International Journal For Technological Research In Engineering
Volume 3, Issue 8, April-2016 *ISSN (Online): 2347 - 4718*

DETECTION ELIMINATION AND SIMULATION ANALYSIS OF BLACK AND GRAY HOLE ON AD-HOC NETWORK BY IMPROVED ZRP PROTOCOL

Kaushal Dev Singh[1], Sachin Kumar Mishra[2]
M.Tech (Computer Science), Manav Bharti University.

ABSTRACT: Wireless networks are gaining popularity to its peak today, as the user's wants wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to that of the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack others nodes and networks knowing that it has the shortest path [4]. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. Previously the works done on security issues in MANET were based on reactive routing protocol like Ad Hoc On Demand Distance Vector (AODV). Different kinds of attacks were studied, and their effects were elaborated by stating how these attacks disrupt the performance of MANET. The scope of this thesis is to study the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad Hoc On Demand Distance Vector (AODV). Comparative analyses of Black hole attack for both protocols were taken into account. The impact of the attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. The measurements were taken in the light of throughput, end to end delay and network load. Simulation is done in NS

Keywords: MANET, Black Hole, Routing protocols.

I. INTRODUCTION

Mobile Ad Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas for researchers. Many routing protocols have been developed for MANETS.

Security in Mobile Ad Hoc Network is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is quite challenging and vital issue as there is increasing threats of attack on the Mobile Network. Security is the cry of the day. In order to provide secure communication and transmission engineer must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources

1.1 Problem statement

Previously the works done on security issues i.e. attacks (Black Hole attack) involved in MANET were based on reactive routing protocol like Ad Hoc On Demand Distance Vector (AODV). Black Hole attack is studied under the AODV routing protocol and its effects are elaborated by stating how these attacks disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the

vulnerability of both these protocols against the attack. There is a need to address both these types of protocols as well as the impacts of the attacks on the MANETs.

1.2 Aims and Objectives

Aims and objectives of this thesis work are summarized as follow

- The study focus on analysis of black hole attack in MANET and its consequences.
- Analyzing the effects of black hole attack in the light of Network load, throughput and End to End delay in MANET.
- Simulating the black hole attack using Proactive and Reactive routing protocols.
- Comparing the results of both Proactive and Reactive protocols to analyze which of these two types of protocols are more vulnerable to Black Hole attack.
- Previously proposed plans are suggested for counter measurement of Black Hole attack.

II. WIRELESS NETWORKS

Wireless networks are gaining popularity to its peak today, as the users' wants wireless connectivity irrespective of their geographic position. Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them. One of the reasons of the popularity of these networks is widely penetration of wireless devices. Wireless applications and devices mainly emphasize on Wireless Local Area Networks (WLANs). This has mainly two modes of operations, i.e. in the presence of Control Module (CM) also known as Base Stations and Ad Hoc connectivity where there is no Control Module. Ad Hoc networks do not depends on fixed infrastructure in order to carry out their operations. The operation mode of such network is stand alone, or may be attach with one or multiple points to provide internet and connectivity to cellular networks.

These networks exhibits the same conventional problems of wireless communications i.e. bandwidth limitations, battery power, enhancement of transmission quality and coverage problems.

2.1 Network

Before going into the details of wireless network it is important to understand what a network is and different kind of networks available today.

Any collection of devices/ computers connected with each other by means of communication channels that help the users to share resources and communicate with other users. There are two main types of network i.e. wired network and wireless network.

2.1.1 Wired Networks

Wired network are those network in which computer devices attached with each with help of wire. The wire is used as medium of communication for transmitting data from one point of the network to other point of the network.

2.1.2 Wireless Networks

A network in which, computer devices communicates with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lay within the radio range of each other. Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

2.2 Why Wireless Networks?

Wireless networks are getting popular due to their ease of use. Consumer/user is no more dependent on wires where he/she is, easy to move and enjoy being connected to the network. One of the great features of wireless network that makes it fascinating and distinguishable amongst the traditional wired networks is mobility. This feature gives user the ability to move freely, while being connected to the network. Wireless networks comparatively easy to install then wired network. There is nothing to worry about pulling the cables/wires in wall and ceilings. Wireless networks can be configured according to the need of the users. These can range from small number of users to large full infrastructure networks where the number of users is in thousands.

Wireless networks are very useful for areas where the wire cannot be installed like hilly areas.

On the basis of coverage area the wireless network can be divided into.

a) Personal Area network
b) Local Area Network
c) Wide Area Network

a) Personal Area Network

Personal area network is used for communication between computer devices close to one person [1]. Some of the personal area networks are zigbee, Bluetooth, sensor networks. Bluetooth is low cost wireless connection that can link up devices. These devices normally work within 10 meters, with access speed up to 721 Kbps. This technology is widely used in a range of devices like computer and their accessories i.e. mouse and keyboard, PDAs, printers and mobile phones etc. It is important to understand that Bluetooth as Wireless Personal Area Network (WPAN) is not 802.11 wireless as it do not perform the same job, rather used as wireless replacement for cable in order to connect devices. Bluetooth works at 2.4 GHz band and this may cause interference with Wireless LAN equipments (802.11b, 802.11g).

b) Local Area Network

Wireless local area network (WLAN) is standardized by Institute of Electrical and Electronics Engineer (IEEE). In local area network the users communicate with each other in local coverage area i.e. building or a campus. WLANs are the substitute of the conventional wired LANs. WLAN is wireless medium that is shared by the devices within the WLAN.

WLANs have gained a great amount of popularity. Keeping in mind their mobility feature, they are implemented in mobile devices like laptop, PDAs, Mobile Cell phones etc. In WLAN, wireless Ethernet Protocol, IEEE 802.11 is used. WLAN is mainly used for the connection with internet. The

data rate of WLAN is low that is between 11 and 54 Megabits per second (Mbps) as compared to the wired LAN which operates at 100 to 1000 Mbps. This means that any activity that required high bandwidth, are better done on wired network rather than on wireless.

c) Wide Area Network

Wireless wide area network (WWAN) cover geographically larger area then local area network. The wide area networks almost consist of one or two local area networks. Examples of WWAN are Satellite Systems, Paging Networks, 2G and 3G Mobile Cellular.

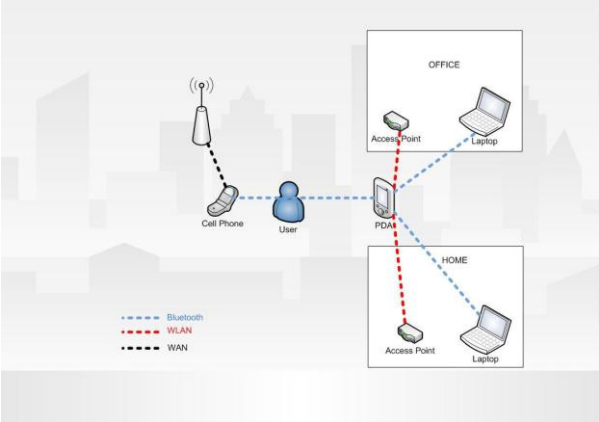

Fig. 2.1 Communications in Wireless Networks

2.3 IEEE Standard for Wireless Networks

Institute of Electrical and Electronics Engineers (IEEE) define the standards for related technologies. IEEE defined three main operational standard for wireless LAN i.e. IEEE 802.11a, 802.11b and 802.11g. The entire three standards belong to IEEE 802.11 protocol family. In 1999 802.11a standard was ratified by IEEE. The 802.11 has a nominal data rate of 54Mbps, but the actual data rates varies between 17-28Mbps. The most established and frequently deployed wireless network standard is 802.11b. Most of the public wireless "hotspots" use this standard. It operates in 2.4 GHz spectrum and the nominal data transfer is 11 Mbps. Practically, approximately 4-7 Mbps is the actual data transmission rate achieved by this standard.

2.4 Ad Hoc Networks

Ad hoc networks have no infrastructure where the nodes are free to join and left the network. The nodes are connected with each other through a wireless link. A node can serve as a router to forward the data to the neighbors' nodes. Therefore this kind of network is also known as infrastructure less networks. These networks have no centralized administration. Ad hoc networks have the capabilities to handle any malfunctioning in the nodes or any changes that its experience due to topology changes. Whenever a node in the network is down or leaves the network that causes the link between other nodes is broken. The affected nodes in the network simply request for new routes and new links are established Ad hoc network can be categorized in to static ad hoc network (SANET) and Mobile ad hoc network (MANET).

2.4.1 Static Ad hoc Networks:

In static ad hoc networks the geographic location of the nodes or the stations are fixed. There is no mobility in the nodes of the networks, that's why they are known as static ad hoc networks.

2.4.2 Mobile Ad hoc Networks

Mobile ad hoc network is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile ad hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology.

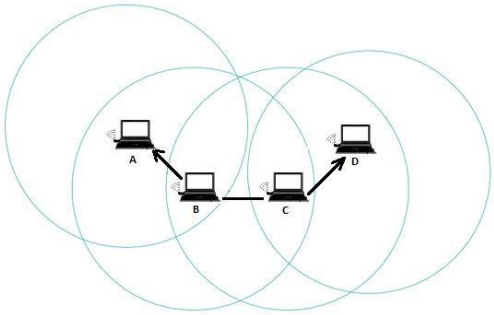

Fig. 2.2 Mobile Ad Hoc Network

2.4.3 Characteristics of MANETs

When a node wants to communicate with another node, the destination node must lies within the radio range of the source node that wants to initiate the communication. The intermediate nodes within the network aids in routing the packets for the source node to the destination node. These networks are fully self organized, having the capability to work anywhere without any infrastructure. Nodes are autonomous and play the role of router and host at the same time. MANET is self governing, where there is no centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other. The network can be set up anywhere without any geographical restrictions. One of the limitations of the MANET is the limited energy resources of the nodes.

Types of Mobile Ad Hoc Network:

1. Vehicular Ad Hoc Networks (VANET's)
2. Intelligent Vehicular Ad Hoc Networks (InVANET's)
3. Internet Based Mobile Ad Hoc Networks (iMANET's)

1 Vehicular Ad Hoc Networks (VANET's)

VANET is a type of Mobile ad hoc network where vehicles are equipped with wireless and form a network without help of any infrastructure. The equipment is placed inside vehicles as well as on the road for providing access to other vehicles in order to form a network and communicate.

2 Intelligent Vehicular Ad Hoc Networks (InVANET's)

Vehicles that form Mobile Ad Hoc Network for communication using WiMax IEEE 802.16 and WiFi 802.11. The main aim of designing InVANET's is to avoid vehicle

collision so as to keep passengers as safe as possible. This also help drivers to keep secure distance between the vehicles as well as assist them at how much speed other vehicles are approaching. InVANET's applications are also employed for military purposes to communicate with each other.

3 Internet Based Mobile Ad Hoc Networks (iMANET's)

These are used for linking up the mobile nodes and fixed internet gateways. In these networks the normal routing algorithms does not apply [2].

2.5 Applications of MANETs

The properties of MANET make it so much favorable that would bring so many benefits. There are so many research areas in MANET which is under studies now. The most important area is vehicle to vehicle communication. Where the vehicle would communicate with each other, keeping a safe distance between them as well as collision warnings to the drivers. MANET can be used for automated battlefield and war games. One of the most important areas where MANETs are applied is emergency services such as disaster recovery and relief activities, where traditional wired network is already destroyed. There are so many other application areas such as entertainment, education and commercial where MANETs are playing their role for connecting people.

2.6 Short comings of Mobile Ad Hoc Networks

Some of the disadvantages of MANETs are as follows.

Limited Resources.

Scalability problems.

No central check on the network.

Dynamic topology, where it is hard to find out malicious nodes.

2.7 MANETs Routing Protocols

Mobile Ad hoc Network is the rapid growing technology from the past 20 years. The gain in their popularity is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs created a new set of demands to be implemented and to provide efficient better end to end communication. MANETs works on TCP/IP structure to provide the means of communication between communicating work stations. Work stations are mobile and they have limited resources, therefore the traditional TCP/IP model needs to be refurbished or modified, in order to compensate the MANETs mobility to provide efficient functionality. Therefore the key research area for the researchers is Routing. Routing protocols in MANETs is a challenging and attractive tasks, researchers are giving tremendous amount of attention to this key area.

2.8 Classification of MANETs Routing Protocols:

Routing protocols in MANETs are classified into three different categories according to their functionality

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

The hierarchy of these protocols is shown bellow in the figure 2.1. Fig. 2.3 MANETs Routing Protocols

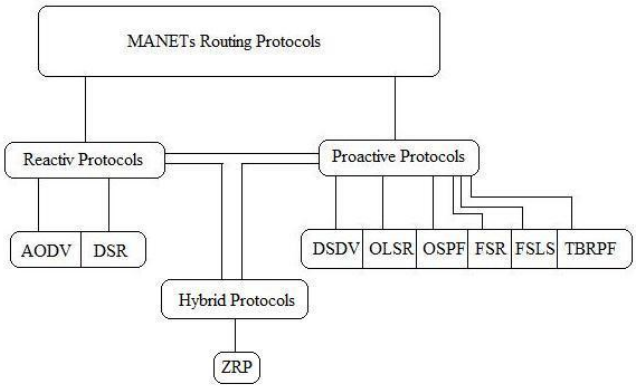

Fig. 2.3 MANETs Routing Protocols

1) Reactive Protocols:

Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded [3, 4]. When a node wants to communicate with another node in the network, and the source node don't have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. Normally reactive protocols

- Don't find route until demanded
- When tries to find the destination "on demand", it uses flooding technique to propagate the queuery.
- Do not consume bandwidth for sending information.
- They consume bandwidth only, when the node start transmitting the data to the destination node.

2.9 Ad Hoc On Demand Distance Vector Protocol (AODV):

AODV is described in RFC 3561 [5]. It's reactive protocol, when a node wishes to data to a node, to which wishes to transmit data to a node to which it has no route, AODV will provide topology information for the node. There are three types of control messages in AODV which are discussed bellow.

Control Messages:

There are three types of control messages for route discovery and maintenance which are described below.

Route Request Message RREQ:

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message RREP:

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message RERR:

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, Route error (RERR) message is generated by the node in order to notify other nodes that the link is down.

2.9.1 Route Discovery Mechanism in AODV

When a node "A" wants to initiate transmission with another node "G", it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forward to the neighbors, and those node forward the control message to their neighbors' nodes. This process of goes on until it finds a node that has a fresh enough route to the destination or destination node is located. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is establish node "A" and "G" can communicate with each other. The following diagram show exchange of control messages between source node and destination node.

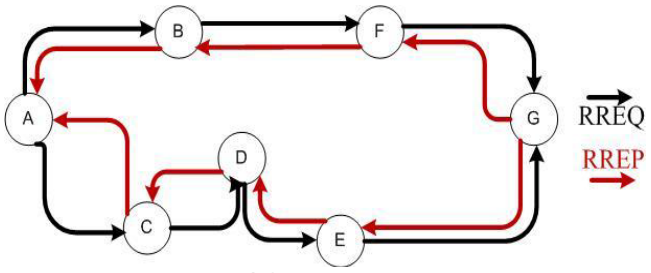

Fig. 2.4 AODV Route Discovery

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node i.e. from node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error. The scheme is shown in the Fig.2.3 bellow.

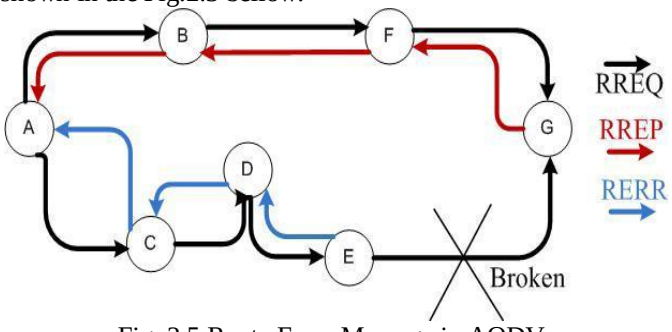

Fig. 2.5 Route Error Message in AODV

2.10 Dynamic Source Routing Protocol:

Dynamic source routing protocol abbreviated as DSR is also a reactive protocol. DSR used to updates its route caches by finding new routes. It updates its cache with new route discovered or when there exist a direct route between source and destination node. When a node wants to transmit data, it defines a route for the transmission and then starts transmitting data through the defined route. There are two processes for route discovery and maintenance which are described below.

III. SECURITY ISSUES IN MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. Recently in the past few years security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However mobile ad hoc networking was still in need of further discussions and development in terms of security [21]. With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network Mobile ad hoc network is different. The routing protocols designed majorly for internet is different from the mobile ad hoc networks (MANET). Traditional routing table was basically made for the hosts which are connected wired to a non dynamic backbone [22]. Due to which it is not possible to support ad hoc networks mainly due to the movement and dynamic topology of networks. Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks [23]. Major vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction and also open network medium. Despite of the above said protocols in MANET, there are attacks which can be categorized in Passive, Active, Internal, External and network-layer attacks, Routing attacks and Packet forwarding attacks. MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

3.1 Flaws in MANETS

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed bellow.

3.1.1 Non secure boundaries:

MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes

in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. The links are compromised and are open to various link attacks. Attacks on the link interfere between the nodes and then invading the link, destroying the link after performing malicious behavior. There is no protection against attacks like firewalls or access control, which may result the vulnerability of MANET to attacks. Spoofing of node's identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised [10].

3.1.2 Compromised Node:

Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous [11]. Due to this autonomous factor for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. It can be seen that these threats from compromised nodes inside the network is more dangerous than attacking threats from outside the network.

3.1.3 No Central Management:

MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets [12]. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale ad hoc network is very difficult due to no central management. When there is a central entity taking care of the network by applying proper security, authentication which node can join and which can't. The node connect which each other on the basis of blind mutual trust on each other, a central entity can manage this by applying a filter on the nodes to find out the suspicious one, and let the other nodes know which node is suspicious.

3.1.4 Problem of Scalability:

In traditional networks, where the network is build and each machine is connected to the other machine with help of wire. The network and the scale of the network, while designing it is defined and that do not change much during the use. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network. The case is quite opposite in MANETs because the nodes are mobile and due to their mobility in MANETs, the scale of the MANETs is changing. It is too hard to know and predict the numbers of nodes in the MANETs in the future. The nodes are free to move in and out of the ad hoc network which makes the ad hoc network very much scalable and shrinkable. Keeping this property of the MANET the protocols and all the services that a MANET provides must be adaptable to such changes.

3.2 Classification of attacks

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

3.2.1 External and Internal Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

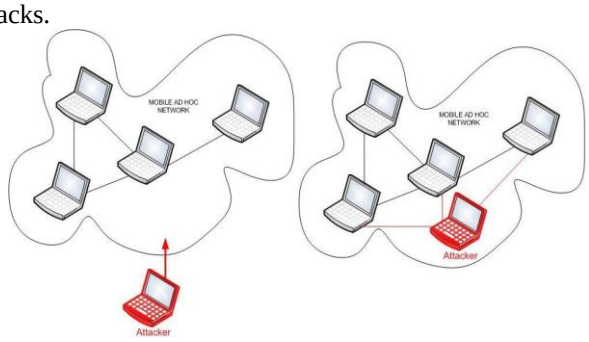

Fig. 3.1 External and Internal Attacks in MANETs

3.2.2 Active and Passive Attack

When the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network [13]. Active attacks can an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings the attacker in strong position

where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network [13]. In Passive attack, the attacker listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

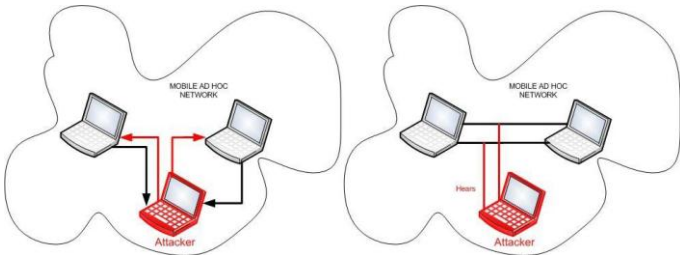

Fig. 3.2 Active and Passive Attack in MANETs

IV. BLACK HOLE ATTACK IN MANET

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter "security issues in MANET" on the basis of their nature. In these attacks, black hole attack is that kind of attack which occurs in Mobile ad hoc networks (MANET). This chapter describes Black Hole attack and other attacks that are carried out against MANETs.

4.1 Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [21]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [22].

The method how malicious node fits in the data routes varies. Fig. 4.1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

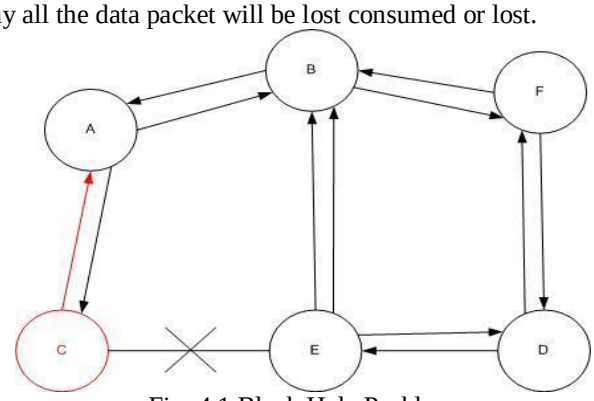

Fig. 4.1 Black Hole Problem

4.1.1 Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

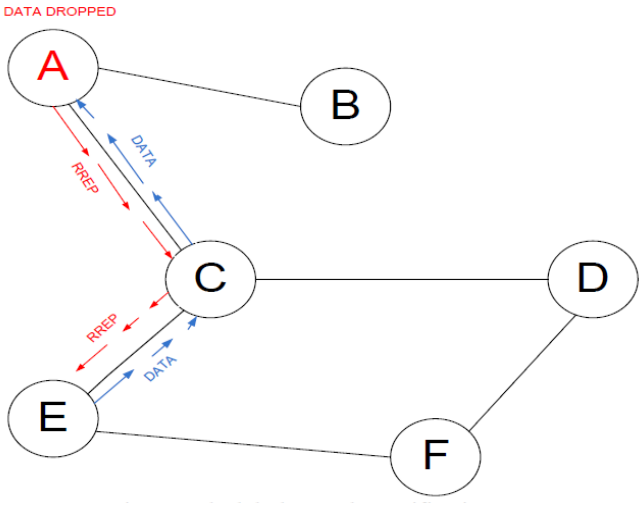

Fig. 4.2 Black hole attack specification

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the
malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

4.1.2 Black hole attack in OLSR

In OLSR black hole attack, a malicious node forcefully selects itself as MPR which is discussed in chapter 3.Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack.

The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes.

4.2 Other Attacks on MANET

4.2.1 Gray Hole Attack

In this kind of attack the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receive the packets from the neighboring node, the attacker drop the packets. This is a type of active attack. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [14]. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack [15].

4.2.2 Flooding Attack

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding [16]. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

4.2.3 Selfish Node

In MANET the nodes perform collaboratively in order to forward packets from one node to another node. When a node refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disruption [16]. The selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes. The concern of the node is only to save and preserves it resources while the network and traffic disruption is the side effect of this behavior. The node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network.

The selfish node can sometime drop the packets. When the selfish node see that the packets need lot of resources, the selfish node is no longer interested in the packets it just simply drop the packets and do not forward it in the network.

4.2.4 Wormhole Attack

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. The fig.3.5 bellow shows the two attackers placed themselves in a strong strategic location in the network.

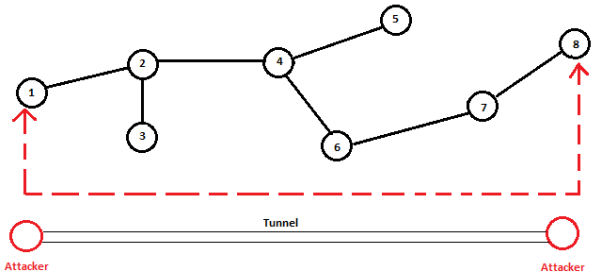

Fig. 4.3 Wormhole attack

In wormhole attack, the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes as shown in the Fig. 4.5 above. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network [12].When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such position the attack is known as out of band wormhole [17].

The other type of wormhole attack is known as in band wormhole attack [17]. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

4.2.5 Sleep Deprivation Torture Attack

One of the most interesting attack in MANETs, where the

attacker tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep. This attack is known as sleep Deprivation torture attack [18]. The nodes operating in MANETs have limited resources i.e. battery life, the node remain active for transmitting packets during the communication. When the communication cease these nodes go back to sleep mode in order to preserve their resources. The attacker exploit this point of the nodes by making it busy, keeping it awake so as to waste all its energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily walk into the network and exploit rest of the network.

4.2.6 Jellyfish Attack

In jellyfish attack, the attacker attacks in the network and introduce unwanted delays in the network [19]. In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are propagated then packets are released in the network. This enables the attacker to produce high end to end delay, high delay jitter and considerably effect the performance of the network.

4.2.7 Modification Attack

The nature of ad hoc network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack [13]. Misrouting and impersonation attacks are two types of modification attack.

4.2.8 Misrouting Attack

In misrouting attack a malicious node which is part of the network, tries to reroute the traffic from their originating nodes to an unknown and wrong destination node. As long as the packets remain in the network make use of resources of the network. When the packet does not find its destination the network drops the packet.

4.2.9 Impersonation Attack

In ad hoc networks a node is free to move in and out of the network. There is no secure authentication process in order to make the network secure from malicious nodes. In MANETs IP and MAC address uniquely identifies the host. These measurements are not enough to authenticate sender. The attacker use MAC and IP spoofing in order to get identity of another node and hide into the network. This kind of attack is also known as spoofing attack [13].

4.2.10 Routing Table Overflow Attack

Routing Table Overflow attack is usually done against proactive protocols. In this attack, non-existent node data is sent in the network, more ever corrupting and degrading the rate, when routing tables are updated. Proactive routing protocols updates route periodically before even they are required. This is one of the flaws that make proactive protocols vulnerable to the routing table attack. The attacker tries to create so many routes to nodes that do not exist in the network. This is done by using RREQ messages. The attacker sends RREQ messages in the network to non-existent nodes. The nodes under attack results its routing table full and doesn't have any more entry to create new. In other words the routing tables of the attacked nodes are overflow with so many route entries [20].

V. RESEARCH METHODOLOGY

Research methodology defines how the development work should be carried out in the form of research activity. Research methodology can be understand as a tool that is used to investigate some area, for which data is collected, analyzed and on the basis of the analysis conclusions are drawn. There are three types of research i.e. quantitative, qualitative and mixed approach as defined in [29].

5.1 Quantitative Approach

This approach is carried out by investigating the problem by means of collecting data, experiments and simulation which gives some results, these results are analyzed and decisions are made on their basis. This approach is used when the researchers' wants verify the theories they proposed, or observe the information in greater detail.

5.2 Qualitative Approach

This approach is usually involves the knowledge claims. These claims are based on a participatory as well as / or constructive perspectives. This approach follows the strategies such as ethnographies, phenomenology and grounded theories. When the researcher wants to study the context or focusing on single phenomenon or concepts, they used qualitative approach to achieve their desired goals.

5.3 Mixed Approach

Mixed approach glue together both quantitative and qualitative approaches. This approach is followed when the researchers wants to base their knowledge claims on matter of fact grounds. Mixed approach has the ability to produce more complete knowledge necessary to put a theory and practice as it combined both quantitative and qualitative approaches.

5.4 Author's Approach

Author's approach towards the thesis is quantitative. This approach starts by studying the elated literature specific to security issues in MANETs and MANETs. Literature review is followed by simulation modeling. The results are gathered and analyzed and conclusions are drawn on the basis of the results obtained from simulation.

5.5 Research Design

The author divided the whole research thesis into four stages.

1) Problem Identification and Selection.
2) Literature study.
3) Building simulation.
4) Result analysis.

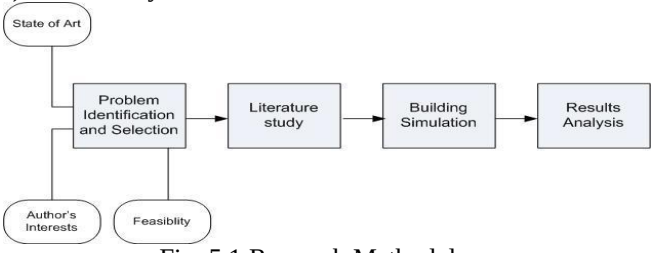

Fig. 5.1 Research Methodology

1) Problem Identification and Selection
The most important phase where, it is important to select the proper problem area. Different areas are studied with in mind about the interest of authors. Most of the time is given to this phase to select the hot issue. The authors selected MANET as the area of interest and within MANET the focus was given to the security issues
2) Literature Study
Once the problem was identified the second phase is to review the state of the art. It is important to understand the basic and expertise regarding MANETs and Security Issues involve in MANETs. Literature study is conducted to develop a solid background for the research. Different simulation tools and their functionality are studied.
3) Building Simulation
The knowledge background developed in the literature phase is put together to develop and build simulation. Different scenarios are developed according to the requirements of the problems and are simulated.
4) Result Analysis
The last stage and important and most of the time is given to this stage. Results obtained from simulation are analyzed carefully and on the basis of analysis, conclusions are drawn.

VI. RESULTS

This chapter focuses on result and its analysis based on the simulation performed in OPNET modeler 14.5. Our simulated results are provided in Figures (7.1-7.12) gives the variation in network nodes while under Black Hole attack. To evaluate the behavior of simulated intrusion based black hole attack we considered the performance metrics of packet end to end delay, throughput and network load. These parameters are already defined in chapter 6 "performance analysis".
6.1 Packet End-to-End Delay
Packet end to end delay in case of Black Hole attack and without attack depends on the protocol routing procedure and number of nodes involved. In Fig. 7.1, delay in case of 16 nodes for AODV and OLSR is high in case when there is no attack on the network nodes. This is because during the Black Hole attack there is no need of RREQs and RREPs because the malicious node already sends its RREQs to the sender node before the destination node reply having less delay. Also comparatively AODV show more delay than OLSR because of its route search and reactive nature as explained in chapter 3 "MANET Routing Protocol".

VII. CONCLUSIONS AND FUTURE WORK

Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis we have analyzed the behavior and challenges of security threats in mobile ad hoc networks with solution finding technique.
Although many solutions has been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After studying all the approaches our conclusion is that the approach offered by Deng [27] suit well in our scenario. The intermediate reply messages if disabled leads to the delivery of message from destination node will not only improve the performance of network rather it will secure the network from Black Hole attack.
In our study we analyzed that Black Hole attack with four different scenarios with respect to the performance parameters of end to end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR.
Based on our research and analysis of simulation result we draw the conclusion that AODV is more vulnerable to Black Hole attack than OLSR.

Future Work
Wireless Ad hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still need in this area. We tried to discover and analyzed the impact of Black Hole attack in MANETs using AODV and OLSR protocols. There is a need to analyze Black Hole attack in other MANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior has to be carried out for further research.

REFERENCES

[1] http://en.wikipedia.org/wiki/Personal_area_network , last visited 12, Apr, 2010.
[2] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010.
[3] C.E.Perkins and E.M.Royer, "Ad Hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.
[4] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[5] http://www.faqs.org/rfcs/rfc3561.html
[6] M.Abolhasan, T.Wysocki, E.Dutkiewicz, " A Review of Routing Protocols for Mobile Ad Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, 2003.
[7] http://www.faqs.org/rfcs/rfc3626.html
[8] http://www.netmeister.org/misc/zrp/zrp.html#SECTION00041000000000000000, last visited 12 Apr, 2010.
[9] P.V.Jani, "Security within Ad Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
[10] M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile ad hoc networks"
[11] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad Hoc Neworks," International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.
[12] N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad Hoc Network".

