Volume 2, Issue 2 ISSN: 2320-5288

International Journal of Engineering Technology & Management Research
Journal homepage: www.ijetmr.org

Simulation of Blackhole Attack

Dr. Mamta Lambert
Associate Professor
Department of Computer Applications
Jabalpur Engineering College
Jabalpur , India
Email: lambert_mamta@yahoo.co.in

Mr. Sharda Prasad Patel
Email :- sharda21patel@gmail.com

***Abstract*—**A mobile Ad hoc network (MANET) is a wireless decentralized and self-configuring network in which nodes communicate with each other either directly or through intermediate nodes. Each node plays role of both transmitter and receiver. Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery. Hence it is vital to develop some security mechanism to protect MANET from attacks. In this paper performance of AODV Protocol is analyzed in presence of the network layer active attacks namely Black hole .

Keywords- MANET, AODV,DSR, OLSR, DSDV.

1. INTRODUCTION

A mobile Ad Hoc Network is a collection of wireless nodes that are capable of communicating with each other without the help from a fixed infrastructure. It is formed dynamically by autonomous systems of mobile nodes that are connected wirelessly without support of any existing network infrastructure or centralized administration. MANET could be deployed in applications such as search and rescue, automated battlefields, disaster recovery, and sensor networks. A Mobile Ad Hoc Network is an autonomous system in which mobile hosts moves in a free and random manner. MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are absent or less severe in wired networks. MANETs are vulnerable to various types of attacks [1].
A MANET can be examined on the basis of availability, confidentiality, authentication, integrity and non repudiation.

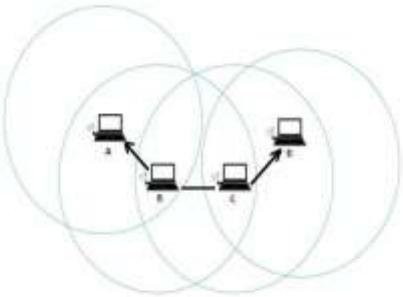

Figure 1 Mobile Ad-Hoc Network

2. ROUTING IN MANET

In MANETs nodes communicate with each other by using some routing protocols. According the dynamic topology and characteristic there are three main routing protocol used in MANETs. These all are discussed below.

A. REACTIVE (ON-DEMAND) ROUTING PROTOCOL:

Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. The reactive protocols have the low routing overhead at the expense of delay to discover the route when desired by the source.

The two kinds of protocols are there in it AODV (Ad hoc on Demand Distance Vector Protocol), DSR (Dynamic source routing).

B. Proactive (Table Driven) Routing Protocol:

This protocol is also called as table driven protocol because routing information of nodes is exchanged, periodically and accordingly the routing table is maintained, even when there is no communication. Proactive protocols have low latency rate in discovering the route but high routing overhead. This is because the nodes periodically exchange control messages and routing table information in order to keep up-to-date routes to any active node in the network. [6]

The two main kind of proactive protocols are Optimized link state routing (OLSR) protocol and Destination sequenced distance vector routing (DSDV) protocol.

C. Hybrid Routing Protocol:

This type of protocols combines the advantages of both proactive and reactive routing. The routing is initially established with some pro actively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Two types are: Zone routing protocol (ZRP) and temporally ordered Routing protocol (TORA).

2. RELATED WORK

A. Improved AODV Routing Protocol

It is an enhanced version of AODV and is hybrid in nature. IAODV mainly integrates two features: Multipath and Path accumulation.[6]

Multipath: Multipath AODV reduces the route discovery frequency as compared to single path AODV. It finds multiple paths between a source and a destination in a route discovery process. Single path AODV initiates a new route discovery when it detects one path failure to the destination, whereas in multipath it creates a fresh route in case all the existing routes fail or expire. It also reduces the number of similar routes between source and destination nodes. A path with most similar nodes has a higher probability to create common links.

Path accumulation: Path accumulation feature enables us to append all discovered paths between source and destination nodes to the control messages as shown in figure 3(a). Hence, at any intermediate node the route request (RREQ) packet contains a list of all nodes traversed. Each node receiving these control messages updates its routing table. It adds paths to each node contained in these messages.

B. MAC Based

A solution for Black hole attack detection and prevention is proposed that uses the one-way-hash function H to generate MAC for RREP packet.[4]

A Message Authentication Code (MAC) is a small part of information, which is used to authenticate and to provide integrity on the message. Cryptographic Hash Function is the only possible way to generate MACs. A MAC algorithm, accepts a variable length message as input, and outputs a fixed length MAC, also known as tag.

In cryptography, a keyed-hash message authentication code (HMAC) is a unique method for generating a MAC. It uses a cryptographic hash function with a mixture of secret cryptographic key. There are so many cryptographic hash function, such as Message-Digest algorithm (MD5) or Secure Hash Algorithm (SHA-1), they can be used in the generation of an HMAC; the resulting MAC algorithm is known as HMAC-MD5 or HMAC-SHA1 respectively.

C. Fidelity Table

A better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source; thereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented [9].

D. DPRAODV (Detection, Prevention and Reactive AODV Scheme)

In this paper authors proposed have proposed the method DPRAODV .In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends ALARM packet to its neighbors. The routing table for that malicious node is not updated, nor is the packet forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet[13] .

E. Trust Value

The solution that we have proposed here is that we develop black hole AODV which allows some degree of node maliciousness to give an motivation to selfish nodes to state its malicious behavior to its neighbors which decreases searching time of misbehaving nodes. In proposed model the trust among nodes is represented by trust score. The trust calculation is based on packets loss rate if data packet is successfully transmitted then node trust value is incremented by 1, otherwise it becomes zero.[14]

3. AODV ROUTING SCHEME

It's reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of

control messages in AODV which are discussed bellow.

A. Route Request Message (RREQ):
Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a Hop Count value in every RREQ message, the value of hop count states the number of hops the RREQ should be transmitted.

B. Route Reply Message (RREP):
A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

C. Route Error Message (RERR):
Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

The format of RREQ and RREP packets are in Fig 2.1 and 2.2 respectively.[8]

Src_ a d - dres	Src_ sequene	Broad_ Cast_i d	Dest_ addres	Dest_ s e - quence	Hop count

Figure 2.1. AODV RREQ Field

Src_ a d - dres	Dest_ addres	Dest_ sequence	Hop count	Life time

Figure 2.2 AODV RREP Field

D. Route Discovery Mechanism in AODV
When a node "A" wants to initiate transmission with another node "G" as shown in the Fig. 2.4 , it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes. This process of finding destination node goes on until it finds a node that has a fresh enough route to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other.

The given Fig 2.3 shows the propagation of the RREQ packets to all the neighbouring nodes, and the path of RREP packet towards the source respectively.

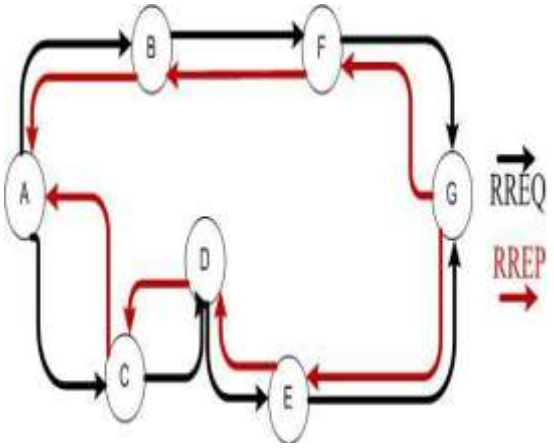

Figure 2.3 AODV Route

Recently, most research on ad-hoc routing protocols, has been assumed trusted environment but, many usages of ad-hoc network run in untrusted situations. Therefore, most ad hoc routing protocols are vulnerable to different types of attacks. These attacks are divided into two categories, called external attacks and internal attacks. Internal attacks are done by authorized node in the network, where as external attacks are performed by the node that they are not authorized to participate in the network.

4. BLACK HOLE ATTACK ON AODV PROTOCOL

Black hole attack is a big problem in MANETs in which an intermediate node works as malicious and consumes data before reaching to the destination. Black hole attack works in two phases in first phase; it advertises that it has a fresh route to the destination to deliver data packets with intention to drop data packets. In second phase it drops data packets without forwarding it. In this whenever any intermediate node gets a RREQ it immediately generates a RREP with high destination sequence number and sends it to the initiator. (Source) source stops receiving RREP and starts sending data packet to that node which has sent RREP to the source.[10]

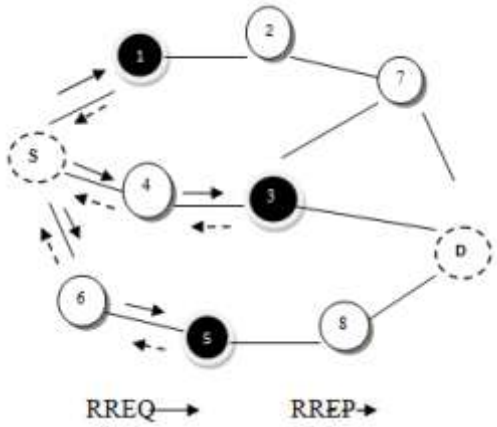

Fig: 3. Multiple Black Hole Nodes

In above figure, there are more than one black hole node i.e. 1,3 and 5 exists in the network at different places in order to drop the data packets.

4. IMPLEMENTATION

A. NS2 Simulator

We have use NS-2 (v-2.34), a network simulation tool to simulate the AODV routing protocol with attack and with the solution. It provides a good platform for MANET simulation. We simulate our model for 25 nodes. We have repeated the experiments by changing the number of Black hole nodes to see the performance of network under attacks.

Table I. Simulation Parameters

PARAMETERS	DEFINITION
Examined protocols	AODV
Simulation area (m x m)	500 x 500
Number Of Nodes	25
Traffic Type	CBR
Performance Parame-ter	Throughput, PDF, DropPackets,
No. of malicious node	1,2,3,4
Pause time	5 sec
Max Speed(M)	50

B. In our approach we have introduced Black hole module with AODV routing then IDS behavior module. Very first we attach Black hole and IDS module in the NS-2 package and update the make file through following command:

blackhole/blackhole_logs.o blackhole/ blackhole.o blackhole/blackhole_rtable.o blackhole/blackhole_rqueue.o

idsaodv/idsaodv_logs.o idsaodv/ idsaodv_rtable.o idsaodv/idsaodv_rqueue.o idsaodv/idsaodv.o \

After that we also add the agents of IDSAODV and BlackholeAODV and recompile again.

C. Performance Metrics

Some important performance metrics can be evaluated:-

***Drop Packets*—**It is defined as how many routing packets are Dropped during transmission from source to destination.

Throughput — The ratio of the number of data packets sent and the number of data packets received.

Packet Delivery Ratio (Fraction)- It is calculated by dividing the number of packet received by destination through the number packet *originated* from source.

5. RESULTS

A. Drop Packets

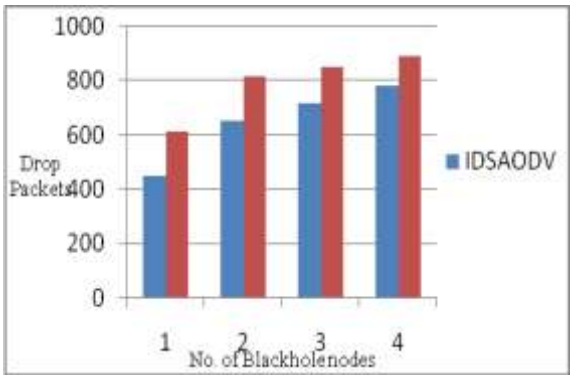

Figure 4 (a) Drop Packets

B. Packet Delivery Ratio

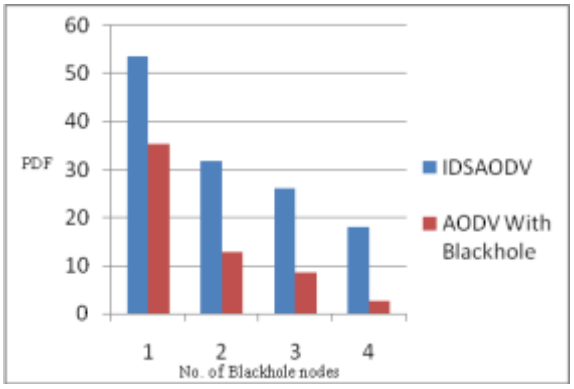

Figure 4(b) Packet Delivery Ratio

C. Throughput

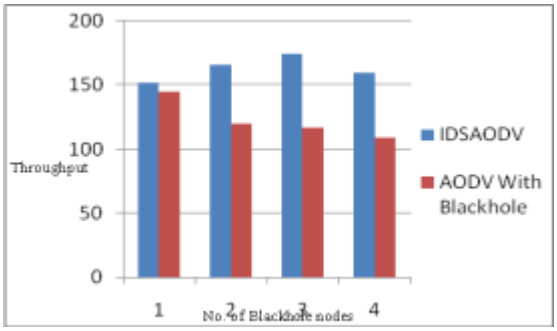

Figure 4(c) Throughput

6. CONCLUSION AND FUTURE WORK

In this paper, effect of the Black Hole attack analyzed. Simulation results in an AODV protocol of MANET shows Black Hole attack degrade the performance, but presence of IDS increases the performance.

In future this approach can be extended to other proactive routing protocol like DSDV and reactive routing protocols like DSR. We can also extend this research to secure routing protocols against other attacks such as Wormhole attack, Jellyfish attack etc.

REFERENCES

[1] Pooja Jaiswal, Dr. Rakesh Kumar "Prevention of Black Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] Y. Khamayseh, A. , Bader, W. Mardini and M. BaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks "International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE Wireless Communications October 2007. PP: 85-90.

[4] Pooja Vinod Kumar Department of Computer Science and Applications"A Review on

Detection of Blackhole Attack Techniques in MANET" Volume 4, Issue 4, April 2014 ISSN: 2277 128X International

[5] *Journal of Advanced Research in Computer Science and Software Engineering.*

[6] *Modified AODV Protocol against Black hole Attacks in MANET by K. Lakshmi1, S.Manju Priya, A.Jeevarathinam, K.Rama, K.Thilagam, Lecturer, Dept. of Computer Applications, Karpagam University, Coimbatore, International Journal of Engineering and Technology. Vol.2 (6), 2010.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.*

[7] *Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010*

[8] *Jaspal Kumar, M. Kulkarni, Panipat Institute of Engineering & Technology, India National Institute of Technology, Karnataka, India "Effect of Black Hole Attack on MANET Routing Protocols" I. J. Computer Network and Information Security, 2013, 5, 64-72 Published Online April 2013 in MECS*

[9] *C. Kim, E. Talipov and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks," Proceeding from EUC'06: The 2006 International Conference on Emerging Directions in Embedded and Ubiquitous Computing, Seoul, 1-4 August 2006, pp. 522-531.*

[10] *Ravi KantvM.tech Scholarv ABES EC, Ghaziabad" A Literature Survey on Black Hole Attacks on AODV Protocol in MANET" International Journal of Computer Applications (0975 – 8887) Volume 80 – No 16, October 2013*

[11] *S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad -Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.*

[12] *K. Makki, N. Pissinou, and H. Huang, "Solutions to the black hole problem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.*

[13] *S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.*

[14] *Bhoomika Patel Department of Information Technology, Parul Institute of Engineering & Technology, Limda, Vadodara, India." A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,*

[15] *Nirali Modi, Vinit Kumar Gupta Department of computer engineering Hasmukh Goswami College of Engineering, Ahmedabad, India" Prevention Of Black hole Attack using AODV Routing Protocol in MANET" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,*

[16] *"Black Hole Effect Analysis and Prevention through IDS in*

MANET Environment "Kamini Maheshwar; Divakar Singh Dept. of Computer Science & Engineering, BUIT,BU, Barkatullah University, Bhopal European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-90