



ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



A Review on Multicast Routing Protocols and its Foremost Security Issues in Mobile Ad-hoc Network

¹R. Regan and ²J. Martin Leo Manickam¹Department of Computer Science and Engineering, University College of Engineering Panruti, Cuddalore, India²Department of Electronics and Communication Engineering, St. Joseph's College of Engineering, Chennai, India

ARTICLE INFO

Article history:

Article Received: 12 January 2015

Revised: 1 May 2015

Accepted: 8 May 2015

Keywords:

Mobile Ad-hoc Network (MANET),
Multicast Protocol, Black hole attack,
Wormhole attack.

ABSTRACT

MANETs is an autonomous system of wireless nodes connected by wireless links. MANET provides a communication over the shared wireless channel without the support of fixed infrastructure or access point. MANETs are totally dependent on collective participation of all nodes in routing of information through the network. In MANETs, security is one of the most important concerns because a Manet's system is more vulnerable to attacks than a wired network. Multicasting in MANETs is very challenging due to the dynamic nature of the network topology and the stringent node/host constraints. The multicast protocol is found to be more vulnerable towards attacks like black hole and wormhole attacks. With rapid deployment of MANET, security has become one of the major problems that MANETs face today. This paper present a review on detection and prevention mechanism for black hole and wormhole attacks on mesh-based multicast in MANETs.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: R. Regan and J. Martin Leo Manickam, A Review on Multicast Routing Protocols and its Foremost Security Issues in Mobile Ad-hoc Network. *Aust. J. Basic & Appl. Sci.*, 9(21): 97-108, 2015

INTRODUCTION

A Mobile Ad-Hoc NETWORK (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure, or centralized administration. A mobile node can be laptop computer, personal digital Assistant or a cellular phone. In MANETs, routing and resource management are done in a distributed manner; that is, all nodes coordinate to enable communications among themselves. This requires each node to be more intelligent so that it can operate both as a network host for transmitting and receiving data, and as a network router for forwarding packets for other nodes.

MANETs are envisioned to support advanced applications such as military operations (formations of soldiers, tanks, planes), civil applications (e.g., audio and video conferencing, sport events, telematics applications (traffic)), disaster situations (e.g., emergency and rescue operations, national crises, earthquakes, fires, floods), and integration with cellular systems. In addition, applications in this area require a secure communication, as eavesdropping or other security threats can compromise the network and threaten the safety of personnel involved in these military operations.

Secure multicast may also be required. For example, the leader of a group of soldier may want to give an order to the entire soldier, or to a set of selected personnel. Hence, routing protocols in such applications are required to provide secure communication with support for multicast routing. Multicasting is the transmission of data to a group of hosts identified by a single destination address and hence is intended for group-oriented computing. Multicast routing protocols play an important role in MANETs to provide communication for their applications it is always advantageous to use multicast rather than multiple unicast, especially in the Ad hoc environment where bandwidth is constrained.

In MANETs, security is one of the most important concerns because a MANET system is much more vulnerable to attacks than a wired or infrastructure based wireless network. Designing an effective security protocol for MANETs is a very challenging task. This is mainly due to the unique characteristics of MANETs, namely shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among users, limited availability of resources, and physical vulnerability. This paper present a review about multicast routing protocol's security issues and defense mechanism for major security attack like

Corresponding Author: R. Regan, Department of Computer Science and Engineering, University College of Engineering Panruti, Cuddalore, India.
E-mail: Reganr85@gmail.com

black hole and wormhole attacks on multicast in MANETs.

Multicast Communication in Manets:

Multicasting is the transmission of data packets to more than one node sharing one multicasting address. The senders and receivers form the multicast group. Multicast plays an important role in MANET. Multicasting in MANETs is much more complex than in wired networks and faces several challenges like no fixed infrastructure, restrictions on node energy and capacity. Many Ad hoc network applications need the nodes to work as a group to carry out a given job. This kind of application is efficient due to the broadcast nature of wireless network, which can improve the efficiency of the wireless links. As a result, multicast routing has become focus on research recently, and various multicasting protocols in MANET have been proposed. Actually, there could be more than one sender in a multicast group, so it is group-oriented communication.

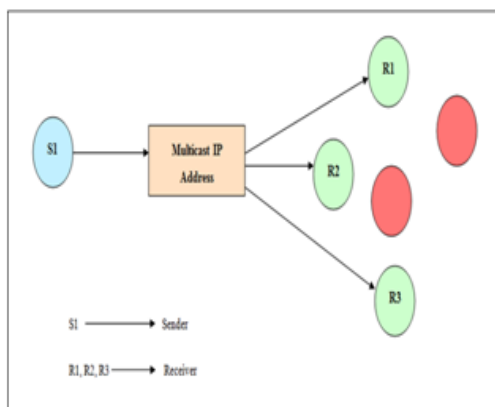


Fig. 1: Multicast routing

Multicast routing protocol design-issues and challenges:

Limited bandwidth availability, an error-prone shared broadcast channel, the mobility of nodes with limited energy resources, the hidden terminal problem, and limited security make the design of a multicast routing protocol for ad hoc networks a challenging one. There are several issues involved here which are discussed below.

Robustness:

Due to the mobility of the nodes, link failures are quite common in ad hoc wireless networks. Thus, data packets sent by the source may be dropped, which results in a low packet delivery ratio. Hence, a multicast routing protocol should be robust enough to sustain the mobility of the nodes and achieve a high packet delivery ratio.

Efficiency:

In an ad hoc network environment, where the bandwidth is scarce, the efficiency of the multicast protocol is very important. Multicast efficiency is defined as the ratio of the total number of data packets received by the receivers to the total number of (data and control) packets transmitted in the network.

Control overhead:

In order to keep track of the members in a multicast group, the exchange of control packets is required. This consumes a considerable amount of bandwidth. Since bandwidth is limited in ad hoc networks, the design of a multicast protocol should ensure that the total number of control packets transmitted for maintaining the multicast group is kept to a minimum.

Quality of service:

One of the important applications of ad hoc networks is in military/strategic applications. Hence, provisioning quality of service (QoS) is an issue in ad hoc multicast routing protocols. The main parameters which are taken into consideration for providing the required QoS are throughput, delay, delay jitter, and reliability.

Dependency on the unicast routing protocol:

If a multicast routing protocol needs the support of a particular routing protocol, then it is difficult for the multicast protocol to work in heterogeneous networks. Hence, it is desirable if the multicast routing protocol is independent of any specific unicast routing protocol.

Resource management:

Ad hoc networks consist of a group of mobile nodes, with each node having limited battery power and memory. An ad hoc multicast routing protocol should use minimum power by reducing the number of packet transmissions. To reduce memory usage, it should use minimum state information.

Security and Reliability:

Security provisioning is a crucial issue in MANET multicasting due to the broadcast nature of this type of network, the existence of a wireless medium, and the lack of any centralized infrastructure. This makes MANETs vulnerable to eavesdropping, interference, spoofing, and so forth. Reliability is particularly important in multicasting, especially in these applications, and it becomes more difficult to deliver reliable data to group members whose topology varies.

Multicast protocol description:

Multicasting consists of concurrently sending the same message from one source to multiple destinations. It plays an important role in video-

conferencing, distance education, co-operative work, and video on demand, replicated database updating and querying, etc. Several multicast routing protocols have been proposed for Mobile Ad hoc networks, which are classified as mesh based Routing, tree based Routing and Hybrid based Routing.

Tree Based Routing:

Tree-based multicast routing protocols can be further divided into source-rooted and core-rooted schemes according to the roots of the multicast trees. In a source-rooted tree-based multicast routing protocol, source nodes are roots of multicast trees and execute algorithms for distribution tree construction and maintenance. AM Route is an example for source-rooted tree multicast routing protocol. In a core-rooted tree multicast routing protocol, cores are nodes with special functions such as multicast data distribution and membership management. Some core-rooted multicast routing protocols utilize tree structures. But unlike source-rooted tree-based multicast routing, multicast trees are only rooted at core nodes. Shared Tree Ad-hoc Multicast Protocol (STAMP) and Adaptive Core-based Multicast Routing protocol (ACMP) are core-based multicast routing protocols proposed for MANETs. Their disadvantage is that until the tree is reconstructed after movement of a node, packets possibly have to be dropped. In a mesh-based multicast routing protocol [27], packets are distributed along mesh structures that are a set of interconnected nodes.

Mesh based Routing:

Mesh-based approaches sacrifice multicast efficiency in comparison to tree-based approach. Mesh-based Multicast Routing Protocol with Consolidated Query Packets (CQMP), Enhanced On-Demand Multicast Routing Protocol (E-ODMRP [28]) and Adaptive Demand-Driven Multicast Routing (ADMR) are the mesh-based multicast routing protocols proposed for MANETs. A mesh network can be designed using a flooding technique or a routing technique. When using a routing technique, the message propagates along a path, by hopping from node to node until the destination is reached. To ensure all its paths' availability, a routing network must allow for continuous connections and reconfiguration around broken or blocked paths, using self-healing algorithms.

Hybrid based Routing:

Hybrid-based multicast routing protocols combine the advantages of both tree and mesh-based approaches. Hence, hybrid protocols address both efficiency and robustness. Using this scheme, it is possible to get multiple routing paths, and duplicate messages can reach a receiver through different paths. Efficient Hybrid Multicast Routing Protocol

(EHMRP) is an instance for hybrid-based multicast routing protocol. This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. We have chosen the mesh based protocol in MANETs for our analysis, because in case of mesh based protocol, we have multiple paths from the source to destination. Whereas in case of tree based protocol we have exactly one path from source to destination.

Multicast routing protocols in manets:

A review some of list of multicast protocols will be discussed in below.

Mesh-Based Multicast Routing Protocol with Consolidated Query packets (Harleen Dhillon 2005):

The Mesh-based multicast routing Protocol with Consolidated Query packets (CQMP) is a reactive mesh-based multicast routing protocol with an idea of "query packet consolidation" to address this scalability problem. This feature is a crucial contributing factor to the scalability of multicast routing for MANETs. Instead of each source sending advertising packets to the network, in CQMP, each core disseminates to the network the mappings of multicast addresses to one or more core addresses. CQMP, however, assumes the availability of routing information from a unicast routing protocol. This unicast routing protocol is also required to provide correct distances to known destinations within a finite amount of time.

The Enhanced On Demand Multicast Routing Protocol (EODMRP):

The Enhanced On-Demand Multicast Routing Protocol (EODMRP) is an enhancement of On Demand Multicast Routing Protocol ODMRP, which is a reactive mesh-based multicast routing protocol. It is an enhanced version of ODMRP with adaptive refresh. Adaptation is driven by receivers' reports. The second enhancement is the "unified" local recovery and receiver joining scheme. As the time between refresh episodes can be quite long, a new node or a momentarily detached node might lose some data while waiting for the routing to it to be refreshed and reconstructed. Upon joining or upon detection of broken route, a node performs an expanding ring search to proactively attach itself to forwarding mesh or to requests a global route refresh from the source. The major advantage is reduced overhead, which translates into a better delivery rate at high loads, yet keeping the same packet delivery ratio as the original ODMRP.

Ad hoc on-demand distance vector (AODV):

The AODV routing protocol is based on DSDV and DSR algorithm. It uses the periodic beaconing and sequence numbering procedure of DSDV and a similar route discovery procedure as in DSR. However, there are two major differences between DSR and AODV. The most distinguishing difference is that in DSR each packet carries full routing information, whereas in AODV the packets carry the destination address. This means that AODV has potentially less routing overheads than DSR. The other difference is that the route replies in DSR carry the address of every node along the route, whereas in AODV the route replies only carry the destination IP address and the sequence number. The advantage of AODV is that it is adaptable to highly dynamic networks. However, node may experience large delays during route construction, and link failure may initiate another route discovery, which introduces extra delays and consumes more bandwidth as the size of the network increases.

Location- Based Geocasting and Forwarding (LGF) (Latiff, 2005):

In this protocol has implemented by real-time integration of GPS- free indoor location tracking mechanism with geocast-enhanced Adhoc On-Demand Vector (AODV) . The LGF protocol will provide distance information to each and every other node in the network. When a node has packet to send, it will broadcast the route request packet to all its neighbours within its transmission area. The request packet has additional information that is the distance from the source to destination. Hence, every node that received RREQ packet it will compare its distance to the destination. If its distance is less than the source to destination, the node will rebroadcast the packet; otherwise, it will discard and cancel its scheduled rebroadcast of the packet. Along the route, participating nodes will send a route reply packet (RREP) to the source via intermediate nodes. With path accumulation (PA), these routes will be stored and used in the packet forwarding phase via the routes discovered beforehand. Hence, routing overhead and flooding of packets will be reduced significantly. In AODV, packet will be lost if a node moves from its current location and out of the original neighbors' coverage or running low on batteries and there is no indication sent to the source to initiate route re-discovery. With GAODV, the re-route discovery phase will be invoked in the source node when it did not receive a RREP after a specified time.

Multicast Ad Hoc On-Demand Distance Vector (MAODV) Protocol (Royer, 2000) Description:

The MAODV protocol is extended from AODV. It maintains a shared tree for each multicast group, which consists only of receivers and relays (forwarding nodes). It determines a multicast route

on demand by using a broadcast route discovery mechanism. The first member of a multicast group becomes the leader of that group. The multicast group leader is responsible for maintaining the multicast group sequence number and broadcasting this number to the multicast group. This is done through a group HELLO message. Nodes use the group HELLO information to update their Request Table. If a node wants to join a multicast group, it originates a route request (RREQ) packet and unicasts it if it has the address of the group leader. If the address of the group leader is unknown, then the node broadcasts the RREQ packet. Only the group leader, or a member of the desired multicast group with a sequence number larger than that in the RREQ packet, can respond to a Join RREQ packet. When the group leader or a member of the desired multicast group receives multiple RREQ packets, it selects the one with the highest sequence number and the lowest hop count, and unicasts a route reply RREP packet to the requesting node. The RREP packet contains the distance of the replying node from the group leader and the current sequence number of the multicast group. When the receiving node receives more than one RREP packet, it selects the most recent one and the shortest path from all the RREP packets. Then, it sends a multicast activation message MACT to its next hop to enable that route

Adaptive Demand Driven Multicasting:

ADMR is an on-demand protocol, thus it does not maintain route information regularly. Member nodes that constitute the tree are refreshed as needed and do not send explicit leave messages. In ADMR, group membership and multicast routes are established and updated by the source on demand. Multicast senders and receivers using ADMR cooperate to establish and maintain forwarding state in the network to allow multicast communication. The multicast forwarding state for a given multicast group G and sender S in ADMR is conceptually represented as a loosely-structured multicast forwarding tree rooted at S. Each multicast packet is dynamically forwarded from S along the shortest-delay path through the tree to the receiver members of the multicast group.

Multicast attacks on Manets:

Attacks on the security of a MANET are characterized by viewing the function of the MANET as providing information. The attacks in MANETS are classified into two major categories, namely passive attacks and active attacks. Passive attacks are those, launched by the adversaries solely to snoop the data exchanged in the network. These adversaries in any way don't disturb the operation of the network. Identification of such attacks, becomes very difficult since network itself does not get affected. But an active attack tries to alter or destroy the information that is being exchanged, thereby disturbing the

normal functionality of the network. The attacks can also be classified into two categories, namely external attacks and internal attacks. External attacks are those, launched by the adversaries that do not belong to the network. Internal attacks are launched by the compromised nodes within the network. This node tries to collect security information and can access the protected rights of the network. Since the compromised node is an authorized one in the network, it is very difficult to identify the internal attacks. The attacks which are chosen are found to be more vulnerable in the Mobile Ad hoc NETWORKS are black hole and wormhole. The first attack which is chosen is black hole attack [9], before implementing black hole attack the rushing attack has to be implemented. These attacks are chosen due to the drastic impact made in the network due to the presence of these attacks. The solution given to the black hole attack will also solve the rushing attack problem. The second attack which is chosen is wormhole attack in which, a pair of colluding attackers will be present and it will drop the packets which traverse through them. This attack will decrease the packet other attacks.

Black Hole Attack:

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listens the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device succeeds in inserting itself between the communicating nodes, it is able to do anything with the packets passing between them.

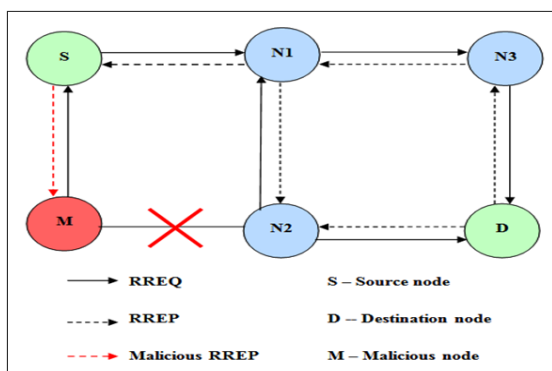


Fig. 2: Black Hole Attack

Figure 2 shows how black hole attack arises, here node “S” want to send data packets to node “D” and initiate the route discovery process. So if node “M” is a malicious node then it will claim that it has active route to the specified destination as soon as it

receives RREQ packets. It will then send the response to node “S” before any other node. In this way node “S” will think that this is the active route and thus active route discovery is complete. Node “S” will ignore all other replies and will start sending data packets to node “M”. In this way all the data packet will be lost consumed or lost.

Wormhole Attack:

In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole. The wormhole attack is particularly dangerous for many Ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node.

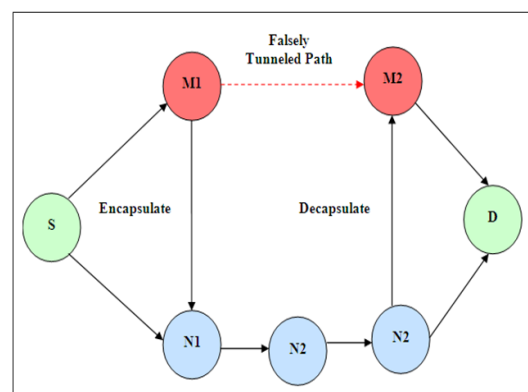


Fig. 3: Wormhole attack.

In the figure 3, an attacker M1 colludes with another attacker M2 in order to deceive destination of a packet into regarding the route including both M1 and M2 as the most efficient path. Since most routing protocols for ad hocnetwork select cost effective path, the path between M1 and M2 may be chosen as the communication route from source to destination Solid lines denote actual paths between nodes and the dotted line denotes the tunnel path that M1 and M2 falsely claim is between them. Let the node S want to form a route to D and initiates route discovery. When M1 receives a RDP (Route Discovery Process) from S, M1 encapsulates the RDP and tunnels it to M2 through an existing data route, in this case (M1, N1,N2, N3, M2). When M2 update the packet header to reflect that the RDP, it x forwards the RDP on to D as if it had only travelled (S, M1, M2, D). M1 or M2 update the packet header to reflect that the RDP also travelled the path (N1, N2, N3,). After route discovery, it appears to the

destination that there are two routes from S of unequal length: (M1, N1, N2, N3, M2) and (S, M1, M2, D). If M2 tunnels the RREP back to M1, S would falsely consider the path to D via M1 a better choice in terms of path length than the path to D via N1.

The related work:

Various surveys have been done against the solutions for attacks like black hole attack and Wormhole attacks for MANETs.

Black Hole Attack Solutions:

K. Aishwarya, N.Kannaiah Raju and A. Senthamarai Selvan proposed a solution for blackhole attack in E-ODMRP[28]. According to this proposed solution the Source node in E-ODMRP does not accept every first RREP but calls Previous received RREQ which stores all the RREPs in the newly created(EODMRP_RREP_Tab) table till ODMRP_WAIT_TIME. Then it analyses all the stored RREPs from EODMRP_RREP_Tab table and discards the RREP having exceptionally high destination sequence number. The node that sent this RREP is suspected to be the malicious node. EODMRP maintains the identity of the malicious node as Mail node. So that in future it can discard any RREPs from that node. Now since malicious node is identified the routing table for that node is not maintained and also control messages from the malicious node will not be forwarded in the network. EODMRP_RREP_Tab is flushed once an RREP is chosen from it. The solution after detecting the malicious node acts as normal EODMRP by accepting the RREP with lower destination sequence number.

Feng Li, Jie Wu and Avinash Srinivasan proposed a solution for black hole attack. In this paper they propose a novel monitoring approach that overcomes some watchdog's shortcomings, and improves the efficiency in detection. To overcome false detections due to nodes mobility and channel conditions we propose a Bayesian technique for the judgment, allowing node redemption before judgment. Finally, they suggest a social-based approach for the detection approval and isolation of guilty nodes.

Dynamic Learning System using DPRAODV[6]:Payal N. Raj, Prashant B. Swadas proposed DPRAODV[6] (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value

is dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. This solution increases the average end to end delay and normalized routing overhead.

Dr Karim Konate and Abdourahime Gaye proposed a solution for blackhole attack The Threshold of sequence number consists in performing a check to find if RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated in each interval of time. As the value of RREP_seq_no proves higher than the threshold value, one suspects the node to be malicious and adds it to the black list. This mechanism is implemented in the routing protocol named Detection, Prevention and Reactive AODV (DPRAODV(Payal Raj, 2009). The Watchdog or monitoring (watchdog) is a solution which makes it possible to identify malicious nodes. The Watchdog assigns positive values with a node which successfully forwarded packages and a negative value after a threshold level of bad behavior was observed. It's implemented in the protocol called mobile Secure Watchdog for Ad hoc Network (SWAN). Path rater which makes it possible the protocol to avoid nodes corrupted register in a black list. The DRI or the data table of information's routing which is used to identify nodes of cooperative black hole, it consists in adding two additional bits of information. These bits have as values 0 for "FALSE" and 1 for " TRUE " for intermediate nodes answering the RREQ of node source, AODV implements this mechanism . The Cross checking solution which consists in hoping on reliable node to transfer from the packets of data.

AODV-SABH (AODV Secured against Black Hole attack) Fatima Ameza, Nassima Assam and RachBeghdad proposed two different approaches for securing RREQ and RREP packets.

Securing RREQ packets:

To secure RREQ packets two additional fields are added in the RREQ packet. The first field will be used to include the list of the addresses of all the intermediate nodes between the source and the destination, in order to detect the address of the attacker. On the other hand, each node will use the second field to record the sequence number of the destination node that it knows. On receipt of the RREQ packet, the destination node D compares its own sequence number (SN_D) to the one of the received packet. If the sequence number of the received packet is greater than SN_D then the packet will be rejected, D will use the first added field in the

packet to find the intruder, and it will alert the other nodes.

Securing RREP packets:

To secure RREP packets, every node will record the addresses of all nodes to whom it will forward the RREQ packet in a local table. To do that, every node receiving RREQ packet during the route discovery process must send its address to the sender. So, when a node receives a RREP packet it can check if the address of the sender belongs or not to its local table. If the address of the sender of RREP does not match any address recorded in its local table, then the receiving node concludes that the sender is a malicious node. So, it will reject the packet, and will alert the other nodes.

Prevention of Co-Operative Black Hole Attack (PCBHA) (Latha Tamilselvan 2008) Latha Tamilselvan and Dr.V Sankaranarayanan proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. This approach is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. The fidelity level of each RREP is checked and if two are having same level then one is selected having highest level. The responses are collected in the response table. A valid route is selected from among the received responses based on the following methodology. A fidelity table is maintained that will hold the fidelity levels of the participating nodes. The basic idea is to select the node with a high fidelity level. Initially the fidelity levels of the responded node and its next hop are looked for. If the average of their levels is found to be above the specified threshold, then the node is considered to be reliable. On the receipt of multiple responses, the one with the highest fidelity level is chosen. In case, two or more nodes seemed to have the same fidelity levels, then the one with the minimum hop count is chosen. When the fidelity level of a node drops to 0, it implies it has not forwarded the data packets faithfully and hence a Black hole. The detection of a Black hole has to be intimated to the other participating nodes in the network. This is accomplished by sending alarm packets.

Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park proposed two different approaches to solve the black hole attack (Mohammad AL-Shurman, 2004). In the first solution, the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. Since any packet can be arrived to the destination through many redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe

route is identified. Once a safe route has identified, these buffered packets will be transmitted. When a RREP arrives to the source, it will extract the full paths to the destinations and wait for another RREP. Two or more of these nodes must have some shared hops. From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. This solution can guarantee to find a safe route to the destination, but the main drawback is the time delay. In the second solution, every node needs to have two additional small-sized tables; one to keep last-packet-sequence-numbers for the last packet sent to every node and the other to keep last-packet-sequence-numbers for the last packet received from every node. These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last-packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last-packet-sequence-numbers received from the source by this intermediate node. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol.

The Distributed and Cooperative Mechanism:

The proposed distributed and cooperated "black hole" node detection mechanism composes of four sub-steps. With the local data collection step, each node in the network is required to evaluate if there is any suspicious node in its neighborhood by collecting information through overhearing packets and using the collected information to construct an estimation table. The estimation table, which is maintained by each node, contains information regarding to nodes that are within its power range (Node field), whether there is any data packet sent from the neighboring nodes to itself (From field), whether there is any data packet routed from itself to the neighboring node and received corresponding ACK reply (Through field), ratio of received and transmitted packets of the neighboring node (RTS/CTS field), and a field indicating whether that neighboring node has been verified as being "suspicious" (Suspicious field). The estimation table can be used to identify suspicious black hole nodes. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop

neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network.

N.H. Mistry, D.C. Jinwala and M.A. Zaveri focused on improving the Secure Ad hoc On demand Distance Vector (AODV), Multicast Ad Hoc On-Demand Distance Vector (MOSAODV (Mistry, 2009) routing protocol to safeguard it against the Black hole attack. Unlike AODV, source node in MOSAODV (Mistry, 2009) does not accept every first RREP but calls Pre_ReceiverRREP (Packet p) which stores all the RREPs in the newly created (Cmg_RREP_Tab) table till MOS_WAIT_TIME. Then it analyses all the stored RREPs from Cmg_RREP_Tab table, and discards the RREP having exceptionally high destination sequence number. The node that sent this RREP is suspected to be the malicious node. MOSAODV (Mistry, 2009) maintains the identity of the malicious node as Mali node so that in future it can discard any RREPs from that node. Now since malicious node is identified the routing table for that node is not maintained and also control messages from the malicious node will not be forwarded in the network. Cmg_RREP_Tab is flushed once an RREP is chosen from it. Our solution; after detecting the malicious node acts as normal AODV by accepting the RREP with higher destination sequence number.

Sukla Banerjee proposed to modify AODV protocol by introducing three more tables maintained at each node. First one is DRI (Sukla Banerjee, 2008) (Data Routing Information) table maintained at each node for the purpose of monitoring each of its neighbors. Another table is the find Malicious table which keeps the track of the nodes suspected as malicious with their vote Count. And the Black hole table which keeps the track of the black listed nodes. We also modified the routing table of the AODV by adding a new field called find Hole Status which is set as true if a malicious node is found in the route.

Bo Sun, Yong Guan, Jian Chen, Udo W.Pooch, used two additional control packets for collecting the neighborhood information (Wassim Znaidi, 2008) for detecting the black hole node. The formats of these packets are RQNS {Scr_addr, Dest_Addr, Request_neighbor_seq#, Next_hop} and RPNS {Scr_Addr, Dest_Addr, Request_neighbor_seq#, Neighbor_Set}. The basic idea of this approach is that the neighbor set difference of one node at different time instance is less than or equal to one, and the probability that the neighbor set difference of two nodes at same time instance is very small. After getting RREP from more than one node the sender sends the RQNS packet. After receiving more than one RPNS packet the sender node compare the received neighbor set, if the difference is larger than

some pre defined threshold value then the current network is affected by black hole attack. But the drawback of this approach is after comparing the neighbor set they use a cryptographic method to identify the actual infected node. This is a costly and less reliable technique in case of ad hoc network.

Worm Hole Attack Solutions:

An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks (Gunhee Lee, 2008) Gunhee Lee, Dong-kyoo Kim and Jungtaek Seo: Proposed an effective wormhole attack defense method that can properly detect wormhole attacks. Each node maintains the neighbor's information (neighbor list and key table). When a node sends or forwards a packet, it attaches a pair of information to the packet such as identity and a message authentication code (MAC) of the identity. The MAC is computed by a keyed hash function such as HMAC. The session key is used to compute the MAC. With the information, the next hop of the sender on the route is able to detect the wormhole. When a node n_3 receives a packet from its neighbor n_2 , it performs two tests for the packet such as one-hop neighbor correctness and two-hop neighbor correctness. For the former test, n_3 searches the neighbor list for the identity of n_2 . If an entry (n_2 , null) exists, n_3 acquires a session key shared with n_2 from the key table, and it verifies validity of the MAC of n_2 by calculating a MAC of the n_2 's identity with the key. If they are the same, n_3 believes n_2 is not a wormhole node. Otherwise, it drops the packet and distrusts n_2 . For the latter test, n_3 checks whether the node n_1 is a two-hop neighbor or not. The test is carried out only if one or more pairs that do not contain null value and each object of the pair is the same as the identity in the received packet. If the entry (n_2 , n_1) exists and the MAC of n_1 is valid, the node n_3 trusts the truth that n_1 is a two-hop neighbor.

MANET Routing Protocols and Wormhole Attack against AODV (Ashish Patel, 2010) Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah: Proposed a mechanism "packet leashes" to prevent and detect wormhole attack. This mechanism is suggested in which all nodes in the MANET can obtain authenticated symmetric key of every other node. The receiver can authenticate information like time and location from the received packet. "Time of Flight" is a technique used for prevention of wormhole attacks. It calculates the round-trip journey time of a message; the acknowledgement estimate the distance between the nodes based on this time, and conclude whether the calculated distance is within the maximum possible communication range. If there is a wormhole attacker involved, packets end up traveling further, and thus cannot be returned within the short time.

SAM (Statistical Analysis of Multi-path) Lijun Qian, Ning Song, and Xiangfang Li proposed to detect exposed wormhole attacks in Multi-path

routing protocol. The main idea of the proposed scheme SAM is based on the observation that certain statistics of the discovered routes by routing protocols will change dramatically under wormhole attacks. Because wormhole links are extremely attractive to routing requests so it will appear in more routes than normal links. By doing statistics on the relative frequency of each link appear in the set of all obtained routes, they can identify wormhole attacks. This technique is only used to detect exposed attacks. It is unable to detect hidden attacks because in this kind of attack wormhole links does not appear in obtained routes.

DeLPHI (Hon Sun 2006) (Delay per Hop Indicator), Hon Sun Chiu and King-Shan Lui, proposed to detect both hidden and exposed wormhole attacks. In this mechanism, they try to find every available disjoint path between a sender and a receiver. Then, they calculate delay time & length of each path, computing Delay per Hop value (average delay time per hop along each path). Delay per Hop values of paths are used to identify wormhole: the path containing wormhole link will have greater Delay per Hop value. This mechanism can detect both kind of wormhole but they cannot pinpoint the wormhole location. Moreover, because lengths of paths are changed by every node (including wormhole nodes) so wormhole nodes could change the path length in a certain way to make them unable to be detected.

DeWORM (Thaier Hayajneh, 2009), Thaier Hayajneh, Prashant Krishnamurthy and David Tipper proposed a simple protocol called DeWorm to detect wormhole in wireless ad hoc networks. Generally, for a wormhole attack to have a successful impact on the network it must attract a significant amount of network traffic by providing a perceived short-cut through the network. Hence, routes going through the wormhole must be shorter than alternate routes through valid network nodes. This observation is the basis of the wormhole detection protocol "DeWorm". Specifically, in DeWorm, we use routing discrepancies between neighboring nodes along a path from a source to a destination to detect wormhole attacks. The protocol is simple and localized, can be applied on demand (when the existence or lack thereof of a wormhole needs to be verified), needs no special hardware, localization, or synchronization and can detect physical layer wormholes. Basically it has 10 stages to detect the presence of wormhole in a network.

LITEWORLD AND MOBIWORLD (Khalil, 2008.) Khalil, S. Bagchi, and N. B. Shroff have developed two protocols to defend against wormholes: A Lightweight Countermeasure for the Wormhole Attack (LITEWORLD) and Mitigation of the Wormhole Attack in Mobile Multihop Wireless (MOBIWORLD). LITEWORLD works with a static network and assumes that there is a guard node within the transmission range of any two neighboring

nodes. The guard will monitor all traffic and detect selective forwarding by the wormhole attack. Thus LITEWORLD requires overhead in terms of guard nodes and a dense network for successful operation. MOBIWORLD (Khalil, 2008) works with mobile networks but requires location information, a trusted central authority, and assumes the network to be loosely time synchronized. They collect information about neighbors that exist in two hops distance, and some nodes, which can overhear both the forwarder and the next node of it, monitor forwarding packet. Monitoring nodes check whether both two packets transmitted by them are the same or not. To do so, several monitors should be activated for a link, and they should have a buffer that saves the information of packets delivered via the link. The Mobi World (Khalil, 2008) requires a certified authority to verify the truth of node's location information. Moreover, in the Mobi World, each node should acquire an authentication message from the authority in order to transmit a message whenever it moves to other place.

Trust Based Detection: Pirzada and C. McDonald present a trust-based wormhole detection scheme. In this scheme, a node sends a packet and waits for overhearing retransmission of the same packet, which is done by its neighbor. If the same packet is forwarded, the sender increases the trust value of the neighbor. Otherwise, the sender distrusts the neighbor, and it drops all packets to the neighbor. Every node should place its wireless interface into the promiscuous mode for every time interval. Moreover, it can only be applied to DSR routing protocol.

S. Vijayalakshmi and S. Albert Rabara proposed a solution for wormhole attack. Two solutions have been proposed for preventing wormhole attack. First solution is given by the concept of leash for detecting and preventing wormhole attack. A leash is any information added to a packet in order to restrict the distance that the packet is allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash. Two types of leashes are considered, namely geographical leashes and temporal leashes. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet. As a result, the packet can only travel a limited distance. A receiver of the packet can use these leashes to check if the packet has traveled farther than the leash allows and if so can drop the packet. Another approach for detecting wormhole attacks is deploying directional antennae. The approach here is based on the use of packet arrival direction to detect that packets are arriving from the proper neighbors. Such information is possible due to the use of directional antennae. This information about the direction of packet arrival is expected to lead to accurate information about the set of neighbors of a

node. As a result, wormhole attacks can be detected since such attacks emanate from false neighbors.

Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo proposed a solution for wormhole attack proposed a graph theoretic model to characterize the wormhole attack and as certain the necessary and sufficient conditions for any candidate solution to prevent wormholes. They used a Local Broadcast Key (LBK) based method to set up a secure ad-hoc network against wormhole attacks. In other words, there are two kinds of nodes in their network: guards and regular nodes. Guards access the location information through GPS or some other localization method like Se RLoc and continuously broadcast location data. Regular nodes must calculate their location relative to the guards' beacons, thus they can distinguish abnormal transmission due to beacon retransmission by the wormhole attackers. All transmissions between node pairs have to be encrypted by the local broadcast key of the sending end and decrypted at the receiving end. As a result, the time delay accumulates per node traveled. In addition, special localization equipment has to be applied to guard nodes for detecting positions

Wassim Znaidi, Marine Minier and Jean-Philippe Babau proposed a solution for wormhole prevention in wireless networks. They propose an algorithm for detecting and thus defending against wormhole attacks in wireless. This algorithm uses only local and neighborhood information without requiring clock synchronization, location information or dedicated hardware. Moreover, the algorithm is independent of wireless communication models. The algorithm is able to detect wormhole attacks in all cases whereas the number of false alarms (false detections) decreases rapidly if the network is sufficiently dense. The algorithm presented above requires only the knowledge of 1-hop and 2-hop neighbor lists for each node. It runs locally and it can be executed periodically or every time the topology has changed in the network but it can be run again only by the nodes affected by this modification. So the wormhole attacks will be detected as soon as they are in place in the network.

Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung proposed a solution for called Wormhole Attack Prevention (WAP) without using specialized hardware. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. All nodes monitor its neighbor's behavior when they send RREQ messages to the destination by using a special list called Neighbor List. When a source node receives some RREP messages, it can detect a route under worm hole attack among the routes. Once wormhole node is detected, source node records them in the Wormhole Node List. Even though malicious nodes have been excluded from routing in the past, the nodes have a chance of attack once more. Therefore, we store the

information of wormhole nodes at the source node to prevent them taking part in routing again. Moreover, the WAP has the ability of detecting both the hidden and exposed attacks without special hardware.

Conclusion:

Routing in Mobile Ad-hoc NETWORKS faces additional problems and challenges. The problem of routing in such environments is aggravated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth, and high error rates. Thus MANETs are prone to many attacks during its operation in the wireless networks. Such major attacks are Black hole and Wormhole. Many researchers are focused on these attacks and have provided many solutions to overcome these attacks. An extensive survey has been made here about the various types of attack scenarios and the solutions that are provided to overcome it. In this paper section 7.1 describe they literature survey on black hole attack and their various solutions have been listed based on various scenarios. And section 7.2 is done on survey of wormhole attack, which sorts out all possible vulnerabilities of the mobile ad hoc networks for the attack scenario.

REFERENCES

- Ashish Patel, D., D. Jain Parmer and I. Behaving Shah, 2010. "MANET Routing Protocols and Wormhole Attack against AODV," *IJCSNS International Journal of Computer Science and Network Security*, 10(4): 12-18.
- Bounpadithkannhavong, Hidehisanakayama, Yoshiaki nemoto and Neikato, 2007. "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Communications.
- Hoang Lan Nguyen and UyenTrang Nguyen, 2006. "Study of Different Types of Attacks o Multicast in Mobile Ad Hoc Networks," Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06).
- Aishwarya, K., N. Kannaiah Raju and A. Senthamarai Selvan Counter, 2011. "Measures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol In Mobile AD-HOC Networks", in the Proceedings of International Journal of Technology And Engineering System (IJTES).
- Feng, Li., Jie Wu and Avinash Srinivasan, 2010. "Struggling Against Selfishness and Black Hole Attacks in MANETs", in the Proceedings of International Journal on Computer Networks and Security (IJCNS).
- Payal Raj, N. and B. Prashant Swadas, 2009. "DPRAODV: A dyanamic learning system against black hole attack in aodv based Manet", in the

Proceedings of International Journal of Computer Science Issues (IJCSI), Vol. 2.

Dr Karim Konate and Abdourahime Gaye, 2011. "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", in the *Proceedings of the International Journal of Future Generation Communication and Networking*, Vol. 4, No. 2.

Fatima Ameza, Nassima Assam and Rachid Beghdad, 2010. "Defending AODV Routing Protocol Against the Black Hole Attack," (IJCSIS) International Journal of Computer Science and Information Security, 08(2): 112-117.

Latha Tamilselvan and V. Sankaranarayanan, 2008. "Prevention of Co-operative Black Hole Attack in MANET," JOURNAL OF NETWORKS, 3(5): 13-20.

Mohammad AL-Shurman, Seon-Moo Yoo and Seungiin Park, 2004. "Black Hole Attack in Mobile Ad Hoc Networks," ACMSE'04, pp: 96-97, Huntsville, AL, USA.

Chang, Wu., Yu. Tung-Kuang, Wu. ReiHeng Cheng and Shun Chao Chang, 2007. "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks," pp: 538-549.

Mistry, N.H., D.C. Jinwala and M.A. Zaveri, 2009. "MOSAODV: Solution to Secure AODV against Black hole Attack," International Journal of Computer and Network Security (IJCNS), 1(3): 42-45.

Sukla Banerjee, 2008. "Detection/Removal of Cooperative Black and Gray Hole Attack," Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, San Francisco, USA.

Bo Sun, Yong Guan, Jian Chen, W. Udo Pooch, 2003. "Detecting Black-hole Attack in Mobile Ad Hoc Network," The institute of Electrical Engineers. Printed and published by IEEE.

Gunhee Lee, Dong-kyoo Kim and Jungtaek Seo, 2008. "An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks," International Conference on Information Security and Assurance, pp: 220-225.

Rutvij Jhaveri, H., D. Ashish Patel, D. Jatin Parmar and I. Bhavin Shah, 2010. "MANET Routing Protocols and Wormhole Attack against AODV," IJCSNS International Journal of Computer Science and Network Security, 10(4): 12-18.

Lijun Qiana, Ning Songa, Xiangfang Lib, 2007. "Detection of wormhole attacks in multi path routed wireless ad hoc networks: A statistical analysis approach", in the *Proceedings of Journal of Network and Computer Applications*.

Hon Sun Chiu King-Shan Lui, 2006. "DelPHI (2006). Wormhole Detection Mechanism for Ad Hoc Wireless Networks," International Symposium on Wireless Pervasive Computing ISWPC.

Thaier Hayajneh, Prashant Krishnamurthy and David Tipper, 2009. "DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks," Third International Conference on Network and System Security, pp: 73-80.

Khalil, S. Bagchi and N.B. Shroff, 2007. "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks," Computer Networks, 51(13): 3750-3772.

Khalil, 2008. "Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks," Ad Hoc Netw, 6(3): 344-362.

Pirzada and C. McDonald, 2006. "Detecting and evading wormholes in mobile ad-hoc wireless networks," International Journal of Network Security, 3(2): 188-199.

Vijayalakshmi, S. and S. Albert Rabara, 2011. "Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques - LP3 and NAWA2", in the *Proceedings of International Journal of Computer Applications*, (0975 - 8887) Volume 16- No.7.

Shang-Ming, Jen., Chi-Sung Laih and Wen-Chung Kuo, 2009. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", in the *Proceedings of Sensors*, ISSN 1424-8220.

Wassim Znaidi, Marine Minier and Jean-Philippe Babau, 2008. "Detecting Wormhole Attacks in Wireless Networks Using Local Neighborhood Information", in the *Proceedings of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*.

Sun Choi, Doo-young Kim, Do-hyeon Lee and Jae-ilJung, 2008. "Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", in the *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*.

Harleen Dhillon and Q. Hung Ngo, 2005. "CQMP: A Mesh-based Multicast Routing Protocol with Consolidated Query Packets", IEEE Communications Society / WCNC.

Soon, Y.O., J.S. Park and M. Gerla, 2005. "E-ODMRP: Enhanced ODMRP with motion adaptive refresh," in Proc. ISWCS, pp: 130-134.

Latiff, L.A., AAli, chia-ching, Ooi, N. Fisal, 2005. "Location-based Geocasting and Forwarding (LGF) Routing Protocol Mobile Ad Hoc Network," Telecommunications.

Advanced industrial conference on telecommunications/service assurance with partial and intermittent resources conference/e-learning on telecommunications workshop.Aict/sapir/elete2005.(July 2005).Proceedings on 17-20.

Nital Mistry, C. Devesh Jinwala, Member, IAENG, Mukesh Zaveri, 2010. "Improving AODV Protocol against Blackhole Attacks," Proceedings of the International Multi Conference of Engineers And

Computer Scientists 2010 Vol II, IMECS 2010, March 17-19, Hong Kong.

Jorjeta Jetcheva and B. David Johnson, 2001. "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks," In Proceedings of the Second ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp: 33-44.

Perkins, C.E. and E.M. Royer, 1999. Ad hoc on demand Distance Vector routing, mobile computing

systems and applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, pp: 90-100.

Royer, E.M. and C.E. Perkins, 2000. "Multicast ad hoc on demand distance vector (MAODV) routing," Internet-Draft, draft-ietf-draftmaodv-00.txt. IETF MANET Working Group, <http://www.ietf.org>.