International Journal of Advanced Trends in Computer Applications
www.ijatca.com

DETECTION AND PREVENTION OF MULTIPLE BLACK HOLE ATTACK IN MOBILE ADHOC NETWORK

[1]Er. Ashu Bansal, [2]Er. Robin Khurana
[1]Assistant Professor, Computer Science & Engineering,
BFCET, Bathinda, India
[2]Technical Trainer, Computer Science & Engineering,
CGC Landran, India

Abstract: *A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV protocol. The security of the AODV protocol is threaded by a particular type of attack called 'Black Hole' attack. In this attack a malicious node advertises itself as having the shortest path to the destination node. If there is more than one black hole present in AODV network than problem becomes serious. In this paper we simulated MANET with or without Black hole to study the effects of black hole attacks on network performance. All the proposed work performed on NS-2.*

Keywords: *Ad hoc network, black hole attack, MANET, NS-2.*

I. INTRODUCTION

Ad hoc network is a wireless network without having any fixed infrastructure. Each mobile node in an ad hoc network moves arbitrarily and acts as both a router and a host. A wireless adhoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band.

We attempt revisiting the routing protocols applicable in MANETs, in this research exercise and investigate whether it is possible to strengthen the existing attempts on devising secure routing protocols for MANETs. The routing protocols are especially susceptible in MANETs because of the major reliance on the cooperative routing algorithms employed for establishing the network routes, with underlying assumptions about the sanctity of the peer network nodes.

The network layer in MANETs is vulnerable to various attacks viz. overhearing with a malicious intent, spoofing the control and/or data packets transacted, malicious modification/alteration of the packet contents and the Denial-of-service (DoS) attacks viz. Wormhole attacks, Sinkhole attacks, Blackhole attacks.

Amongst these, in this paper, we endeavor in analyzing and refining the security of the routing protocol AODVin contradiction of the Blackhole attacks. We propose the adaptive algorithm to rectify the black hole attack against AODV routing protocol.

II. THEORETICAL BACKGROUND AND RELATED WORK

Overview of AODV

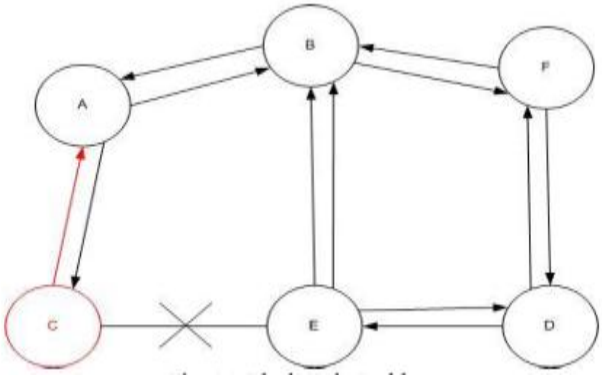
AODV is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on-demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated. AODV uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. In general, the nodes joining in the communication can be classified as source node, an intermediate node or a destination node. With every

role, the behavior of a node actually varies. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors.

This RREQ message will supplementary be forwarded by the intermediate nodes to their neighbors. This process will continue until the destination node or an intermediate node having a fresh route to the destination, receives this message. At this stage ultimately, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be acknowledged. Since AODV has no security apparatuses, malicious nodes can perform many attacks just by not behaving conferring to the AODV rules.

Black Hole attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.
The method how malicious node fits in the data routes varies. Figure shows how black hole problem arises, here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” 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 “A” before any other node. In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start seeding data packets to node “C”. In this way all the data packet will be lost consumed or lost.

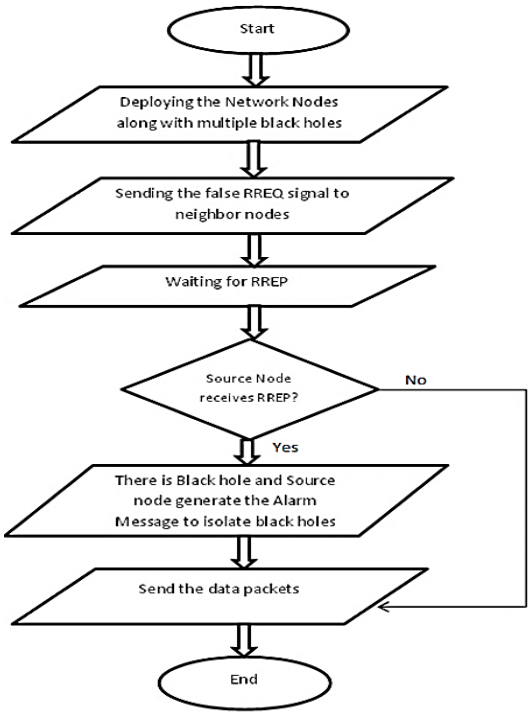


Black Hole Problem

III. METHODOLOGY

In this work, we experimentally examine the performance of purposed algorithm we firstly randomly deployed the nodes. We also deploy the manifold black holes in the network and examine the consequence of black hole attack. As we already know, the black hole always responds positively with RREP message to every RREQ and the resultant is there are too many chances to lose the data packets.

In this experiment, we propose a solution that is an enrichment of the basic AODV routing protocol, which will be talented to avoid black holes. To diminish the probability of losing the data packets it is anticipated to source node firstly generate the fake RREQ to all the neighbor nodes and wait for request replies from the same. If any nodes in the whole network generate the RREP on fake RREQ, than source node receive and examine it. Afterexamine, source node send alarm message to each and every the node present on network, to isolate the black holes. By isolating the black hole nodes we can eliminate the problem of black hole attack.



Proposed methodology for AODV

For simulation, we have used ns2 network simulator. Mobility scenarios are generated by using a Constant waypoint model by 21 nodes including 2 black holes moving in a terrain area of 800m x 800m. The Query packet size and Data packet size are taken to be 100 bits and 1024 bits. In proposed work, the whole results are obtained by taking 360 seconds simulation time with terrific mode of Constant Bit Rate (CBR). The

simulation parameters are summarized in Table 1.

Table 1: Simulation Parameters

Parameters	**Values**
Simulator	NS-2
Simulation Time	360s
Number of Nodes	21
Routing Protocol	AODV
Traffic Mode	CBR
Pause Time	2s
Number of Sources	1
Terrain Area	800m x 800m
No. of malicious nodes	2

IV. RESULTS AND DISCUSSION

The proposed algorithm is evaluated under different scenarios to check their efficiency in the AODV. The various factors that influence the design of AODV are evaluated and analyzed to study their impact on the anticipated results. This part of paper comprises the performance evaluation parameters, various factors that affect performance and the obtained results in detail.

In our simulation, the communication is started between source nodes to the destination node in presence of the malicious node. The node number of source node, destination node and malicious node are 2, 7 and 0 respectively.

SIMULATION EVALUATION METHODOLOGY

The simulation is done to analyze the performance of the network's various parameters. The metrics used to evaluate the performance are given below:

- Packet Delivery Ratio: The ratio of the data delivered to the destination to the data sent out by the source.
- Packet Throughput: Amount of packets send from source to destination with the consent of time.
- Average End-to-end delay: The difference in the time it takes for a sent packet to reach the destination. It includes all the delays, in the source and each intermediate host, caused by the routing discovery, queuing at the interface queue etc.

PERFORMANCE EVALUATION

We evaluate the performance of purposed algorithm and compare with algorithm having black hole. In this we assume that, we have one black hole in the AODV network. As we know, all time whenever a source node required to find out path towards the destination node than, black hole represent itself as a shortest path between source and destination. In this scenario, firstly we simulate the problem definition.

In our simulation result as reported in Fig. 1, shows the performance in term of packet loss. From the said figure 1, it is observed that with the presence of black hole number of packet loss is increase with the times. Just because of source node send packet to black hole in the place of required actual path. In the others words all the packets are lost during transmission.

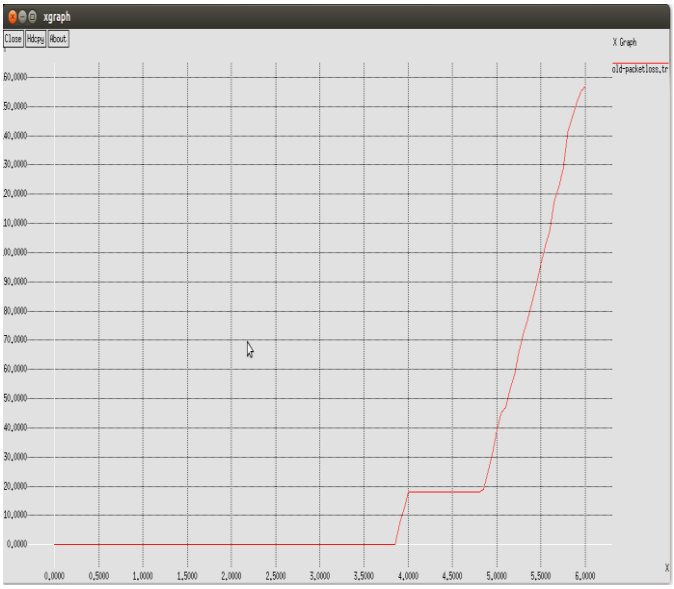


Figure 1: Packet loss under Black Hole attack

As the simulation result of our proposed algorithm reported in figure 2, shows the performance in term of packet loss. Where we can observe that there is no packet loss just because of whenever source node wants to send the data packets to the destination node, firstly with the fake RREQ, we can find out the all black holes present in the network. As a result the node who gives his presence with RREP on fake RREQ can easily be considered as a black hole. After it just generates the alarm message to all the nodes regarding black hole presence and isolates the black hole. In the other words with all the above process we eliminate the black hole from the network. As a final result all packets can be sent on required path without any packet loss.

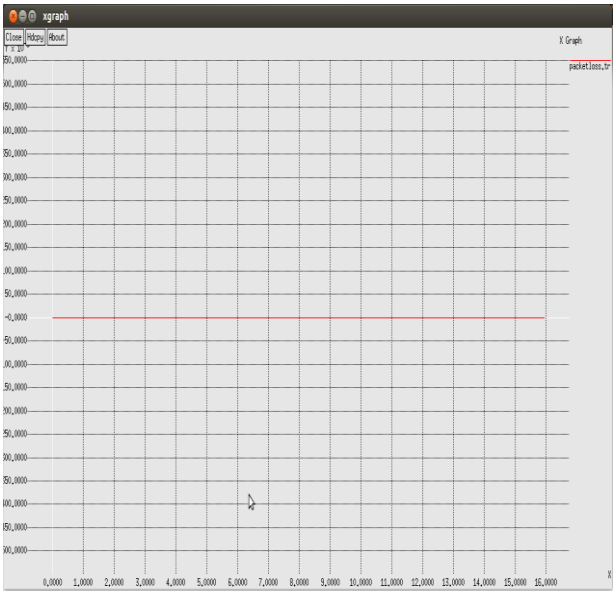


Figure 2: Packet Loss under Proposed Algorithm

From all the above observation we compare both the problem definition along with proposed algorithm. From the Figure 3, we can conclude that there is massive packet loss in AODV network black hole attack but no packet loss with our proposed algorithm.

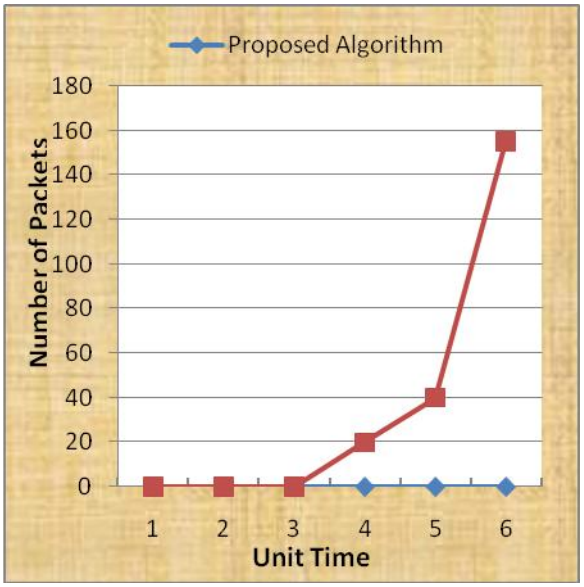


Figure 3: Proposed Algorithm vs. AODV under attack

As the simulation result of our problem definition reported in figure 4, show performance in the term of throughput. i.e., suddenly increases with time at maximum transmission speed. Here its kind to note that actually all the packets are dropped by the black hole that means no packet is delivered to the destination.

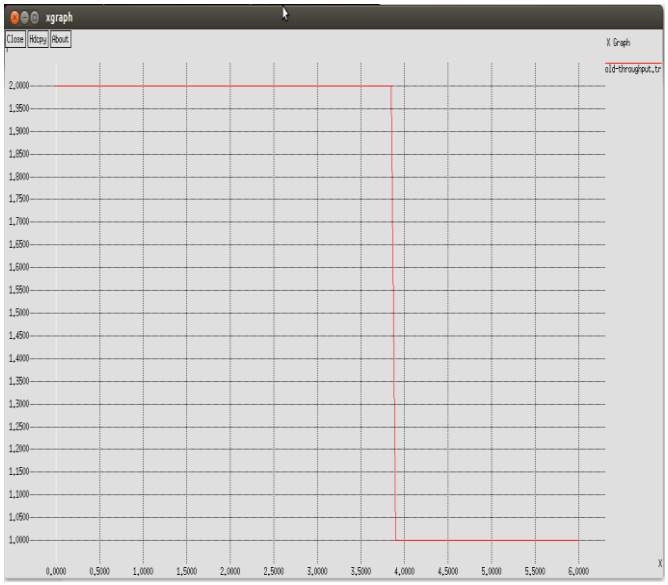


Figure 4: Throughput under Black Hole attack

From the figure 5, we can conclude that under black hole attack throughput in increase with sudden of time as compare to in our proposed algorithm throughput increase with time constraints. But it is important to intimate once again all the packets lose in the case of black hole attack as compare to no packet lose in our proposed algorithm.

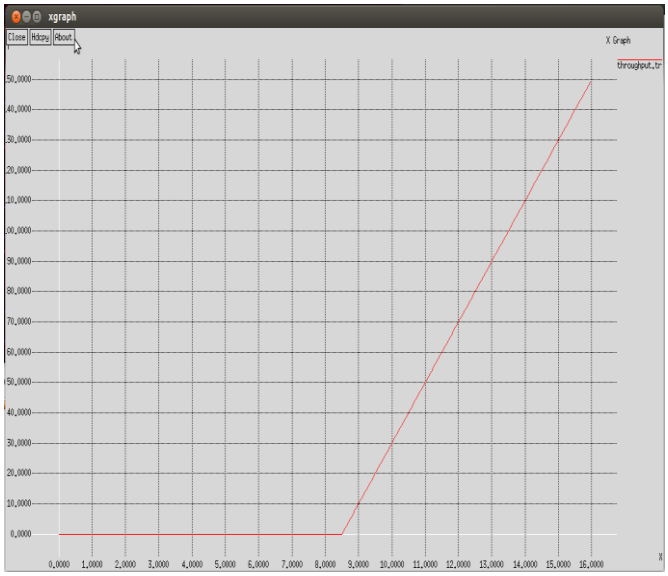


Figure 5: Throughput under proposed algorithm

From all the above observation we compare both the problem definition along with proposed algorithm. From the Figure 6, we can conclude that there is somewhere throughput is decrease in case of our proposed algorithm. The reason behind is all the time black hole represent himself as an highest threshold value mean to say it directly communicate with source node without the involvement of intermediate node. But in the actual scenario there will be requirement of intermediate nodes to communicate. That is supposed

in our proposed algorithm.

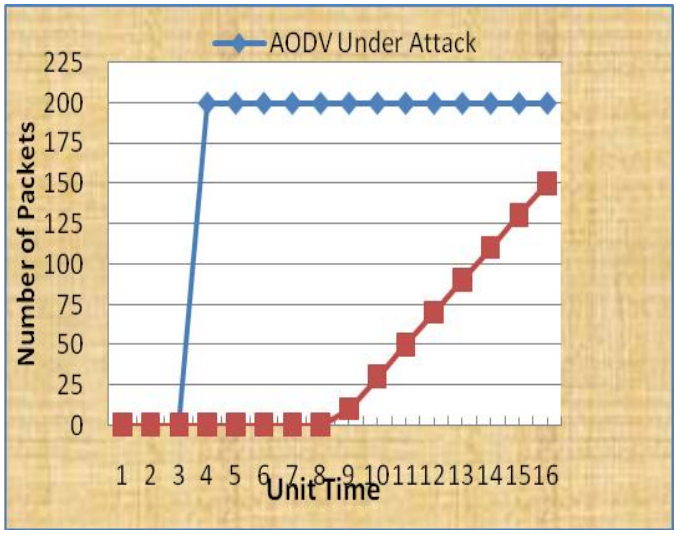


Figure 6: Throughput comparison under black hole attack vs. proposed algorithm

CONCLUSION

Packet distribution is the main issue in the mobile adhoc network. There is always a chance that an unauthorized node (Black hole) presents into network and try to discard the packets and degrade the overall performance of network. We can enhance performance of adhoc network by eliminate the black hole attack. This thesis, investigate the impact of black hole attack on mobile adhoc network using ns2. Throughout the analysis, it was seen that the performance of the adhoc network in the term of throughput and packet delivery ratio is improved by eliminating the black hole. With the implementation of proposed algorithm we can elimination of black holes from the network there is no chance of packet loss. In simple words there is 100% packet delivery ratio.

SCOPE FOR FUTURE WORK

As the research work presented in this thesis has been tested in the simulation environment, so the applicability of the proposed algorithm on the real mobile adhoc network needs to be checked.

REFERENCES

[1] Mahmood, R., Khan, A.I. "A survey on detecting black hole attack in AODV-based mobile ad hoc networks", High Capacity Optical Networks and Enabling Technologies, 2007, pp. 1 – 6, 18-20 Nov. 2007.

[2] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 775 – 780, 20-23 April 2010.

[3] Jaydip Sen, SripadKoilakonda, ArijitUkil "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", 2nd International Conference on Intelligent Systems, Modeling and Simulation (ISMS'11), pp. 338-343, Phnom Penh, Cambodia, January 25-27, 2011.

[4] J.W. Cai; P. Yi, Y. Tian, Y.K. Zhou, N. Liu, "The Simulation and Comparison of Routing Attacks on DSR Protocol", WiCOM 2009, in press.

[5] B. Sun; Y. Guan; J. Chen; U.W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks"; 5th European Personal Mobile Communications Conference, 2003, 490-495.

[6] Salehi, M., Samavati, H. ; Dehghan, M., "Evaluation of DSR protocol under a new Black hole attack", Electrical Engineering (ICEE), 2012 20th Iranian Conference, pp. 640 – 644, 15-17 May 2012.

[7] Dokurer, S. ; Erten, Y.M. ; Acar, C.E."Performance analysis of ad-hoc networks under black hole attacks", SoutheastCon, 2007. Proceedings. IEEE, pp. 148 – 153, 22-25 March 2007.

[8] Patel, M., Sharma, S.,"Detection of malicious attack in MANET a behavioral approach", Advance Computing Conference (IACC), 2013 IEEE 3rd International, pp. 388 – 393, 22-23 Feb. 2013.

[9] Satoshi K., Hindehisa N, Nei Kato, Abbas J., Yoshaki N., "Detecting Black hole attack on AODV based mobile adhoc Networks by dynamic learning system method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[10] Songbai Lu, Longxuan Li, Kwok-Yan Lam, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", Computational Intelligence and Security, 2009. CIS '09. International Conference on , Vol no. 2, pp. 421 – 425, Dec. 2009.