Security Assessment of Routing Protocols in Mobile Adhoc Networks

Megha Soni
Research Scholar
SVCE, Indore
India
meghasoni@svceindore.ac.in

Brijendra Kumar Joshi
Professor
MCTE, Mhow
India
brijendrajoshi@yahoo.co.in

***Abstract*—Mobile Ad-hoc Network (MANet) is a set of wireless mobile nodes forming flexible networks, thus they do not need infrastructure and central access points. With increase in the use of Mobile Adhoc Networks security became an essential requirement due to its dynamic topology, limited processing capacity, bandwidth limitations, high bit error rate etc. To provide secured communication among mobile nodes, there is a need to build multi fence security and routing solutions to overcome these challenges. In this paper, we present security analysis of routing protocol in general and Ad-hoc On demand Distance Vector in particular under different type of attacks.**

Keywords- Manet, Security parameters, AODV, Black Hole, Gray Hole

I. INTRODUCTION

MANets are formed by mobile nodes without infrastructure and each node acts as router. Mobile ad-hoc networks are new paradigm of wireless communication. Node mobility causes frequent changes in network topology. The wireless nature of communication and lack of any security infrastructure increases several security problems discussed in further sections.

There are mainly five MANet security parameters as described next [1]:

A. Confidentiality

Protection of any information from being exposed to the unauthorized entities, because intermediate mobile nodes receive the packets for other recipients, the information being routed in MANet can be eavesdropped.

B. Availability

Services should be available whenever required and should endure survivability regardless of attacks. An attacker can interrupt the routing mechanism on network layer and on other higher layers the attacker can bring down high level services such as key management service.

C. Authentication

Allow a node to define the characteristics of the peer node it is communicating with, without which an attacker would impersonate other node.

D. Non-repudiation

Ensures that the receiving and sending nodes can never deny ever sending and receiving of the messages. Non-repudiation is useful in identifying, isolating and compromised nodes.

E. Integrity

Guarantees that a message transmitted is never altered.

II. ROUTING PROTOCOLS IN MANETS

MANet routing protocols can broadly be classified into three categories as [1]:

A. Proactive Protocols

Proactive Protocols or Table-Driven Protocols roots are always maintains between nodes in the network, also when the routes are not being used. Each node updates to the other node within the network in such a way that all nodes in the network eventually consistently knows the state of the network. The advantage of this approach is that there is small or no time delay involved when a node wants to starts communicating with a new node. The disadvantage is that in very large networks, the control message overhead of maintaining all routes within the network can rapidly reduced the capacity of the network. Pro-active protocols are the Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV), etc.

B. Reactive Protocols

Reactive Protocols or On-Demand Protocols involve searching for routes to other nodes only as they want to communicate. When a node wishes to communicate with another node for which it has no information in its route table a route discovery process is invoked. Ones a route is discovered it maintained as long as it is required by route maintenance process. Routes which are inactive eliminated at regular intervals. The advantage of reactive protocol is that it is more scalable than proactive routing protocols. The disadvantage of these methods is that an additional time delay is required in order to find a new root. Adhoc on Demand Distance Vector (AODV) is reactive protocol.

C. Hybrid Routing Protocols

These protocols works on combination of reactive and

978-1-5090-5515-9/16/$31.00 ©2016 IEEE

proactive methods Proactive methods are used for routing between members of a zone, and routing between different zones is based on reactive method. Zone Routing Protocol (ZRP) is Hybrid Routing Protocols.

III. OVERVIEW OF AODV

The impact of AODV algorithm on the operation of ad-hoc networks is noteworthy. Each node of the network works as a specialized router and routes are obtained as needed [2]. Unlike the other protocol AODV does not depend on the recurring advertisement of the routing therefore bandwidth demand by the nodes is reasonably less. The foregoing properties make AODV free from cycle or loop as for as router are connected.

Just like Dynamic Source Routing (DSR) AODV also uses broadcasting for route discovery, but for route table entries at intermediate node AODV do not use source routing. It establishes routes dynamically.

AODV inherits destination sequence numbers from DSDV and maintain the most recent routing information between nodes. The combination of DSR and DSDV yields an algorithm that minimizing the network load for control, and data traffic and uses bandwidth efficiently.

A. Path Discovery

Whenever a source node wants to communicate with another node for which it has no routing entries in its routing table, it stars path discovery process. Every node maintains and use two separate number counters: a node sequence number and a broadcast ID. The source node broadcast a Route REQuest (RREQ) packet to its neighbors to initiates path discovery.

B. Reverse-Path Setup

In addition to the *broadcast_id* there are two sequence number contained in a RREQ *i.e*. the source sequence number and the last destination sequence number and both are known to the source. The purpose of source sequence number is to maintain newness information about the reverse route to the source, and the destination sequence number is used specifies that how fresh a route to the destination before it can be applied by the source. When RREQ start from source and travels to various destinations, it automatically sets up the reverse path from all nodes back to the source.

Every node makes a record of address of the neighbor from which it received the first copy of the RREQ and use it to set up a reverse path. It is compulsory for every node to maintain the reverse path route entries at least for time in which the RREQ passes through the network and give a reply to the sender.

C. Forward-Path Setup

When a RREQ will reach at a node that has a recent route to the destination. If node has a route entry for the destination, it checks whether the route is fresh by using the destination sequence number in its own route entry table to the destination sequence number mentioned in the RREQ. The intermediate node can reply only when it has a route with a sequence number that is greater than or equal to that in the RREQ otherwise it rebroadcasts the RREQ. Node send a route reply packet (RREP) back to its neighbor from which it received the RREQ only if it does have a recent route to the destination and the RREQ has not been received previously.

D. Route Table Management

The route table stored some other useful information such as “soft state” and a timer called the “route request expiration timer”. The timer is used to wash out reverse-path routing entries from those nodes that do not lie between the source and destination. The expiration time depends upon the size of the ad-hoc network. Another important parameter in routing entries is the route-caching time out; it is the time after which the route is considered to be invalid.

E. Path Maintenance

During an active session, if the source node moves it can restart the route discovery process to find a new route to the destination. If any valid node moves along an active path it does not affect the routing path. When either the destination or some other node moves, a special RREP is sanded by these nodes to the source nodes. To detect link failures and to ensure symmetric links, the periodic Hello messages can be used.

F. Local Connectivity Management

There are two ways by which the Nodes discover their neighbors. Whenever a node receives a broadcast from a neighbor, it updates its local connectivity information to include this neighbor. When a node has not sent any packets to all of its active neighbors during a Hello interval, it broadcasts to its neighbors a special unwanted RREP which contains its identity and sequence number.

IV. SECURITY ATTACKS ON MANETS

MANets are unsecure from various types of attacks. Attacks can cause drop of network traffic and modification of control message fields or forwarding routing message.

Main goals of Attacks are-

- Decrease overall network throughput.
- Increase latency of particular packets.
- Break down a particular link.
- Divert packets to affect link bandwidth

The attacks in MANets are done in order to disrupt the communication or to steal the information. The attacks can be broadly classified into two distinct categories, Active attacks and Passive attacks. An active attack is the attack in which any information or data is inserted into the network so that information and operation may damage. It involves modification, disruption and fabrication and affects the operation of the network. Example of active attacks is spoofing, impersonation. A passive attack exchanges data in the network without disturbing the communications. It is difficult to detect passive attack. Due to passive attack, operations are not affected, but attacker tries to discover valuable information by listening to traffic and observing

the network. Some of the most common attacks on MANet are-

A. Black Hole Attack

In this type of attack, attacker first sends fake route related information to the source node and state that it has the shortest route to the destination and after establishment of the route, attacker receives the data packet from the source node then drops or misuses these packets. In AODV Black Hole attack can be acted via two ways *i.e.*, External Black Hole Attack and Internal Black Hole Attack [3].

- Internal Black Hole Attack

A malicious node is present inside the network and it enters into current data route as it gets the opportunity. After receiving the packets intended from other node, it starts dropping them. It is difficult to detect this type of attack because it is due to an internal malicious node.

- External Black Hole Attack

This attack is due a node which is malicious and outside from the network. The malicious node first detects the information about active data route and destination node and then forwards its RREP packet to the nearest node present in the active path. The neighbor node update route entry in the routing table and forward the packet, in this way malicious node receives the packet from source node and then drops the packets.

For example in Fig.1, S is source nod wants to communicate to destination D. S will send Root Request RREQ packet to its neighbors which will again forwarded it until it reaches to destination. In active path the malicious node G will send a RREP packet to neighbor node, thereby able to connect to the source node. Thus, the malicious node will begin dropping the packets [4].

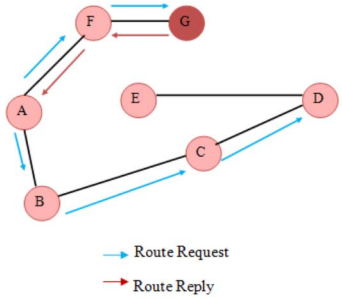


Fig. 1 Black Hole Attack

B. Gray-hole attack:

Gray Hole attack is also called as routing misbehavior attack, in this attack the messages dropping in two phases in the first phase a legitimate route to destination is advertise by node itself. In second phase, with a certain probability nodes drops intercepted packets [1].

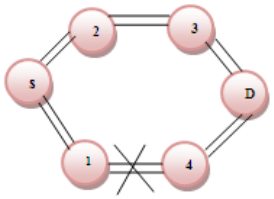


Fig.2 Gray Hole Attack

C. Worm Hole Attack

This attack is due to formation of tunnel between two malicious nodes. One attacker received packets at one point and then tunnels it to the other malicious node on the other point [5]. Thus, a sending node thinking that it has passed this packet through shortest route in the network. This attack is also known as *tunneling* attack.

For Example, in Fig. 2, Source node A wants to communicate with node M. Node A will send RREQ packet to immediate neighbors B and I and Malicious node C. C will tunnel the packet directly to other malicious node F, thereby, shortening the path. Thus, M will accept the shortest path through F and ignore other paths.

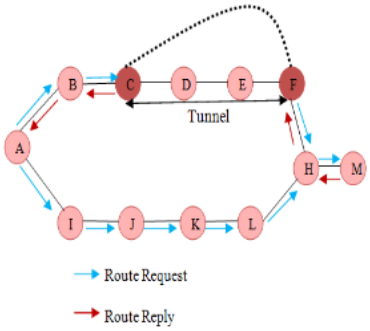


Fig. 3 Worm Hole Attack

V. PERFORMANCE PARAMETER

For evaluating the performance of the communication system different parameter is used such as throughput, PDR, end to end delay and Normalized Routing Load NRL etc. The description of this parameter is depicted below [6] [7].

A. Throughput

Throughput is defined as the ratio of total number of packets, delivered and total simulation time.

Mathematically, it can be defined as:

$$\text{Throughtput} = \frac{\text{N}}{100} \qquad (1)$$

Where N is the number of packets received successfully by all destinations.

B. Packet Delivery Ratio(PDR)

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source.

$$PDR = \frac{\Sigma CBRrecv}{\Sigma CBRsour} \qquad (2)$$

C. *End-to-End Delay(E_to_E)*

end-to-end delay is the average time acquired by the packets to pass through the network.

$$E\_to\_E\_ = \frac{\Sigma(CBRstime - CBRrtime)}{\Sigma CBRrec} \quad (3)$$

D. *Normalized Routing Load (NRL)*

It is the amount of routing packets transmitted per data packet transported at the pursuit. Each hop-wise transmission of a routing packet is counted as one transmission [8];

$$NRL = \frac{Numberof Packet\ received}{Numberof Packet\ transmitted} \quad (4)$$

VI. SECURITY ANALYSIS OF AODV

A. Security threats in AODV

The main causes of Black Hole and Gray Hole attacks on AODV are the following-

- It is completely on demand protocol.
- It uses message broadcasting process.
- It has flat routing or no mobility management.
- AODV uses shortest path algorithms.
- It does not have any process of authentication of non-mutable field.
- It only keeps the track record of next hop.
- In AODV real time attack is possible.
- It does not have proper authentication process for communicating nodes.
- AODV has no mechanism to observe the neighbor node activities [9].

B. *Effects of Black Hole and Gray Hole attacks on AODV performance*

When size of network is small the throughput, pdr, and routing overhead is very low because the ratio of number malicious nodes and number of total nodes is high and by increasing the number of nodes this ratio will decrease. Therefore the effect of attacks is severe on small network see figures. In other words for large networks, the effects of these attacks on protocol performance parameter is not very high because *Availability* of AODV is high.

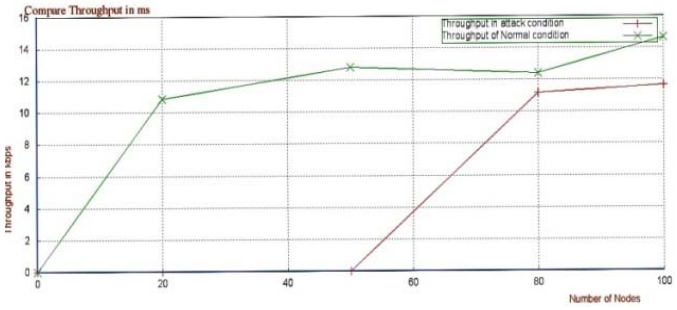
Both attacks degrade the performance of AODV but the impact of Black Hole attack on performance parameter is more serious as comparative to Gray Hole attack because in Gray hole attack a malicious node refuses to forward only certain packets and drops them. AODV acts as counter measure of Gray Hole attack. It minimizes its effect and improves the reliability of MANet.

VII. SIMULATION

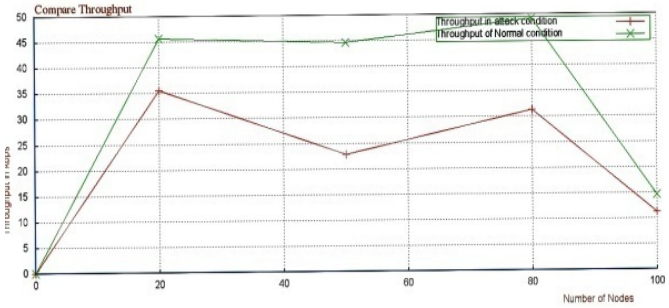
To analyze the performance of AODV in normal as well as under different attacks condition such as Black hole and Gray Hole. The NS-2(ver. 2.34) simulator was used.

TABLE I: PARAMETERS FOR SIMULATION

S.No	*Parameter*	*Value*
1	Simulation Time	100s
2	Number of Nodes	20,50,80,100
3	Max. no. of Connections	8,16,24,32,40
4	Pause time	20s
5	Terrain Area	750 x 750
6	Max. speed	20s
7	Routing Protocol	AODV
8	No. of Malicious Nodes	1

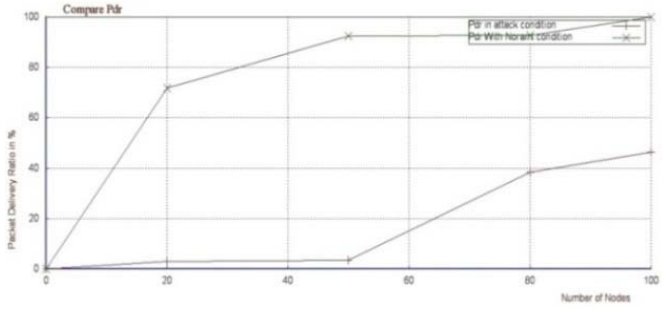


(a)

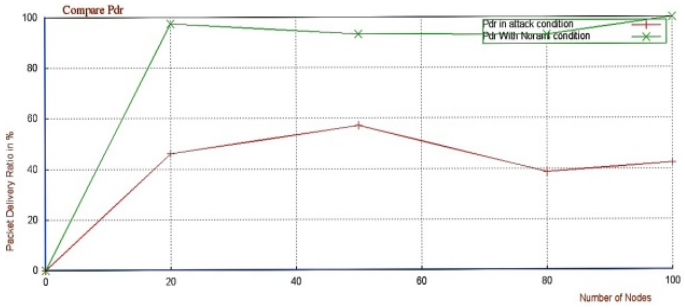


(b)

Fig. 4 Effect of (a) Black Hole and (b) Gray Hole attack on Throughput

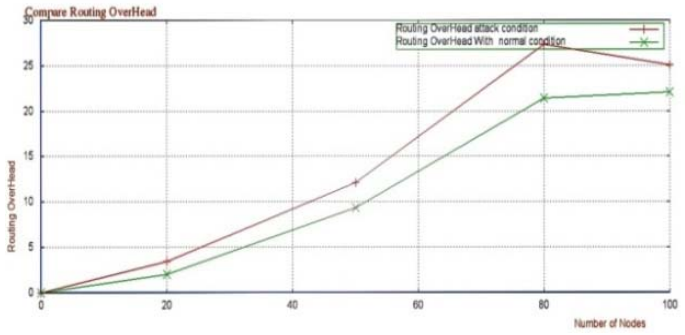


(a)

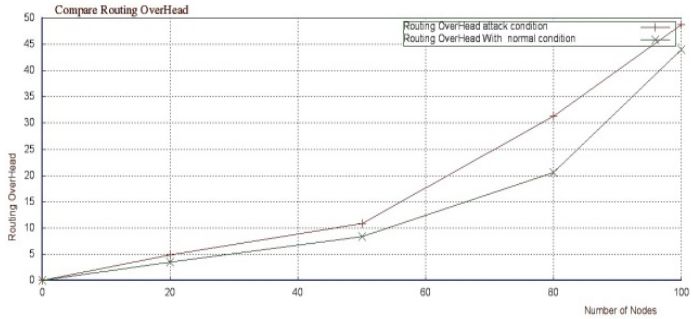


(b)

Fig. 5 Effect of (a) Black Hole and (b) Gray Hole attack on pdr



(a)



(b)

Fig. 6 Effect of (a) Black Hole and (b) Gray Hole attack on Routing Overload

CONCLUSION

This paper mainly focused on various security attacks in AODV routing algorithms in MANets along with their comparison on various parameters have given. We have examined the AODV routing protocols under the different attacks to a certain level and we find that it has drawbacks such as less throughput, low packet delivery ratio and less network routing overhead. Small network is more vulnerable for Black Hole and Gray Hole attacks. To provide more security and immovability in MANets it is required to develop efficient security mechanism and secure routing.

REFERENCES

[1] S. Kaur A. Gupta "A Review On Different Secure Routing ProtocolsAnd Security Attacks In Mobile Ad Hoc Networks" International Journal of Advanced Engineering Technology, vol. 5, pp. 01-05, December 2014.

[2] S. K. Sarkar, T.G. Basavaraju and C. Puttamadappa "Adhoc Mobile Wireless Network" Auerbach Publication, pp.59-98, New York 2008.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, and, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Communications, vol. 14, Issue 5, pp.85-91, 2007

[4] P. Goyal, V. Parmar, and R Rishi, "MANET, Vulnerabilities, Challenges, Attacks, Application ", IJCEM International Journal of Computational Engineering & Management, vol. 11, 2011

[5] S. Kapoor and P. Saini"A Survey on Routing Protocols and Attacks in Mobile Adhoc Networks (MANETs)" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, pp. 453-460, March 2015.

[6] A. Khare and P. S. Chauhan "Exposure of Black Hole Attack DSDV, DSR Based Routing Protocol in Mobile Ad Hoc Network" International Journal of Engineering Science and Computing, vol. 6, pp. 2757-2761, March 2016.

[7] R. Kaur and A. Kaur , "blackhole detection in manets using artificial neural networks", International Journal For Technological Research In Engineering, vol. 1, Issue 9, pp. 2347 – 4718, May-2014.

[8] "Performance Evaluation of AODV routing Protocol under Black Hole attack with varying Black hole nodes", 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science

[9] C. E. Perkins, "Ad hoc Networking", pp. 175-179, Pearson Publication, India, 2008,.

[10] L. Abusalah, A. Khokhar, and M. Guizani, " A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE Communications Surveys & Tutorials, vol. 10, No. 4, pp. 78-93, 2008.

[11] A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L.Bölöni, & D.Turgut,"Routing protocols in ad hoc networks: A survey", Elsevier Computer Networks ", pp 3032–3080, 2011.

[12] J. Arshad, M. A. Azad," Performance Evaluation of Secure on-Demand Routing Protocol fo Mobile Ad hoc Networks", 2006 IEEE.