ISSN:0975-9646

Network Layer Attacks and Protection in MANET- A Survey

Athira V Panicker, Jisha G

Rajagiri School of Engineering and Technology,
Department of Information Technology
Rajagiri Valley P O, Cochin, Kerala, India

Abstract: **A Mobile ad hoc network is a network of mobile devices with dynamic structure. Here each node participates in routing by forwarding data to other nodes. Security has become a primary concern to provide protected communication between nodes in ad hoc networks. There are a number of challenges in security design as ad hoc network is a decentralized type of wireless network. There are five layers in MANET and each of these layers are vulnerable to various type of attacks. In this paper we discuss about various attacks in network layer, their defense mechanisms and comparison between these defense mechanisms.**

Keywords- MANET, Network Layer attacks

I. INTRODUCTION

In MANET each device is free to move in any direction, so the links to other devices will change frequently. Here each node acts as a router. The main challenge in building MANET is that each device in it should maintain updated information to properly route traffic. Each layer in MANET is subjected to attacks. Mainly the attacks can be at two levels one is at routing level and other is to destroy the security mechanism used in network.

Attacks in MANET can be divided into two types they are active attack and passive attack. In passive attack they add unauthorized listening in network and data is transferred without change. In active attack they extract information and they allow information flow between nodes. The active attack can be divided into four categories they are:

- Dropping attacks: Here data packets that are transmitted are dropped at compromised or selfish node.
- Modification attacks: In this type of attack they alter the packets and disrupt the communication between the nodes in the network
- Fabrication attacks: Here the attacker node send fake message without getting any related message and this can be called as forge reply.
- Timing attacks: Here attacker attack other nodes to it by advertising itself as node near to actual node Indicate that it is having a fresh shortest path to destination.

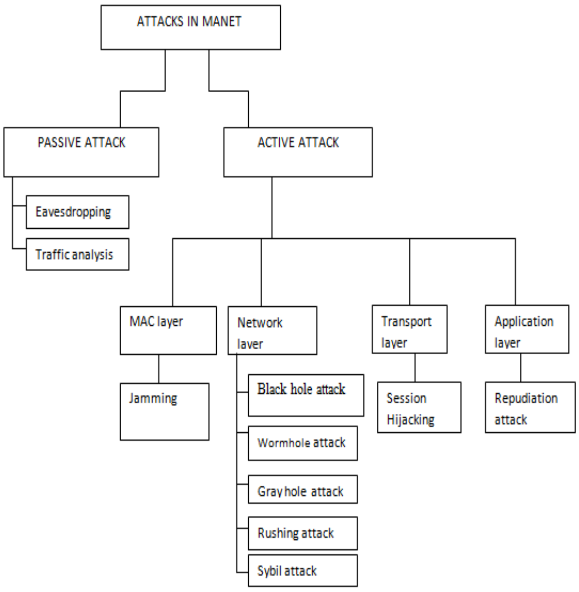

Fig1: Classification of attacks

Section II describes about various types of attacks in MANET. Section III describes about various network layer attacks and their defense mechanisms. Section IV deals with comparison of different protocols and section V concludes the topic.

II. ATTACKS IN MANET

MANET has five layers they are:

TABLE 1MANET PROTOCOL STACK

APPLICATION LAYER	Defines application protocols and how host programs interface with transport layer services to use the network.
TRANSPORT LAYER	Defines the level of service and status of the connection used when transporting data.
NETWORK LAYER	Packages data into IP datagrams and Performs routing of IP datagrams.
DATA LINK LAYER	Provides error-free transfer of data frames from one node to another
PHYSICAL LAYER	Concerned with the transmission and reception of the unstructured raw bit stream over a physical medium

Physical layer Attacks: physical layer contains three types of attack they are

- Eavesdropping: In this type of attack the attacker place themselves in communication path between sender and receiver. They extract information by receiver tuning to proper frequency.
- Jamming: This is one of the categories of denial of service attack by malicious node. This attack is initiated after determining the communication frequency.
- Active interference: This is also a denial of service attack which distorts the communication.[1]

Data link layer Attacks: This layer also contains three types of attack they are:

- Selfish misbehavior of nodes: These are selfish nodes that intentionally drops packet to conserve battery power or prevent unwanted share of bandwidth.
- Malicious behavior of nodes: They Disrupts operation of routing protocol and its effect will be considerable only when more communication takes place between neighbouring nodes.[1]
- Traffic Analysis: In this type of attack they analyze the traffic flow to get important information on network topology that in turn reveals the information about the nodes.

Network layer: Network layer contains the following attacks they are:

- Black hole attack: In this type of attack node advertises itself having shortest route to destination and thus attracts the data in the network.
- Wormhole attack: This type of attack makes a tunnel between two malicious nodes and attracts the data flow through these attacker nodes.
- Rushing attack: In this attack it floods the RREQ packet faster before other node react to the request. Thus it attracts all the packet through the rushing attacker.[1]

Transport layer: Transport layer contains two types of attack they are:

- Session hijacking: In this type of attack the victims IP address is used to find the correct sequence number and causes DoS attack. They aim at collecting secure data about the nodes.
- SYN flooding attack: In this attacker forms many number of half opened TCP connection so that handshake will not be done completely to establish connection.[1]

Application layer: It includes two types of attack

- Malicious code attack: It includes virus, worm, Trojan horse.
- Repudiation attack: This type of attack is caused by refusing to take part in communication .In this attack the attacker act as selfish node and deny the information or operation that is meant for communication [17].

III. ATTACKS IN NETWORK LAYER

The main three layers of ad hoc that take part in routing mechanism are physical layer, MAC layer and network layer. As the structure of MANET is vulnerable to attacks, there could be routing disorders cause by it. In MANET each node acts as a router and forward packets so it is easy for attacker to get into network. Main idea behind network layer attack is to place itself between the source and destination. Thus attacker can capture the data transmitted, can drop the transmitted packet and can create routing loops. These all can cause congestion in the network. The different types of network layer attacks are

TABLE 2 CLASSIFICATION OF ATTACKS IN DIFFERENT LAYER

LAYERS	ATTACK TYPE	MODE OF ATTACK	RESULT OF ATTACK
Physical	Eaves dropping	By receiver tuning to proper frequency	Reading messages by unintended receiver.
	Jamming	By malicious node with known communication frequency	Prevents reception of legitimate packets
	Active interference	Blocks the communication channel	Change order of messages
Data link	Selfish misbehaviour of nodes	Selfish nodes	Drops the packet
	Malicious behaviour of nodes	Disrupts operation of routing protocol	Misdirects traffic
	Traffic Analysis	Topology information	Information to unintended receiver
Network	Black hole attack	Fake optimum route message	Loss of confidential information on packet
	Wormhole attack	Tunnel between malicious nodes	Loss of safe route
	Rushing attack	Subvert route discovery process	Loss of safe route
Transport	Session hijacking	Spoofs victim node IP address	DoS attacks
	SYN flooding attack	Open TCP connection with victim node	DoS attacks
Application	Malicious code attack	Viruses worms	Attack to OS
	Repudiation attack	Denial of participation in parts of communication	Communication failure

A. BLACK HOLE ATTACK

In black hole attack, the attacker makes use of vulnerabilities in routing discovery method of AODV, DSR routing protocols [4]. When a source node needs to send data to destination node it broadcast RREQ request to all. So that the node with highest destination sequence number than the current destination sequence number of node will reply and the destination sequence number is higher than current destination sequence number. Then they send this to the source node. Receiving this false RREP packet the source node will select the path through this malicious node assuming that it is the fresh shortest path towards destination. The source node then rejects the RREP packet from other nodes and start sending packet through malicious node. Then this malicious node can drop the packet instead forwarding it. This type of attack is called black hole attack [1].

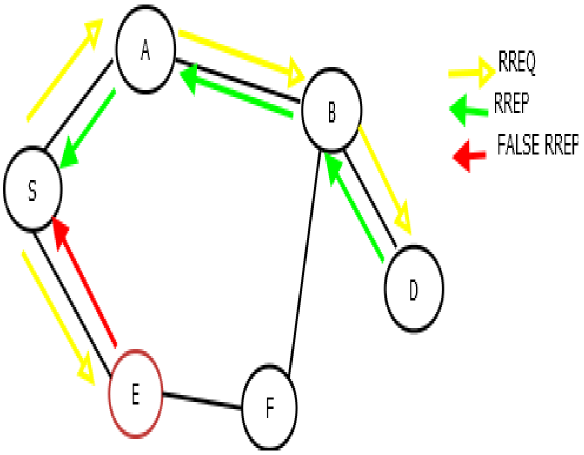

Fig2:Black Hole Attack

In this example when a data packet is need to be send from source node "S" to destination node "D" it sends RREQ packet to the neighbors. When node "E" ,that is the malicious node receives the RREQ request it sends RREP packet advertising itself having shortest route to destination and it rejects the RREP packet from the legitimate route <S,A,B,D>.The source node S starts sending the packet through <S,E,F,B,D> route and node E that is the black hole attacker can drop the packet passing through them.

B.PROTECTION AGAINST BLACK HOLE ATTACK

Mainly three mechanisms are used to defend against black hole attack. They are TOGBAD, SAR protocol and DPRAODV protocol.

1.) *TOGBAD:* TOGBAD is a black hole detection mechanism based on topology graph. It compares the number of neighbors a node should have and actual number of neighbors a node have in accordance with the graph.

 TOGBAD protocol have a drawback that it is possible only for pro-active routing protocol-OLSR where we can obtain topology information but obtaining complete topology information for reactive routing protocol will not be feasible.[4]

2.) *SAR (Secure aware routing protocol):*The secure aware routing protocol is based on on-demand protocol like AODV or DSR. In original protocol if a node want to send information to other node it broadcasts a Route request packet to its neighbors and they get RREP packet in return indicating the shortest path to destination. In most of the routing protocol they mainly aim at discovering the shortest path from source to destination that is they are considering only the length of the route. But in SAR it incorporates a security metric into the RREQ packet, so that the change of forwarding action depends on RREQs. Whenever a RREQ packet is received by an intermediate node the SAR ensures that the node can process that packet or forward it only if that intermediate node provides required authorization. The RREQ packet is dropped if the node cannot provide the required security.

 The main drawback of SAR protocol is that we cannot guarantee that the route discovered by SAR between source and destination is the shortest route. But it finds route which guarantee security.SAR is not able to find shortest route because all the nodes in the shortest route may not satisfy the security requirements. If all the nodes in shortest route satisfy the security requirements then SAR can find the shortest route.[13]

3.) DPRAODV (Detection, Prevention and Reactive AODV): In DPRAODV protocol it uses a dynamically updating threshold value .In normal routing protocol like AODV the RREP packet is accepted only if they have a destination sequence number higher than one in the routing table. But in DPRAODV it uses a threshold value. Here it checks whether the destination sequence number of RREP is higher than the threshold value or not .If it is higher than threshold value then the node is said to be malicious node and this node is added to a blacklist .Then the neighbors of this node are alerted by sending a control packet called ALARM packet. These ALARM packets parameters are blacklisted nodes. So if node receives packet from the blacklisted node they simply discard the RREP packet. It also blocks the repeated reply from the malicious node there by reducing the network traffic and thus DPRAODV isolates the malicious node from the network.[16]

C. WORM HOLE ATTACK

In wormhole attack, two malicious nodes make a tunnel between them. This tunnel between them is called wormhole .Here the data packets are attracted to it by advertising itself having shortest path to destination. When a wormhole attack happens in a network it prevents the discovery of other routes than route through wormhole. Thus all the data will be passing through wormhole only. So it can drop the packets as well as can listen to confidential information or can alter the transferred data packets.

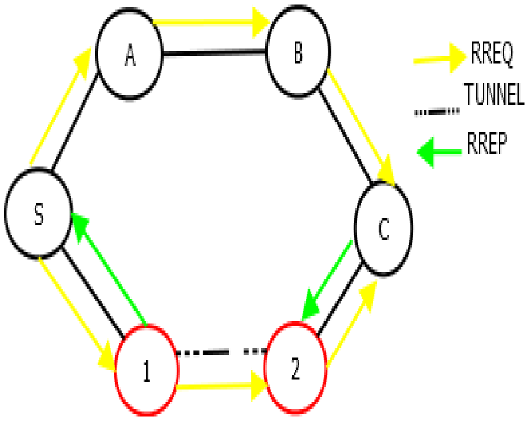

Fig3: Wormhole attack

In figure3, the nodes “1” and “2” are malicious node and they together form the tunnel in network. The source node “S” sends the RREQ message to immediate neighbours to find the route. The immediate neighbours of source node “S” are “A” and “1”. When node 1 receives the RREQ request it immediately shares with node 2 and then sends RREQ message to its immediate neighbour C that is the destination.As the link between 1 and 2 having high speed the source node selects the route <S,1,2,C> for destination. It results in “D” to ignore RREQ that arrives from legitimate route <S,A,B,C>.

D.PROTECTION AGAINST WORMHOLE ATTACK

The wormhole attack can be defended in two ways they are Packet leashes and sector.

1) *.PACKET LEASHES:*One of the mechanisms used for wormhole detection is called packet leashes. Mainly leashes means packet that restrict the maximum allowed transmission distance of a packet. There are two types of leashes they are geographical leashes and temporal leashes.

   a.Geographical leashes:This type of leashes makes sure that that the recipient of the packet is within a certain distance from the sender. To create a geographical leash, each node should know its own location and all nodes clock should be synchronized loosely. The mechanism in geographical leashes is that when a sending node sends a packet it includes two parameters within it. They are location of sending node (p_s) and the time at which it sends the packet(t_s).When a receiving node receives this packet they compares these values to its own location(p_r) and time at which it receives the packet(t_r). If senders and receivers clock are synchronized within ±Δ, and v is an upper bound on the velocity of any node then the receiver can compute an upper bound on the distance between the sender and itself, say *dsr.* Using the parameters timestamp *ts* in the packet, the local receive time *tr*, the maximum relative error in location information , the locations of the receiver *pr* and the sender *ps*, the *dsr* can be bounded by $dsr \_ ||ps - pr|| + 2v \cdot (tr - ts + \Delta)$ +sigma for authentication of location by receiver. We can use authentication techniques like RSA for this.

   The main disadvantage of geographical leashes is that if any obstacle comes in communication between two nodes that would otherwise in transmission range then bounding of distance between sender and receiver method fails.[10]

   *b. Temporal leashes:*This type of leashes make sure that packet have a particular lifetime, that allows packet to travel only at a certain distance .In temporal leashes the sender sending the packet will contain a packet expiration time that doesn’t allow the packet to travel further than a particular distance say L. Consider that the maximum synchronization error is Δ and value of this should be known by all the nodes in the network .Thus $L>L_{min} = \Delta.C$ where c is the propagation speed of our wireless signal. Let the local time at which sender sends the packet is t_s so the expiration time is set as te = ts + L/c −Δ .When the receiver get this packet at local time t_r it checks whether the expiration time is exceeded or not that is it check that t_r greater than t_e or not. If this is true the receiver will drop the packets. Here TIK protocol is used for authentication of broadcast communication [10]. The main disadvantage of temporal leashes is that within restricted time the packet should be passed through the wormhole [15].

2) *SECTOR (Secure tracking of node):*In this method the wormhole attack is prevented by bounding the maximum distance between two neighbouring nodes by a series of first one bit exchange. This uses a special hardware to make sure the accuracy of time as well fast processing between the sender and receiver [8].

E. GRAYHOLE ATTACK

Gray hole attack is special variation of black hole attack. In black hole attack the attacker places itself in between the source .The attacker attracts the data packets to it by advertising itself having the shortest route to destination and then they capture the data packet and drops it. In gray hole attack the data packets are dropped selectively or in statistical manner. For instance they may drop packets from a particular node or in some other pattern[4]

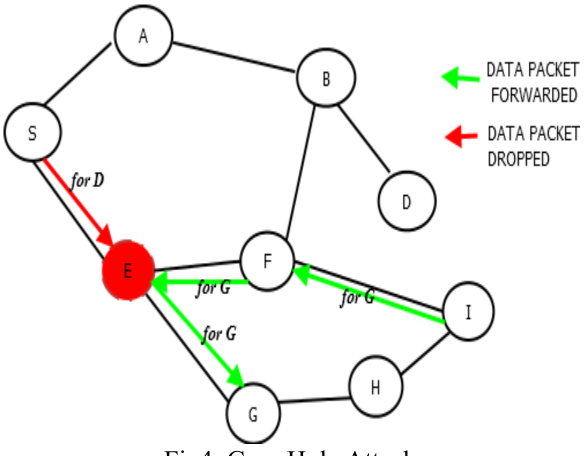

Fig4: Gray Hole Attack

Here the attacker that is node E drops the packet only to node D and it forwards packet from other nodes creating a gray hole.

F.PROTECTION AGAINST GRAYHOLE ATTACK

In a gray hole detection mechanism each node have to generate all evidence on forwarding packets by making use of a aggregated signature algorithm. This algorithm detects whether packets have dropped or not and thus finds the malicious node. Another mechanism used in the gray hole attack is that all nodes maintain their neighbours data forwarding information .After a time interval each node checks if any neighbour with whom it has not communicated and then it starts the detection procedure for the node. This detection is done by comparing the number of RTS and CTS messages. If they found the node to be suspicious then it enquires its neighbours and after that they take decision about the suspected node[4].

G. RUSHING ATTACK

One of the property of an on-demand routing protocol is that nodes are only allowed to forward the first RREQ that arrives for routing discovery and it discards all other RREQ that come late. This property is exploited by rushing attack.

The attacker will transmit the RREQ request earlier and thus it suppresses the legitimate RREQ. In most powerful rushing attack they use a wormhole to rush packets.

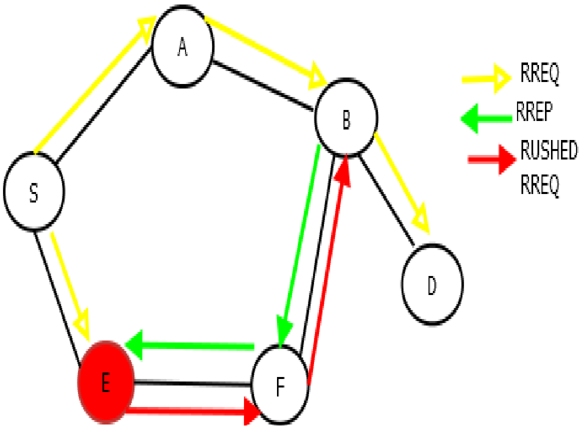

Fig5: Rushing attack

For example, in figure the node "E" represents the rushing attack node, where "S" and "D" refers to source and destination nodes. The rushing attack of compromised node "E" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than those from other nodes. This result in when "C" i.e. neighbouring node of "D" when get the legitimate route request from source, they simply ignore the request. So in the presence of such attacks "S" fails to discover any useable route or safe route without the involvement of attacker.

H.PROTECTION AGAINST RUSHING ATTACK

To prevent the rushing attack we can use three mechanisms together they are secure neighbour detection, secure route delegation and randomized route request forwarding. In on demand protocol if node2 receives broadcast message from node1 then node2 consider node1 as neighbour. If we finds that node1 is neighbour to node2.It gives a route delegation message to allow node2 to forward the route request. If node2 finds that node1 is within range then it gives a accept delegation message. The randomized selection of the route request message to forward make sure that selected path is a low latency path through which requests are forwarded.

In secure neighbour detection, each neighbour are allowed to verify that the other node is within a given maximum transmission range. Here we use a three round mutual authentication protocol that uses tight delay timing that make sure that the other node is within the transmission range. In the first round the starting node sends a neighbour solicitation packet by unicast method or broadcast method. In next round by receiving the neighbour solicitation packet the received node sends back a neighbour reply packet. At final round the starting node sends neighbour verification packet containing broadcast authentication of a timestamp and source to destination link.

Source route delegation mechanism is used to verify that all the secure neighbour detection procedure are performed between two neighbouring nodes. To explain the mechanism let us consider two neighbouring node n1 and n2,here n1 gets a route request from node S with sequence id, that is destined to node R. Node n1 does the neighbouring detection protocol and find that n2 is the neighbouring node that is within range and then it delegates the route request to n2.The delegation of route request to n2 is given as follows:

MA = (ROUTE DELEGATION; A; B; S; R; id)
□MA = Sign (H (MA))
A->B: (□MA)

Here node n2 can rebuilt the message fields and verify the signature. The node n2 will accept the route delegation if n2 find n1 within the range and this procedure is done to next neighbours and so on. The route delegation message can be incorporated with the last message of secure neighbour detection protocol.

In randomized message forwarding random selection technique can be used to prevent the rushing attackers in dominating all other routes to destination. Two parameters are used for selection of randomized forwarding they are the number of request packets to be collected and algorithm which can choose timeouts. If the number of requests chosen is very large, the randomized forwarding will reply more on the time out, which increase the latency and reduce the security. If we can know the complete topology information the timeout must be based on the number of legitimate hope between the starting node and node forwarding the request. But when topology information is not available then node can choose the timeouts randomly [9].

I. SYBIL ATTACK

In MANET the medium of transmission of packet is air and they doesn't have a central node to control the network. So the routing is mainly based on a unique node address. This property of MANET can be exploited by the attacker by using fake identities. That is the attacker can either use random identity or the identity of legitimate node. This type of attack is called Sybil attack. These attack cause lot of packets to be routed towards the fake identity nodes which makes severe attacks. The presence of this type of attack makes it difficult to find misbehaving node, and also this prevent a fair resource allocation among the nodes [1].

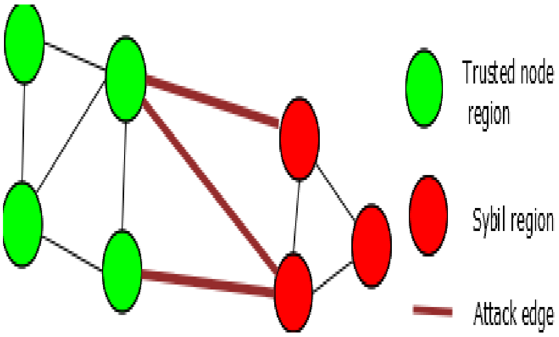

Fig6:Sybil attack

In figure 6 it is shown two types of nodes one is trusted group of nodes and other is Sybil attacker nodes .The Sybil attackers are basically nodes with random identity or identity of a legitimate node. The link from the trusted node region to Sybil attacker region helps the Sybil attacker to capture information send through it.

J.PROTECTION AGAINST SYBIL ATTACK

There are mainly two methods to detect the Sybil attack they are PASID (Passive ad-hoc Sybil identity detection) and PASSIVE-GD.

In passive ad-hoc Sybil identity detection a single node can detect Sybil attacker by recording the identities like MAC or IP addresses of other nodes that hears transmission. By this addresses the node builds a profile of which nodes are heard together. Thus this method helps in revealing the Sybil attackers. When the network contains more nodes in less space the rate of false positives will increase. Thus the node will have only fewer chances to hear its neighbours. To prevent this we have a method where multiple trusted nodes can share their observation with other nodes to increase the accuracy of detection.

Next method used for detection of Sybil attack is PASID-GD that is mainly an extension of PASID. This method is used to reduce false positives that may occur when a group of nodes moving together is identified as a single Sybil attacker. Here they exploit the property of channel, that is a single channel transmits only serially and independent nodes transmit in parallel that makes considerably higher collision. So by detecting collision at MAC level we can identify the Sybil attacker of this type[7].

IV. COMPARISON

Table 3 describes about the merits, demerits and detection mechanism used in each protocol. Here each protocol is proposed inorder to detect and prevent attacks at different layer.

V.CONCLUSIONS AND FUTURE WORK

The dynamic nature of MANETs makes it more vulnerable to attacks at different layers. One of the MANET layers that are mostly attacked is network layer. In this paper we have done a survey on network layer attacks and their possible detection mechanism. The comparison between different detection methods are also done here. In future there may be ways to defeat these protection mechanisms. So this is a further potential area of research that more powerful detection mechanisms can be invented.

TABLE 3 COMPARISON OF DIFFERENT PROTOCOLS

NAME OF ALGORITHM	ATTACK TYPE	DETECTION TECHNIQUE	ROUTING PROTOCOL	MERITS	DE-MERITS
TOGBAD	Black hole	Compares number of neighbouring node it have with number of neighbouring node in accordance with topology graph	OLSR	Black hole detection for OLSR	Method is ineffective in reacting protocol
SAR	Black hole	Nodes checks if security metrics or requirements are satisfied or not	AODV DSR	Black hole detection	Cannot guarantee shortest route discovery
DPRAODV	Black hole	Checks if destination sequence number of RREP is higher than the threshold value or not	AODV	Black hole detection	Identifies normal node as malicious node and enter to blacklist ALARM broadcast make network overhead
TELSA	Wormhole	Checks if recipient is in certain distance or not	AODV DSR	Wormhole detection	Strict requirements in timing
SECTOR	Wormhole	Bounding maximum distance between two neighbouring nodes by series of fast one bit exchange	Not specified	Wormhole detection	Need special hardware to ensure accuracy of time
NONE	Gray hole	Detection by checking the number of CTS and RTS messages	AODV	Gray hole detection for AODV	Trust in neighbours
PASID	Sybil	Recording identity and mobility pattern	AODV	Sybil attack detection	Shows that mobility can identify Sybil identities

REFERENCES

[1] Gangandeep,Aashima,Pawan kumar "Analysis Of Different Security Attacks In MANETs On Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[2] Mangesh M Ghonge,Pradeep M Jawandhiya,Dr M S Ali "Countermeasures Of Network Layer Attacks In MANETs" IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[3] G S Mamatha, Dr s c Sharma "Network Layer Attacks And Defense Mechanisms In MANETS-A Survery" International Journal of Computer Applications (0975 – 8887)Volume 9– No.9, November 2010.

[4] Adnan Nadeem ,Michael p Howarth ,"A Survey of MANET Instrusion Detection & Prevention Approaches for Network Layer Attacks",Proc. IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013.

[5] Isha V Hatware,Athul B Kathole,Mahesh D Bompilwar "Detection of Misbehaving Nodes in Ad Hoc Routing" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459,Volume 2,Issue 2,February 2012).

[6] Jyoti Thalor, Ms. Monika," Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review" International Journal of Advanced Research in Computer Science and Software Engineering (ISSN: 2277 128X Volume 3, Issue 2, February 2013).

[7] Chris Piro ,Clay Shields ,Brian Neil Levine "Detecting the Sybil Attack in Mobile Ad hoc Networks".

[8] Xia Wang, Johnny Wong "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks"2007 31st Annual International Computer Software and Applications Conference (ISBN: 0-7695-2870-8).

[9] Yih-Chun Hu, Adrian Perrig, David B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols",Proc.2nd ACM workshop on Wireless security Pages 30 - 40 .

[10] Yih-Chun Hu, Adrian Perrig, David B. Johnson "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks"Proc. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. 2003 , Page(s): 1976 - 1986 vol.3 .

[11] Diogo Miguel da Costa e Castro M´onica Oliveira "Thwarting the Sybil Attack in Wireless Ad Hoc Networks".

[12] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee "Transmission Time-based Mechanism to Detect Wormhole Attacks".Proc.2nd IEEE Asia-Pacific Service Computing Conference (APSCC 2007), ISBN: 0-7695-3051-6.

[13] Seung Yi, Prasad Naldurg, Robin Kravets "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks"Proc.MobiHoc '01 Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing Pages 299-302.

[14] Brian Neil Levine, Clay Shields, N. Boris Margolin "A Survey of Solutions to the Sybil Attack",Tech report 2006-052,University of Massachusetts Amherst, Amherst, MA, October 2006.

[15] Jackson Kwok "A Wireless Protocol to Prevent Wormhole Attacks"proc. A Thesis in TCC 402 March 23, 2004.

[16] Ketan S. Chavda , Ashish V.Nimavat "Comparative Analysis Of Detection and Prevention techniques of black hole attack In aodv Routing protocol of MANET " International Journal of Futuristic Science Engineering and Technology, Vol 1 Issue 1 January 2013 ISSN 2320 – 4486.

[17] Amit M Holkar, Neha Shinde Holkar and Dhiiraj Nitnawwre " Investigative analysis of repudiation attack on MANET with different routing protocols" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 3, May – June 2013 ISSN 2278-6856 .