage.

This chapter deals with a protocol that is capable of performing multiple session. As it is being required for a protocol to mitigating black hole effect, process is divided into two parts:
1) Detection Algorithm – This method deals with the detection of malicious node and saving of malicious id in the black list.
2) Mitigation Algorithm – This method deals with discarding of malicious node from the network.

In order to achieve this goal, we adopt a strategy for detection and mitigation of black hole effect which is listed below:

4.1 Approach for detection against Black hole attack

We have used check_mal() function for detecting malicious behavior. Moreover promiscuous mode is used for detection of malicious node. Neighbor node is used to keep the track of activities performed by immediate neighbor nodes which are in transmission range of that particular node.
Two counters as *fcount* and *rcount* are used for performing a check on malicious node. If fcount reaches a *threshold* value and rcount is found to be zero, then node is considered to be malicious and is discarded from the network.

If check_mal returns 1 then node is malicious and INTNOT packet is being broadcasted, else 0 is being returned.

4.2 Approach for mitigation against Black hole attack

Mitigation of malicious node using our present method (EMEAODV) is same as in our earlier method (MEAODV). The only difference lies in detection process of both methods. The brief description of difference in both of the detection processes is being mentioned in chapter 4.

We have used a global boolean variable as *rt_modify* for mitigating purpose. Depending on the return value of check_mal () function as 0 or 1 during detection process, value of rt_modify variable is updated to true or false and accordingly corresponding activity is being performed. If node is found to be malicious, packets coming from it are being discarded and node is isolated from the network. Moreover if packets come from destination node, it is being accepted.

4.3 Detection Algorithm against Black hole attack

In our approach, AODV protocol is modified to simulate proposed method. Real time monitoring and broadcasting mechanism is used for detection of malicious node.

a) Detection Algorithm

Notations

SN- Source Node DN- Destination Node

IN- Intermediate Node RT- Routing Table

MN- Malicious node NM- Neighbor of malicious node

PM- Promiscuous mode

INTNOT- Intruder Notification

Check_mal()

1. SN broadcasts RREQ

```
2. IN receives RREQ
3. if(IN.RT has Route to DN)
4.      Send RREP to SN;
5. else
6.     Forward RREQ to Neighbor nodes;
7. MN receives RREQ
8. Send RREP to SN;
9. SN receives RREP from MN
10. Starts transmission;
11. while(fcount < threshold)
12      {
13          if(Current node is NM)
14            {
15                  increment fcount;
16                          if(in PM received Packet From MN)
17                          increment rcount;
 18.            }
 19.      }
 20  if(rcount = 0)
 21. { Broadcast INTNOT;
 22.    return 1;
 23.  }
 24.   return 0;
```

Notification mechanism

On the identification of black hole node, Neighbor Node takes an initiative to notify all nodes by broadcasting a packet called INTNOT in the network. Figure 4.1 shows format of INTNOT packet.

Type of packet	Id of intruder detector	Id of intruder node	Id of destination node	Life time of packet	Time Stamp of packet

Figure 4.1 INTNOT packet format

This packet contains fields like Packet type, Malicious detector id, Malicious id, Destination id, Lifetime and Time Stamp. Packet type is used to distinguish this packet from data and control packets. Malicious detector id is used for Neighbor Node detecting malicious node. Figure 4.2 shows black list format. It contains id of malicious node, id of intruder detector and time stamp of packet.

Id of intruder node	Id of intruder detector	Time stamp of packet

Figure 4.2 Black List format

4.4 Mitigation Algorithm against Black hole attack

```
Modified Enhance AODV

1. RecvReply(Packet P){
2. Save P.srcIPadd and P.ds_seqno to rreply_table
3.  if(rt_modify is false){
4.          if(P.srcIPadd in intrud_list){
5.                      Drop packet P
6.                      flush rreply_table
7.                          return}
8.          else{
9.              if(!check_mal()){
10.                         set rt_modify to true}
11.             else{
12.                 save P.srcIPadd in intrud_list;
13.                 Drop packet P
14.                 flush rreply_table
15.                 return}
```

```
16.                 }
17.                                 }
18.  if(P.dsIPadd not in RT routing table entry)
19.   {
20.      Add P.dsIPadd to RT entry}
21. Select ds_seqno from RT
22. if(rt_modify and((P is from destination node)
23.      or (P.ds_seqno > RT.ds_seqno)
24.      or(P.ds_seqno= RT.ds_seqno and
25.      P.hopcount < RT.hopcount)))
26.      {
27.          if (P is from destination node)
28.                { set rt_modify to false;
29.                 update RT entry with P;
30.              send out data packets in buffer}
31.  else if (intermediate node){forward packet}
32.  else { discard packet}
33.     }
```

Working of detection method:

1. Figure 4.3 illustrates that whenever a source node wants to transmit some data to destination node, it will broadcast RouteRequest (RREQ) packet.

2. As soon as an intermediate node receives the request packet from source, it will start checking whether it has a route to the destination node or not. If it has a route to destination node, it will generate a RouteReply (RREP) packet and unicast that packet towards source node else, it will forward RREQ packet to its immediate neighbor nodes.

3. When an intermediate node (suspected node) receives an RREQ packet, it will generate a RREP packet and unicast that RREP packet towards source node.

4. Our method first recognizes the neighbor node of RREP originator node i.e. suspected node and instructs that neighbor node to overhear/listen all the packets sent by malicious (suspected) node.

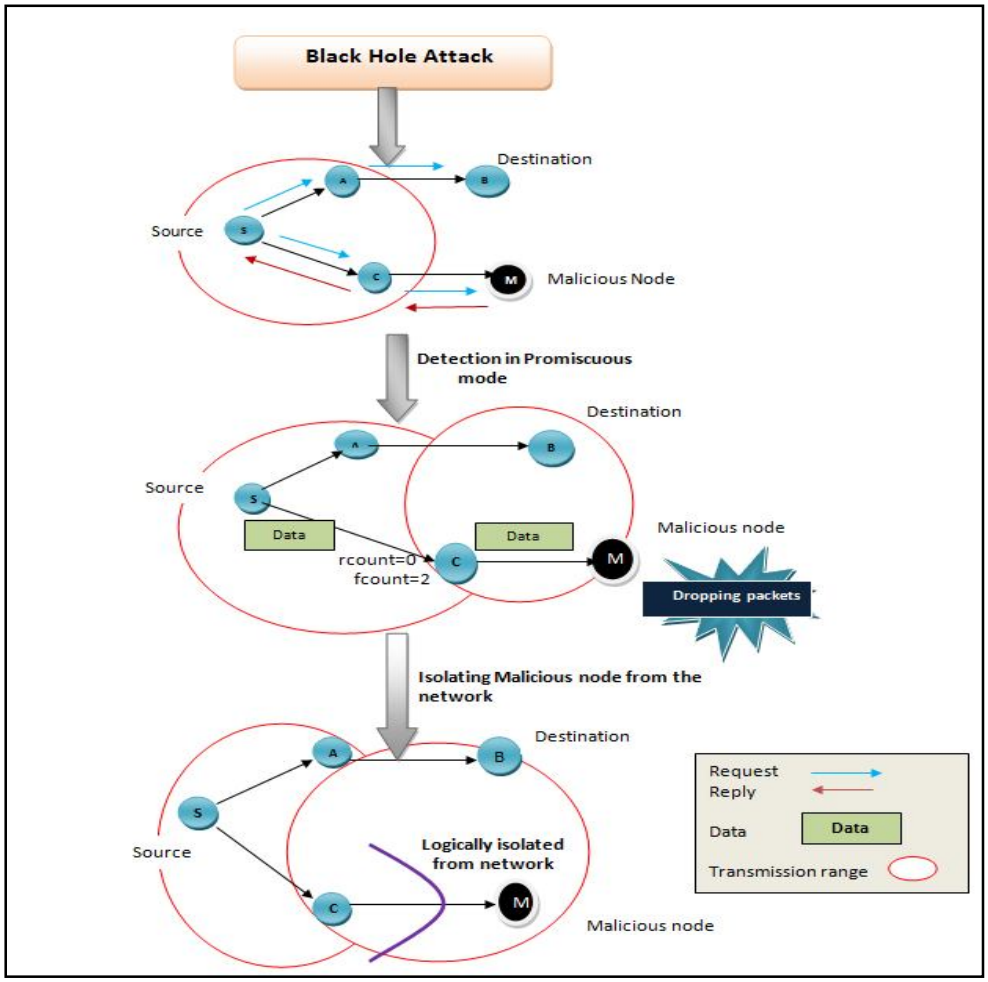

Figure 4.3 Detection of malicious node

5. In order to overhear packets sent by suspected node, neighbor node will put itself in Promiscuous mode.

6. Neighbor node maintains two counters *fcount* and *rcount* which is used for counting number of forwarded packets and number of received packets respectively. The value of *fcount* is incremented by Neighbor node when it transmits a packet to suspected node.

7. If malicious (suspected) node forwards the packet, it will be overheard by Neighbor node and it increments *rcount*.

8. Finally, Neighbor node will forward packets to malicious (suspected) node until *fcount* reaches a threshold; thereafter if *rcount* is 0, RREP originator node is identified as malicious node.

9. In real, Black hole node does not forward any packets instead of that it simply drops them thus, Neighbor node will have *fcount* greater than *threshold* and *rcount* as 0.

10. The *threshold* value is calculated according to network. The value of Threshold depends totally on how many packets we can consume for testing malicious node.

Working of mitigation method:

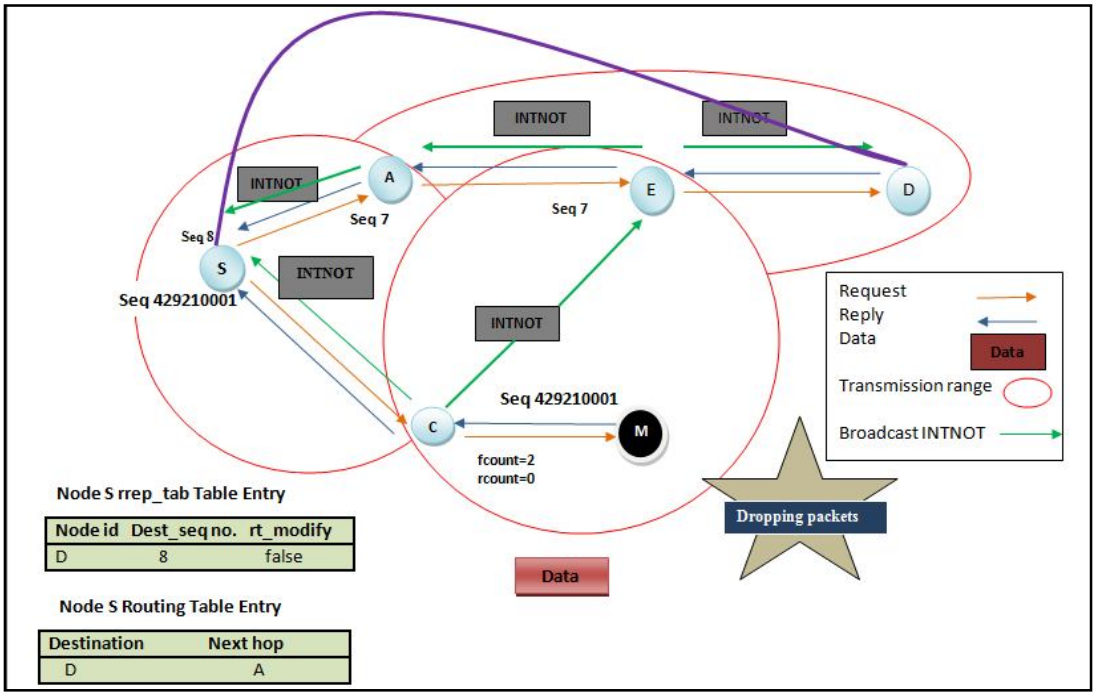

Figure 4.4 Mitigation of black hole attack

The process of mitigation is same as in our previous method MEAODV. The only difference lies in way of detecting malicious node. Moreover malicious notification packet (INTNOT Packet) is being broadcasted to the network which our previous method fails to do so. During detection process, the return value of check_mal() function decides the value of *rt_modify* parameter, and corresponding activity is being performed for discarding malicious node.

In figure 4.4, it is shown that when source node S wants to communicate with destination node D, then it starts route discovery process. Request packets with sequence number 7 are broadcasted to the immediate node till it reaches destination. But malicious node M without checking its table sends reply with higher sequence number (seq 429210001) to source node.

The process gets completed and false route is discovered. Moreover source node starts transmitting data packets to node M via node C. But after sometimes neighbor node C in promiscuous mode finds that node M is not forwarding any packet ,instead it is dropping all packets as *rcount* of node C is 0.Hence node C will broadcast the INTNOT(intruder notification)packet .

In this way, finally the packet reaches to source and source node will stop transmitting data packet to current path and moreover route discovery process will be re-initiated.

The EMEAODV method behaves differently from our earlier method MEAODV in following ways:

1) The detection process in our present method is detection using Promiscuous mode and in our earlier method was packet drop ratio.
2) Our present method is used for multiple session/connection where as earlier method has single session/connection usage.
3) No broadcasting of malicious notification packets is being done in our earlier method, due to which it results in single session.
4) Our present method provides multiple session usage because of broadcasting of malicious notification packets.

CHAPTER 5

Simulation Work and Result Analysis

This chapter deals with simulation, analysis and results of the proposed mitigation algorithm. The tool used for simulation work is Network Simulator 2. We have to make some changes in NS-2 for incorporating Black hole attack and our mitigation frame wok. Afterwards graphs are generated whose performance is analyzed.

5.1 Incorporating Black hole attack and our mitigation framework in NS-2

In this work, we have made an attempt to evaluate the effects of the Black hole attacks in the Mobile Ad-hoc Networks. In order to achieve this we have simulated the Mobile ad-hoc network scenarios which includes Black hole node using NS Network Simulator program.
We have implemented a new protocol in order to simulate the black hole node in a mobile ad-hoc network that detect and mitigate malicious behavior by real time monitoring of nodes in a network.

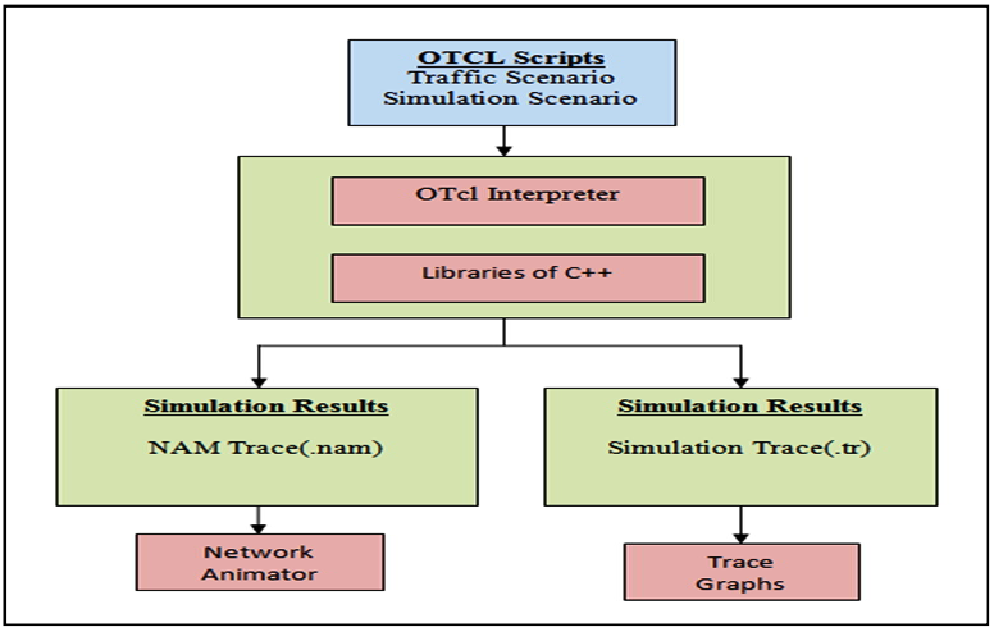

Figure 5.1NS-2 Architecture

5.1.1 NS Network Simulator

NS is developed at the University of California, Berkley [31]. It is an event driven network simulator program and includes variety of different network objects for example protocols, applications and traffic source behavior. The NS is a part of software of the VINT project that is supported by DARPA since 1995.

NS uses OTcl (Object oriented Tool Command Language) programming language for interruption of user scripts at the simulation layer. OTcl language is actually an object oriented extension of the Tcl Language. There is a full compatibility between Tcl language and C++ programming language. At the top layer, NS interprets Tcl scripts of the users, Tcl script is being taken together with C++ codes.

NS interprets OTcl script which is being written by user. While NS interprets OTcl script, two main analysis reports are being created simultaneously by NS as shown in above figure 5.1. One of the reports is NAM (Network Animator) object which reflects the visual animation of the simulation. The other report is the trace Object which reflects the behavior of all objects in the simulation. NS creates both of them as a file. Former is known as ".nam" file which is used by NAM software that is included in NS. Latter is known as ".tr" file where all the simulation traces are being included in the text format. NS project is generally distributed along with various packages (ns, nam, tcl, otcl etc.) known as "all-in-one package", but they can easily be found at different locations and can be downloaded separately. For this study we have used version 2.35 of ns all-in-one package and installed the package in the linux environment using Ubuntu. After launch of version 2, NS is commonly known as NS-2 and in our thesis we shall refer to it as NS-2. Text editor is used for writing the ".tcl" files and we have analyzed the results of the ".tr" file using "**awk**", commands of Unix Operating System. C++ language is used for implementing Black hole behavior to the AODV protocol.

5.2 Implementing a New Routing Protocol in NS to Simulate Black hole Behavior

In order to implement our contribution we have explained in details about the new protocol in this thesis. In our work, we have made nodes to exhibit Black hole behavior in AODV protocol in wireless ad-hoc network. Since the nodes behave as a Black hole they must be using a new routing Protocol for participating in the AODV messaging. The implementation details of this new routing protocol is explained below**. Directory of "ns-2.35" has all routing protocols in NS.**

For implementing black hole behavior, we have made changes in original aodv.h and aodv.cc files in aodv folder.

The changes which are made in aodv.h files for including malicious behavior are as follows:

bool malicious;

The changes which are made in aodv.cc files for including malicious behavior are as follows:

```
int AODV:: command(int argc, const char* const * argv)
{
   if (argc == 3)
     {
        if (strcmp(argv[1], "hacker") == 0)
          {
            MALseqno = atoi(argv[2]);
            malicious = true;
           return TCL_OK;
          }
    }
}
```

5.3 Implementing proposed mitigation scheme over NS-2

In order to incorporate our proposed framework in NS-2, we have made changes in various files of aodv folder. The files are mentioned as follows:

1) **aodv.cc**
2) **aodv.h**
3) **aodv_packet.h**
4) **aodv_rtable.cc**
5) **aodv_rtable.h**
6) **cmutrace.h**

We have made various functions in aodv.cc file for implementing our proposed framework. The functions are listed as check_mal(), mal_print(), recvMal(), sendMalicious(). check_mal() is the function where our proposed algorithm is being implemented. Here we check for condition (fcount>threshold and rcount==0) whether its true or not. If it is true then MALNOT is broadcasted.

There is some modifications in the inbuilt functions of aodv.cc file. Like, command(), recvReply(), recvRequest(), rt_resolve, recvAODV().In the command() function, if detection is enabled(detection==1) then maltimer event will be called. Moreover if second argument is "hacker" then malicious behavior is being incorporated in aodv protocol by initializing malicious=true. In the recvAODV() function, depending on the type of packet being received, corresponding function is called. Like if AODVTYPE_MALNOT packet is received, then recvMal() function is called. In recvMal() function, we check initially whether this particular mal node is present in Malicious table or not. If it is present, we simply discard packet, else we delete its id from routing table and insert the id of mal node in the Malicious table. Moreover in a file named dumpFile, printing of mal id along with id of node which detects malicious node at current time, is being done in mal_print() function.

Moreover, rt_resolve() fuction checks the condition whether (malicious == true) or not. If condition is true, then packet is being dropped. In recvReply() function, we simply check

whether this particular mal node is present in Malicious table or not. If it is present, we simply discard packet.

In the similar way, changes are being reflected in various files. We have declared a class named MalTimer in aodv.h file along with some data type declarations.

File named as aodv_rtable.cc has defined mal_entry() constructor and ~mal_entry() destructor in addition with mal_lookup() and mal_insert() function. In mal_lookup function, we looking for mal entry, whether it is present in malicious table or not and mal_insert() fuction is used for inserting mal entry in malicious table.

aodv_rtable.h file has declared mal_entry class and mal_store class.

The modifications incorporating our proposed algorithm can be found in appendix A.

After all these changes are made in various files of aodv folder, NS-2 is being recompiled by using following commands:

1. **sudo ./configure**
2. **sudo make clean**
3. **sudo make**

5.4 Generating mobility scenario for Random Waypoint model, Random and Walk, Gauss Markov and Manhattan Grid model TCP Traffic scenario for simulation

5.4.1 Generation of movement scenario

In order to generate the traffic movement file for random waypoint, following command is used:

./bm -f <file name> <name of model> -d <simulation duration> -n <no. of nodes> - x <grid size> -y <grid size> -R <random seed> -l < min speed> - h <max speed> -o <dimension> -p<pause time>

In order to generate the traffic movement file for random walk, following command is used:

./bm -f <file name> <name of model> -d <simulation duration> -n <no. of nodes> - x <grid size> -y <grid size> -R <random seed> -l < min speed> - h <max speed> -o <dimension> -p<pause time> -t<time till node walk > or –s(distance traversed by a node)

In order to generate the traffic movement file for gauss markov, following command is used:

./bm -f <file name> <name of model> -d <simulation duration> -n <no. of nodes> - x <grid size> -y <grid size> -R <random seed> -m < min speed> - h <max speed> -g<gauss distribution>

In order to generate the traffic movement file for manhattan grid, following command is used:

./bm -f <file name> <name of model> -d <simulation duration> -n <no. of nodes> - x <grid size> -y <grid size> -R <random seed> -c < min speed> -e <max speed> -m <> -o <pause time> -t <simulation time> -u <block size> -v <block size>

5.4.2 Generation of traffic pattern:

CBRGEN is the default tool of NS-2 used for the generation of traffic pattern file. The parameters are being passed to cbrgen.tcl file. The traffic file which is generated after executing

cbrgen.tcl file can be incorporated in TCL code in order to simulate the traffic on the network.

In order to generate the traffic pattern, following command is used:

ns cbrgen.tcl -type <tcp|cbr> –nn<no. of nodes> -seed<seed value > -mc <max no. of connections > -rate<rate> <name of traffic file>

5.5 Simulation

We have simulated AODV, EAODV, IAODV, MEAODV and our proposed mitigation scheme (MEAODV) and compared them on the basis of certain parameter metrics.

The simulation parameters for the aforesaid simulations are shown in the following table 5.1.

Parameter	Value
No. of nodes	20 to 80 nodes
Simulation area	600*600
Simulation time	600 seconds
Speed	30 m/s
Mobility model	Random walk, Random waypoint, Manhattan Grid, Gauss markov
Traffic/connections	TCP
MAC	802.11
Transmission range	150 m
Protocol	AODV

Table 5.1 Simulation Parameters

The graphs are plotted using gnuplot.

Command for making graphs using gnuplot are as follows:

```
plot "file name-1" using 1:2 with lines, \
"file mae-2" using 1:2 with lines, \ "nrl-dsr" using 1:2 with linespoints
```

The next section gives an account of performance metrics and the resultant graphs with their analysis.

5.6 Results and analysis

The following metrics are used to analyze the simulation results.

5.6.1 Packet delivery ratio

Packet Delivery ratio (pdr) defines the network efficiency and hence the efficiency of the routing protocol used is defined by packet delivery ratio.

It is defined as Packet Delivery Ratio = $\frac{Total\ No.\ of\ packets\ recieved}{Total\ No.\ of\ packet\ sent}$ (1)

Figure 5.2 shows the comparison between different mobility models with packet delivery ratio as the metrics using EMEAODV protocol. It is being shown that Random walk model has highest packet delivery ratio as compared to other models and Manhattan Grid has lowest packet delivery ratio.

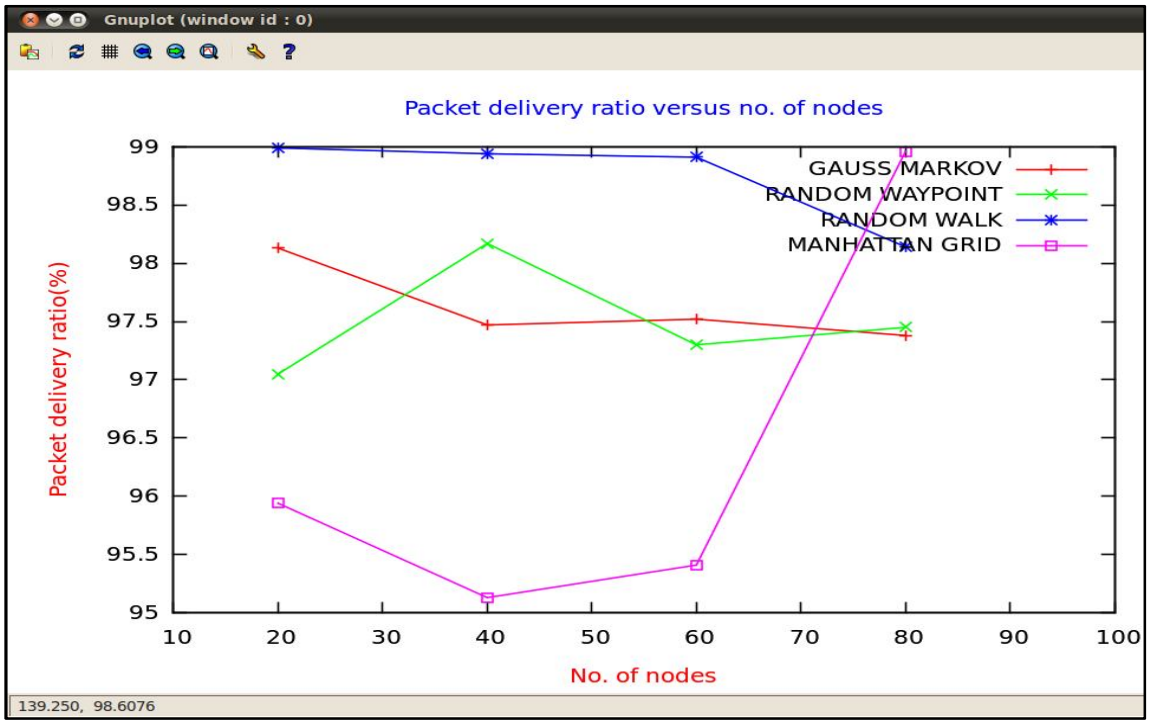

Figure 5.2 Packet delivery ratio versus no. of nodes

Figure 5.3 shows comparison of different routing protocols by varying number of nodes. Our mitigation scheme (EMEAODV) offers highest packet delivery ratio as compare to other mitigation schemes. IAODV method offers lowest packet delivery ratio. Moreover on increasing number of nodes, packet delivery ratio gets increase in our scheme. Whereas in other methods, it keeps on gradually decreasing. Random walk model is used for simulation.

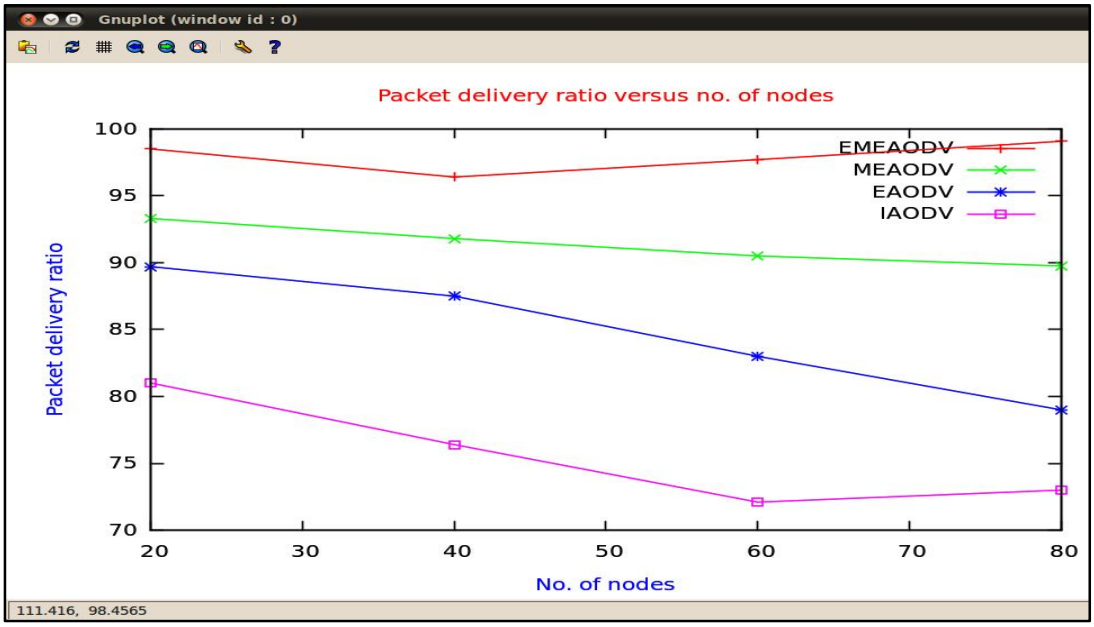

Figure 5.3 Packet delivery ratio versus no. of nodes

Figure 5.4 shows comparison of different routing protocols by varying number of malicious nodes. Here also, our mitigation scheme (EMEAODV) offers highest packet delivery ratio as compare to other mitigation schemes. IAODV method offers lowest packet delivery ratio. Moreover on increasing number of malicious nodes, packet delivery ratio is almost constant in our scheme. Whereas in other methods, it keeps on gradually decreasing. Random walk model is used for simulation.

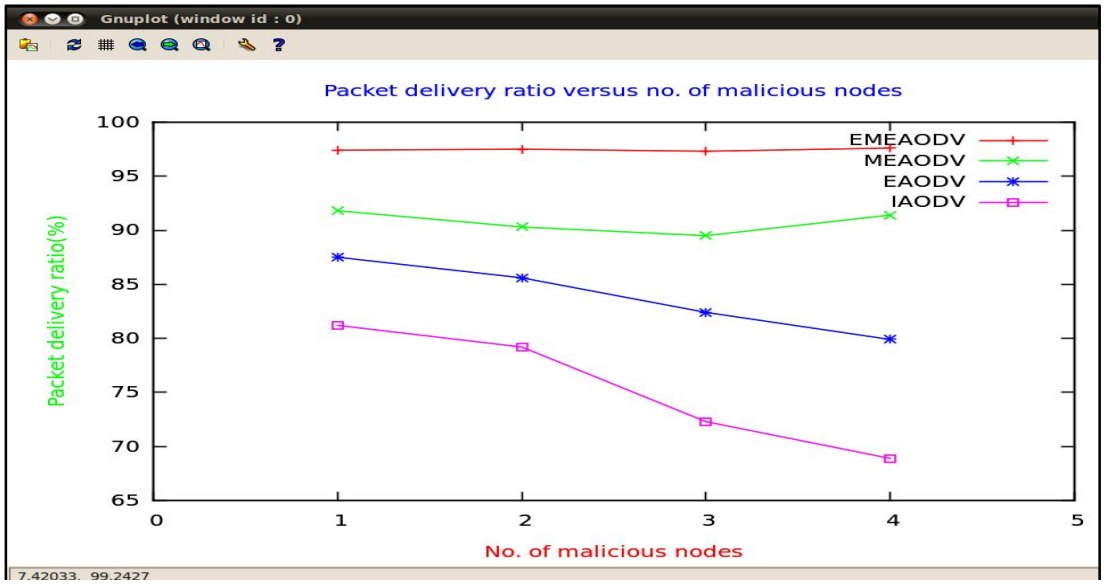

Figure 5.4 Packet delivery ratio versus no. of malicious nodes

Figure 5.5 shows comparison of different routing protocols by varying number of TCP connections. Our method(EMEAODV) again offers highest packet delivery ratio as compare to other mitigation schemes. IAODV method offers lowest packet delivery ratio. Moreover on increasing number of connections, packet delivery ratio gets slightly decrease in our method. Whereas in other methods, it keeps on fluctuating. Here also, Random walk model is used for simulation.

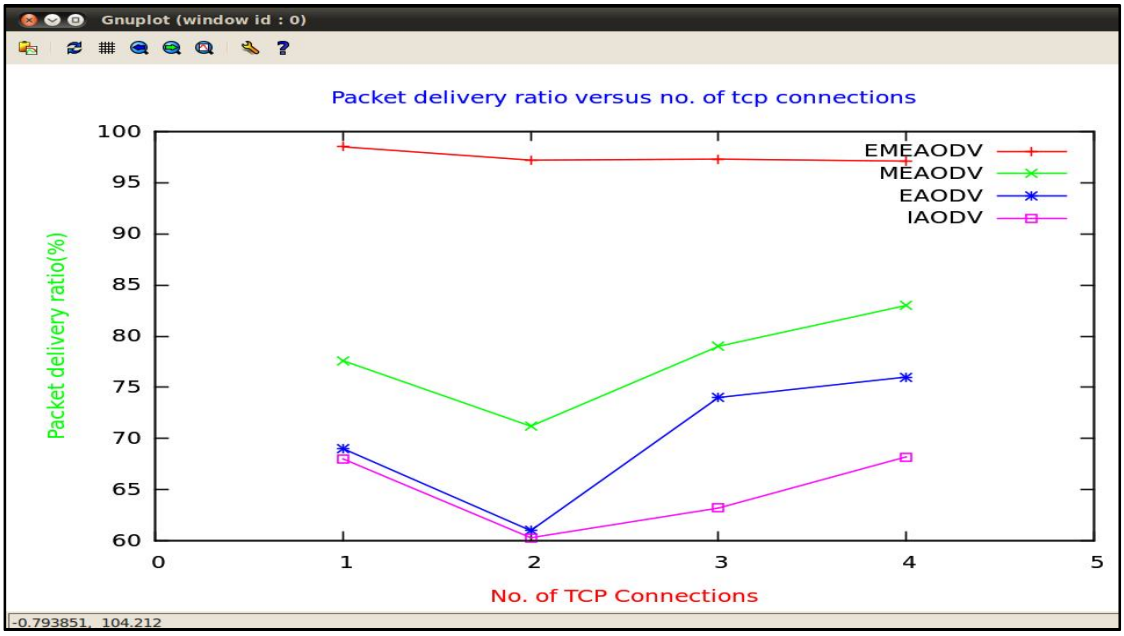

Figure 5.5 Packet delivery ratio versus no. of TCP Connections

Figure 5.6 shows comparison of different routing protocols by varying speed. Our method(EMEAODV) again offers highest packet delivery ratio as compare to other mitigation schemes. IAODV method offers lowest packet delivery ratio. Moreover on increasing speed, packet delivery ratio is slightly increasing in our method. Whereas in other methods, it keeps on fluctuating except EAODV. In EAODV, packet delivery ratio keeps on decreasing on increasing mobility speed. Random walk model is used for simulation.

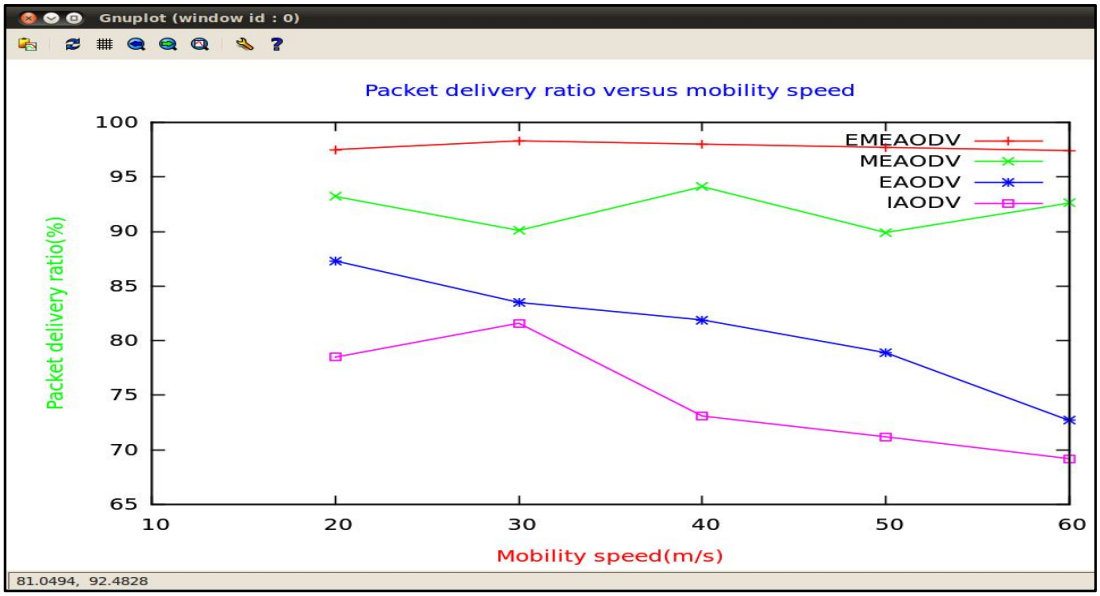

Figure 5.6 Packet delivery ratio versus mobility speed

5.6.2 Normalized routing load

Normalized routing load indicate the stress that is being offered by a specific protocol.

It is defined by the mathematical formula as

$$\text{Normalized Routing Load} = \frac{Number\ of\ routing\ packet\ sent}{Number\ of\ data\ packets\ sent} \qquad (2)$$

Figure 5.7 shows the comparison between different mobility models with normalized load as the metrics using EMEAODV protocol. It is being shown that Manhattan Grid model offers highest normalized routing load as compared to other models and Random walk offers lowest normalized routing load.

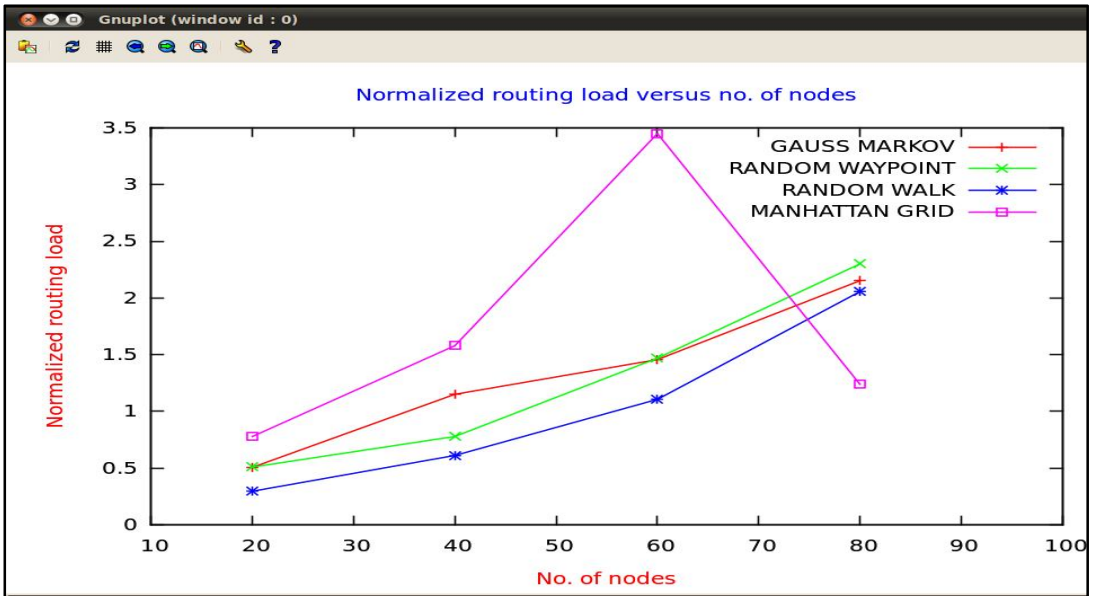

Figure 5.7 Normalized routing load versus no. of nodes

5.6.3 End to End delay

Average end-to-end delay includes the delay experiences by packet from the time it is being sent by a source node till the time it reaches the destination node.

Total congestion factor is being indicated by average end-to-end delay in the network.

$$\text{Average End to End delay} = \frac{\sum_{t-0}^{no\ of\ packets} end\ time(i) - start\ time(i)}{Total\ no\ of\ packets} \quad (3)$$

Figure 5.8 shows the comparison between different mobility models with end to end delay as the metrics using EMEAODV protocol. It is being shown that Random walk model offers highest delay as compared to other models and Manhattan Grid offers lowest delay. Moreover on increasing number of nodes, end to end delay keeps on increasing in random walk model where as other models offer fluctuating delay.

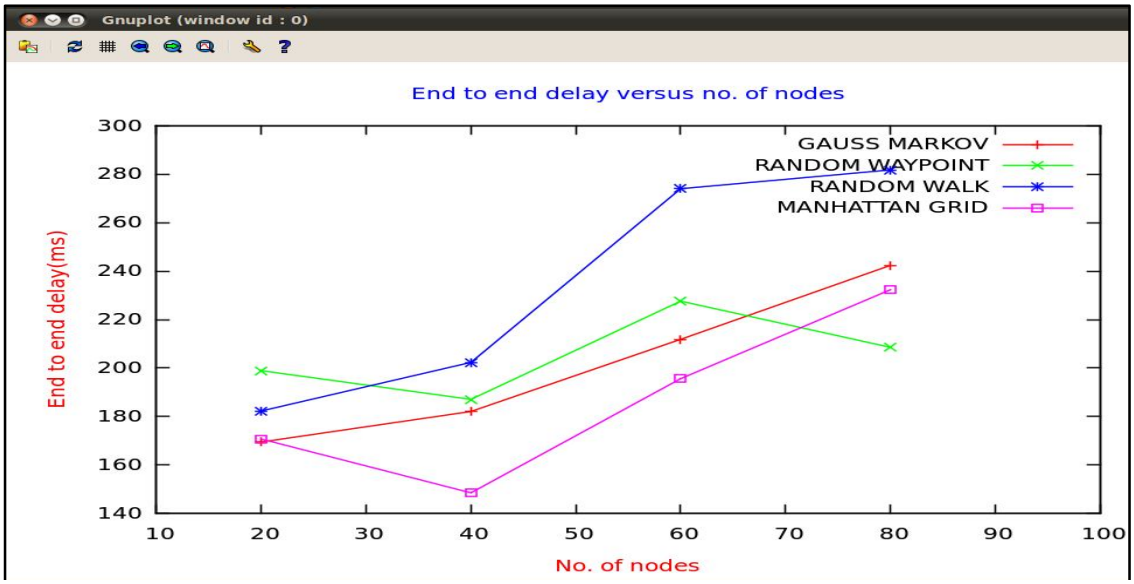

Figure 5.8 End to end delay versus no. of nodes

Figure 5.9 shows comparison of different routing protocols by varying number of nodes. Our mitigation scheme (EMEAODV) offers lowest end to end delay as compare to other mitigation schemes. IAODV method offers highest delay. Moreover on increasing number of nodes, end to end delay gets increase in our scheme. Whereas other methods offer fluctuating delays. Random walk model is used for simulation.

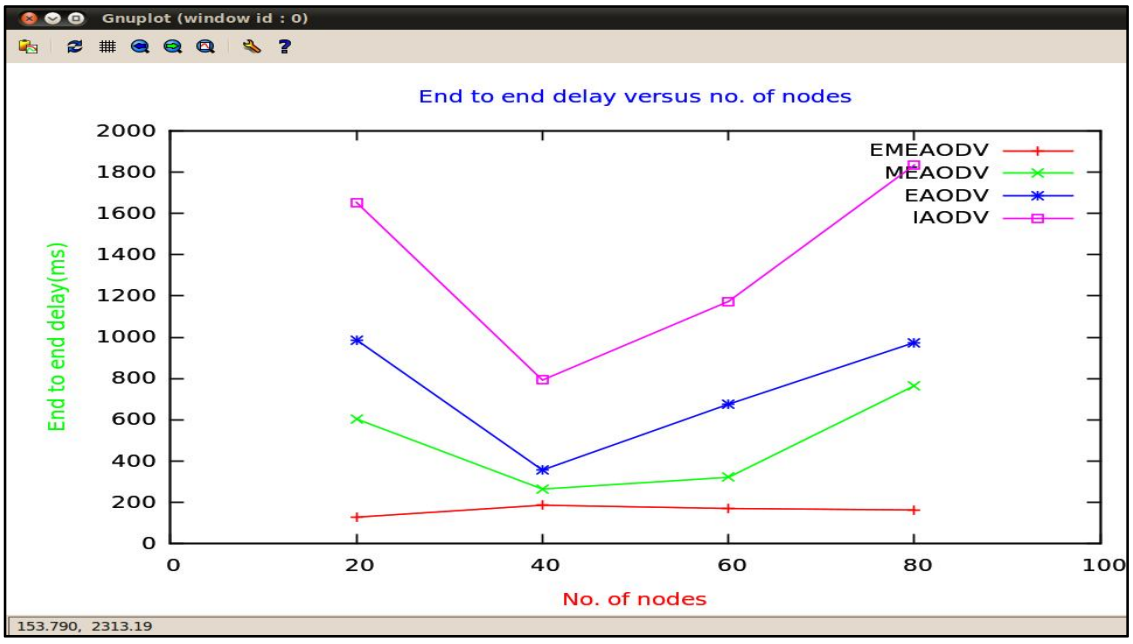

Figure 5.9 End to end delay versus no. of nodes

Figure 5.10 shows comparison of different routing protocols by varying number of malicious nodes. Here also, our mitigation scheme (EMEAODV) offers lowest end to end delay as compare to other mitigation schemes. IAODV method offers highest delay. Moreover on increasing number of malicious nodes, end to end delay is almost constant in our scheme. Whereas in IAODV method, it keeps on gradually increasing. EAODV method offers fluctuating delay and in MEAODV method, delay keeps on gradually decreasing. Random walk model is use for simulation.

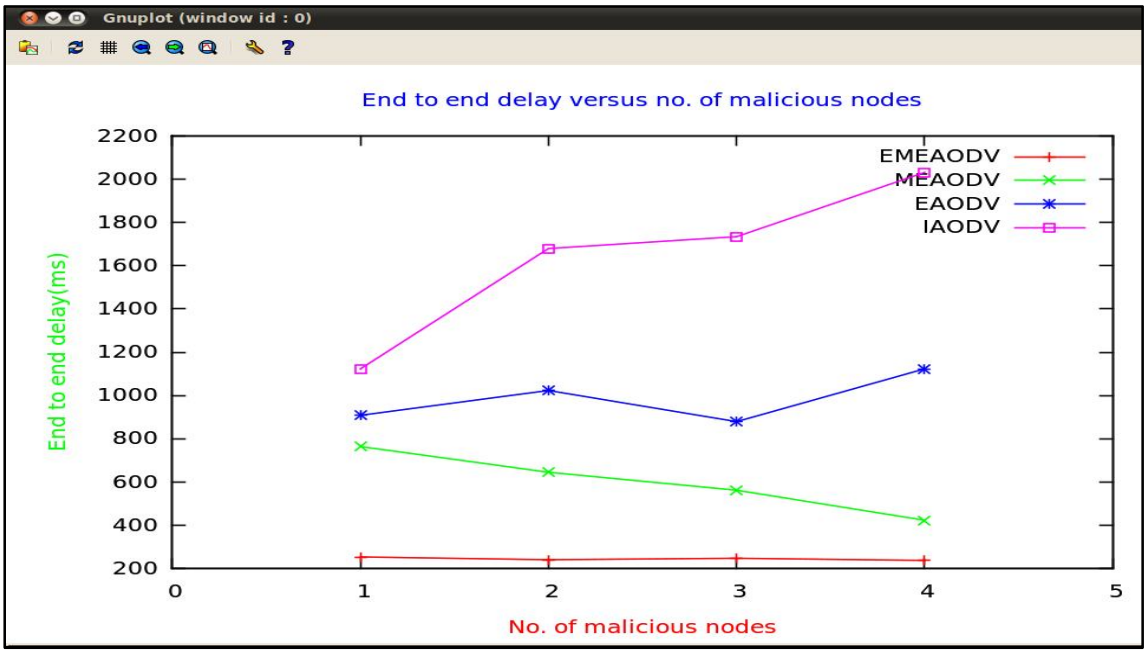

Figure 5.10 End to end delay versus no. of malicious nodes

Figure 5.11 shows comparison of different routing protocols by varying number of TCP connections. Our method (EMEAODV) again offers lowest end to end delay as compare to other mitigation schemes. IAODV offers highest delay. Moreover on increasing number of connections, end to end delay gets gradually increase in all methods.

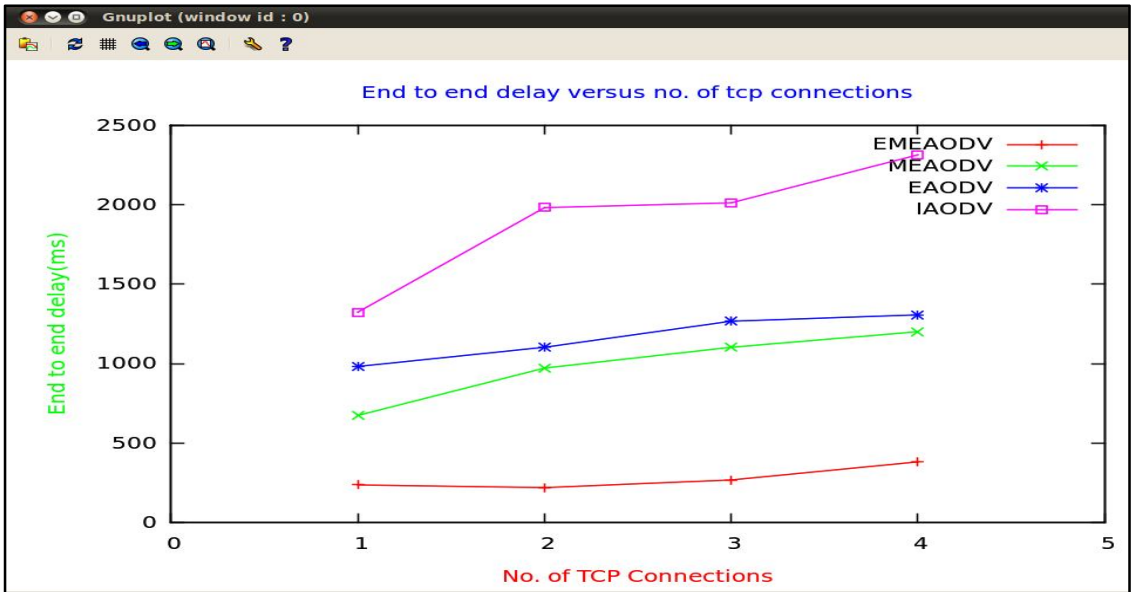

Figure 5.11 End to end delay versus no. of TCP Connections

Figure 5.12 shows comparison of different routing protocols by varying speed. Our method (EMEAODV) again offers lowest end to end delay as compare to other mitigation schemes. IAODV method offers highest delay. Moreover on increasing speed, end to end delay remains almost constant in our method. Whereas in other methods, it keeps on fluctuating. Random walk model is used for simulation.

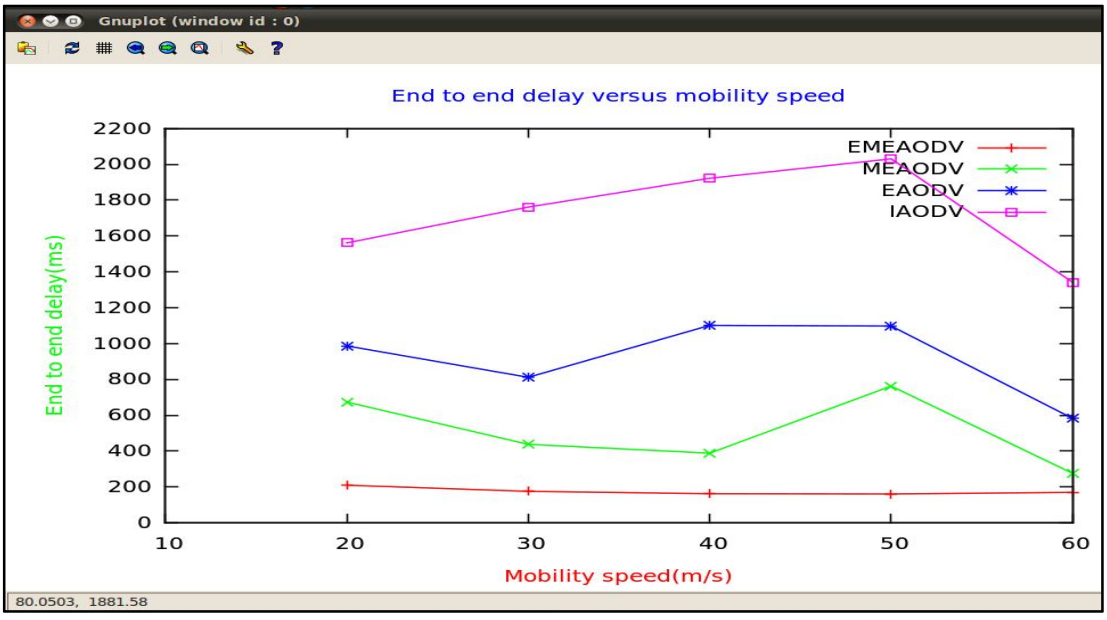

Figure 5.12 End to end delay versus mobility speed

5.6.4 Average Throughput

Average throughput defines the total size of useful data packets that is being received at all the destination nodes.

The actual data rate of the network is being indicated by average throughput.

It is defined by the mathematical formula as follows:

$$\text{Average Throughput} = \frac{Total\ data\ sent(Kb)}{Total\ time\ (s)} \qquad (4)$$

Figure 5.13 shows the comparison between different mobility models with throughput as the metrics using EMEAODV protocol. It is being shown that Random walk model offers highest throughput as compared to other models and Manhattan Grid offers lowest throughput.

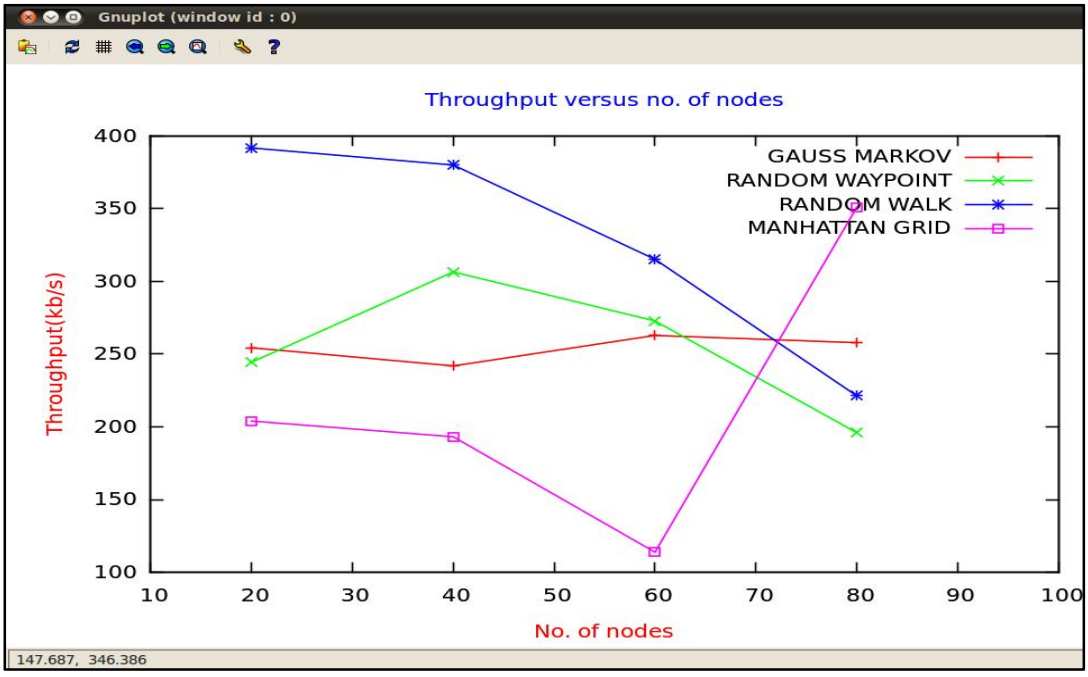

Figure 5.13 Throughput versus no. of nodes

Figure 5.14 shows the graph between threshold and false positive rate. On varying threshold we come to know that rate of false positive gets decrease. But on taking threshold as 50, number of dropped packets get rise, so we take our simulation by taking threshold as 30.

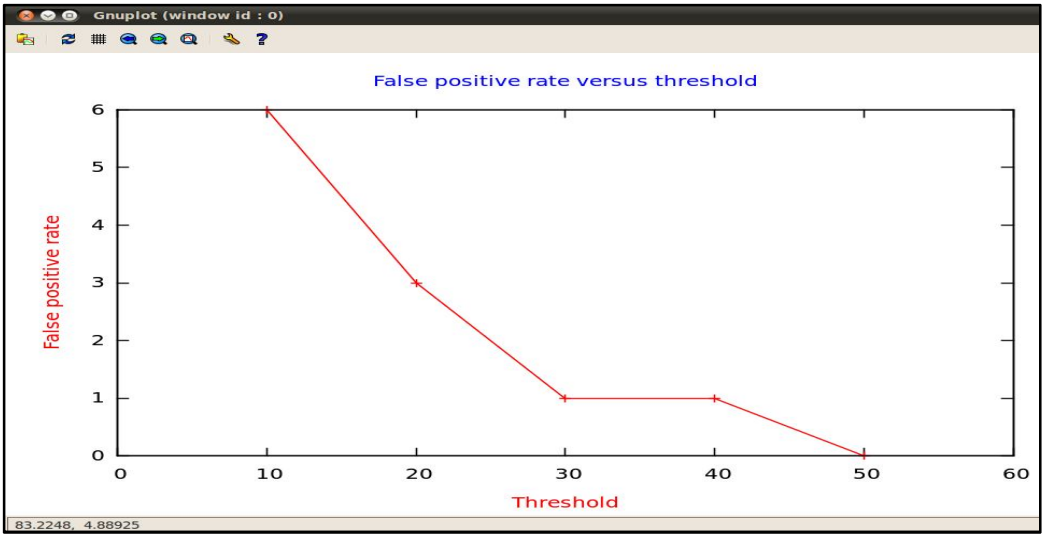

Figure 5.14 False positive versus threshold

Figure 5.15 illustrates the graphical view of nodes in a network using network animator. Blue color circle indicates Source and Destination nodes. Red color circle indicates Black hole node and Black color circle indicates normal intermediate nodes. Transmission range of nodes is being indicated by blue color large circle.

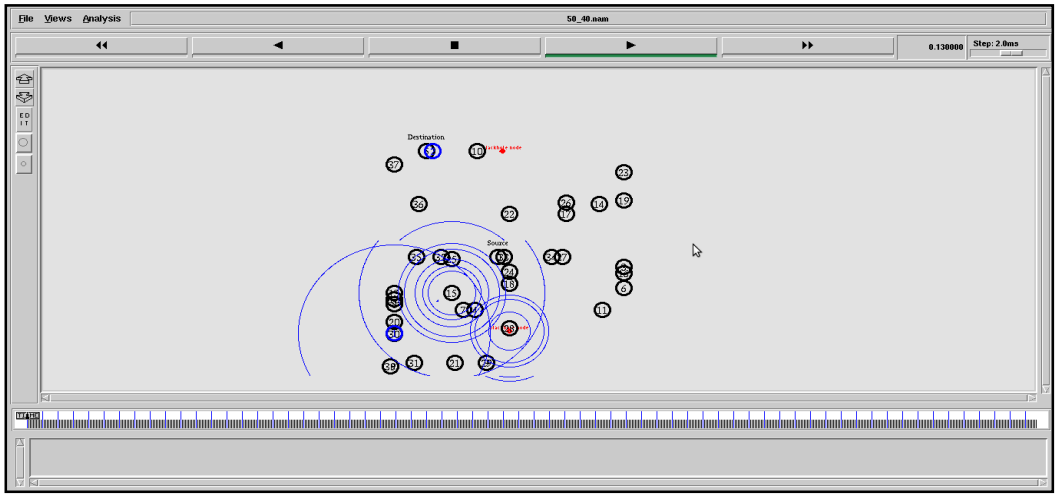

Figure 5.15 Graphical representation of nodes in Network Animator

CHAPTER 6

Generic Framework of Black hole attack on Network layer with different Mobility Models

After the study and analysis of different routing protocols, they are being concluded in following table 6.1.

Protocols	*PDF*	*End to End delay*	*Network overhead*	*Less space usage*
IAODV	Lowest	Highest	Higher than MEAODV and EAODV	Maximum space is required
EAODV	Higher than IAODV	Lower than IAODV	Lowest	Less space as compare to IAODV
MEAODV	Higher than EAODV	Lower than EAODV	Lowest	Less space as compare to IAODV
EMEAODV	Highest	Lowest	Higher than MEAODV and EAODV	Less space as compare to IAODV

Table 6.1 Comparison of Routing Protocols

By looking above at table, we come to an conclusion and drawn a generic framework for guiding users to choose an appropriate routing protocol according to an environment.

As shown below in figure 6.1, different mobility models are used to generate mobility scenario and traffic patterns are being generated by using tcp or udp connections. These files are being send to simulator for simulation and trace file is generated. Here in our paper we have used various routing protocols such as EMEAODV, MEAODV, EAODV and IAODV for mitigating *black hole* effect on network layer. This framework is used to guide the users to choose appropriate protocol depending on metrics. Like here in the above framework, our present protocol EMEAODV offers high pdf and less delay as compare to other given protocols.

Moreover for less space usage we can choose any one of the protocols from EMEAODV, MEAODV, and EAODV. All of these protocols are using only one extra table that is malicious table for storing id of malicious nodes.

But IAODV does not use any malicious table then too it has large space usage. The reason being, id of malicious node is being stored in routing table of corresponding node. So for multiple replies from same malicious node, routing table of a node will gradually keep on increasing by storing same id of malicious node multiple times. Hence more space is required. MEAODV and EAODV protocols offer less network overhead as compare to other given protocols. These protocols do not broadcast malicious notification packets and hence offer less network overhead.

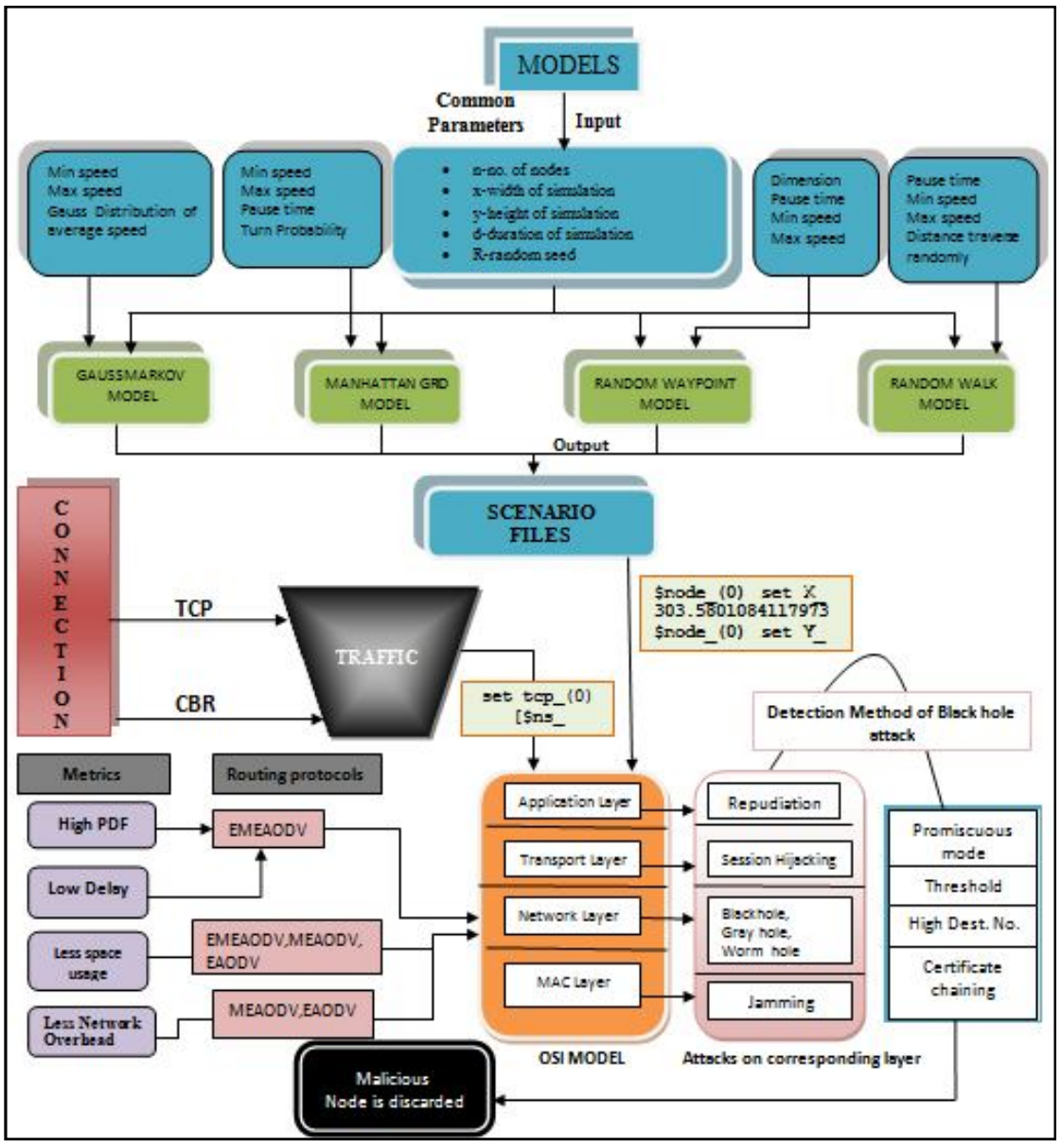

Figure. 6.1 Generic Framework of black hole attack on Network layer

CHAPTER 7

Conclusion and Future work

7.1 Conclusion

In this thesis, we analyzed effect of the Black hole and our proposed mitigation algorithm in an AODV network over Mobile adhoc environment. Moreover we have drawn a Generic Framework for guiding users to choose appropriate protocols in an environment. For this purpose, we have modified the same AODV protocol to incorporate our proposed mitigation scheme. Also we have implemented few existing routing protocols for generating a generic framework.

We have simulated four scenarios each for all the protocols where the network had 20, 40, 60 and 80 nodes respectively. We implemented our mitigation solution (EMEAODV) that attempted to reduce the Black hole effects in NS-2 and simulated our method using the same scenarios. Moreover we have implemented different mitigation schemes such as EAODV, MEAODV, IAODV in AODV protocol. We have done analysis on the basis of four performance metrics. These metrics are Packet delivery ratio, normalized routing load, Average end to end delay, and Average throughput. It is clearly been reflected that packet loss is increased after simulating black hole attack in the network.

The graphs drawn above shows that our solution offers highest packet delivery ratio and lowest end to end delay as compare to other mitigation methods. Moreover we have simulated our solution by using different mobility models such as Random Waypoint, Random Walk, Manhattan Grid and Gauss Markov model.

7.2 Future work

We have simulated the Black hole attack in the Mobile adhoc network and investigated its affects.

We have used the AODV routing protocol for our study. But there can be simulation of other routing protocols as well. There is formulation of different results by all routing protocols. Therefore, the best routing protocol for minimizing the Black hole attack may be determined.

We have used the various mobility scenario for simulation such as Random Walk, Random Waypoint, Gauss Markov and Manhattan Grid. Other MANET scenarios may also be simulated for understanding the effects of Black hole attack as well our mitigation scheme.

In our thesis, we have tried to mitigate the effects of the black hole effect in the MANET. Moreover, we have found whether our mitigation method is better than other proposed methods. For this we have simulated other schemes and compared them with our proposed solution. In order to analyze our work, we have used four performance metrics such are Average end-to- end delay, Average throughput, Normalized routing load and Packet delivery ratio. Other parameter metrics such as node energy, packet drop ratio etc. may also be used for analyzing the performance of routing protocol. We have also simulated the scenarios by changing the speed of vehicles, changing the pause Time etc. These simulations have let us analyzed our mitigation framework in a better way. And at last we may incorporate other routing attacks and analyze their comparative performances over MANETs.

CHAPTER 8

Publications from the Thesis

8.1 Published Paper

1. **Anishi Gupta**, "Black Hole Attack Mitigation Method based on Route Discovery Mechanism in AODV Protocol", **IEEE International Conference on Computational Intelligence and Computing Research, 2013**.

8.2 Communicated Papers

1. **Anishi Gupta**, and **Daya Gupta**, "Mitigation Framework against Black hole attack and comparison with various mitigation schemes of AODV routing protocol in MANET", **Wireless Network, the Journal of Mobile Communication, Computation and Information, Springer.** ISSN: 1022-0038 (print version) ISSN: 1572-8196 (electronic version) Journal no. 11276.

2. **Anishi Gupta**, **Daya Gupta** and **Jaspal Kumar**, "Black hole attack mitigating algorithm based on real time monitoring for AODV routing protocol in MANET", **International Journal of Information Processing System of International Journal of Korea Information Processing Society(KIPS)**, ISSN: 1976-913X(Print), ISSN: 2092-805X(Online).

Black Hole Attack Mitigation Method based on Route Discovery Mechanism in AODV Protocol

Anishi Gupta
Department of Computer of Engineering, Delhi Technological University, New Delhi, India
anishi.anishi@gmail.com

Abstract- **Ad hoc On Demand Vector (AODV) is a reactive routing protocol in Mobile Ad hoc Network (MANET).There have been several past works done to mitigate black hole effect but most of the methods incur overhead to the existing protocols. For the aforesaid reason, in this paper, we propose a new method MEAODV(Modified Enhanced AODV), based on the previous work EAODV(Enhanced AODV).The MEAODV is based on route discovery process for mitigating black hole effect. It does not incur any overhead to the network. It has similar logic as in EAODV but has few different condition parameters for checking the RREP message for better route discovery mechanism. In simulation, MEAODV has outstanding results in terms of better Performance Delivery Ratio(PDR) and less End-to-End Delay as compare to EAODV method by varying malicious nodes whereas it offers better PDR than EAODV by varying number of nodes.**

Keywords- **AODV, Black hole, EAODV, End-to-End Delay, MANET, MEAODV, Packet Drop Ratio, Performance Delivery Ratio, RREP message, RREQ message.**

I. INTRODUCTION

AODV, a reactive routing protocol uses a broadcast route discovery mechanism[1]. The protocol functions in two phases: route discovery and route maintenance. Initiation of a Route Discovery process is held whenever a source node wants to communicate with another node for which no routing information is present in its table. In Route Maintenance, symmetric links are being assured by Periodic hello messages . AODV protocol is vulnerable to many attacks such as black hole, warm hole and so on. Black hole effect on AODV protocol is more severe as compare to other protocols. In this paper, We have focus on black hole attack on a wireless network.

To carry out a Black hole attack, malicious node waits for neighboring nodes to send RREQ messages [1]. When RREQ message is being received by the malicious node receives, it sends a false RREP message without checking the routing table, and quickly gives a route to destination over itself, before other nodes send a real one. It assigns high sequence number to in order to get down in the routing table of the victim node. Therefore route discovery process is assumed to be completed by requesting nodes and ignore RREP messages of other nodes and begin to send data packets to malicious node. All RREQ messages are being attacked by malicious node.

Review of past works mostly have disadvantage of network overhead. Since mobile devices have limited resources, thus give an adverse effect due to high processing overhead on an overall network performance including power usage. The main idea behind our proposed algorithm is to introduce a new method called MEAODV (Modified Enhanced AODV) which has more packet delivery ratio as compare to previous work EAODV method to mitigate the black hole attack. This method is an enhancement of previous work called EAODV [2].

MEAODV has given more control to routing updates in order to mitigate black hole effect. This paper is organized as follows. Section II discusses past works. Section III presents the MEAODV method. Section IV discusses simulation results and lastly, conclusion and future works are presented in Section V.

978-1-4799-1597-2/13/$31.00 ©2013 IEEE

II. RELATED WORK

Many techniques have been proposed by researcher to prevent black hole attack. P. Raj and P. Swadas [3], proposed an adequate solution based on A DYANAMIC LEARNING SYSTEM. In this system they check RREP messages which comes from intermediate nodes. E.A Mary[4], proposed authentication based on certification in order to counter the black hole effect. Kamarularifin Abd. Jalil, Zaid Ahmad2[5], proposed an Efficient Routing Discovery Algorithm (ERDA) whose aim was to reduce overhead and latency. Kamarularifin Abd. Jalil, Zaid Ahmad2[2] , proposed an Enhanced AODV(EAODV) algorithm based on process of route discovery.Main drawback of this algorithm is that, if multiple reply messages come from the same malicious node which is already present in the malicious list, then every time we are using detection method(Packet drop ratio) to check for malicious reply. This increases end to end delay. Instead of detecting again, we should discard the packet.
Rajesh Yerneni, and Anil k. Sarje[6], proposed an Opinion AODV to mitigate black hole attack. Vrutik Shah, and Nilesh Modi[7], proposed a mitigation algorithm whose main drawback is that if multiple reply comes again from the same malicious node, then Reply is not discarded, moreover it is being accepted. This algorithm does not run if multiple reply comes from the same malicious node.

III. MITIGATION METHOD FOR BLACK HOLE ATTACK

The MEAODV is an enhancement of EAODV routing protocol [2], which provides better Packet Delivery Ratio as compare to EAODV method against black hole attack. In MEAODV, there is a revision of logic as described in EAODV but with few different condition parameters for checking the RREP message for better route discovery mechanism. The MEAODV method works similar to EAODV method except redundancy in the process of detecting malicious node is prevented. The MEAODV, by getting rt-modify parameter "false" exhibits a detection of malicious node only when malicious node has not previously send the RREP message(malicious node is not already present in intrud_list). If malicious node is already present in intrud_list, there is no need to detect for malicious node,simply a packet of malicious node is dropped.
Moreover, in the previous EAODV work, when rt-modify parameter is "false", there is always a check on malicious node. This is done by detecting malicious node, even if it is already present on intrud_list. So this kind of redundancy is also prevented in the propose work named MEAODV.
This method also prevents RREP message of multiple malicious nodes from getting into the network and updating the routing table.
The code of MEAODV method is as follows:
Modified Enhance AODV

```
1. RecvReply(Packet P){
2. Save P.srcIPadd and P.ds_seqno to rreply_table
3. if(rt_modify is false){
4.          if(P.srcIPadd in intrud_list){
5.                              Drop packet P
6.                              flush rreply_table
7.                                   return}
8.          else{
9.                   if(0<packet drop ratio<1){
10.                                  set rt_modify to true}
11.                  else{
12.                                  save P.srcIPadd in intrud_list;
13.                       Drop packet P
14.                       flush rreply_table
15.                       return}
16.              }
17.                          }
18. if(P.dsIPadd not in RT routing table entry)
19.  {
20.     Add P.dsIPadd to RT entry}
21. Select ds_seqno from RT
22. if(rt_modify and((P is from destination node)
23.     or (P.ds_seqno > RT.ds_seqno)
24.     or(P.ds_seqno= RT.ds_seqno and
25.     P.hopcount < RT.hopcount)))
26.     {
27.        if (P is from destination node)
28.             { set rt_modify to false;
29.               update RT entry with P;
30.           send out data packets in buffer}
31. else if (intermediate node){forward packet}
32. else { discard packet}
33.    }
```

The working of MEAODV is as follows:

1. At the beginning, rt_modify parameter is set to "false".
2. Since malicious node is the first node to reply, so it(M1) will send a RREP message to a sender node S.
3. The ip_address and destination sequence number will be stored in reply table.
4. Since rt_modify parameter is "false", so detection for malicious node gets started.
5. Since the node is the malicious one, its id is being saved in a intruder list, the RREP packet is dropped, reply table is flushed and recvReply function is returned.
6. Again when a RREP packet is received from destination node D, then also a detection process for malicious node gets started.
7. In the process of detection, Packet Drop Ratio comes out to be less than one, so rt-modify parameter is set to "true".
8. Now since rt_modify parameter is "true" and a node is destination, we make rt_modify "false". RT Entry is updated with packet 'P' of destination node and packets are send out in buffer. Hence sender node S updates its routing table with new route information.
9. Now, rt_modify becomes false, any reply message that comes after reply of destination node, will be ignored until the process of isolating malicious node is completed.

Thus this method prevents malicious node from entering routing table.

The MEAODV method behaves differently from EAODV in the following ways:

1. In EAODV method, logic begins with rt_modify parameter initially set to "true", where as in MEAODV method, rt_modify is initially set to "false".
2. EAODV initially stored the value of "srcIPadd" and "DSN seq no." of packet of malicious node which is being overwritten by packet information of destination node; where as, in MEAODV method, packet information of only destination node is stored as shown in fig.1[2] and fig.2.

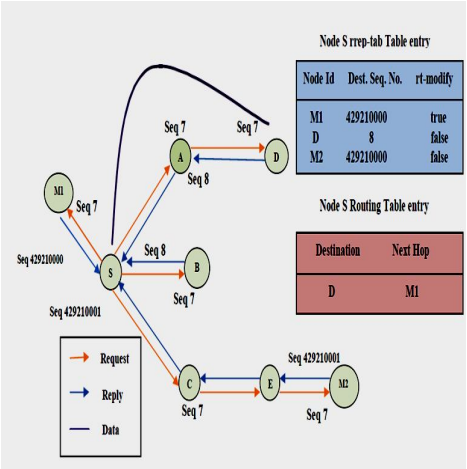

Fig. 1[2]. Route Discovery in the EAODV

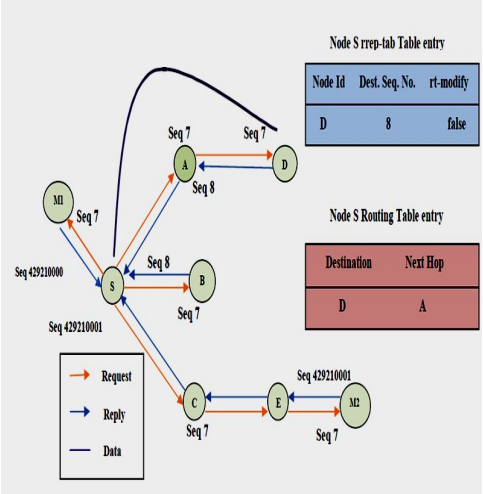

Fig. 2. Route Discovery in the MEAODV

IV. SIMULATION ENVIRONMENT

A simulation model was developed NS-2.35. AWK files are used to generate data after analyzing trace files. The results were analysed by using following three conditions:
1)Normal AODV protocol(without attack)
2)AODV protocol with EAODV method
3)AODV protocol with MEAODV method
Performance Delivery Ratio (PDR) and End-to-End Delay are used as an evaluation metric to measure the performance. The result of performance delivery ratio using normal AODV(without attack), AODV with EAODV method and AODV with MEAODV method are analysed.PDR of normal AODV is highest under absence of malicious node. When network is under attack, PDR of normal AODV drops drastically as compare to AODV with EAODV or MEAODV. By comparing EAODV and MEAODV method, MEAODV has slightly more PDR and less End to End Delay comparatively to EAODV method by varying malicious nodes as shown in figures . On increasing number of nodes, PDR of MEAODV increases comparatively to EAODV but end-to-end delay fluctuates. Overall simulation parameters are confined in Table 1.

TABLE 1
SIMULATION PARAMETERS

Parameters	Values
Simulator	NS 2.35
Protocol	AODV
Simulation Duration	600 seconds
Simulation Area	600*600
Movement Model	Manhattan Grid
Traffic Type	CBR
Data Payload	512 bytes/packet
Pause Time	0.2 seconds
Maximum Speed	55 m/s
Number of Nodes	30

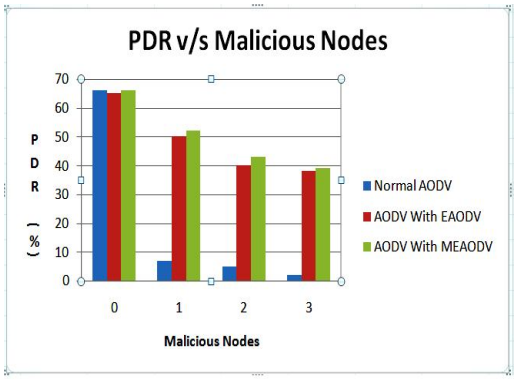

Fig. 3. Performance Delivery Ratio versus number of malicious nodes

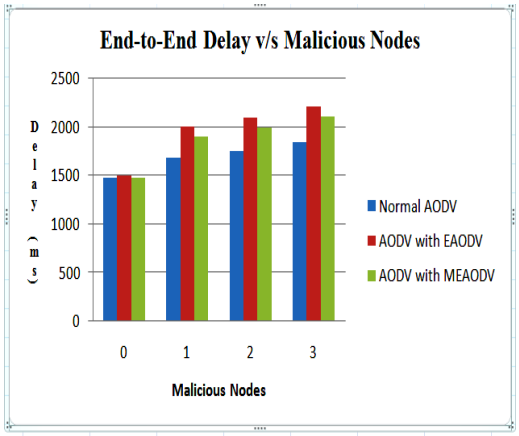

Fig. 4. End-to-End Delay versus number of malicious nodes

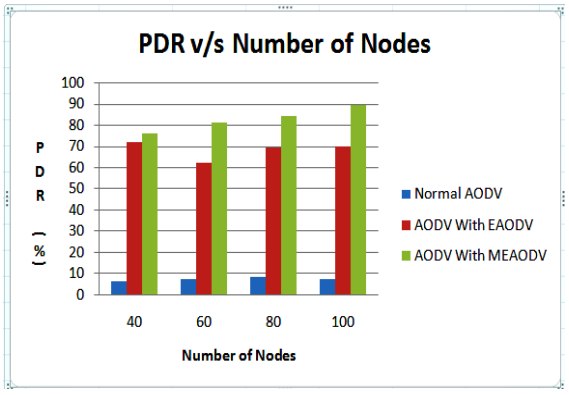

Fig. 5. Performance Delivery Ratio versus number of nodes

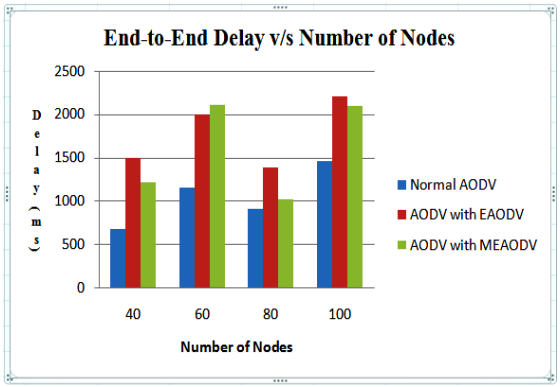

Fig.6 End-to-End Delay versus number of nodes

TABLE 2
COMPARISON OF MEAODV WITH EAODV (IN PRESENCE OF THIRTY NODES)

Parameter Metrices	Performance Delivery Ratio (%)		
No. of Malicious Nodes	MEAOD V	EAODV	Normal AODV
Zero malicious node	66	65	66
One malicious node	59	50	7
Two malicious node	47	40	5
Three malicious node	43	38	2

TABLE 3
COMPARISON OF MEAODV WITH EAODV (IN PRESENCE OF ONE MALICIOUS NODE)

Parameter Metrices	Performance Delivery Ratio (%)		
No. of Nodes	MEAODV	EAODV	Normal AODV
40 nodes	76	72	6
60 nodes	81	62	7
80 nodes	84	69	8
100 nodes	89	70	7

TABLE 4
COMPARISON OF MEAODV WITH EAODV (IN PRESENCE OF THIRTY NODES)

Parameter Metrices	End-to-End Delay (msec)		
No. of Malicious Nodes	MEAODV	EAODV	Normal AODV
Zero malicious node	1471	1469	1467
One malicious node	1701	1993	1679
Two malicious node	1808	2090	1745
Three malicious node	2101	2203	1835

TABLE 5
COMPARISON OF MEAODV WITH EAODV (IN PRESENCE OF ONE MALICIOUS NODE)

Parameter Metrices	End-to-End Delay (msec)		
No. of Nodes	MEAODV	EAODV	Normal AODV
40 nodes	1209	1501	678
60 nodes	2103	2003	1156
80 nodes	1023	1386	908
100 nodes	2101	2203	1456

V. CONCLUSION

In this paper, we propose a black hole mitigating algorithm known as MEAODV whose performance delivery ratio is slightly greater and end to end delay is slightly less than EAODV method by varying malicious nodes. On increasing number of nodes, PDR increases comparatively to EAODV but end-to-end delay fluctuates. Our method provides a solution for mitigating black hole attack by controlling the routing update with new condition parameters and removing the redundancy in detecting malicious nodes. Results from above simulation shows that AODV with MEAODV method gives comparatively better performance as compare to AODV with EAODV method.

ACKNOWLEDGMENT

The author would like to thanks Dr. Daya Gupta for her guidance and support.

REFERENCES

[1] Charles E. Perkins, and Elizabeth M. Royer, "Ad-Hoc On- Demand Distance Vector Routing", Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999, pp. 90-100.

[2] Zaid Ahmad, Kamarularifin Abd., and JalilJamalul-lail Ab Manan, "Black hole Effect Mitigation Method in AODV Routing Protocol", 2011 7th International Conference on Information Assurance and Security (IAS) IEEE 2011.

[3] P. Raj and P. Swadas, *A dynamic learning system against black hole attack in AODV based MANET*, IJCSI International Journal of Computer Science, Vol.2, (2009).

[4] E. A .Mary Anita, V. Vasudevan, Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining, International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12 (2010).

[5] Kamarularifin Abd. Jalil, Zaid Ahmad2, and Jamalul-Lail Ab Manan, "An Enhanced Route Discovery Mechanism for AODV Routing Protocol ", ICSECS 2011, Part III, CCIS 181, pp. 408–418, Springer- Verlag Berlin Heidelberg 2011.

[6]Rajesh Yerneni, and Anil k. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks," ICCCNT' 2012 26th _28th July 2012, IEEE-20180, Coimbatore, India.

[7]Vrutik Shah, and Nilesh Modi, " An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks," International Journal of Computer Applications (0975 – 8887) Volume 69– No.7, May 201