Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Packet Update Scheme for Prevention of Blackhole Attack in MANETs

Ritu Sharma[1,]
[1] Research Scholar,
Department of Electronics & Communication,
CGC, Landran, India

Chanpreet Kaur[2]
[2] Assistant Professor,
Department of Electronics & Communication,
CGC, Landran, India

Abstract— Communication has different terms for different users in the technology. Wireless and Ad-hoc communication are two main communication medium which are fulfilling different domain requirement for the users. Talking about Ad-hoc networks, usually communication is based on the ad-hoc protocol policies. Most of the users in allover ad-hoc network using Ad-hoc On Demand Distance Vector Protocol (AODV) for the basic communication due to simplicity and reliability of protocol. More usage also attracts number of attackers which tends to disturb the communication. Most occurred attack in AODV network is Black-hole attack which provide lowest destination id to the source so t become the part of shortest selected path by AODV process. 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 attack affects the network performance and overall network performance degraded a lot. To eliminate the effects of blackhole attack, we have proposed a packet update scheme in which we fetch information from the neighbors for the enquiry of the suspected nodes in the network. Proposed scheme eliminate the blackhole affects by finding all the malicious nodes which are present in the network and send broadcast to whole network for elimination of malicious nodes. Throughput and delay are the parameters for the performance measurements of the network. Proposed scheme provides better results with 37 % less delay as compared to the previous proposed schemes. Previous scheme provides slighter better results of 6% more throughput than our proposed scheme.

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

I. Introduction

A MANET consists of mobile nodes, a router with multiple hosts and wireless communication devices. The wireless communication devices are transmitters, receivers and smart antennas. Mobile Ad hoc Network (MANET) [1] is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed. MANET is the quick remedy for any disaster situation. MANET is a spontaneous network. It is useful when dealing with wireless devices in which some of the devices are part of the network only for the duration of a communication session [2]

II. Blachole Attack

The black hole attack[5] is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to announce itself as having a accurate route to a destination node, even though the route is counterfeit, with the intention of intercepting packets.

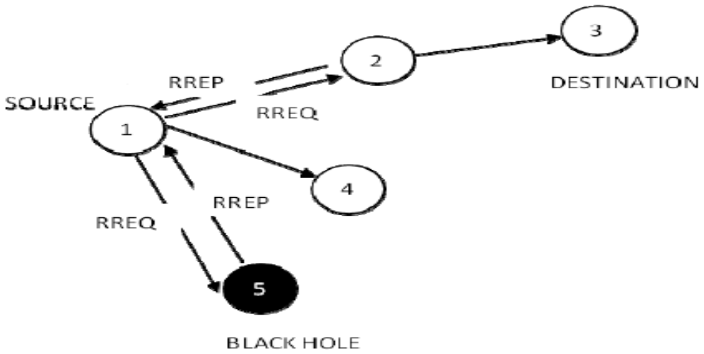

Figure 1: Blackhole attacker in the normal network

In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have a fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node instatly responds with an RREP message that contains the highest sequence number and this message is received as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source considers that the destination is behind the black hole and rejects the other RREP packets coming from other nodes. The source then starts to transmit out its data packets to the black hole believing that these packets will reach the destination. The basic attack demonstration is shown in figure 1.

Vulnerabilities of ad-hoc networks against black hole attacks have solution based on modification of the AODV protocol.

III. 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. 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. Our research has focused on providing solution for this problem by enhancing packet update scheme. This scheme has been used to limit the effects of blackhole in mobile ad-hoc network by providing information from neighbors.

IV. PROPOSED ALGORITHM

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.

```
/* S is the source node and D represents the Destination Node over the network*/
{
State 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.
State 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.
State 3: As transmission begin it will search for all the intermediate nodes called Neighbor List.
State 4: If number of packet drop is large then start discovery of malfunctioning nodes.
State 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.
State 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
}
State 7: Blackhole Detection
{
```

```
Hop count <Threshold
Then Check Delay
}
State 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
}
```

State: 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.

State 10: End.

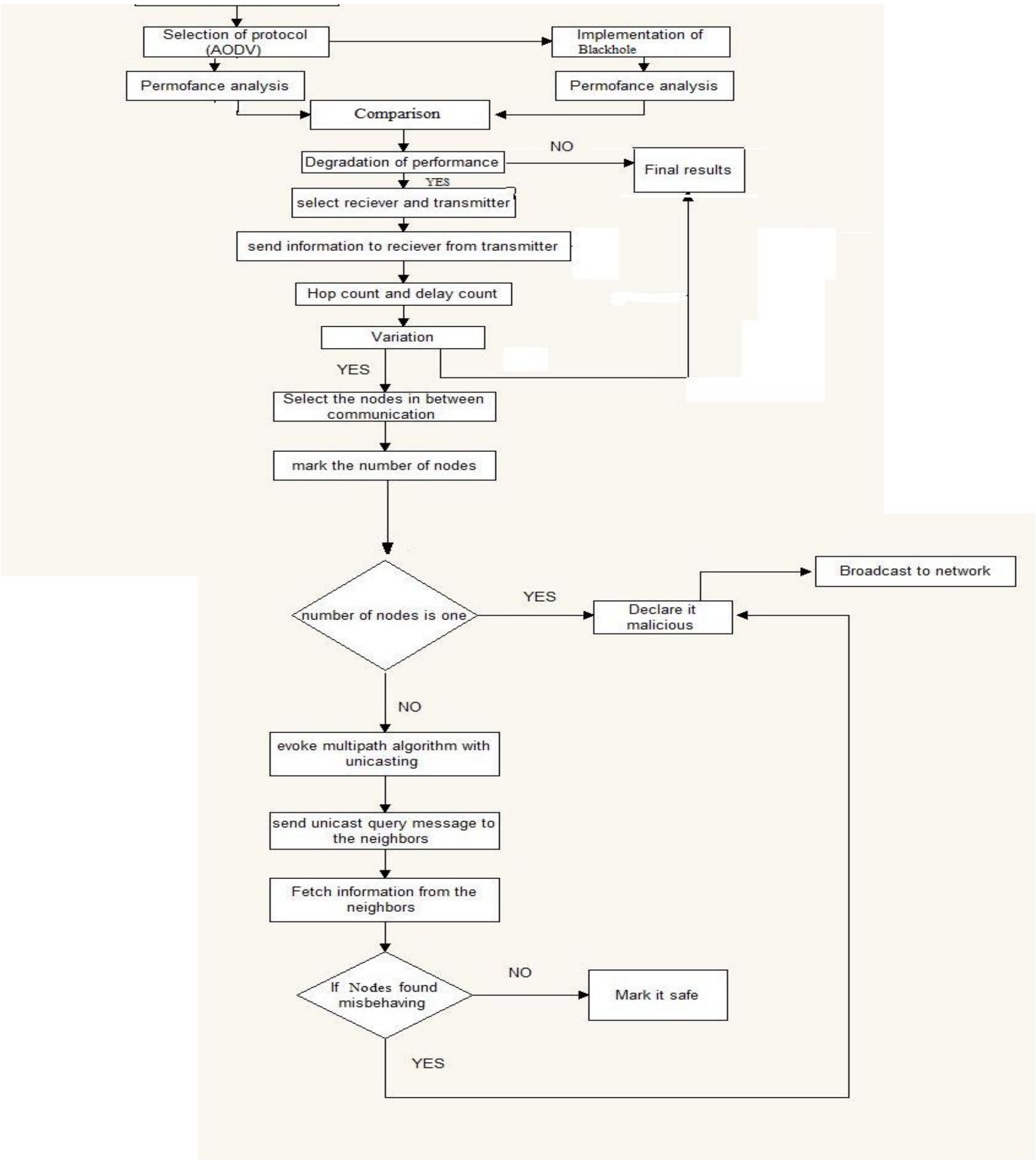
Selection of protocol (AODV)
Implementation of Blackhole
Permofance analysis
Permofance analysis
Comparison
Degradation of performance
NO
Final results
YES
select reciever and transmitter
send information to reciever from transmitter
Hop count and delay count
Variation
YES
Select the nodes in between communication
mark the number of nodes
Broadcast to network
number of nodes is one
YES
Declare it malicious
NO
evoke multipath algorithm with unicasting
send unicast query message to the neighbors
Fetch information from the neighbors
If Nodes found misbehaving
NO
Mark it safe
YES

Figure 2: Proposed Algorithm Overview

V. EXPERIMENTAION

Basic parameters used for experimentation with OPNET simulator. Area for communication is 1500 × 1500 meters with 50 mobile nodes.

The performance comparison of three scenarios in term of throughput is explained in figure 3.

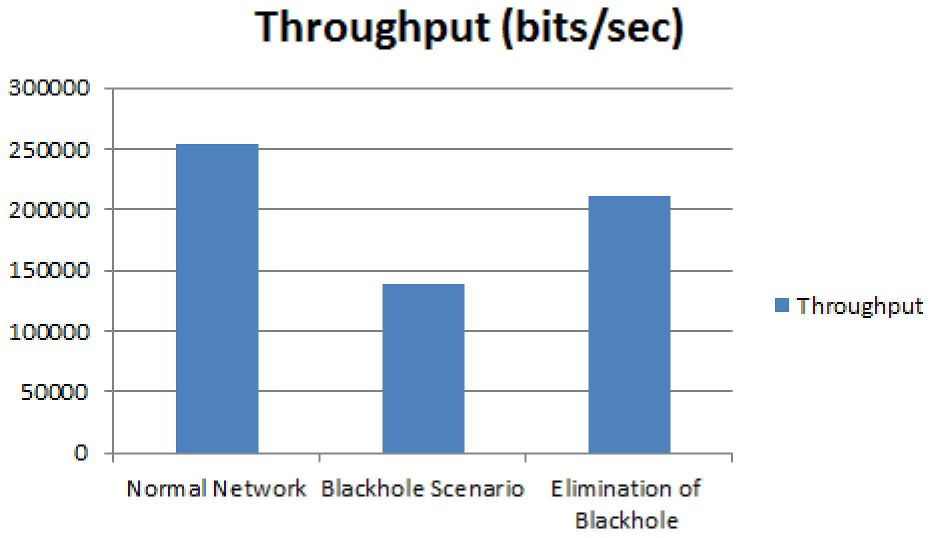

Figure 3: Throughput variation for three scenarios

The performance comparison of three scenarios in term of delay is explained in figure 4.

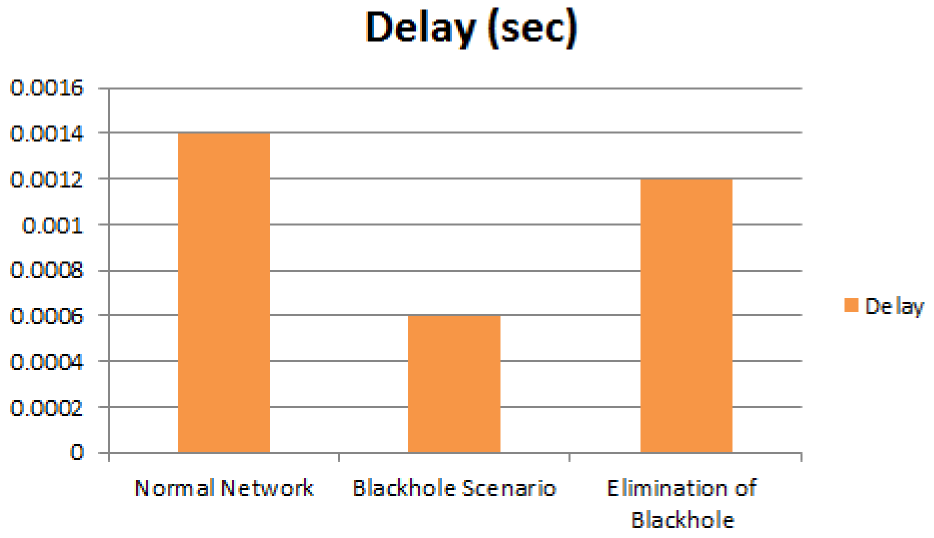

Figure 4: Delay variation for three scenarios

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

Table .1: Result Summary with various parameters

Attributes	Simulation Time (sec)	Normal Scenario	Blackhole Scenario	Elimination Scenario
Throughput (bits/sec)	900	250000	139000	210000
Delay (sec)	900	0.0014	0.0006	0.0012
Packets Sent	900	47	47	47
Packet Received	900	16	8	13

The Throughput represents the packets travels from source to destination. In first scenario of our experimentation, packets travels are shown as throughput with peak value of approx. 248553 and it is represented as bits per second. In second scenario which is with blackhole attack, packets drops which are represented as throughput, decreases to value of approx. 138933 bits per second. This drop of packets in form of throughput is due to the blackhole effect as in case of blackhole packet drop increases as explained in this s scenario with throughput decrease. The recovery of the throughput takes place with proposed mechanism by elimination of the blackhole attack as throughput comes to similar to the normal scenario. Similiarly delay decreases due to the blackhole introduction into the second scenario due to the property of blackhole scenario as in blackhole attack, delay is low so in our experimentation delay is low and with solution of blackhole delay comes to normal.

The validation of the proposed work has been done by comparing it to the results based on similar research done previously [1]. In previous study, blackhole elimination has been done on the bases of prominent mode algorithm but concept used broadcasting which used huge resources. In this research, unicasting process has been used instead of broadcasting which can save resources and provided useful better results. In previous study similar parameters have been used and it shows that throughput reduces by 54% approx. In this research, the total reduction in throughput is 34% approx. Total recovery of throughput is shown is 48% to 49% approx. in previous study and in case of this research it is 24%. In case of delay in previous case, reduction of delay is 45% and it goes on higher side with value equal to 62%. In this research, reduction is 47% and it goes to value of 35%. The results clearly suggest the good recovery around 18% more than the previous results as delay is 27% less with proposed work.
The results are summarized in below table (Table 2).

Table.2: Results comparison of proposed work with previous work.

Scenario	Decrease in Throughput	Rise of Throughput	Decrease Percentage in Delay	Rise Percentage in Delay
Previous Work[1]	54%	48%	45%	62%
Proposed Work	38%	24%	47%	35%

VI. 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. The performance of the network with attack in term of throughput decreases around 51% and with our proposed solution, we have recovered around 49% in throughput. The performance of the network with attack in term of delay decreases around 54% and with our proposed solution, we have recovered around 45% in delay. 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, we have used neighbor updates scheme in prominent scheme. Normally with various attacks communication suffers a lot as mobile devices only have limited range for communication so attacks can be act as bottleneck in the communication of nodes which inturns could delayed the services provided by overall network. In this research we tried to prevent the blackhole effects in ad-hoc on demand distance vector protocol communication in mobile ad-hoc networks. Concept has shown improved results after elimination of the black-hole attack in the simulation. Elimination of malicious nodes takes place on Network layer by broadcasting the information of malicious nodes.

Overall, elimination of blackhole attack has been done so that ad-hoc communication can be normalized as normal communication. It will be very useful in saving a lot of resources for mobile ad-hoc communication as we have used unicasting process instead of broadcasting which saves resources as malicious nodes are only detected through partial multicasting process.

.

References

[1] Pramod Kumar Singh, Govind Sharma," An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[2] 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.

[3] Pravin Ghosekar, "Mobile ad hoc networking: imperatives and challenges," Ad Hoc Networks, Vol.3, pp.13–64, 2003.

[4] M.S. Corson, J.P. Maker, J.H. Cernicione, "Internet-based mobile ad hoc networking, IEEE Internet Computing, Vol.3, Issue.4, pp.63–70, 1999.

[5] Routing protocols and concepts, CCNA exploration companion guide. ''Introduction to dynamic routing protocols''. Chapter three, pp 148-177.

[6] R.Vidhya, G. P. Ramesh Kumar, "Securing Data in Ad hoc Networks using Multipath routing", International Journal of Advances in Engineering & Technology, Vol.1, No. 5, pp 337-341, November 2011.

[7] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, Heejo Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks, IEEE Conference on Consumer Communications and Networking, pp 593 - 598, January 2007.

[8] Turgay Korkmaz, "Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Ad Hoc Networks", Information Technology: Coding and Computing, International Journal of Information Technology , Vol. 2, No. 2, pp 704-709, April 2005.

[9] Van Phuong T., Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, Heejo Lee, " Transmission Time-based Mechanism to Detect Blackhole Attacks", IEEE Conference on Asia-Pacific Service Computing Conference, pp 172- 178, December 2007.

[10] Amol A. Bhosle, Tushar P. Thosar, SnehalMehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications , Vol.2 , No. 1, pp 325-331, February 2012.