Comparative on AODV and DSR under Black Hole Attacks Detection Scheme Using Secure RSA Algorithms in MANET

Meenakshi Jamgade[1], Vimal Shukla[2]

[1]PG Scholar, KNPCST, Bhopal(India), [2]Head PG,CSE ,KNPCST, Bhopal(India)

Abstract - MANETs (Mobile Ad hoc Networks) are De-Centralized wireless networks with Self-configuring mobile nodes. Due to the absence of trusted centralized authority or openness of network topology, these networks are susceptible to security threats. Black hole attack is one of the route disruption attacks that cause a greater damage to the network. In this attack a malicious node belie that it is having shortest path and traps packets thereby degrading network performance. MANETs pose a greater challenge for routing protocols. In this paper AODV (Ad hoc On Demand Distance Vector Routing) protocol is used for route establishment since it is an efficient routing protocol but it lack with security issues. Hence well-known cryptographic algorithm such as RSA Algorithm is used for providing a secure routing between mobile nodes even in presence of malicious nodes .In brief, this paper presents a counter measure to overcome black hole attack.

Keywords - AODV, DSR, Cryptographic, black hole, RSA, Secure RSA.

1. INTRODUCTION

1.1 Ad-hoc networks

Wireless networks [1] can be broadly classified into infrastructure based wireless networks or ad-hoc networks. In ad-hoc networks [2], the nodes are mobile and routing between source and destination node is achieved by intermediate nodes acting as routers if not in radio range. As ad-hoc networks are highly dynamic, routing protocols play a crucial role to achieved quality of service and performance. Basically MANET is defined as a group of wireless computing devices like Laptop, Personal digital assistant (PDA), cell phones or other similar devices [4].

Mobile Ad Hoc Networks challenges and features are:

1.1.1 Dynamic topologies

Nodes are allowed to move randomly. Thus, the network topology may change randomly and rapidly at unpredictable times [3].

1.1.2 Bandwidth - constrained, variable capacity links Wireless links have significantly lower capacity than their Hard wired counterparts. In addition the examined throughput of wireless communications, because of the effects of multiple access, noise, fading and instance of interfering conditions, is often much less than a radio's maximum transmission rate [5].

1.1.3 Energy-constrained operation

All the nodes in MANET may depend on batteries and other exhaustible means for their energy. For these nodes, the most important design criteria are energy conservation [5].

1.1.4 Security

Mobile wireless networks are generally more likely to physical security threats than fixed-cable networks. The various problems like spoofing, eavesdropping, and denial-of- service attacks should be carefully considered these characteristics and challenges make a set of necessary assumptions and performance issues for protocol design which extend beyond those guiding the design of routing within the high speed, semi static topology of the fixed Internet.

1.2 Routing protocols

In mobile ad-hoc networks routing protocols are broadly classified into Reactive routing protocol, Proactive routing protocol and Hybrid protocols. Routing protocols in MANET are used to discover different path between nodes. They do not use any access points for connecting each node to other node in network. They generally divided into three categories: it will describe the comparison of these three protocols. These comparisons were based on parameters like number of input, time analysis, and rate of sending data for packet delivery ratio (PDR), end to end delay and load [4].

in proactive routing each node maintains a table containing routing related information. Any node wants to transmit data can start transmitting data using routes already present in the routing table enabling data transmission. proactive routing protocol includes destination sequence distance vector (DSDV) routing protocol as well as many other routing protocol like optimized link state routing protocol (OLSR), wireless routing protocol (WRP). Here the advantage of proactive protocols updates its routing table data irrespective of data traffic [4].

Reactive protocols update routing information only when route is required, these protocols reduce the overhead in mobile networks. Some of the famous ad-hoc routing protocols falling in this type are Dynamic Source Routing (DSR), Ad-hoc On Demand Distance Vector (AODV) routing and Temporarily Ordered Routing Protocols (TORA) [4].

1.3 AODV Reactive routing protocol

AODV is a remodeling of destination sequence distance vector (DSDV) protocol used in wireless mobile networks. This solves the disadvantages of DSDV by implementing a sequence number. Not like DSR [9] which carries the entire route from source to destination in the packet, the nodes in AODV carry out the next hop information corresponding to each data flow. Being a Reactive protocol route is discovered as when needed and maintained as long as they required. Hybrid protocols have well combination form of both reactive and proactive routing protocols methods [4].

1.3.1 Various Possible Attacks in MANET

Many possible attacks can compromise the security of AODV in mobile ad hoc network

Internal attacks: In this type, the attacker acts as one of the nodes and gains direct access to the network either by impersonation or by compromising a proper node and using it to do its malicious activities.

External attacks: In this type, the attacker attacks from outside the network, due to congestion in the network traffic by propagating non meaningful messages, thereby disturb the entire communication of the network.

2. PROBLEM IDENTIFIED

AODV [7] is based on distance vector routing. When security is applied to it, the performance of the network degrades. So the problem solved here is to incept security in such a manner that the performance degradation is as low as possible.

Here the considered problems are:

1) If nodes or links fails then error message is sent back to the source this will activate the source nodes to resend the data back to destination and this will take too much time to perform the procedure again.
2) It is time consuming.
3) Traffic congestion increases as same packet is send again and again.
4) The effect of traffic congestion will pay impact on the Performance/Throughput of AODV system due to resending of same packet will cause other nodes waited to send data. The security of AODV will be based on one-way hash, two-way hash and digital Secure

All the three security procedure consists of several steps. It required many inbuilt functions. This general Procedure needs to be proceeding before sending and receiving the packet. Now if nodes or links fails, so all the process inbuilt functions needs to be conducted again to same packet.

3. PROPOSED METHODOLOGY

In Secure RSA security schemes:

Here an encryption algorithm with Secret key is proposed to secure AODV messages. This mechanism calculates Secure RSA using appropriate encryption algorithm for all the fields of an AODV message. It also calculates Secure RSA with secret key and then both Secure RSA s will be transmitted along with the AODV messages. Cryptographic mechanisms are commonly used to protect routing protocols by enforcing mutual trust relationships among the wireless nodes [8].

1. In AODV routing, sender node produces the Secure RSA with an encryption algorithm and concatenates it with each of the AODV messages. It reforms the below operations:

2. Subsequently, every time an intermediate node receives the message, it calculates the following calculations to recheck the genuine message:

- It makes use of the concatenated Secure RSA to compare the newly generated Secure RSA by intermediate node; if it matches then node will carry forward the message to the next node. But before re-broadcasting a message it will check the index of upcoming node to check whether it is destination or not.

3. Finally if receiving node matches the value of index and find it is destination node then, it will calculate the Secure RSA with using secret key for more security purpose and compare it with concatenated special Secure RSA with key.

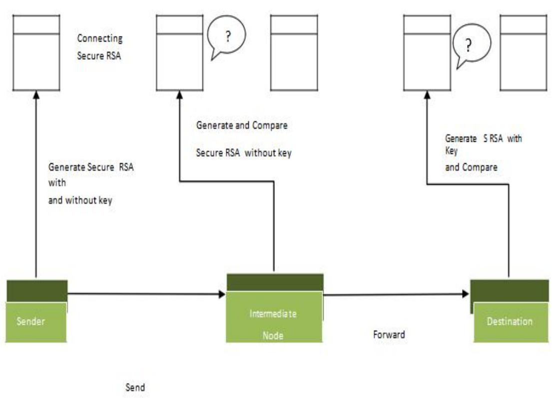

Fig 1: Secure DSR using Secure RSA security scheme

First Secure RSA is used for intermediate nodes while second Secure RSA is for destination. As shown in the figure 1, sender first generate Secure RSA , and it concatenates those Secure RSA in the original DSR packet, intermediate nodes will verify the packet using first Secure RSA , if first Secure RSA will match it will accept the packet and forward it to the next node. When packet will arrive to the destination node it will check for second Secure RSA and verify its authenticity that packet was sent by legal sender and it is not being modified. In this way, packets will transfer from source to destination securely.

Here it has been proposed that, send the data packet from the last nodes it received when particular node or link fails instead of sending it back.

Improvements done are:

- Network performance and throughput both increased.
- It is less time consuming.
- Traffic congestion will not occur.
- Other nodes will not be going to wait for nodes that are sending.
- No need to apply security steps, procedure and functions again and again on the same data packet and hence security increase.
- As DSR is dynamic in nature therefore its topology changes quickly so it helps to send the data quickly before changing its topology

The proposed scheme will be highly flexible, easily expanded and efficient and mainly reduces end to end delay in high mobility cases. Also this scheme will improve security for routing protocol. For implementation, NS2 simulator [11] is used for DSR routing protocol. As NS2's documentation is good and easy to get support from many researchers using it. Additionally, many papers related to my field of research have used it and they recommend using NS2 to simulate MANET protocols. Thus NS2 provide the best solution to the said Purpose. Many factors have been applied for improving performance along with security. That methodology was applied in NS2 simulator to improve the performance factor.

Table 1 General Simulation Parameters

Parameter	Value
MANET Area	1500*300 sq.m.
Total number of nodes	50
Node speed	0 up to 20 m/s
Application	Constant bit rate
Number of generated packets	10000 packets per CBR
Size of packets	512 bytes
Simulation time	300 sec

The above simulation action were used in the propose methodology. The different configuration values which were used for implementation are given below in the table.

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83 GHz machine using Ubuntu 12.0.4 with 2 GB RAM and the network simulator NS2 version NS-2.34. The choice of this simulation package in specific is due to the various reasons. The simulated network consists of 50 mobile nodes in a space of 1500*300 square meters. Propagation style is Two Ray Ground, 32 Antenna type is Omni Antenna. As for the MAC layer communication, the IEEE 802.11 is used. Total simulation time is 300 seconds. The above table shows the values that were used in all performed simulations.

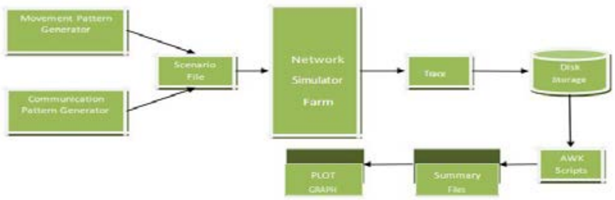

Fig 2: Simulation model overview [12]

Now for specially destination node sender make use of a secret key to produce another Secure RSA and generate the same and also concatenates it with message. this section author need to mention his simulation/experimental research model with neat block diagrams and flow charts.

4. SIMULATION/EXPERIMENTAL RESULTS

In After implementation of successful proposed secure DSR, There were two different situations to be highly regarded. First is without attack situation and second is with attack situation. Total three times the simulation was ran and three different trace files were generated. With the use of AWK scripts the three different trace files were analyzed.

4.1 Comparative Analysis of Results

4.1.1 Packet Delivery Fraction (PDF)

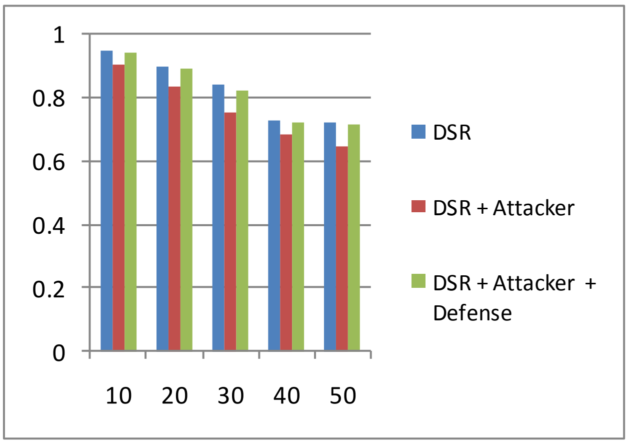

Fig.3 Packet Delivery Fraction (PDF)

It is the ratio of packets delivered to that produced by the traffic analyses generator. It is shown by received packets/sent packets. The packet delivery ratio is directly influenced by loss of packets, which may be caused by general network faults or uncooperative behavior.

From the above figure it can be concluded that in case of proposed DSR without attack the PDF is decreasing marginally, which is good indication of showing there is not much difference in delivery rate even after adding the security. While in case of proposed DSR with attack the PDF decreasing noticeably due to the attack

4.1.2 Average End to End Delay (Average E2E Delay)

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. In this experiment, the average end-to-end delay is being measured for the Normal DSR, Proposed DSR without attack and Proposed DSR with attack.

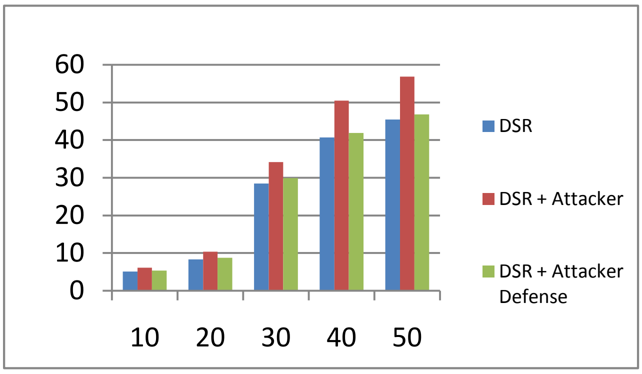

Fig .4 Average End to End Delay (Average E2E Delay)

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. In this experiment, the average end-to-end delay is being measured for the Normal DSR, Proposed DSR without attack and Proposed DSR with attack.

4.1.3 Average Throughput

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., useful information whether or not data packets correctly delivered to the destinations.

From the below figure it can be concluded that in case of proposed DSR without attack the throughput is decreasing marginally, which is good indication of showing there is not much difference in throughput even after adding the security. In case of proposed DSR with attack, throughput decreasing noticeably due to the attack.

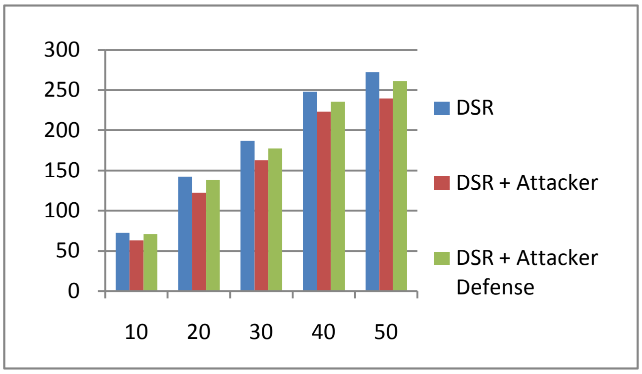

Fig .5 Average Throughputs

5. CONCLUSION

Security of MANETs can be achieved using two approaches such as secure routing and intrusion detection system. In this thesis, a cryptographic approach such as RSA algorithm is used for secure routing. Here malicious nodes can be detected since hop count field and sequence numbers are encrypted. Hence Latest sequence number packets are received by destination node thereby decreasing memory overhead and to make network loop free. Finally the paper explained the counter measures for Black hole attack. This mechanism must be tested for larger networks can be considered as future work.

6. FUTURE SCOPES

In future, we will further propose some ideas that can be integrated to the proposed scheme and they are presented as follows: The same kind of secure mechanism will be integrated and implemented to secure other routing protocols of MANET like DSDV, TORA etc. the same kind of secure mechanism will be designed to secure wireless sensor networks also. Even the performance factor improvement of other protocols by optimization between different layers is in line.

REFERENCES

[1] S. Doshi, T. X. Brown, Minimum Energy Routing schemes in Wireless Ad hoc networks, IEEE INFOCOM 2002

[2] Ram Ramanathan and Jason Redi, “A brief overview of Ad-hoc Networks: Challenges and Directions”, IEEE Communications Magazine May 2002, pp. 20-25

[3] Mitigating Black Hole Attacks in DSRISSN 0975-3303Mapana J Sci, 11, 4(2012), 65-76 Routing Protocol Using Dynamic Graph

[4] Brijesh Soni, Biplab Kumar Sarkar, Arjun Rajput, "Improvising the Ad hoc on Demand Distance Vector Routing Protocol When Nodes or Links Fails," *in Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE 2012) © Springer India*

[5] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011 DOI : 10.5121/ijnsa.2011.3518 229Securing DSR Routing Protocol in MANET Based on Cryptographic Authentication Mechanism

[6] A Study of Secure Routing in MANET: various attacks on DSR in MANET.

[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance Vector (DSR) routing," *IETF RFC 3591*, 2003.

[8] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," *Proceedings of the 27th Australasian Computer Science Conference (ACSC)*, vol. 26, no. 1, pp. 47–54, 2004.

[9] Weichao Wang, Yi Lu, Bharat Bhargava, "On Security Study of Two Distance Vector Routing Protocols for Mobile Adhoc Networks", (IEEE) 2003, 0-7695-1893-1/03

[10] Eastlake D, Jones P (2001) US Secure Hash Algorithm (SHA1). RFC 3174.

[11] E. Altman and T. Jimenez, Lecture Notes on NS Simulator for Beginners, December 03, 2003.

[12] The Network Simulator – NS2. (http://www.isi.edu/nsnam/ns/index.html).

AUTHOR'S PROFILE

Meenakshi Jamgade has received her Bachelor of Engineering degree in Computer Science Engineering from Millennium Institute of Technology & Science Bhopal in the year 2013. At present he is pursuing M.Tech. with the specialization of Cyber Security in Kailash Narayan Patidar College of Science and Technology, Bhopal . Her area of interest Networking , Operating System .