ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Enhanced Multipath Approach for Prevention and Elimination of Black Hole Attack in Mobile Ad-Hoc Networks considering the Enhancement of Network Throughput

Maninderpal Singh[*1], Manmohan Sharma[2]
[*1] Assistant Professor, Chandigarh University, Mohali, Punjab, India
[2] Assistant Professor, Lovely Professional University, Phagwara, Punjab, India
mpvirdi@gmail.com

Abstract

Mobile Ad-Hoc Networks are highly dynamic, infrastructure lacking and resource constrained networks. These networks consist of set of nodes which are performing the routing functions and simultaneously acting as hosts. The structure of these networks imposes restrictions on monitoring or employing heavy security checks on the activities of the various participants in the network, which is possible with fixed infrastructure networks. Because of these limitations there are possibilities of security breaches in MANET's. The security concerns come from within the network or from outside. It becomes more challenging task to detect and eliminate when the attack is being executed from inside the network. Black hole attack is one such attack which comes from within the network, where a participant of the network starts misbehaving in terms of packets. Packets supposed to be relayed through the node are not forwarded. It also manipulates the routing process of adaptive routing algorithm like AODV to get itself as most preferred route. If the attacker in black hole attack succeeds in gaining the route, it can intercept the coming and perform eavesdropping, denial-of-service, or man-in-the-middle attacks. The node which is performing the black hole attack shows itself as either having the highest sequence number or it shows that it can provide the shortest path from the source to the destination. Multipath algorithm can be a possible solution to this security attack. If more than one, routes are available from source to destination it is possible to find and identify a misbehaving/attacking node and also report it to the network. In this thesis the problem of black hole attack has been identified and use of multipath algorithm for dealing with it is selected. Further enhancements are done on the multipath approach so as to get better network utilization. We have considered OPNET (Optimized Network Engineering Tools) for our simulations.

Keywords: AODV(Ad-Hoc on demand distance vector), DSN(Destination sequence number), MANET(Mobile Ad-Hoc Network), PMP(Proactive MANET Protocol), RERR(Route Error), RREP(Route Reply), RREQ(Route Request), TTL(Time to live)..

Introduction

A huge value of wireless technology is based upon the principle of direct point-to-point, semi direct system communication. Some of the useful solutions like Global Standard for Mobile communications (GSM) and Wireless Local Area Network (WLAN) both use an approach where mobile nodes communicate directly to each other with some centralized access point device which assists them for energy and communication. This type of network setup has to configure manually or automatically for different operations. In multi-hop scenarios, nodes can communicate by utilizing other nodes as relays for traffic if the endpoint is out of direct communication range.

Mobile ad-hoc networks, MANET [11], use the multi-hop model. These are networks that can be set up randomly and on-demand. They should be self-moving and self-configuring and all nodes can be on move which results in highly dynamic network topology.

Ad-hoc Networks

Centralized networks, such as GSM, don't have capability to be used everywhere in all situations. Some popular examples of these types of networks include establishing survivable monitoring, reliable with efficiency, dynamically adaptive communication for rescue operations in emergency, disaster relief efforts and different type of unique/ non-unique military networks. These types of network scenarios cannot be a centralized and organized connectivity and

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

it can be act as applications of MANETs. The huge chunk of applications for MANETs is widely ranging from small to largely diversify, ranging from small to big, static to dynamic networks that are constrained by very limited power sources, mobility terms comes in scene always, and highly movable or dynamic networks.

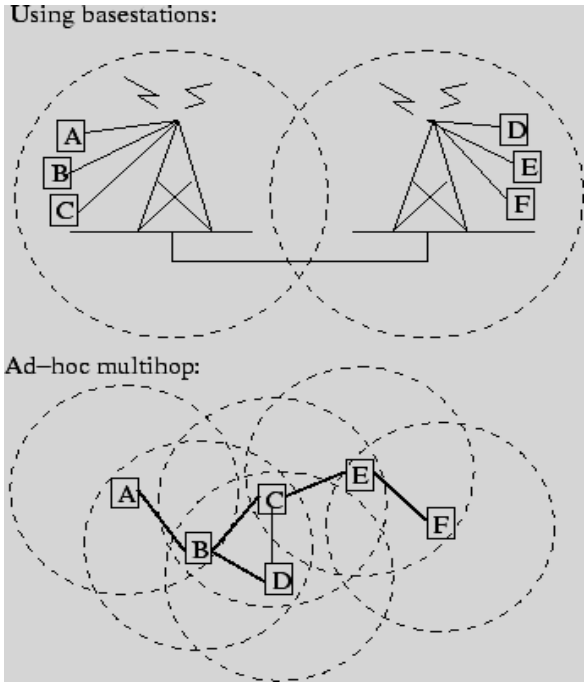

Figure 1: Traditional base station scheme compared to an ad-hoc multi-hop network[19]

To use or enable multi-hop communication in a widely driven and distributed environment, all nodes should be capable of acting as small transferring router/ switch according to demand (see Figure 1). Intermediate path (Routes) has been created and maintained by some routing protocol. MANET routing protocol designed in a complexity of having capability to handle the dynamically changing environment as discussed earlier so that rapidly changing topologies and environments can be covered by these protocols.

For route maintenance one has two main approaches in MANETs, reactive and proactive. Reactive routing protocols create on demand routes which saves huge resources. On the other hand proactive protocols have to maintain whole table of topology in timely dynamic environment.

AODV (Ad hoc On-demand Distance Vector)

AODV is an on demand routing protocol. It provides ease of link failure detection in case of failure of link happens in the network. In case a link failure is noticed then failure notifications are sent to only the affected nodes in the network. This notification cancels all the routes through this affected node. It builds unicast routes from source to destination and that's why the network usage is least. Since the routes are build on demand so the network traffic is minimum. AODV does not allow keeping extra routing which is not in use [27]. If two nodes wish to establish a connection in an ad hoc network then AODV is responsible to enable them to build a multihop route. AODV uses Destination Sequence Numbers (DSN) to avoid counting to infinity that is why it is loop free. This is the characteristic of this algorithm. When a node send request to a destination, it sends its DSNs together with all routing information. It also selects the most favorable route based on the sequence number [8].

There are three AODV messages i.e. Route Request (RREQs), Route Replies (RREPs), and Route Errors (RERRs) [9]. By using UDP (user datagram protocol) packets, the source to destination route is discovered and maintain by these messages. For example the node which request, will use its IP address as Originator IP address for the message for broadcast. It simply means that the AODV not blindly forwarded every message. The number of hops of routing messages in ad hoc network is determined by Time-To-Live (TTL) in the IP header.

When the source node wants to create a new route to the destination, the requesting node broadcast an RREQ message in the network [13]. In the figure 2 the RREQ message is broadcasted from source node A to the destination node B. The RREQ message is shown by the black line from source node A to many directions. The source node A broadcasts the RREQ message in the neighbor nodes. When the neighbor nodes receive the RREQ message it creates a reverse route to the source node A. This neighbor node is the next hop to the source node A. The hop count of the RREQ is incremented by one. The neighbor node will check if it has an active route to the destination or not. If it has a route so it will forward a RREP to the source node A. If it does not have an active route to the destination it will broadcast the RREQ message in the network again with an incremented hop count value. The figure 1.4 shows the procedure for finding the destination node B. The RREQ message is flooded in the network in searching for finding the destination node B. The intermediate nodes can reply to the RREQ message only if they have the destination sequence number (DSN) equal to or greater than the number contained in the packet header of RREQ.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

The intermediate nodes forward the RREQ message to the neighbor nodes and record the address of these nodes in their routing cache. This information will be used to make a reverse path for RREP message from the destination node, it is shown in the below figure 2. The destination node B replies with RREP message denoted by the dotted orange line, the shortest path from destination B to source A. The RREP reached to the originator of the request. This route is only available by unicasting a RREP back to the source. The nodes receiving these messages are cached from originator of the RREQ to all the nodes.

When a link is failed an RERR message is generated. RERR message contains information about nodes that are not reachable. The IP addresses of all the nodes which are as their next hop to the destination.

All the routing information about the network is stored in the table. The routing table has these route entries;

(i) Destinations IP address.
(ii) Destination Sequence Number (DSN).
(iii) Valid Destination Sequence Number flag.
(iv) Other state and routing flags (e.g., valid, invalid, repairable being repaired).
(v) Network interface.
(vi) Hop count (number of hops needed to reach destination).
(vii) Next hop.
(viii) The list of precursors and lifetime (Expiration time of the route).

In AODV routing mechanism, the AODV protocol first broadcasts RREQ packet in order to discover the paths required by a source node to destination node as shown in fig. 3. In response, once the RREQ packet reaches the destination or an intermediate node (any node on the route between the source and destination node) with a fresh enough route to destination node, the destination or intermediate node responds by unicasting a route reply (RREP) packet as shown in Fig. 4.

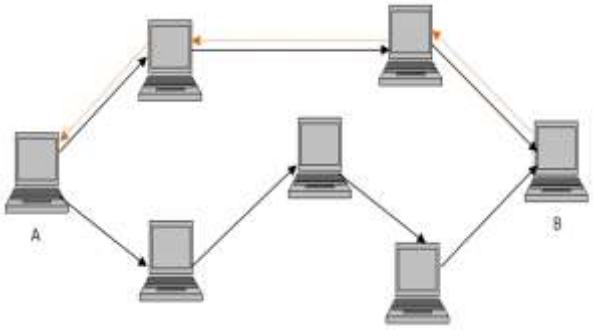

Figure 2: RREQ and RREP messages in MANET using AODV

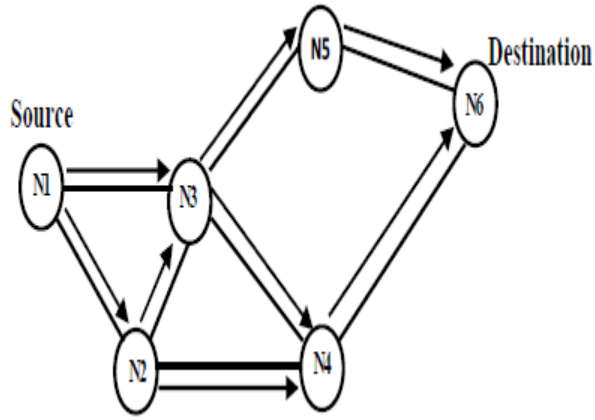

Figure 3: Propagation of route request (RREQ).

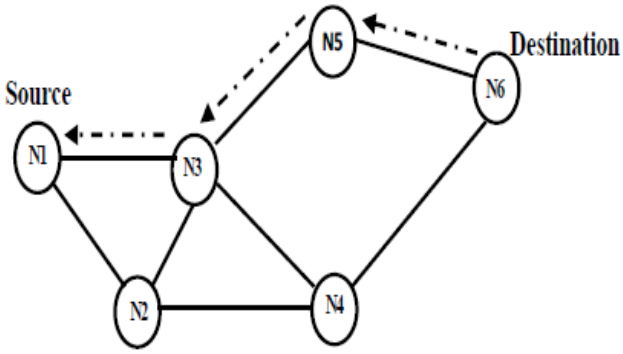

Figure 4: The path of a routing reply (RREP).

Once the source node receives the RREP packet, it starts sending its data packets through the route enclosed within the RREP packet.

Attacks in MANET

Routing Table Overflow:

The attacker node floods the network with bogus route creation packets to fake (non-existing) nodes or simply sends excessive route advertisements to the network [30]. The purpose is to overwhelm the routing-protocol implementations, by creating enough routes to prevent new routes from being created or to overwhelm the protocol implementation.

Routing Table Poisoning Attack:

Different routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks, the attacker node generates and sends fictitious traffic, or mutates legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. Another possibility is to inject a RREQ packet with a high sequence number.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

This causes all other legitimate RREQ packets with lower sequence numbers to be deleted[41] . Routing table poisoning attacks can result in selection of non optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.

Wormhole Attack:

The wormhole attack involves the cooperation between two attacking nodes. One attacker captures routing traffic at one point of the network and tunnels it to another point in the network that shares a private high speed communication link between the attackers, and then selectively injects tunnel traffic back into the network. The two colluding attacker can potentially distort the topology and establish routes under the control over the wormhole link.

Location Disclosure Attack:

In this attack, the privacy requirements of an ad hoc network are compromised. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, and the structure of the network.

Selfish/ Blackmail Attack:

The attack incurs due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

Black Hole Attack

MANET attacks are categorized according to their emission into two main categories: passive attacks, and active attacks. In passive attacks, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information, e.g. an eavesdropping attack. In active attacks, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by causing routing disruption, network resource exhaustion, and node breaking. One of the dangerous active attacks is the BHA(Black hole Attack) . BHA in MANETs is a serious security problem to be solved, in which the attacker injects false routing information in the received routing packets in order to advertise itself as having the best route to the destination. If the attacker in BHA succeeds in gaining the route, it can intercept the coming and perform eavesdropping, denial-of-service, or man-in-the-middle attacks. For example, in fig. 5 node N1 wants to send data packets to node N6 and initiates the route discovery process. It is assumed that node N2 to be an attacker node with no fresh enough route information to the destination node N6. However, node N2 claims directly that it has the route to the destination whenever it receives RREQ packet from node N1 and sends the RREP packet response directly to source node N1. In this case, the node N2 forms a black hole in the network. Node N2can easily misroute the network traffic to itself and cause an attack to the network.

In order to fake AODV using BHA, the attacker may use one of the two methods:

- sending a RREP packet towards the source node with a high enough sequence number.
- sending a RREP packet to the source node with a small enough hop count number.

In most cases, the BHA attacker gains the route if the routing protocol does not protect itself. This is because the BHA attacker does not follow the routing protocol rules by responding directly to the source node. Hence, the BHA attacker replies quicker than the real destination node or any other nodes in the network.

As MANET has dynamic topology, no centralized monitoring and limited physical security so it is more vulnerable to attacks and one of them is Black Hole Attack which in turns made difficult to decrease the overhead for whole network.

Particularly in Protocols like AODV in which overhead is more and if it is attacked by some sort of attack like Worm hole or Black hole. So some solutions are proposed to avoid these types of attacks which include traditional multipath algorithms. Due to large deployment of applications in different specific networks, black hole attacks increased exponentially which produces difficult results to handle.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

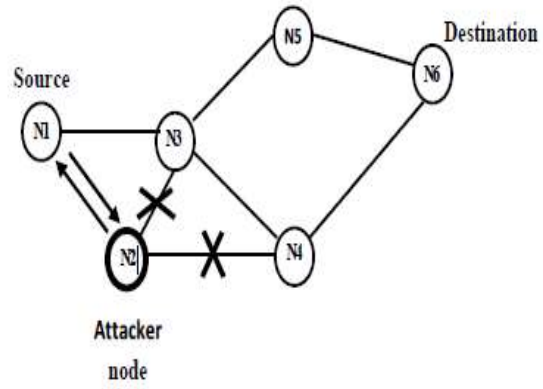

Figure 5: The Black Hole Attack.

Multipath Routing Algorithm:

- In MANET, all the nodes in the networks are equity, and functions as terminal as well router. There is difference in performance instead of function. The main advantage of the structure is that there are multiple paths between source-destination pairs. So it can distribute traffic into multiple paths, decrease congestion and eliminate possible "bottleneck". But MANET with the plane structure will increase routing control overhead; the scalability problem is likely to happen.
- Utilizing clustering algorithm to construct hierarchical topology may be a good method to solve these problems. An adaptive mobile cluster algorithm can sustains the mobility perfectly and maintains the stability and robustness of network architecture.
- To support the multi hop and mobile characteristics of wireless ad hoc network, the rapid deployment of network and dynamic reconstruction after topology changes are effectively implemented by clustering management. Clustering management has five outstanding advantages over other protocols. First, it uses multiple channels effectively and improves system capacity greatly. Second, it reduces the exchange overhead of control messages and strengthens node management. Third, it is very easy to implement the local synchronization of network. Fourth, it provides quality of service (QOS) routing for multimedia services efficiently. Finally, it can support the wireless networks with a large number of nodes.

Literature Survey

E. A .Mary Anita, V. Vasudevan, in 2010 [16] explains the security in wireless ad-hoc networks. They propose a certificate based authentication mechanism to counter the effect of black hole attack. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online centralized authority. The proposed scheme is implemented in two phases: certification phase and authentication phase following the route establishment process of On Demand Multicast Routing Protocol (ODMRP). Simulations show that BHS-ODMRP is as effective as ODMRP in discovering and maintaining routes in addition to providing the required security. They proposed some good explanation and solution to avoid black hole attacks.

Rajpal Singh Khainwar, Mr. Anurag Jain, Mr. Jagdish Prasad Tyagi,in 2011 [2] elaborates the multipath algorithm with performance evaluation and elimination of wormhole attacker node in MANET. They explained that more security is required in comparison to wired network. Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack. The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route with fewer. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. They specifically consider Wormhole attack. Instead of detecting suspicious routes as in previous methods and they implement a new method which detects malicious nodes and works without modification of protocol, using a hop-count and time delay analysis from the user's point of view without any special environment assumptions. The proposed work is simulated using OPNET and results showing the advantages of proposed work.

H. A. Esmaili, M. R. KhaliliShoja, Hosseingharaee, in 2011[20] elaborates that Mobile ad hoc networks (MANETs) are dynamic wireless networks without any infrastructure. These networks are weak against many types of attacks. One of these attacks is the black hole. In this attack, a malicious node advertises itself as having freshest or shortest path to specific node to absorb packets to itself. The effect of black hole attack on ad hoc network using AODV as a routing protocol will be examined in this research. Furthermore, they investigate solution for increasing security in these networks. Simulation results using OPNET simulator depict that packet delivery ratio in the presence of malicious nodes, reduces notably.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Ekta Kamboj, Harish Rohil, in 2011 [18] explains that mobile ad-hoc network which dynamically set up temporary paths between mobile nodes which acts both as router and hosts to send and receive packets. As MANET has dynamic topology, no centralized monitoring and limited physical security so it is more vulnerable to attacks and one of them is Black Hole Attack. This attack can be easily implemented in AODV during the routing discovery process. In the Black Hole attack, a malicious node impersonates as destination node either by showing highest destination sequence number or by advertising itself as having the shortest path to destination node. Once the forged route has been established the malicious node is able to become a member of the active route and intercept all communication packets across that node. An intrusion detection system is introduced to detect Black Hole Attack on AODV in MANET using fuzzy logic. This IDS uses two factors that is forward packet ratio and destination sequence number. These factors are implemented using fuzzy logic in which fidelity level is checked and compared against threshold value and detected whether there is black hole attack or not. The proposed IDS have been tested using NS2.

Dr Karim Konate, Abdourahime Gaye, in 2011 [14] done work dedicated to study attacks and countermeasure in MANET. After a short introduction to what MANETs are and network security they present a survey of various attacks in MANETs pertaining to fail routing protocols. They present the different tools used by these attacks and the mechanisms used by the secured routing protocols to counter them. They also study a mechanism of security, named the reputation, proposed for the MANETs and the protocol which implements it as well as its vulnerabilities. This work ends with a proposal to fend off some of these attacks like Blackhole cooperative, Blackmail, Overflow, Selfish and an implementation of this solution on a compiler of C named Dev.-C++ in order to make comparative tests with the mechanisms already proposed.

Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre[5] in 2012 studied the AODV under Black Hole Attack and Worm Hole attack. They give the overview of various routing mechanisms that are employed in the Ad-Hoc environment. They say that the Black Hole Attacker node takes advantage of the vulnerability of mutual trust during route establishment phase of AODV protocol. Further they say the Black hole Attacker pretends as the best route from a source to destination by showing least hop count or greatest sequence number. They point out that when source gets the first reply and doesn't listen to any other replies leads to the success of Black Hole Attacker. In their work they have proposed a watch dog mechanism which they have proposed to store additional information in tables at all nodes to detect the presence of attacking node. The nodes keep track of the packets they have sent. Another table is used to store the rating of various nodes which acts as a counter measure for the attacking node. They are keeping a check on the packet drop ratio of all nodes, beyond a threshold the node is regarded as a attacking node.

Research Methodology

This research has focused on providing solution for the black hole problem by enhancing multipath algorithm resulting in regaining of the average no. of hops by excluding the attacker nodes. Research has started with building a MANET network in opnet simulator with Random Waypoint mobility Model for providing mobility with AODV as routing protocol as described in figure 5. The parameters for Random Waypoint have been shown in table 1.

Basic parameters like energy carrying capacity, buffer size, speed of nodes, mobility rate and average error rate for AODV have been used. Mobility for all the nodes is random waypoint and the trajectory selected for the nodes movement is Vector.

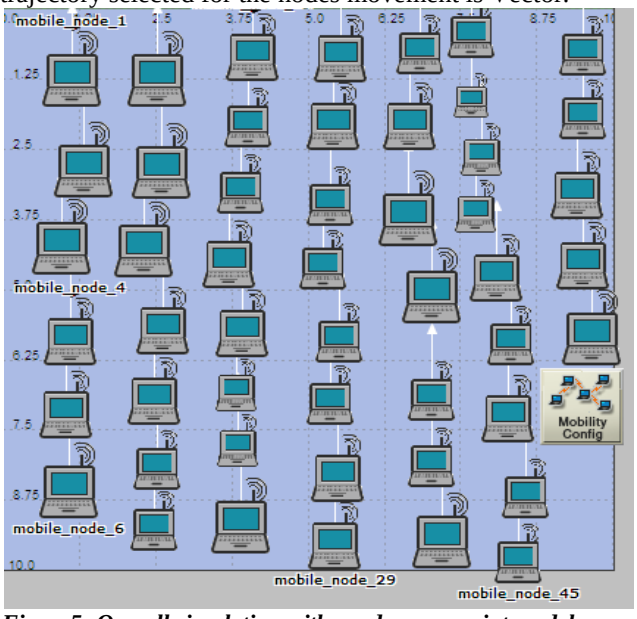

Figure5: Overall simulation with random waypoint model for mobility

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

X_Min (Meters)	0.0
Y_Min (Meters)	0.0
X_Max (Meters)	500
Y_Max(Meters)	500
Speed (meters/second)	Uniform_int(0,10)
Pause Time(Seconds)	Constant(100)
Start Time(Seconds)	Constant(10)

Table 1: Configuration of Random Waypoint model for mobility

After basic building, implementation of blackhole attacks has been implemented by making an attacker transmitter and attacker receiver. Implementation has shown the blackhole attack effects on normal MANET network. Both scenarios have been compared on the bases of parameters like throughput, number of hops, end to end delay and traffic received.

To avoid the blackhole attack, proposed algorithm has been implemented in scenario affected by blackhole attacks and this tried to normalize the scenario to its original state. Proposed algorithm, randomly generate a number in between 0 to maximum number of nodes and make the node with same number as transmitter node as blackhole attack is done by transmitter and receiver so have to decide the transmitter and receiver. Then generate the route from selected transmitting node to any destination node with specified average route length. After this it will send packet according to selected destination and start timer to count hops and delay. By repeating the whole process up to this point will be required as to store routes and their hops and delay. Now for detection of malicious node; if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker. Algorithm checked the delay of all previous routes which involve any on node of the suspicious route. The node not encounter previously should be malicious. Now to find out exact malicious node, there is need to repeat the whole algorithm if more than one node is misbehaving and that will take time and resources. So to avoid this condition, transmitter will be seeking help from directly connected neighbors. Neighbors can tell the history of particular node under suspect. The node which is not involved in any of the previous activity considered to be the malicious node. Malicious nodes have been blacklisted by the nodes and hence they are not involved in future routes**.**

For elimination of the blackhole node, architecture based changes has been done for overtaking the effect of blackhole. The node architecture of normal scenario (Figure 6) and node architecture changes (Figure 7) are given below.

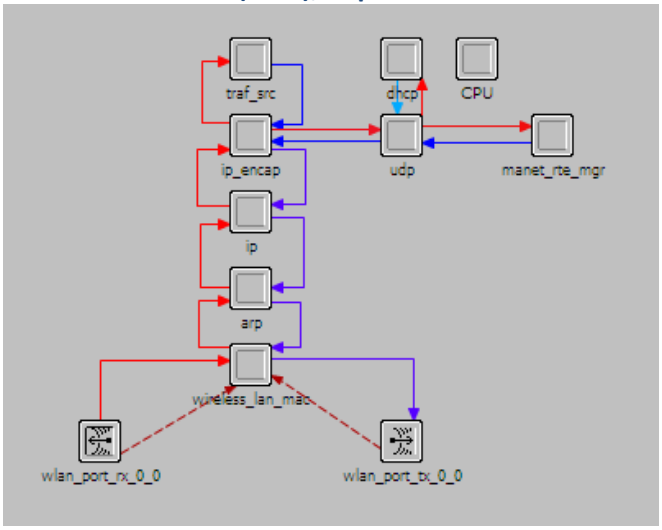

Figure 6: Node Architecture of normal process of AODV

In the above shown normal node architecture the AODV is not making and records for the various routes it has discovered during the route discovery phase. The AODV only stores the best route based on the route reply RREP received from the destination.

This implies that we have the capabilities of multipath approach but we eliminate storage of multiple paths and choose only the best path depending on the destination sequence number and hop count.

Below is the changes architecture of the AODV process for eliminating the blackhole affected network. In the changes we have added four new logs. One log at the IP layer which is storing the routes for the near future transfer between the source and destination nodes. This log as a result is evoking the inbuilt capabilities of the AODV to act as a multipath algorithm. Second log is introduced at the ARP(address resolution protocol) part of the stack, which is storing the routing information about the delay and hop count experienced on various routes from source to destination, enabling us to identify the attacker. Rest two logs are at the MAC layer, one for the transmitter and other for receiver for logging information for every transmission.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

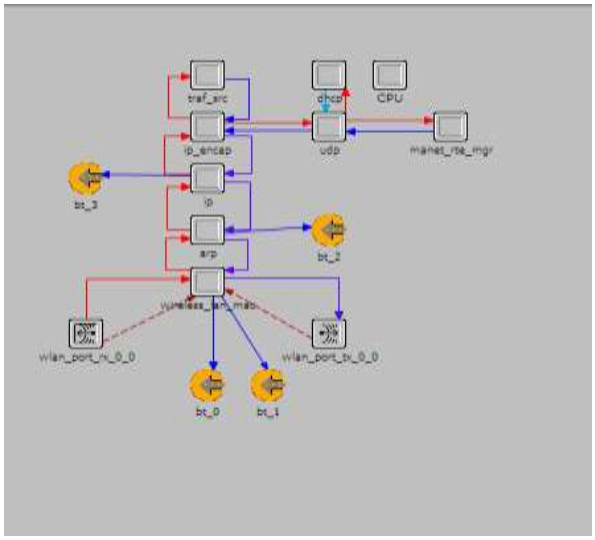

Figure 7: Node Architecture changes done for elimination of Blackhole

Scenarios have shown the improvement after implementation of optimized multipath algorithm by providing the improved results which further compared with previous scenario (normal network and scenario with blackhole attack). Finally this research has shown the improvement done by proposed algorithms in graphs with respect to throughput of the network.

Results

The simulation duration for all three scenarios taken is 15 minutes each.

After all consecutive simulation runs, simulation results were collected network throughput which is discussed for performance of network.

The network topologies used for experimentation are Normal AODV (Figure 8), AODV under blackhole attack (Figure 9), AODV with elimination of blackhole attack (Figure 10). To choose best method for elimination of attacks, blackhole attack has been considered as it is the most occurring attack in Ad-hoc on demand protocols.

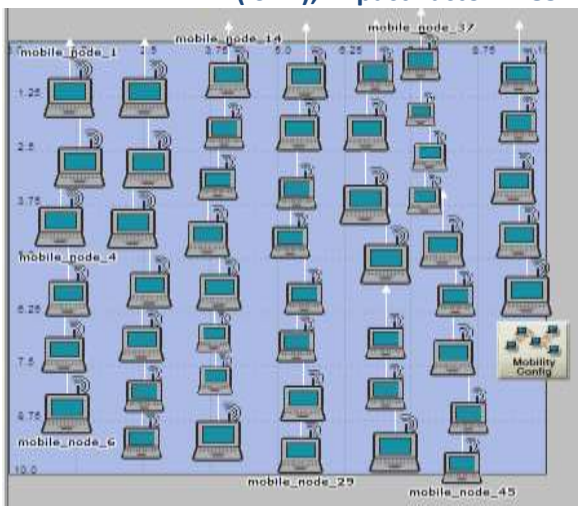

Figure 8: Simulation of Normal AODV

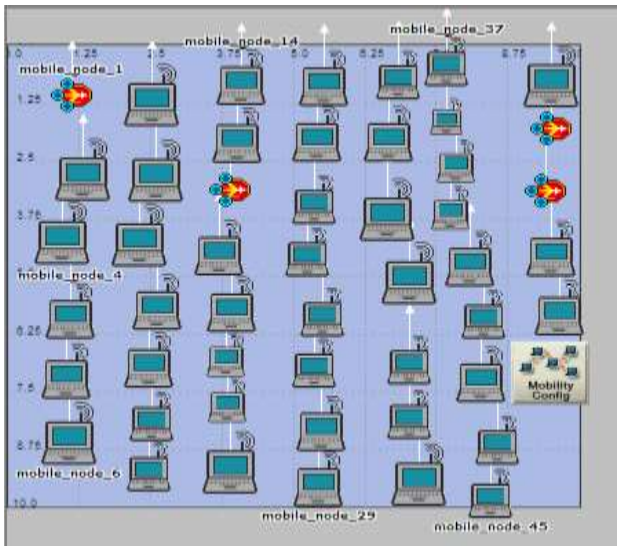

Figure 9: Simulation of AODV under blackhole attack

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

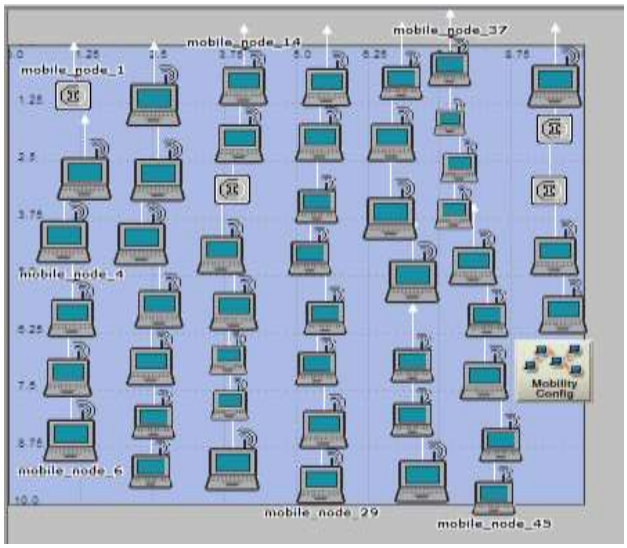

Figure 10: Simulation of AODV with elimination of blackhole attack

Performance of AODV with Throughput of three Scenarios

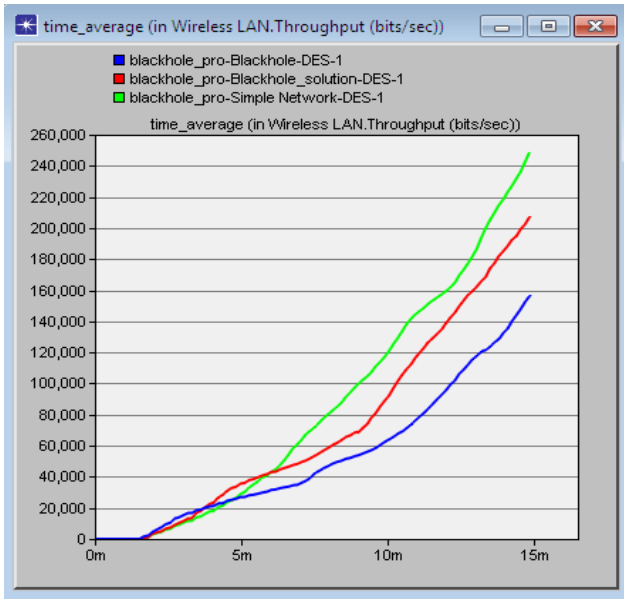

Figure 11: Throughput (bits/sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 11) and it show that the blue line of the throughput for normal AODV scenario. Red line shows the decrease in the throughput in case of blackhole attack scenario. Orange line shows the normalization process of the network as in case of elimination of blackhole throughput gradually increase and tends towards the normal throughput. It is clear from the graph that elimination of blackhole provides great results.

Summary

The overall simulation performance is presented in nutshell in the following table, which indicates that the elimination of blackhole attack scenario provides the better results and try to normalize the blackhole effected network to its normal state as close as possible.

Attributes	Simulation Time (sec)	Normal Scenario	Blackhole Scenario	Elimination Scenario
Throughput (bits/sec)	900	250000	139000	210000

Conclusions

In this work, the performance of the Ad-hoc on demand distance vector routing protocol has been summarized. The main focus was to show the performance of AODV under normal environment, under blackhole attack and performance after elimination of blackhole attack in term of throughput. These malicious nodes provide false information to the network and AODV consider the path defined by malicious nodes as best routing path available and start communication through it. Performance of network decreases after blackhole attack and to eliminate of this attack, multipath approach of AODV protocol has been implemented by introducing logging modules on medium access layer which use to monitor average metric value used by network while communication. It maintains an average value for delay and number of hops. After implementation of this module, it finds the malicious nodes because the metric values of malicious nodes are very less as compare to normal metric value. A summary of suspected nodes has been forwarded to the upper layer where another module has been added to find the sequence of attack. If any sequence found, it is sent to network layer where another module is added to find the solution for attacks. Module use to evoke the multipath properly of AODV process and hence eliminate the nodes by introducing the query messages to the neighbors and find the exact malicious nodes. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes.

In nutshell, elimination of blackhole attack has been done so that ad-hoc communication can be normalized as normal communication.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Refrences

[1] *A.Iwata, C.C.Chiang, G.Pei, M.Gerla and T.W.Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1369-1379, August 1999*

[2] *A.Shevtekar, K.Anantharam, and N.Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., vol. 9, no. 4, pp. 363–65, April 2005.*

[3] *A.Weimerskirch and G.Thonet, "Distributed Light-Weight Authentication Model for Ad-hoc Networks," Lecture Notes In Computer Science; Vol. 2288, pp. 341 354, 2001*

[4] *Akanksha Saini, Harish Kumar, "Efect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCSt Vol. 1, ISSue 2, deCember 2010.*

[5] *Amol A. Bhosle, Tushar P. Thosar and SnehalMehatre," Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012.*

[6] *B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007*

[7] *B.Wu, J.Chen, J.Wu, and M.Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006*

[8] *C.C.Chiang, H.K.Wu, W.Liu and M.Gerla, "Routing in Clustered Multi Hop Mobile Wireless Networks with Fading Channel," Proceedings of IEEE SICON 1997, pp. 197-211, April 1997*

[9] *C.E.Perkins and E.M.Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, pp. 90-100, February 1999*

[10] *C.E.Perkins and P.Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) For Mobile Computers," Proceedings of ACM SIGCOMM 1994, pp. 233-244, August 1994*

[11] *C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.*

[12] *D. Wang, M. Hu, H. Zhi, "A Survey of Secure Routing in Ad Hoc Networks," IEEE Ninth International Conference on Web-Age Information Management, 2008, (WAIM '08), pp.482-486, July 2008*

[13] *D.B.Jhonson and D.A.Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, Kluwer Academic Publishers, vol.353, pp. 153-181, 1996*

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

[15] *E. Ahmed, K. Samad, W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks," AusCERT2006 R&D Stream Program, Information Technology Security Conference, May 2006*

[16] *E.A .Mary Anita, V. Vasudevan,"Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining", 2010 International Journal of Computer Applications (0975 – 8887, Volume 1 – No. 12).*

[17] *Ekta Barkhodia, Parulpreet Singh, Gurleen Kaur Walia, "Performance Analysis of AODV using HTTP traffic under Black Hole Attack in MANET", Computer Science & Engineering: An International Journal (CSEIJ), Vol.2, No.3, June 2012*

[18] *EktaKamboj, Harish Rohil," Detection of Black Hole Attack on AODV in MANET Using Fuzzy Logic", Journal of Current Computer Science and Technology Vol. 1 Issue 6, pp.316-318, 2011.*

[19] *George Aggelou, Mobile Ad Hoc Networks, McGraw-Hill, 2004*

[20] *H. A. Esmaili, M. R. KhaliliShoja, Hosseingharaee,"Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 2, 49-52, 2011.*

[21] *Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004*

[22] *I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Rrotocol", IETF Internet Draft, v.15, November 2008, (Work in Progress

[23] I.Chlamtac, M.Conti, and J.Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, vol. 1, no. 1, pp. 13-64, 2003

[24] J.P.Hubaux, L.Buttyan, S.Capkun, "The Quest For Security In Mobile Ad Hoc Networks," Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), October, 2001

[25] K.Sanzgiri, D.LaFlamme, B.Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer, "Authenticated Routing for Ad Hoc Networks," Proceedings of IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005

[26] M.G.Zapata and N.Asokan, "Securing Ad-Hoc Routing Protocols," Proceedings of ACM Workshop on Wireless Security, pp. 1–10, September 2002

[27] M.Gerla, X.Hong, L.Ma and G.Pei, "Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks", IETF Internet Draft, v.5, November 2002

[28] M.Joa-Ng and I.T.Lu, "A Peer -to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1415-1425, August 1999.

[29] MahaAbdelhaq, Sami Serhan, RaedAlsaqour and Anton Satria," Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol", Australian Journal of Basic and Applied Sciences, 5(10): 1137-1145, 2011

[30] P.Sinha, R.Sivakumar and V.Bharghavan, "CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm," IEEE Journal on Selected Areas in Communications, vol.17, no.8, pp. 1454-1466, August 1999

[31] R. Ogier, F. Templin, M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", IETF Internet Draft, v.11, October 2003

[32] Rajiv Ranjan, Naresh Trivedi and Anoop Srivastava, "Mitigating of Black Hole Attack in Manets", VSRD-IJCSIT, Vol. 1 (2), 2011, 53-57.

[33] Rajpal Singh Khainwar, Mr. Anurag Jain, Mr. Jagdish Prasad Tyagi,"ELimination of Wormhole Attacker node in MANET using performance evaluation multipath algorithm", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459,Volume 1, Issue 2, December 2011).

[34] SudhirAgrawal, Sanjeev Jain, SanjeevSharm," A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal Of Computing, Volume 3, Issue 1, January 2011.

[35] T.R.Andel and A.Yasinsac, "The Invisible Node Attack Revisited," Proceedings of IEEE SoutheastCon 2007, pp. 686 – 691, March 2007

[36] V.D.Park and M.S.Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Ad Hoc Networks," Proceedings of IEEE INFOCOM 1997, pp. 1405-1413, April 1997

[37] X.Lin, R.Lu, H.Zhu, P.H.Ho, X.Shen and Z.Cao, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," IEEE International Conference on Communications, ICC '07, pp. 1247 – 1253, June 2007

[38] Y.C.Hu and A.Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy, vol. 2(3), pp. 28-39, May 2004

[39] Y.C.Hu, A.Perrig, and D.B.Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom'02, Atlanta, GA, pp. 12-13 September 2002

[40] Y.C.Hu, D.B.Johnson and A.Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, pp. 3-13. June 2002.

[41] Z.J.Haas, "The Routing Algorithm for the Reconfigurable Wireless Networks," Proceedings of ICUPC 1997, vol. 2,pp. 562-566, October 1997.