



Various Approaches Used to Overcome From Security Threats in MANET

Yogesh Jadhav*, Seema Ladhe

Department of Computer Engineering
MGM CET, Mumbai University, India

Abstract— Mobile ad-hoc network (MANET) is most commonly used due to its advantages over wired and other wireless networks. Since MANET does not require special infrastructure it is used very commonly in military application and areas where there is no possibility of creating instant infrastructure such as earthquake and flooding affected regions. Due to dynamic topology, no centralized control over network and cooperative protocols security is major area of concern in MANET. MANET is susceptible for various attacks such as black hole, grey hole, tunnelling attack etc., which compromises on security goals such as data integrity, confidentiality and availability. This paper we primarily focuses on the various protocols used for communication in MANET, various attacks, threats and methods used to overcome on these attacks. The main contribution of this paper is we produce detail comparison of various approaches used to prevent and mitigate these attacks.

Keywords— MANET, AODV, DSR, OLSR, DOS

I. INTRODUCTION

Mobile Ad-Hoc Networks are self-configured and without having centralized control over the wireless systems. MANETs consist of mobile nodes that are free to join and leave the network. Nodes may be the computer systems or devices such as mobile phone, laptop, personal digital assistance (PDA), MP3 player and personal computer that are participating in the network and are mobile. They are interconnected by using Bluetooth or Wi-Fi or IrDA. Nodes can be act as host or router or both. Node in network itself acts as router and therefore there is no need of separate router as required in wired network. These nodes have ability to configure themselves without need of infrastructure. Nodes configure themselves dynamically due to mobility. Due to mobility, dynamic topology and lack of central administration different routing protocols are designed, such as AODV, DSR, DSDV, OLSR, ZRP etc. Security in Mobile Ad-Hoc Network is the most important aspect for the basic functionality of network. The security goals such as availability of network, confidentiality of data and data integrity should be achieved. MANETs often vulnerable to attacks due to its features such as open medium, changing topology dynamically, lack of central monitoring and management, use of cooperative algorithms and no well specified defence mechanism. In MANET there is lack of central administration system which monitors the nodes and find out which node is misbehaving. Here each node forwarding the packet to next node on simply trusting it and increase the threat to system. Security goals can be compromised by any node. Security issue also arises in wireless network because attacker can simply overhear the data passing through these links or even participate in the network and modifies the data.

Due to wide applications of MANET should have secure way of communication and data transmission. The system should defend all kind of active, passive attacks and internal, external attacks. Various attacks such as black hole, grey hole, tunneling, flooding, selfish node misbehaving, spoofing, eavesdropping, Sybil, rushing, Denial of Service attack (DoS), impersonation, routing table overflow cause threat to MANET. A MANET is open to all these attacks due to communication among the nodes is on trust based, there is no central point for managing the network, limited resources such as battery and bandwidth, continuous change in topology and no authorization for new nodes before joining to network. This paper we primarily focuses on the various protocols used for communication in MANET, various attacks, threats and methods used to overcome on these attacks. The main contribution of this paper is we produce detail comparison of various approaches used to prevent and mitigate these attacks.

II. CLASSIFICATION OF MANET PROTOCOLS

Routing protocol in MANET can be classified into following categories based on network structure, communication model, routing strategy, and state information. Based on the routing strategy the routing protocols can be classified into two parts: 1. Table driven and 2. On demand (source initiated). Based on the network structure these are classified as flat routing, geographic position assisted routing and hierarchical routing. Flat routing covers both routing protocols based on routing strategy.

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

1. Reactive protocols
2. Proactive protocols

3. Hybrid protocols

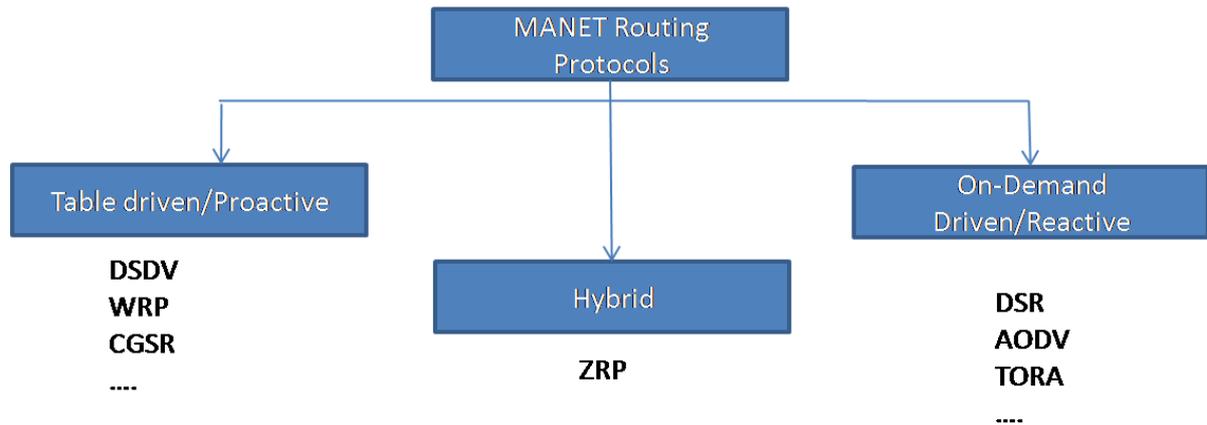


Fig1. Classification of MANET routing protocol

A. Reactive Protocols:

Reactive protocols also called as on demand driven protocols. These protocols called as on demand because they don't initiate root discovery process, until source node doesn't request. These protocols setup the route when demanded. When any node don't have path to reach to destination in the network then reactive protocol establishes route between the source and destination node. Reactive protocols finds route when any node required it uses flooding method to broadcast query and consume very less bandwidth for sending information so, bandwidth mainly used for transmission between source and destination. Examples of reactive routing protocol are AODV, DSR etc.

1. Ad-Hoc on Demand Distance Vector Protocol (AODV):

AODV is most commonly used reactive protocol in MANET, when any node wants to start communication with another node in the network for which it has no active route. AODV will give information regarding topology to node. AODV uses three control messages to find active path with minimum hop count and to gather topology information. Following are the messages used in AODV.

Route Request Message (RREQ):

Source node that wants to communicate with another node wishes to find out path to reach initiate route request message and floods that message through the network. The message uses expanding ring technique while travelling across network. An additional information carries with this message is Time to Live (TTL) so that message can reach up to maximum hop count only.

Route Reply Message (RREP):

A node that's address gets matched with destination address in RREQ sends route reply message to originator. Intermediate node might have active route to that destination also create RREP message and send.

Route Error Message (RERR):

Every node in the network monitors neighbor's link status. If any node finds any link break or link down so, it is impossible to reach to next node then it generate route error message and inform to other node that link is down.

Route Discovery Mechanism in AODV

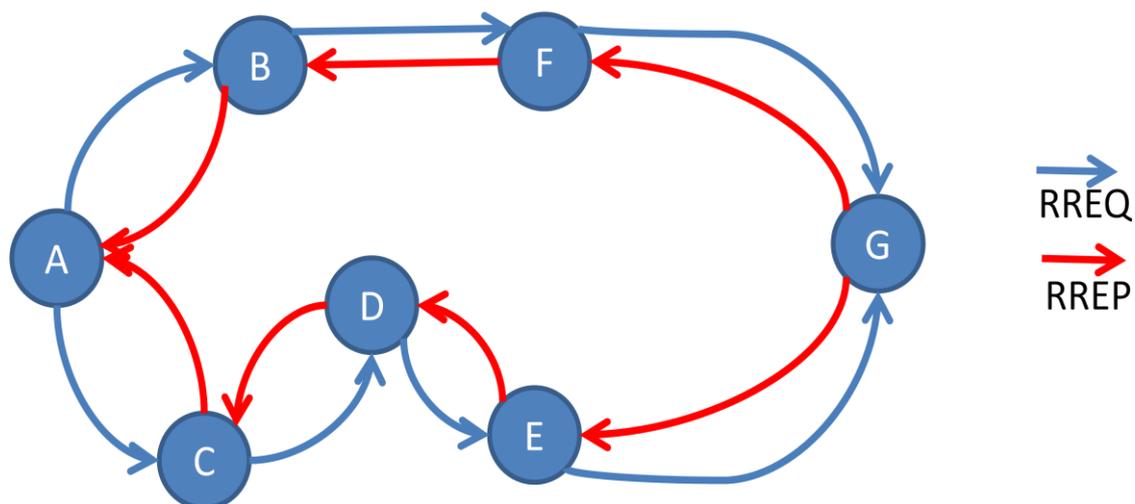


Fig.2 AODV route discovery [7]

When node "A" wants to initiate communication with another node "G" as shown in figure. Node "A" will initiate a route request message RREQ. This control message propagates through the network by using expanding ring technique. In which each node forward the message to its neighbors and those neighbors to their neighbors. When that control message reaches to destination node or intermediate node that have fresh route to reach that destination generate RREP control message and sends to originator. Such way the path gets established between the source node and destination node. Source node transmits data to destination. Every node in the network monitors its neighbors. If any node any link break and it is unable to reach that neighbor then that node generate the RERR message. It will send that message to others. Consider in above example node "A" sends RREQ message while forwarding that message node "E" detect that there is link break between itself and node "G" then node "E" prepares RERR message and sends to node "A".

2. Dynamic Source Routing Protocol:

Dynamic source routing that is abbreviated as DSR is reactive protocol. In DSR provide loop free routing and there is no need to store routing information for intermediate nodes. In this protocol used routing caches to maintain routing information or path. DSR uses routing caches to store obtained path through route discovery process. Mainly two processes used by DSR these are

Route Discovery Process:

A node which wants to communicate another node checks it's cache whether fresh route is in it to reach required destination. If cache does not have route or route which is expired then source node start the route discovery process. Source flooded RREQ message. If intermediate node have fresh route to reach that destination then that intermediate node prepares RREP message and sends it to originator of that message. If any intermediate node does not have fresh route then RREQ message reaches to the destination node prepares RREP message and sends it to originator. When the source gets the RREP message it copy the path in its cache and add that path in every packet's header so intermediate node can forward that packet according to path mentioned in packet's header.

Route Maintenance Process:

When communication starts, its responsibility of every node which is mentioned in the path that its next hop node should receive the data with path in the header. If it's not possible then route error message is send to the source so source node can again start the route discovery process.

B. Proactive Protocols:

Proactive routing protocol works completely different than reactive routing protocols. These protocols continuously maintain the information of updated topology of the network. Every node in the network knows in the advance about the other nodes in the network. That is each node knows about complete network. In reactive protocol each node knows about next hop but in proactive protocol each node have complete information of network. All the routing information kept in tables. Whenever there is change in topology, these tables get updated according to change in topology. This node transfers the information with each other. Therefore they have routing information when they needed and any time.

1. Optimized Link State Routing Protocol (OLSR):

OLSR is proactive routing protocol that is table driven protocol. OLSR uses three types of control messages that are as follows.

Hello: This control message passed through the network to sense the nodes and to calculate multi point distribution relay (MPR) calculation.

Topology Control (TC): These are link state signaling. MPRs are used to optimize these messaging.

Multiple Interface Declaration (MID): MID messages maintains the list of all IP addresses used by any node in the network.

OLSR Working

Multi Point Relaying (MPR):

OLSR spread the network topology information by flooding the packets all the way through the network. These packets flooded through the network such way that node received packets retransmits the packets. These packets having a sequence number to avoid loops. The receiver nodes record this sequence number to make sure that the packet is retransmitted once. The basic concept of use of MPR is to reduce the duplication or loops of retransmissions of the packets.

Only MPR nodes broadcast route packets in the network. The nodes within the network maintain a list of MPR nodes. MPR nodes are selected within the locality of the source node. The selection of MPR is depends on HELLO message sent between the neighbor nodes. The assortments of MPR such way that there must be a path exist to each of its 2 hop neighbors through MPR node. Routes are recognized, once it is done the source node that wants to make transmission can start sending data.

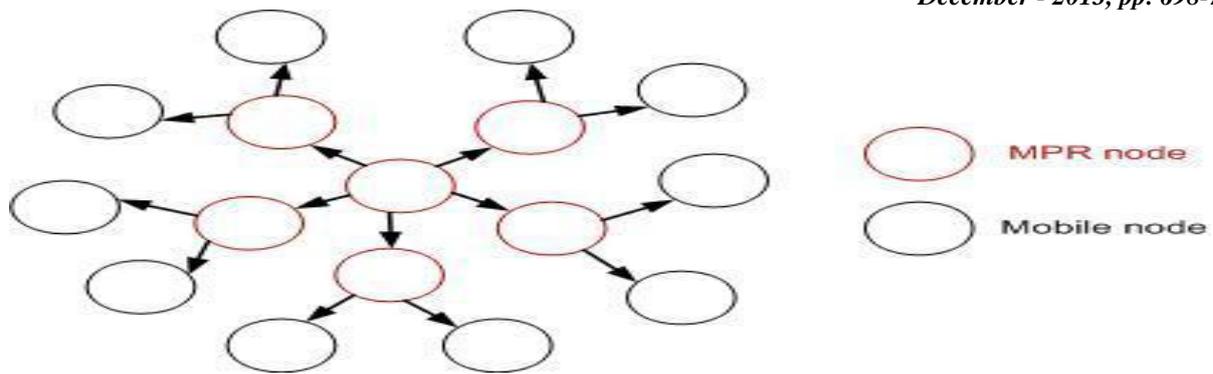


Fig.3 Flooding Packets using MPR [7]

The whole process is shown in figure. The nodes shown in the figure are neighbors. Node in the network sends a HELLO message to the neighbor node. When node receives this message then that link is asymmetric. The same is the case when that node send HELLO message to node from which it receive hello message. Then that link is symmetric with two ways communication is possible. HELLO message contains the information about the neighbors. MPR node transmits topology control message, along with link status information at a predetermined TC interval.

C. Hybrid Protocols:

Hybrid protocols make use of the strengths of both reactive and proactive protocols. The entire network is divided into multiple zones, in these zones different protocol used in different zone. Zone Routing Protocol (ZRP) is the case of Hybrid Routing Protocol. ZRP take advantages of proactive routing mechanism for route establishment within the nodes neighborhood, and to make communication among the neighborhood it make use of reactive protocols. These local neighborhoods are called as zones, and the protocol is named as zone routing protocol. Each zone can vary in size and each node may be come under multiple overlapping zones. The size of zone is specified by radius of length P, where P is the number of hops to the perimeter of the zone.

III. VARIOUS ATTACKS IN MANET

A. Black Hole Attack

In the black hole attack, the malicious node advertises itself having shortest route to the destination. When any node send route request to this node then it will reply to that request without checking it's routing table prepare reply message pretending that it has fresh and shortest route to destination. When source node gets this reply before the actual reply it will start sending packets to this node. This node then discards these packets or modifies these packets or forward to unknown address. Such way malicious node makes entry in routing path. Following figure shows how black hole problem arises in network. Node "A" wants to communicate with node "D" and start the route discovery process. Node "C" is a malicious node then it will pretend that it has active and shortest route to the desired destination when he receives RREQ packets. It sends the response to node "A" before any other node. Node "A" will consider that route discovery has finished and discard all other route reply messages. Node "A" will start sending packets through that route and node "c" might discard these coming packets or forward them to unknown address.

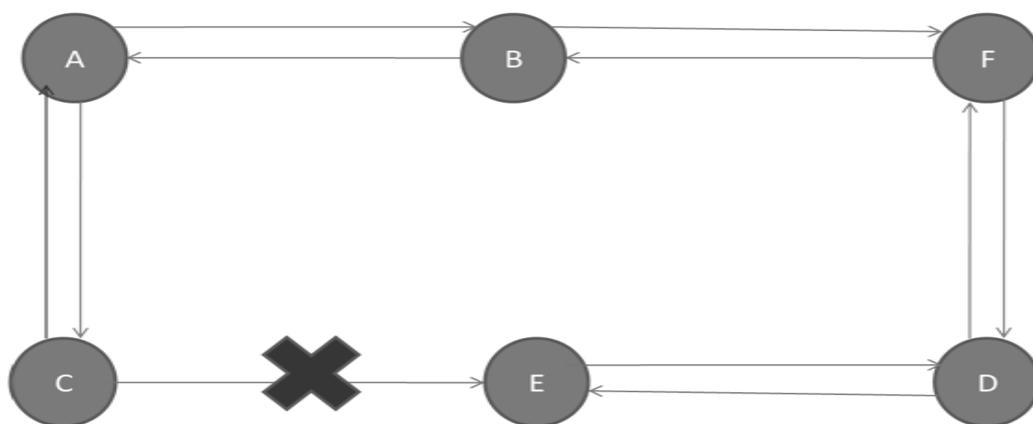


Fig.4 Black Hole Problem

B. Gray Hole Attack

In this kind of attack the node as soon as it receives the packets from its neighborhood it drops the packets. Initially this node behaves normally and replies true RREP to the node who started the RREQ messages. When it starts receiving the packets it drops these packets and launch Denial of service attack (DoS). It is difficult to identify this attack because

node might drop some packets and forward some packets. In some cases, nodes behave maliciously for time until packets get dropped then behaves normally. Therefore such kind of attack is difficult to identify. This attack is also known as node misbehaving attack.

C. Flooding Attack

The flooding attack is most easy way to attack on the network resources to make them unavailable for other nodes. This can be achieved by the using RREQ or data flooding. In RREQ flooding, the attacker floods RREQ packets in whole network which utilize the network resource. This can be done by selecting ip addresses which are not actually present in the network so no other node can reply to these RREQ packets. In data flooding attack the malicious node enters into network establishes path between all other nodes. Once connection established with all other nodes attacker introduce useless data packets or bogus packets in whole network. These unwanted data packets congest the network so network resources are become unavailable to desired nodes.

D. Selfish Node

In MANETs it is responsibility of every node to participate in network operation and forward the data packets. When some nodes in the network compromises on this collaboration to forward packets in order to preserve its resources. Such type of nodes called as selfish nodes. Due to these selfish nodes there is disruption to normal behavior of the network. The selfish node refuses to advertise itself in route discovery process while it might have shortest path. It will advertise the non existing routes among its neighbor nodes. These nodes can use the network only when they want to send packets in the network after doing that node turns itself in silent mode to preserve its resources. These nodes are not visible to the network. These nodes can also drops the packets when it is not interested in forwarding packets.

E. Wormhole Attack

Wormhole attack is a brutal attack in which two attackers placed themselves at very crucial position in the network. The attackers keep on hearing over the network, capture and record the wireless data. The fig.6 bellow shows the two attackers placed themselves in a strong strategic location in the network.

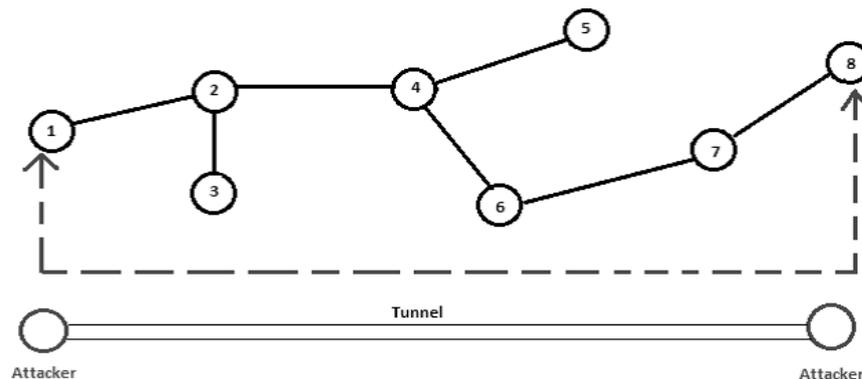


Fig.5 Wormhole attack

In wormhole attack, the attacker gets themselves in strong strategic position in the network. These nodes placed them in the network at very crucial position and advertise themselves having shortest path to the destination. Once they get inside the path they creates tunnel between them. When packets coming to one node it capture the wireless data and record it and forward to another node which present at the other end of tunnel. Such type of attack known as out band wormhole attack. The other type of wormhole attack is known as in band wormhole attack. In this type of attack the attacker builds a superimpose tunnel over the existing wireless medium. This attack is potentially very much destructive.

F. Jellyfish Attack

In jelly fish attack, the attacker introduces delay in the network. In this attack attacker get access to the network then it become a part of the network. Then such node introduces unwanted delay in the network. This delay made in forwarding packets when it receives the packets. Once delay gets introduced in the network it releases the packets. This cause high end to end delay and high delay jitter, which reduce the performance of the network.

G. Modification Attack

In ad hoc network any node can easily, freely join the network and leave it. Nodes whose intention to attack on network join the network. Then malicious node launches the attack and brings irregularities in the network. A node participates in the transmission process and later on starts message modification attack. Impersonation and misrouting attacks are types of modification attack.

H. Misrouting Attack

In misrouting attack node which is part of the network tries to misroute the traffic from the source node to unknown or to wrong destination node. As the packet in the network it utilizes the network resources but when the destination not found the network simply drops the packet.

I. Impersonation Attack

As we know in ad hoc network node is free to join or leave the network. There is no strong authentication process to make network secure from malicious nodes. In MANETs IP address and MAC address uses to uniquely identify the host. This approach is not enough to authentication of sender. The attacker use MAC and IP address spoofing to get identity of another node and hide itself in the network. This attack also known as spoofing attack.

J. Routing Table Overflow Attack

Routing table overflow attack is commonly done in proactive protocol because it is table driven protocol. When routing table updating process happen in the network then nonexistent node data is sent in the network. In proactive routing protocol routes are updated periodically. The attacker creates so many routes to nodes that do not exist in the network. This is done by using RREQ messages in the network. The attacker sends RREQ messages to unknown or nonexistent nodes. Thus nodes under this attack have its routing table full. So that node does not have any place for new entry.

IV. VARIOUS APPROACHES USED TO OVERCOME FROM SECURITY THREATS

A.HSAM (Highly Secured Approach against attacks on MANET) [1]:

Wireless networks always have threat of data tempering and packet dropping. This method covers network layer attack. EHSAM provide approach to overcome on these attack and such malicious nodes should be identified. Such compromised node makes entry in the routing path and disrupts the network. This algorithm uses two main approaches are counter and hash code. The packets are divided in to sub-packets. When packet sent from source the counter at source named as Cpkt incremented. This counter keeps track of how many packets are sent from source node. Hash code is code also sent among these packets. When sub-packets are received at destination node they are reconstructed and compute the hash value. If hash code is matched then no data modification attack happened but if data is tempered then hash code does not get matched then acknowledgement send to source node with field confidentiality lost field set to one. If ack does not come within time limit then it is assumed those packets are lost and increment the counter Cmiss. This method uses flow of conservation which strongly state that number of packets sent from source node should match with number of packets received. When source node receives acknowledgment with confidentiality lost field also ratio of Cmiss/Cpkt above the limit of tolerance. There is possibility of data modification and packet dropping attack. Source node discards that path.

This method cannot provide solution for the misrouting attack. When the path is discarded then source node again does the path discovery process which increases the overhead on the network.

B. Ex-watchdog and Pathrater [2]:

Watchdog relies on DSR and each node in the network works on intrusion detection system. If any node does not forward the packet that means that node is malicious. Watchdog used to identify such node which compromises on packet forwarding. Watchdog has limitation when ambiguous collision, false misbehavior, collusion and partial dropping. Pathrater used to choose path from source to destination based on simple rating run by each node in the network. Another method is routeguard, which is similar to the pathrater. Routeguard classifies the node into five classes that are fresh, member, Unstable, Suspect and malicious. Ex-watchdog tries to overcome from the watchdog weaknesses. In this each node maintain the table that stores entry <source, Destination, sum, path> where sum means that total number of packets current node send and path that is list of nodes addresses that are in path. When intermediate node finds that its next hop is malicious then source will not immediately decrease the rating of that node. It will send message through alternative path in routing table with malicious node address. Then source node searches its own table for next path. If not found it will start route discovery process. When destination node receives a message then it will check its routing table if entry is not found that means node is malicious and report sends to source node.

This method assumes that malicious node cannot tamper the packet which is not always possible. There is possibility of message tempering attack.

C. Detection and accusation of packet forwarding misbehaviour in MANET [3]:

This paper presents a mechanism for detecting and accusing nodes that shows packet forwarding misbehaviour. In this method monitoring process is used to identify nodes which are showing packet forwarding misbehaviour. If node V_i sends packet to the node V_j then node V_i increments the T_{ij} that is transmission counter. If node V_j successfully receives packets then it increment the counter R_{ij} that is receiving counter. If the mismatch among the values of these two counters then there is packet misbehaviour. If node V_i want to check behaviour of V_j node then V_i overhear node V_j and add V_j to overheard table of V_i . After making entry of V_j in table V_i schedule an event to check the V_j 's misbehaviour. If node V_i receives metric request to check V_j 's behaviour. Then V_i broadcasts metric request packet (MREQ) packet with $TTL=1$. If $\sum R_{ij} \leq \sum T_{ij}$ that means number packets received are less than number of packet sent that shows packets are

dropped by the node V_j . If node V_i receive detection alert packet with V_{ij} id then V_i discards all packets coming from node V_j . That is accusation of that node.

This method adds network overhead because of maintaining routing table for overheard node entry. Also nodes have to respond to MREQ request and check the counters for packet dropping is present or not.

D.WAP [4]:

In wormhole attack one malicious node tunnels packets to other malicious node. This paper develops effective method called as wormhole attack prevention (WAP) without using. This method detects the fake route and uses preventive measure to avoid that path in further route discovery. First step used in this method is neighbour node monitoring. This uses wormhole prevention timer (WPT).

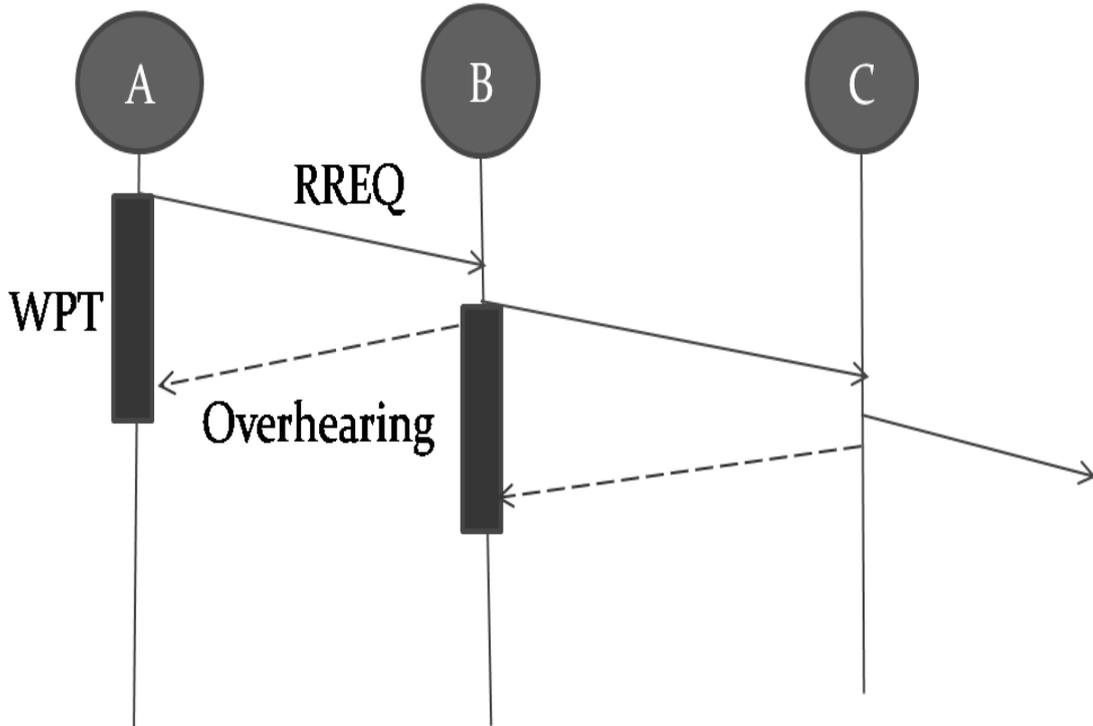


Fig.6 Neighbour node monitoring of node [4]

Node A checks whether the RREQ arrives within timer. If A receives after expiration of timer it suspects node B as wormhole node.

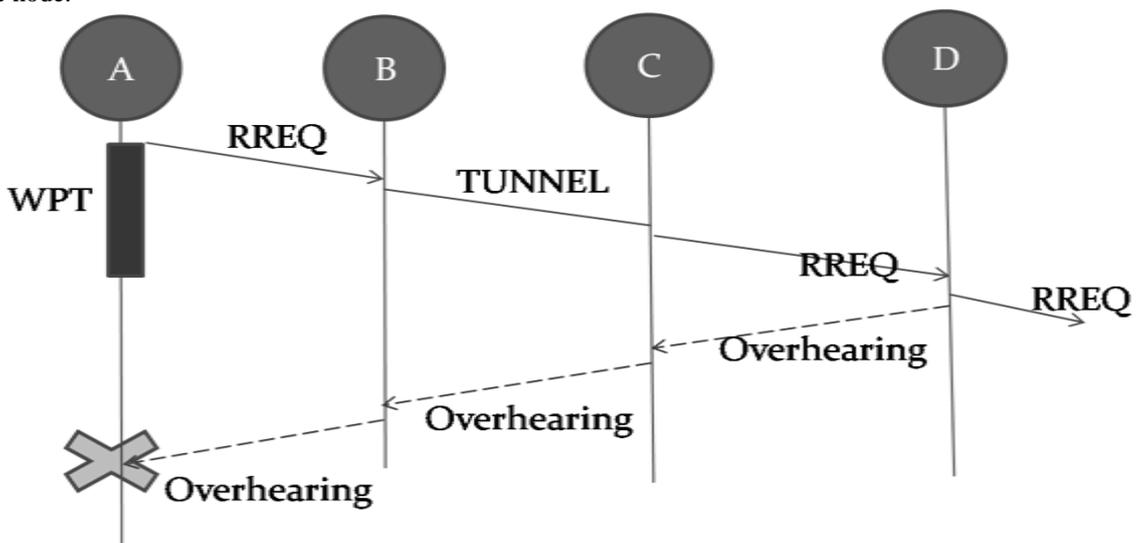


Fig.7 Neighbour node monitoring of wormhole nodes [4]

Each node maintain table \langle RREQ Seq#, Neighbour Node id, Sending Time, Receiving Time, Count \rangle .Count used to find out how many packet receives after WPT. The $WPT=2*TR/V_p$. Here, TR is transmission range and V_p denotes propagation speed of packet. Second step is wormhole route detection.

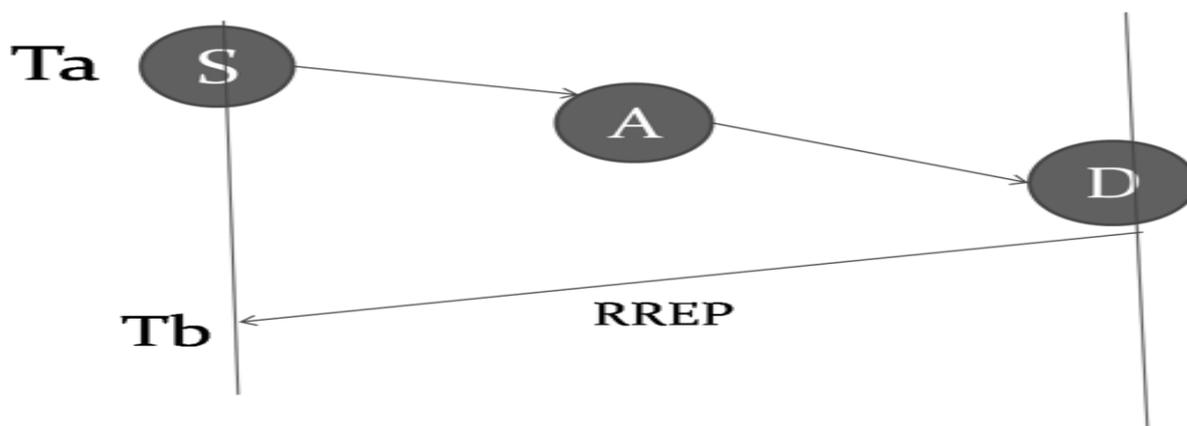


Fig.8 Normal route [4]

To detect wormhole route delay per hop is calculated. $\text{Delay per Hop} = (\text{Tb}-\text{Ta}/\text{Hop Count}) \leq \text{WPT}$ the maximum amount of time required for a packet to travel one hop distance is $\text{WPT}/2$. Therefore the delay per hop value must not exceed the estimated WPT. If it is then it is route under wormhole tunnel. Such route is then added to wormhole node list.

E. A reliable and secure framework for detection and isolation of malicious node in MANET [5]:

This paper detects malicious node and isolates such malicious node. In this multipath routing is used. Initially multipath set is determined by RMR. An MPS of node disjoint path is constructed by successively calculating the node-disjoint, shortest in number of hops, paths. Paths are arranged on reliability index. The reliability index is calculated in packet delivery ratio. $\text{RI}_k = \text{Pdk} * \text{W}$. RI_k is the reliability index of the k th path and Pdk is the packet delivery ratio of the k th path. The primary reliable path used to send transmission information. Second system component is prevention of data by using dispersion technique. After determining MPS, the source S disperses each message, adding redundancy to the data. Separate the information into pieces that are transmitted across the MPS routes one piece per route. Reconstruction of message is done at the destination, even if some of the data pieces are lost or corrupted. $r = N/M$ is redundancy factor. If the dispersed message cannot reconstruct then T waits for S to retransmit the missing pieces. In this approach detection and removal of malicious node is done by the destination. Two new control packets are used PI and NACK. PI (packet information) used to detect misbehaviour. PI sent from source to destination at the start of data transmission. A NACK packet is used to ack the source node when misbehaviour is detected along data transmission path. The source gets the primary reliable path R1 from MPS before sending out data packets. Out on n disjoint reliable paths from MPS, data packets are dispersed through m reliable paths. The PI is send through primary reliable path which includes packet size, number of packet. When destination reconstructed packets and matched with data in PI. If it is not matched then NACK send to the source. Upon receiving NACK packet, the source removes corresponding paths from its MPS and route cache.

This approach uses dispersion technique which uses multiple set paths so network overhead increases. If any node drops the packet then destination node have to wait until that piece received. All paths might not reliable.

V. COMPARISON OF VARIOUS APPROACHES USED TO PREVENT VARIOUS ATTACKS

The following table provides detailed comparison of various approaches used to prevent various attacks.

TABLE 1

Approach	HSAM[1]	Ex-watchdog and Pathrater[2]	Detection and accusation of packet forwarding misbehaviour in MANET[3]	WAP[4]	A reliable and secure framework for detection and isolation of malicious node in MANET[5]
Routing Scheme	AODV	DSR	AODV	DSR	AOMDV
Type of attack it focuses	Packet dropping and message tempering attack(black hole attack)	False reporting and network partition	Packet forwarding misbehaviour and selfish node	Wormhole attack	Daniel of service and data tempering attack
Attack Vulnerability	Cannot deals with colluding attack	Cannot deal with cooperative black hole attack	Cannot deal with denial of service attack and ambiguous collision	Cannot deal with data tempering attack	Cannot deal with wormhole attack

Authentication Scheme	One-Way Hash Chain	Public key cryptography	Threshold secret sharing as SCAN, MACW	DPH	Message authentication code
Drawbacks	Only suspicious path is detected. Routing packets are forwarded to neighbours without checking its authenticity	Decrement in overhead but no increment in throughput	It trusts on node to forward packet. They only consider packet dropping.	Impossible to always monitor ongoing traffic. Focuses on wormhole attack only.	It is not disclosed the complexity

V. CONCLUSIONS

This paper primarily focuses on various routing protocols, their classification based on multiple factors and their working used in MANET. Due to flaws in MANET it is vulnerable to various attacks which are studied. This paper mainly discuss about various methods and techniques used to prevent MANET from various network layer attack. Various cryptographic methods are used to achieve security goals in MANET. This paper emphasises on security approaches based on various routing protocol and provide comparison of these techniques.

REFERENCES

- [1] G. S. Mamatha and S. C. Sharma, "A highly secured approach against attacks in MANETs", Intl. Journal of Computer Theory and Engineering, Vol. 2, No. 5, Oct. 2010.
- [2] N., Nasser and C. Yunfeng, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks", IEEE Intl.Conference on Communications, Vol. 07, No. 24-28 June, pp. 1154-1159,2007.
- [3] O. F. Gonzalez, G. Ansa, M. Howarth, G. Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, Vol. 2, No. 1, pp. 181-192,June 2008.
- [4] S. Choi, D-Y. Kim, D-H Lee, J-I.Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", International Conference on Sensor Networks, Ubiquitous, & Trustworthy Computing,(SUTC' 08), June 11-13, Taichung, Taiwan, pp.343-348, 2008.
- [5] S. Dhanalakshmi, M. Rajaram, "A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET", IJCSNS International Journal of Computer Science and Network Security, Vol. 8,No.10, Oct., 2008.
- [6] P. N. Raj and P. B. Swadas, " DPRAODV: A Dynamic learning system against blackhole attack in AODV based MANET", Intl. Journal of Computer Science Issues, Vol. 2, 2009.
- [7] Irshad ullah ,Shoab ur rehman, "analysis of black hole attack on manets using different manet routing protocols" , *master thesis electrical engineering ,thesis no: mee 10:62 june, 2010.*
- [8] n.shanthi, dr.lganesan ,dr.k.ramar," study of different attacks on multi cast mobile ad hoc network", jatit 2009.
- [9] Pooja Vij,V.K. Banga,"Broadcast id based detection and correction of black hole in manet",*International Journal of Computer Applications (0975 – 8887) Volume 56– No.17, October 2012.*
- [10] Introduction to Ns2 <http://www.cs.ucsb.edu/~gayatri/ta/cs276.html>