Optimized Monitoring Scheme for prevention of Black hole attack in Mobile Ad-hoc Network

POOJA GOYAL[1], Mrs. SUKHJINDER KAUR [2]

[1] Research Scholar, Sri Sukhmani Institute Of Engineering and Technology, Dera Bassi.,

[2] Assistant Professor, Dept of ECE, Sri Sukhmani Institute Of Engineering and Technology, Dera Bassi.,

ABSTRACT:

Mobile Ad-hoc Network is type of network in which devices work independently in a collective manner to fulfill a common task. Due to limited energy carrying property of the mobile ad-hoc nodes, many attacks always seeks to breach into the network. Especially in case of on demand routing, vulnerabilities increases due to nature of routing. Ad-hoc On Demand Distance Vector Routing protocol is one of the most implemented and used protocol for on demand routing. Attacks such as blackhole and phising are most occurring attacks in the AODV due to nature of routing. Blackhole is most occurred network attack in AODV. This attack starts proceeding by introducing the similar metrics which are taken into account by AODV while selecting the route for destination. It introduce lower number of hops and lower value of delay so that AODV will select the fake route defined by attack automatically and after attack launch, attack start decreasing the overall throughput of the network. Blackhole use short coming of routing process and can be implemented easily while routing process of AODV. In this research, focus is on eliminating the blackhole attack effect from AODV network and to have performance analysis of the network affected by blackhole. To accomplish this, a packet update scheme has been used to eliminate the affects of the blackhole from AODV process. While using packet update scheme, a new concept based on neighbor searching has been used in which AODV use the information from the neighbor nodes (node architecture has been modified to initiate the affect of algorithm) to find the malicious nodes. Proposed scheme eliminate the blackhole affects by finding all the malicious nodes which are present in the network and send broadcast to whole network so that blackhole detected nodes can never be part of routing in future routing process. The performance of the network has been judged on the bases of Number of Hops, Delay, Traffic Received and Throughput. The simulation is carried in OPNET Modeler 14.5 simulator.

Keywords: Blackhole Attack, AODV, Multipath Algorithm, On Demand Routing Protocols, Route Request, Route Reply, Mobile Ad-hoc Network,.

1. AODV (Ad hoc On-demand Distance Vector)

AODV is an on-demand routing protocol [2]. The AODV algorithm gives an easy way to get change in the link situation. [3] If link failure occurred than notifications are sent only to the affected nodes within range in the network. Generally after receiving this notification, it cancels almost all the routes through this affected node. [7]

Generally maintenance of AODV process is based on timely updates which suggest that entries into AODV process expired after timer expires. Further updated information is passed to the neighbors so that it can be updated about route breakage. Discovery of various routes from single source to various destinations is totally based on query and reply packets and intermediate nodes use logs to store the information of routes in route table. Various control messages which are used for the discovery and corrupted routes are as follows: [7] Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR), HELLO Messages. [7]

Route Request (RREQ)

Various route request packet are flooded through the network when a route is not available for the destination from source. [3][4][5]

Pair source address and request ID identify RREQ and counter is incremented every time source node sends a new RREQ. [5][6] After receiving of request message, each node checks the request ID and source address pair. The new RREQ is discarded if there is already RREQ packet with same pair of parameters. [8]

Node with no routes information to particularly destination or any destination will be discarded and information is broadcasted to update information to other routes. [9]

A route reply (RREP) message is generated and sent back to source if a node has route with sequence number greater than or equal to that of RREQ.

Route Reply (RREP)

On having a valid route to the destination or if the node is destination, a RREP message is sent to the source by the node. [10]

Route Error Message (RERR)

The neighborhood nodes are monitored. When a route that is active is lost, the neighborhood nodes are notified by route error message (RERR) on both sides of link. [6]

2. BLACKHOLE 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 . 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.1 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 .

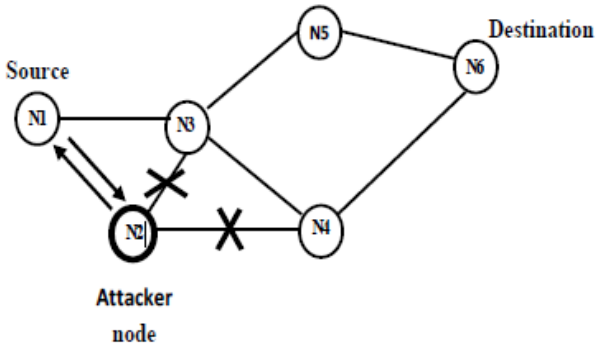

Figure 1: The Black Hole Attack.

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 Black hole. So some solutions are proposed to avoid these types of attacks which include updates from neighbors. Due to large deployment of applications in different specific networks, black hole attacks increased exponentially which produces difficult results to hand. [12]

3. PROBLEM DEFINITION

MANET is a 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. In Black hole attack a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise it as having the shortest path to the node whose packets it wants to intercept [1]. 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.

4. METHODOLOGY

This research has focused on providing solution for said problem by enhancing multipath algorithm resulting in regaining of the average no. of hops as well to get normal delay by excluding the attacker nodes.

This research has focused on the multipath algorithm to avoid the blackhole attack in MANETs.

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 2 below.

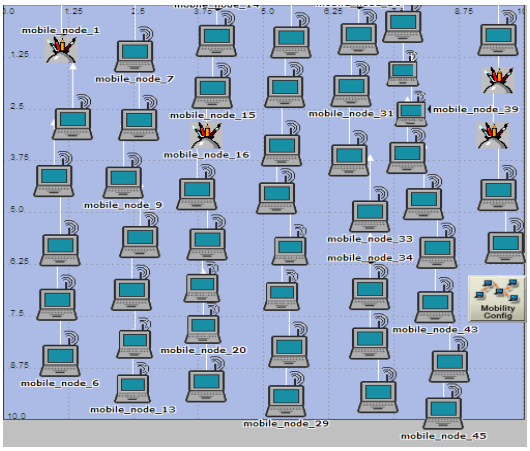

Figure 2: Overall simulation with random waypoint model for mobility.

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.

The steps of Proposed Algorithm are as follows:

BlackHole (S,D)

/* S is the source node and D represents the Destination Node over the network*/
{
Step 1: Whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes. RREQ packet contains destination address and sequence number along with source address. Sequence number provides the freshness of route. Once an RREQ packet is received by an intermediate node and verifies destination address. If the destination address not matches with the RREQ packet then forwards it to its next hop. This process is repeated until it reaches the final destination.
Step 2: While receiving the RREQ packet each node update their routing table. Once the destination node receives RREQ message from neighboring nodes, it then unicast the RREP (route_reply) back to the source node.
Step 3: As transmission begin it will search for all the intermediate nodes called Neighbor List.
Step 4: If number of packet drop is large then start discovery of malfunctioning nodes.
Step 5: Source and destination will be decided. Randomly Generate a Number in between 0 to maximum number of nodes. Initiate a source by making transmitter node same selected.
Step 6: Generate the Route from selected transmitting node to any destination node with specified average route length.
Send packet to destination
{
Start timer (Record (Hop Count, Delay))
Counter (Threshold (Hop Count, Delay))
{
Store (Route, Hop Count, Delay)
Continue the process
}
Step 7: Blackhole Detection
{
Hop count <Threshold
Then Check Delay
}
Step 8: Malicious Node Selection
N is the number of nodes.
{
If N = 1
Then it is the attacker
Else
Send Route Query to neighbors
{
If neighbor detect similar malfunctioning
Then mark it malicious.
Else
{
Repeat process
}
Step 9: Send black_annoucement message to all nodes. Any node receives black_annoucement message it removes blackhole node id from its neighbor table and Routing Table. If any forwarding node receives black_announcement message it will send RERR message to source. It will reinitiate route discovery process, and find the new path to the destination without blackhole node.
Step 10: End..

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 3) and node architecture changes (Figure 4) are given below.

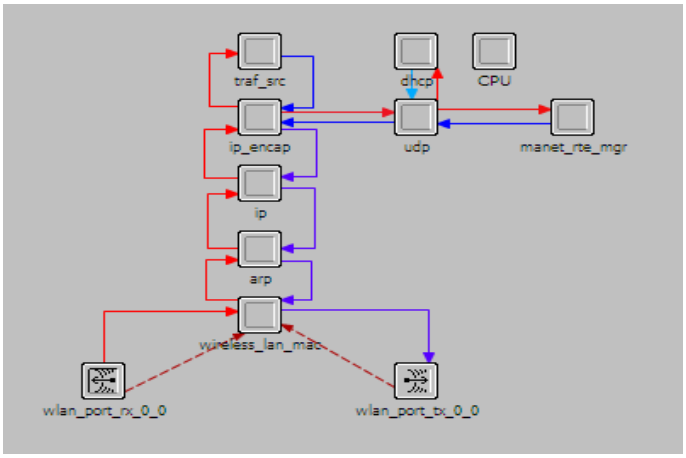

Figure 3: Node Architecture of normal process of AODV

Below is the changes architecture of the AODV process for eliminating the blackhole affected network.

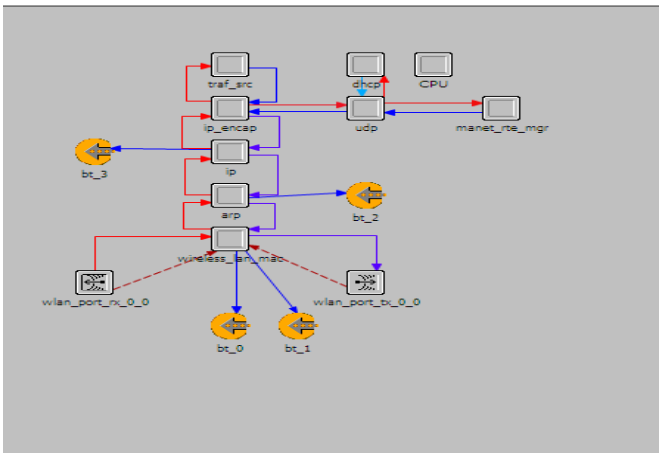

Figure 4: Node Architecture changes done for elimination of Blackhole

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.

Module evokes the multipath properly of AODV process and hence eliminates the nodes by introducing the query messages to the neighbors and finds the exact malicious nodes. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes.

5. EXPERIMENTATION

Basic parameters used for experimentation. Some of the experimentation done for checking the behavior of AODV protocol under blackhole attacks are given below:

Parameters	Value
Simulator	OPNET
Simulation Time	900
No of nodes	50
Routing Protocol	AODV
Traffic Model	CBR
Pause Time	100 sec
Speed	11 mps

Results obtained for normal performance of AODV, Performance of AODV under blackhole attacks and performance behavior of AODV with elimination of blackhole attacks in term of throughput, delay, number of hops and Traffic Received in AODV network is discussed in the following sections.

Performance of AODV with Throughput of three Scenarios

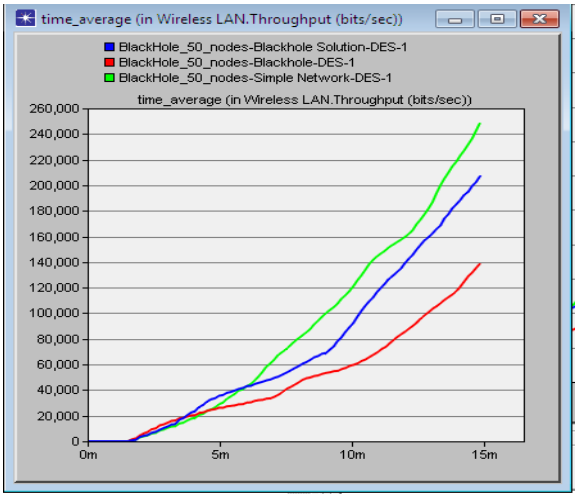

Figure 5: Throughput (bits/sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 5) 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.

Performance of AODV with Traffic Received of three Scenarios

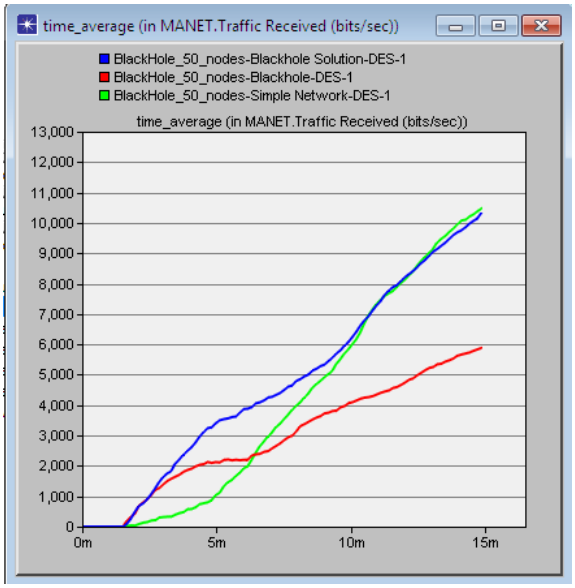

Figure 6: Traffic Received (bits/sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 6) and it show that the blackhole scenario

decreases the traffic received by the normal process of the AODV and blackhole elimination scenario normalized the traffic received similar to the state of traffic received by the normal AODV process.

Performance of AODV with Delay of three Scenarios

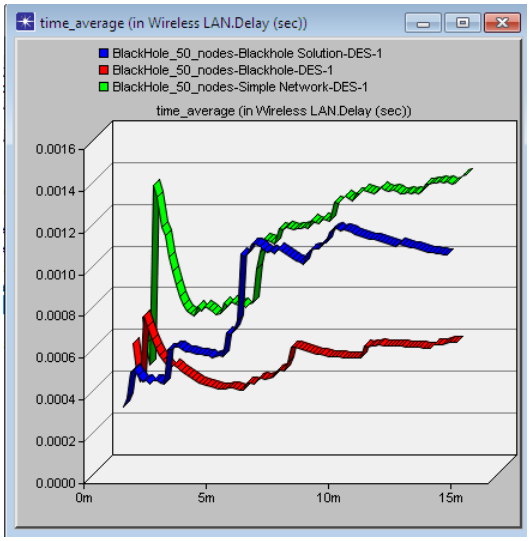

Figure 7: Delay (sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 7) and it show that the blue line shows` the delay of the normal network and red line shows the decrease in the delay which is in case of blackhole attack as in blackhole attack delay introduced by attacker is always low as compared to normal network. Orange line shows the delay normalization process with elimination of blackhole in third scenario.

Performance of AODV with Number of Hops of three Scenarios

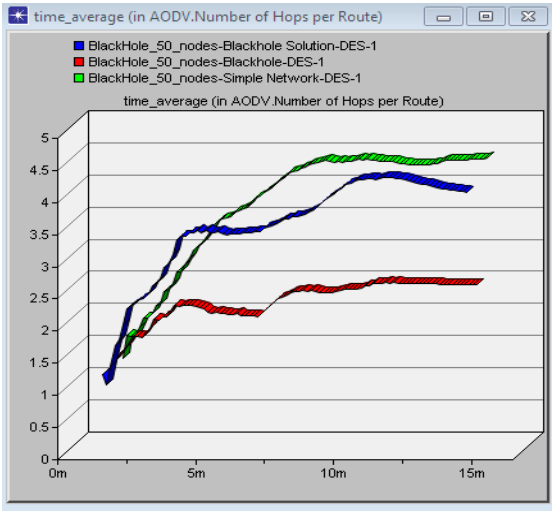

Figure 8: Number of hops per route comparison of all three scenarios

The performance of network is compared in above figure (Figure 8) and Red line shows the blackhole case which use to fake the hops count as lower than normal so that AODV would send data by considering lowest hops count as best path. Blue line shows the number of hops per route of normal AODV scenario and normalized value of hop count shown in orange line in elimination of blackhole scenario.

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.

6. CONCLUSION

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, number of hops per route, delay and traffic received. In doing so, a blackhole scenario has been created and four blackhole attacker nodes have been generated. 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.

It is an important issue for the further study to implement the proposed scheme on the distributed environment of wireless ad-hoc devices. The proposed work need strong testing in scenario where energy saving is a big concern. Moreover implementation of clustering approaches with proposed scheme can be consider providing security with resources saving in the wireless Ad-hoc networks.

REFERENCES

[1] 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.

[2] George Aggelou, Mobile Ad Hoc Networks, McGraw-Hill, 2004.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] T.H.Clausen, G.Hansen, L.Christensen, and G.Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation," Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001, September 2001.

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

[9] 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.

[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] 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.

[12] 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.

[13] 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.

[14] 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..

[15] 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.

[16] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing Rrotocol", IETF Internet Draft, v.15, November 2008, (Work in Progress).