International Journal of Information and Communication Technology Research

http://www.esjournals.org

Survey of Black Hole Attack and Security Scheme in MANET

Sonal Shrivastava, Chetan Agrawal, Anurag Jain
Department of Computer Engineering, RITS, Bhopal (M.P) India

ABSTRACT

Mobile ad hoc networks (MANETs) is a collection of mobile nodes which are self-managed and connected by wireless links automatically as per the delineate routing protocol. These nodes communicate with each other in its range and those which are not in wireless range can communicate the multi hop communication in which other node relay the packets. Due to absent of a defined central authority, securitizing the routing process becomes a challenging job by that leaving MANETs vulnerable to attacks, which results in degrade in the performance characteristics as well as enhance a serious question mark about the reliability of such networks. Black hole is a type of routing attack, an attackers first introduce itself in the forwarding group but it does not forwarding the data packet, it drops all the packet and it result receive a poor packet delivery ratio. In this paper we have acted to present an abstract of the routing protocols, the known routing attacks and to measure misbehavior activity of these attacks in various works. Proposed approaches can be integrated on top of any source routing protocol and based on forwarding acknowledgement packets and calculating the number of data packets of active path.

Keywords: *MANET, routing, attack, black hole, misbehaviour*

1. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) is a collection of mobile nodes, communicating among themselves over multi-hop paths, without use any predefined infrastructure. This network is helpful in any situation where instantaneous network connectivity is needed such as flood recovery, disaster relief and battle field communication. Ensurity in Mobile Ad-Hoc Networks is an important refer for the network functioning. MANET usually know how various security attacks because of its succeeding illuminates: Dynamically changing network topology, lack of central monitoring, cooperative algorithms and absence of a certification authority and etc [20, 21]. The features of Mobile adhoc networks are explained as follow-*(a)Dynamically changing network topology*: Network topologies can be changed without any prior information, it may be frequently or unpredictably which may changes the partitioning of network and routes which causes loss of data or packet.*(b)Lack of centralized monitoring*: MANETs have no established infrastructure or centralized administration and its works without any preexisting infrastructure. Due to lack of centralized management leads MANET is vulnerable to various kinds of attacks. For large scale Ad-Hoc network is very challenging due to no central management.*(c)Cooperative algorithms*: There should be some kind of relationship and trust between the neighboring nodes and routing algorithms which is used in MANET.*(d)Bandwidth constraint*: Capacity of wireless links are lower as compared to the infrastructures networks.*(e)Limited physical security*: Security risks are higher in mobile nodes. As the mobility of nodes increases security risks also increase and results in the Dos attacks, eavesdropping and masquerading or spoofing in the nodes.*(f)Energy constrained operation*: For mobile nodes in Ad-Hoc network, battery is the only means of power which have limited storage capacity and power supply and needs to recharge them frequently.

MANET can be applied to different applications include battlefield communication, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security sensitive computing environments. There are 15 major issues and sub-issues involving in MANET such as routing, multicasting, location, service, clustering, mobility management, TCP/UDP, IP addressing ,fault tolerance, and standard/products. The routing protocol of MANET may generally be categorized as: table driven/proactive and source-initiated (demand driven)/reactive. In proactive routing protocols, such as the optimized link state routing (OLSR),node obtain routes by periodic exchange of topology information. In reactive routing protocols, such as the adhoc on demand distance vector(AODV)protocol nodes find routes only when required. MANET is much more vulnerable to attack than wired networks. This is because of the various factor like open medium, dynamically changing networks topology, energy constrained operation and limited physical security. As shows in fig 1. an adhoc network consist of several home computing device, including laptop, cellular phones and so on. Communication can be done directly between any nodes within its transmission range.

International Journal of Information and Communication Technology Research

http://www.esjournals.org

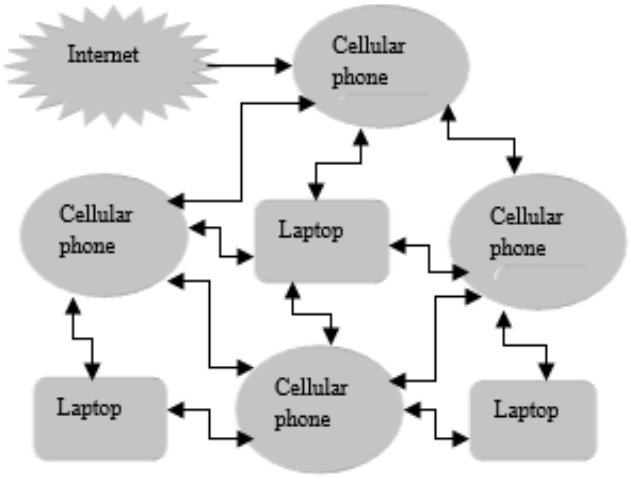

Fig 1. Mobile adhoc networks

The rest of these paper is organized as follows: In section II we present different types of attacks in MANET. Section III discuss security measure against attacks in MANET. Section IV gives the research scope. Finally, the summery and discussion of future work is in session V.

Attack in Manet

Attack can be classified as internal and external attack based on the source of attacks. External attack are done by illegitimate users and these attackers are not need fully disconnected from the network though. The targeted network might be a autonomous entity that is linked to another network using the same infrastructure or communication technology. While internal attack are sourced from inside a particular network. A conceded node with access to all other node within its range poses a high threat to the structural efficiency to the entire network. Another type of classification is active attack and passive attack according to the layer of occurence are discussed below:

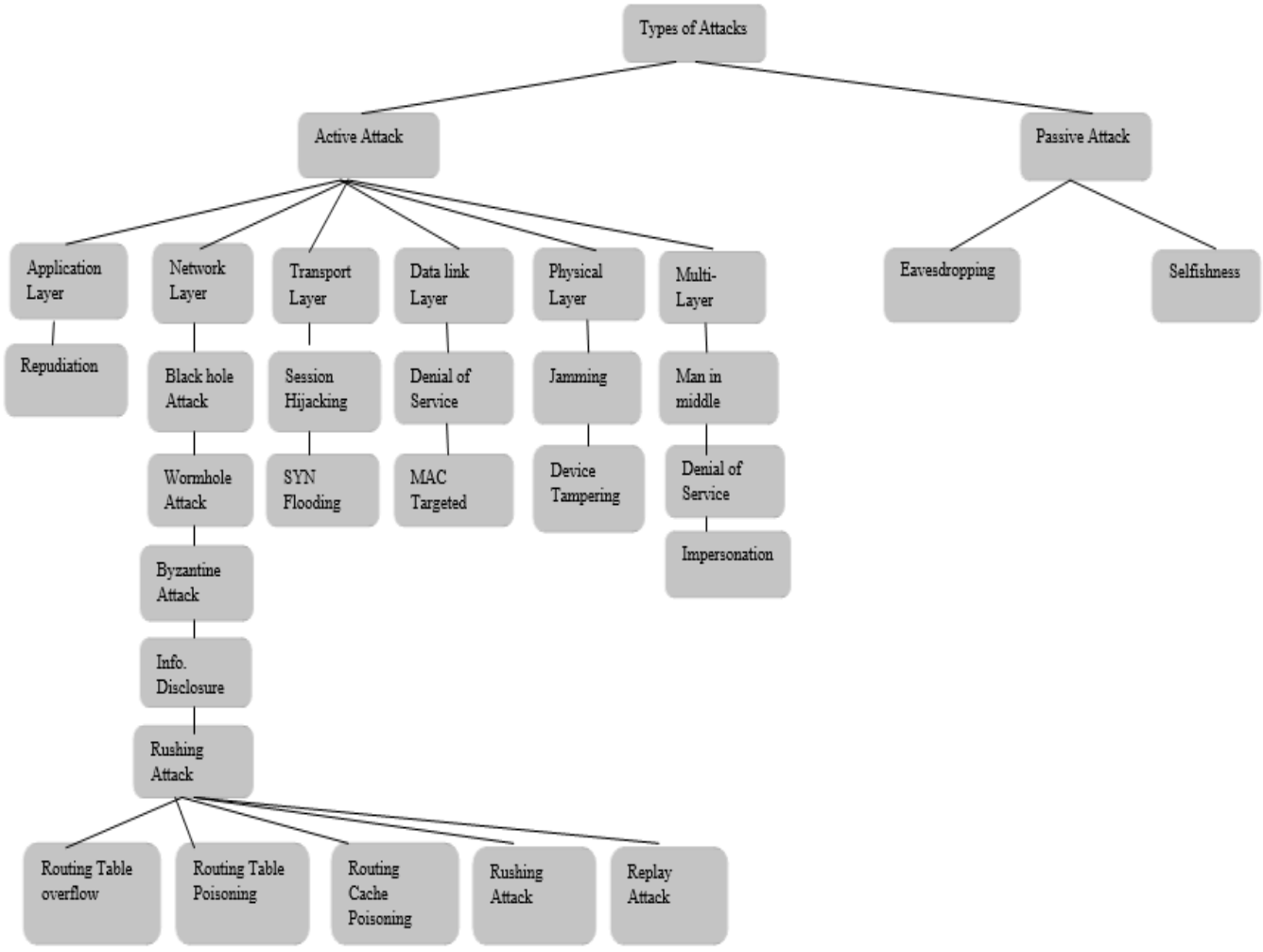

Fig.2 Classification of attacks

International Journal of Information and Communication Technology Research

http://www.esjournals.org

Attacks can be categorised into two classes.

I. Passive Attacks

The attacker just snoops the network without interrupt the network operation. These attacks consist the confidentiality of the data and say which nodes are performing in dissipated mode.

- *Eavesdropping:* It is studying or snooping of messages by an unintentional receiver. In MANET, the nodes overlap a wireless medium so nodes can easily take in interaction of the nodes inside its transmission range. This attack can be admonished by employing encryption.
- *Selfishness:* A selfish node in order to rescue its battery life and resources does not take part in routing either by dropping the packets or not sending them.

II. Active Attacks

Attacks in which attacker interrupt the natural operation of the network by fabricating messages, dropping or modifying packets, replaying packets or tunnelling them to another part of the network. Generally, the contain of message is revised. These can be internal attacks (caused by concessioned nodes inside the network) and external attacks (caused by the nodes external the network). Active attacks can be further categorised corresponding to different layers in MANET:

A) Application Layer Attacks

- *Repudiation:* It is an act of decline in cooperating in all or part of the conversation. For example, repudiation attack on a mercenary system in which a selfish node can decline performing credit card purchase, or any online bank transaction.
- *Malicious Attack:* In this attack, a malicious node interrupt the normal operation of another nodes in the network by attacking the operating system.

  Malicious node sends virus, worm or Trojan horse to a fatality node. A virus is a computer program that affixes itself to legalize program causing ruinous to nodes and remain dispersing around the network. A Trojan horse taciturnly sits behind legalize program and permit an attacker to get some confidential information about a node or the network.

B) Transport Layer Attacks

- *Session Hijacking:* In this attack, an attacker retain retrieve to the session state of a specific user by thievery session ID which is utilize to retain into a system and snoops the data. Since most of the times authentication only appear at the beginning of session, this allows an attacker to deprive access to a node. Hijacking is accomplished after the victim node has established the connection. At first attacker presage the true sequence number and then spoofs victim‘s IP address. Meanwhile to occupy over the session attacker has to establish DoS attack against the victim. The victim node hangs and attacker acquaint as if it is a legalize system.
-

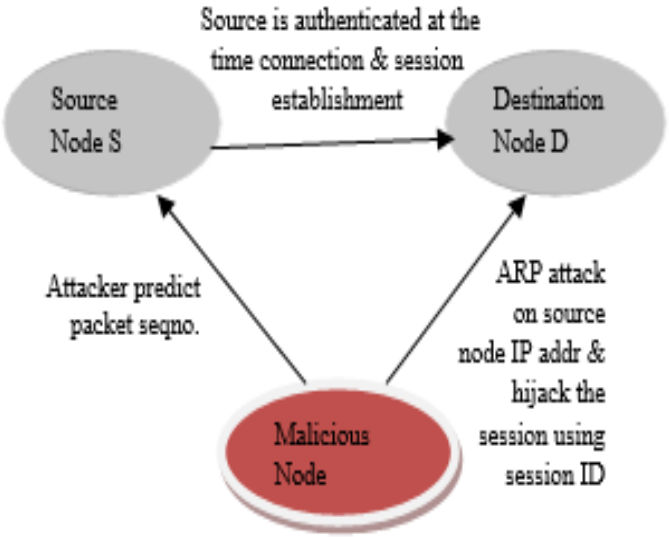

Fig.3 Session Hijacking Attack

- *SYN Flooding:* On the internet, nodes convey using TCP/IP protocol thus they require to establish connection using three-way handshake. A malicious node transfer a large number of SYN packets to a fatal node.

  The fatal node transfer reverse SYN+ACK packets and stay the entry for the deficient connection request. The attacker never transfer ACK so a huge amount of memory of fatal node is devoured for keeping pending requests and node may come to a halt even. Some other way of establishing this attack is spoofing the come back address of SYN packets with vacant node so SYN+ACK packets never reach any node fooling the fatal node.

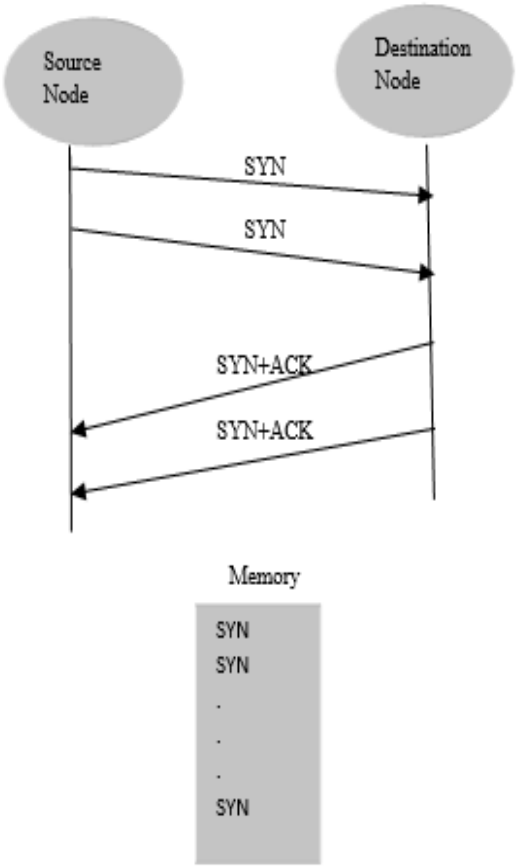

Fig.4 SYN Flooding Attack

C) Network Layer Attacks

Wormhole Attack: In wormhole attack, two concurring nodes are referred and one node tunnels the packet to some other node in the uniform network over a huge speed private wired link or wireless link [1]. These packets are then dislike from that location into the network. This tunnel between two selfish nodes is known as wormhole.

This attack can calmly be established against communications that rendezvous to authenticity and confidentiality. The other type of wormhole attack is known as *in-band* wormhole attack. 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. When the attacker node create a direct link between each other in the network. The wormhole attacker then receive packet at one end & transmit the packet to the other end of the network. When the attacker are in such position the attack is known as *out-of-band* wormhole attack.

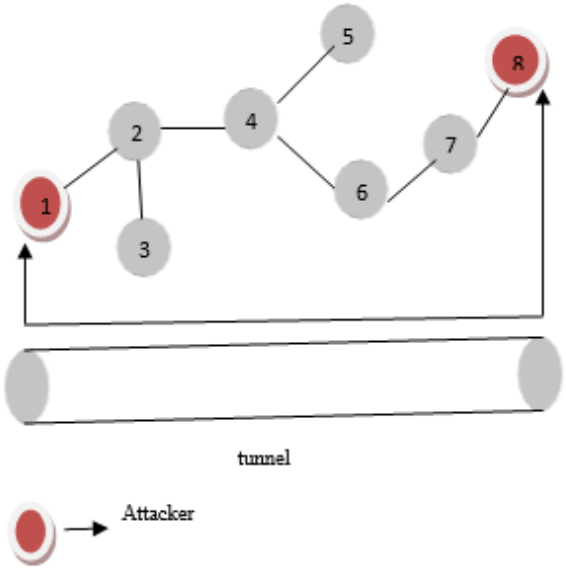

Fig.5 Wormhole Attack

- *Black hole Attack:* In this attack, a selfish node announced valid and precised route to a victim node and there after quietly drops data and control packets as they travel through it. In order to have shortest route, black hole node builds forged packet by modifying hop count and orders number of the routing protocol message such as AODV. For example, source node A desire to communicate with destination node D. It propagate RREQ (route request) messages to its neighbors. An attacker C fake a reply packet by modifying hop count asserted that it has shorter route to D or by incrementing destination sequence number than the legitimate value last advertised by D demonstrate it has unspoil route to D refer Fig 6. This leads to the establishment of a fake route through the attacker when selfish assemble reply reaches A first than authorized reply [2]. So, attacker node can eavesdrop or drop the packets. Selfish node is known as black hole since it devour data packets transmit to it and never sends them.

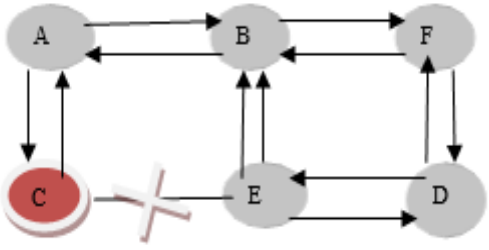

Fig. 6 Blackhole Attack

- *Byzantine Attack:* This attack involves numerous attackers that work in collusion to put down the network performance such as creating loops, selectively dropping packets, choosing non optimal paths for packet forwarding. In Fig 7, attacker A1 sends routing packets of S normally to A2 but second attacker A2 give up or forges these routing packets. In [3] collusion attack in OSLR protocol is talk about and it has been shown that pair of colluding attackers can interrupt 100 % of data packets.

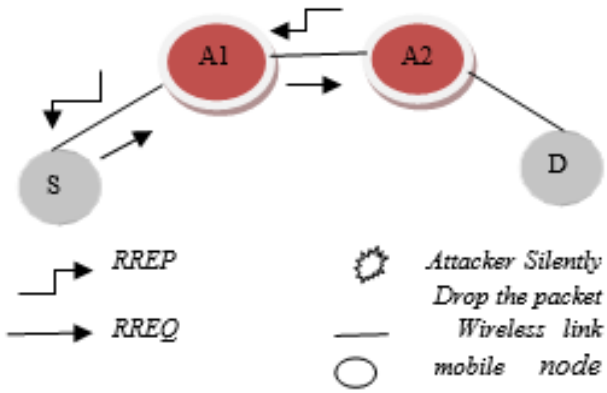

Fig.7. Byzantine Attack

- *Information Disclosure:* A compromised node may disrupt the confidentiality principle of security and expose essential information like private and public keys, status of nodes, passwords, optimal route to authorized nodes, geographic location of nodes and another control data in packet headers to unauthorized nodes exist in the network. The location information showed give better understanding of the network topology. Routing packets are then sent with insufficient hop-limit and ICMP error messages returned by the intercede nodes are recorded [4]. So it provides blueprint of the network i.e. which nodes are situated in close adjacency to the target node.
- *Routing Table Overflow:* This attack inhibit creation of new authorized routes by flooding the routing table with routes to vacant nodes. This utilize the limited memory capacity of mobile nodes. A malicious node initiates route discovery to non-existent nodes so that limited memory of mobile node gets exhausted by having such entries in their routing table which in turn inhibits the formation of new routes to legitimate nodes in the network. The proactive ad hoc protocols are more susceptible to this attack because in such networks, routes to all the nodes are earlier stored before they are needed, in contrast to reactive protocols in which information is detected when needed.
- *Routing Table Poisoning:* In this attack, malicious node transmit fabricated routing update and error messages or modified authorized updates to legitimate nodes in the network. It may result in sending packets along sub optimal routes, congestion in the network, formation of loops or blackmail attack in which an attacker transmit untrue route error messages against benign node in order to report benign node as malicious and thus establishing denial of service attack against it. In on demand ad hoc protocols, like AODV and DSR, there is individual route maintenance phase to agreement with split routes as nodes move or fail.
- *Routing Cache Poisoning:* Route cache is sustained by on demand protocols like DSR that keeps the routes known to it by eavesdropping on neighborhood transmissions in the recent past. A malicious node can establish DOS attack on any node by simply propagating spoofed packets with source routes to D via itself. Any neighboring node overhearing the packet transmission adds the route entry in their route cache [5].
- *Replay Attack:* An attacker instead of modificatory packet‘s contents just replay on original packets in order to impose battery power, bandwidth and computational constraint of mobile nodes. It conduct to congestion in the network and turmoil among the routing nodes because of combating information, thus delaying packet delivery or inhibiting them from reaching destination.
- *Rushing Attack:* This attack comprise entire network traffic to travel through an attacker. The source node is ineffective to find any secure route without the attacker. Malicious node after getting RREQ packet from establishing node reacts promptly and floods the network rapidly with these packets before other nodes receiving the same RREQ can react. Nodes receiving authorized RREQ packets suppose them as duplicates and dispose of them. So every route established has attacker as one of the intercede nodes.
- *Jellyfish Attack*: It is a selective black hole attack in which malicious node attacks the network by rearranges packets, dropping selective packets or expanding jitter of the packets that pass through it in order to defend it from being detected and it seems to the network that loss or delay is due to environmental reason

D) Data Link Layer Attacks

- *Denial of service:* There is a single wireless channel shared by all the nodes so a malicious node stays this channel busy by sending false packets to drain node‘s battery power.
- *MAC targeted Attack:* In MANET, nodes share a wireless medium so medium access control (MAC) protocols are used to coordinate the transmission and to resolve the contention. These attacks interrupt the MAC procedure. For example, an attacker can pervert the frames by introducing extra bits.

E) Physical Layer Attacks

- *Device Tampering*: Nodes in ad hoc wireless networks are small, compact and hand-held unlike wired devices so can be easily stolen or damaged.
- *Jamming:* The attacker supervise the wireless medium in order to find frequency at which destination node is receiving from sender node. An attacker must have influential transmitter to sends the signals to the destination at that frequency, through interfering with its operations. The most common types of signal jamming are random noise and pulse.

F) Multilayer Attacks

These attacks can be establish from several layers instead of a single layer. Examples of multi-layer attacks are jamming, denial of service attacks, impersonation attacks and man-in-the-middle attack.

- *Denial of service attack:* In this, an attacker relinquish a system unusable, or significantly slows it down for authorized users by overloading its resources. The goal is that if an attacker can‘t access the node, it will collide the node.
  In wired networks, DoS is establish against centralized resource, so it is not available to other authorized nodes.
  But in wireless networks there is no single centralized resource so there are numerous other ways by which it can be launched from many layers. At the physical layer, signal jamming interrupt normal communications. At the link layer, malicious nodes inhibit other nodes from channel access. At the network layer, DoS attacks are mounted on routing protocols and disrupt the network performance through routing packets modification, selective dropping or routing table overflow. An example of DoS attack on DSR with changed source route is shown in Fig 8. In DSR, source nodes are explicitly stated in routes in data packets. The routing mechanism inadequate integrity checks so DoS attack can be launched by modifying the source routes in packet headers. Assume a path exists from node S to node D and Y and D cannot take in transmission of each other directly. Let M be a malicious node that wishes to launch DoS attack. S wishes to communicate with D and has an valid route in its route cache to D. S transmits a data packet toward D with the source route (S,X, M, Y, Z, D) encompass in the packet's header. On receiving the packet from X, M alters the source route by deleting Z from the source route in packet‘s header. Consequently, when Y receives the modified altered packet, it attempts to forward the packet to D directly. Since Y cannot hear D, the transmission is unsuccessful. At the transport layer, SYN flooding and session hijacking can cause DOS attacks.

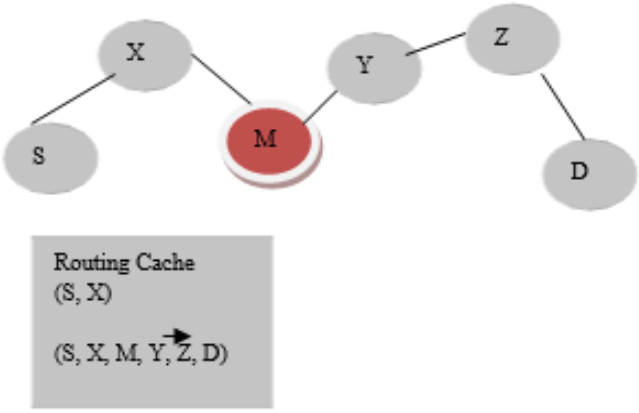

Fig.8 Denial of Service Attack

- *Impersonation attacks:* Impersonation attacks are established by using other node‘s identity, such as MAC or IP address. Impersonation attacks occasionally are the first step for most attacks, and are used to establish further more cultivate attacks. A malicious node can disguise itself as an legitimate user and give untrue routing information or change the configuration of the network. Examples of impersonation attack are Sybil attack and trust attack. In Sybil attack, a malicious node or entity has one physical device and forges multiple identities. A deficient node may present multiple identities to an ad-hoc network in order to function as multiple distinct nodes. After becoming part of the network, the a adversial overhears communications or acts maliciously. In threshold scheme where a message or key shares are

fragmented into different parts and each part takes different path, the attacker may get access to all pieces of smashed information as it has enforce several different identities.

- *Man-in-the-middle attack:* An attacker sits quietly between the sender and the receiver and makes the actual communicator believe that they are communicating to each other but in original they are communicating to the man-in-the-middle who is communicating to each of them.

Some Specific Attack on Routing Protocol

There are many attacks in MANET that target the specific routing protocols. This is due to establishing routing services without considering security issues.

- *AODV* The Ad-hoc On-demand Distance Vector (AODV) routing algorithm is a reactive algorithm that routes data beyond wireless mesh networks. The advantage of AODV is that it is uncomplicated, needs less memory and does not create other new traffic for communication along existing links. In AODV [6], the attacker may promotes a route with a smaller distance metric than the authentic distance or announce a routing update with a big sequence number and unsupportive all routing updates from other nodes.
- *DSR* Dynamic Source Routing (DSR) protocol is similar to AODV in that it also make route on-demand. But the chief difference is that it uses source routing instead of relying on the routing table at each intercede node. It also provides functionality therefore packets can be transmitted on a hop-by-hop basis. In DSR, it is probable to modify the source route menu in the RREQ or RREP packets by the attacker. Deleting a node from the menu or series, switching the order or adjoining a new node into the menu is also the potential insecurity in DSR.
- *ARAN* Authenticated Routing for Ad-hoc Networks (ARAN) is an on-demand routing protocol that observe and defend against malicious actions carried out by third parties and peers in specific ad-hoc environment [8]. This protocol presents authentication, message integrity and non-repudiation as a part of a minimal security policy. Though ARAN is designed to build up ad-hoc security, still it is insusceptible to rushing attack.
- *ARIADNE* ARIADNE is an on-demand secure ad-hoc routing protocol based on DSR that utilize highly efficient symmetric cryptography. It gives point-to-point authentication of a routing message utilize a message authentication code (MAC) and a shared key between the two communicating parties. Although ARIADNE is release from a flood of RREQ packets and cache poisoning attack, but it is insusceptible to the wormhole attack and rushing attack [7].
- *SEAD* Specifically, SEAD creates on the DSDV-SQ version of the DSDV (Destination Sequenced Distance Vector) protocol. It accord with attackers that reorganize routing information and as well with replay attacks and forms use of one-way hash chains instead implementing extravagant asymmetric cryptography operations. Two different approaches are used for message authentication to protect the attackers. SEAD does not manage with wormhole attacks [7].

Security Measures against attacks in MANETs

Network layer is more susceptible to attacks than all other layers in MANET.

A variety of security risks is access in this layer. The active attack like modification of routing messages can be protected through source authentication and message integrity mechanism. For example, digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain is habituate for this role. By an incurable and self-sufficient physical metric including time delay or geographical location can be used to discover wormhole attack. For example, packet leashes are used to battle this attack [10].IPSec is most generally used on the network layer in computer network that could be used in MANET to gives certain level of confidentiality. The secure routing protocol named ARAN defend from several attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source route etc [8]. The research by Deng [9], et al shows that a solution to overcome black hole attack. The solution is to unable the ability to reply in a message of an intercede node, so all reply messages should be sent out only by the target node.

Some approaches to detect/prevent these attack namely Wormhole attack Black hole attack, and their limitation.

1. Detection/Prevention of Wormhole Attack

Various approaches have been proposed to defend against a Wormhole attack; Table I. briefly mentions some of them along with their limitations.

Table1.Wormhole Detection/Prevention Techniques

Approach	Description	Limitations
Geographical Leashes[11]	Ensuring that the receiver must be within certain distance from the sender.	Limitations of GPS technology.
Temporal Leashes[11]	Time stamp given for packet.	All nodes require tightly synchronized clocks.

International Journal of Information and Communication Technology Research

http://www.esjournals.org

End-to-end Leashes [12]	Each intermediate node appends time and location information and Receiver authenticates time and location information of a packet using symmetric key.	Limitations of GPS technology.
Statistical Analysis [13]	Identifying highest frequency link through analyzing relative frequency of each link appearing in obtained routes.	Works only with multipath on demand protocols.
Directional Antennas [14,15]	Each pair of nodes determines the direction of received signals from neighbor; if directions match, relation is set.	Not applicable to network without directional antennas.

2. Detection/Prevention of Blackhole Attack

Various approaches have been proposed to defend against a Blackhole attack; Table II. briefly mentions some of them along with their limitations.

Table II. Blackhole Detection/Prevention Techniques

Approach	Description	Limitations
Reply Packet Authenticity [16]	Verifying the authenticity of node sending reply packet and wait for reply packets from more than two nodes.	Longer time Delay.
Last-Packet-Sequence-Numbers [16]	Every node keeps two additional small-sized tables: one to keep last-packet-sequence-numbers sent to every node and second to keep last-packet-sequence numbers received from every node.	The malicious node can listen to the channel and update the tables for the last packet sequence number.
Common Neighbor Listening [17]	Using common neighbors, acting as watchdogs, to detect attack and discover a new route.	Adds some routing control overhead and works in specific circumstances.
Route Confirmation Request-Reply [18]	The intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and confirmation message, the source determines the validity of path according to its policy.	Doesn't work if two consecutive nodes are malicious.
SAODV [19]	Check path containing repeated next hop node to destination; if there is no repeated node, select random path.	Increases average end-to end delay.

2. RESEARCH SCOPE

The scope of this thesis is to study the effects of Black hole attack in MANET using Reactive routing protocol Ad-Hoc On Demand Multipath Distance Vector (AOMDV). In MANET, all networking works such as routing and packet forwarding, are achieved by nodes themselves in a self-organizing manner. For these reasons, protecting a mobile ad -hoc network is very challenging. The goal is to valuate if mobile ad hoc Comparative analysis of Black Hole attack for reactive protocol is taken into account. The influence of Black Hole attack on the performance of MANET is evaluated finding out protocol is more vulnerable to the attack and how much is the effect of the attack on protocols. The assessment were occupied in the light of throughput, end-to-end delay and network load.

3. SUMMARY

The important disadvantage of the MANETs is the limited resource capability: bandwidth, power back up and computational capacity. Because of ease of deployment and defined infrastructure less feature these networks find

applications in a numerous of script ranging from emergency operations and disaster relief to military service and task forces. Susceptibility of channels and nodes, dynamically developing topology produce the security of MANETs particularly difficult. Also no centralized authority is present to supervise the networking operations. Thus, subsisting security schemes for wire networks cannot be served directly to a MANETs, which forms them much more vulnerable to security attacks. Misbehavior of nodes may cause wick damage, even break down whole of the network. In this paper, investigation is done on the misbehavior of nodes and a new approach is proposed for detection and isolation of misbehaving nodes.

In future we propose a new algorithm for multipath routing for improving network performance from attack like throughput, Routing load and delay.

REFERENCES

[1]. H. Yih-Chun Hu; Perrig, A.; Johnson, D.B., ―Wormhole attacks in wireless networks‖, *Selected Areas in Communications, IEEE Journal on* , vol. 24, no. 2, pp. 370- 380, 2006.

[2]. Usha and Bose, ―Understanding Black Hole Attack in Manet‖, *European Journal of Scientific Research*, vol. 83, no. 3, pp.383-396, 2012.

[3]. sB. Kannhavong, H. Nakayama, A. Jamalipour, ―NIS01-2: A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks‖,*Global Telecommunications Conference, GLOBECOM '06, IEEE*, 2006, pp.1-5.

[4]. [R. mishra, S. Sharma, R. Agrawal, ―Vulnerabilities and security for ad-hoc networks‖, *International Conference on Networking and Information Technology*, *IEEE* 2010, pp. 192-196.

[5]. S. Gupte, M. Singhal, ―Secure routing in mobile wireless ad hoc networks‖, *Ad hoc networks, Elsevier*, vol. 1, no. 1, pp. 152-174, 2003.

[6]. Nishu Garg and R.P.Mahapatra, "MANET Security Issues ," IJCSNS International Journal of Computer Science and Network Security,VOL.9 No.8, August 2009.

[7]. Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[8]. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer,"*Secure routing protocol for ad hoc networks,"* In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci.,California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002, Page(s):78- 87, ISSN: 1092-1648

[9]. H. Deng, W. Li, Agrawal, D.P., "*Routing security in wireless ad hocnetworks,"* Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[10]. Y. Hu, A. Perrig, and D. Johnson, *"Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks,"* Proc. of IEEE INFORCOM, 2002.

[11]. Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[12]. W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[13]. L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath,"IEEE Wireless Commuunication. and Networking Conference,2005.

[14]. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium,pp.131-141, 2003.

[15]. L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[16]. Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96-97.

[17]. Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[18]. S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad HocNetworks", International Conference on Parallel Processing Wowrkshops, August 2002.

[19]. Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp.21-26.

[20]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Issue 3, Nov 2007, pp 338–346.

[21]. Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks" Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93 B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.