Research Paper Engineering

Improvement in Routing for MANET using Double Signature Security Scheme

* Mr. Bhaumik A. Patel ** Prof. Hitesh Ishwardas

* M.E.(CSE) student of S.P.B. Patel Engineering College, GTU, Gujarat, INDIA

* Prof. Hitesh Ishwardas is working with S.P.B. Patel Engineering College, GTU, Gujarat, INDIA

ABSTRACT

In this paper, authors have presented a novel double signature security scheme integrated with existing AODV protocol that improves the security feature of routing in MANET. In MANET, there is infrastructure less environment, open peer-to-peer architecture, shared wireless medium and dynamic topology due to which it is established in insecure environments like disaster sites and military applications. Ad-hoc On-Demand Distance Vector (AODV) is widely used routing protocol. First it is analyzed by its functionality and performance measurements. Then, the different existing security techniques were surveyed to come up with new secure algorithm to integrate with the normal AODV protocol. A scheme of integrating double signature security with normal AODV routing protocol is found capable of handling various attacks. The proposed security scheme was also simulated in the NS2 and it is compared with normal AODV.

Keywords : Classification, Lung Cancer, Lung Cancer dataset, Features.

I. INTRODUCTION

MANET, in which there is no centralized infrastructure to monitor or allocate the resources used by the mobile nodes. Mobile ad hoc networks pose various kinds of security problems, caused by their nature of collaborative and open systems and by limited availability of resources. The absence of any central coordinator makes the routing a complex one compared to cellular networks.

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile devices. AODV uses an on demand approach for finding routes. In survey work we look at AODV in detail, study and analyses various attacks that can be possible on it. Then we look into some existing mechanism for securing AODV protocol. Our proposed work is an extension to the secure AODV protocol extension, which includes double signature strategies aimed at improving normal AODV performance. Here AODV protocol includes secure double signature encryption mechanism aimed at further improving its security with network performance.

We have analyzed secure double signature encryption mechanism that can help in further improvement of security and performance in AODV and also we have compared its performance with normal AODV using simulation in NS2.

II. AODV Routing Protocol

AODV is inherently a distance vector routing protocol that has been optimized for ad-hoc wireless networks. It is an on demand protocol as it finds the routes only when required and is hence also reactive in nature. AODV borrows basic route establishment and maintenance mechanisms from the DSR protocol and hop-to-hop routing vectors from the DSDV protocol. To avoid the problem of routing loops, AODV makes extensive use of sequence numbers in control packets.

When a source node intends communicating with a destination node whose route is not known, it broadcasts a RREQ (Route Request) packet. Each RREQ packet contains an ID, source and the destination node IP addresses and sequence numbers together with a hop count and control flags. The ID field uniquely identifies the RREQ packet; the sequence numbers inform regarding the freshness of control packets and the hop-count maintains the number of nodes between the source and the destination.

When the RREQ packet reaches the destination node a RREP (Route Reply) packet is generated and unicasted back to the source of the RREQ packet. Each RREP packet contains the destination sequence number, the source and the destination IP addresses, route lifetime together with a hop count and control flags. Each intermediate node that receives the RREP packet, increments the hop count, establishes a FORWARD ROUTE to the source of the packet and transmits the packet on the REVERSE ROUTE. For preserving connectivity information, AODV makes use of periodic HELLO messages to detect link breakages to nodes that it considers as its immediate neighbors. In case a link break is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route. Optionally, a Route Reply Acknowledgement (RREP-ACK) message may be sent by the originator of the RREQ to acknowledge the receipt of the RREP.

III. Improving AODV Routing Protocol using Double Signature Security Scheme

Here authors have proposed double signature security scheme to secure AODV messages. This mechanism calculates signature using appropriate encryption algorithm for all the fields of an AODV message. It also calculates signature with secret key and then both signatures will be transmitted along with the AODV messages.

The Proposed Algorithm is as follows:

Step1. In AODV, sender generates the first signature using an encryption algorithm and concate it with each of the AODV messages. It performs the following operations:

- t uses SHA (Secure Hash Algorithm) value to generate signature.
- Sets signature SHA value with the message format.
- Now for specially destination node sender uses secret key to generate another signature and generate the same and also concate it with message.

Step2. When an intermediate node receives a message, it calculates the following calculations to verify the valid message:

- It uses the concated signature to match the newly generated signature by intermediate node and compare it; if it matches then node will forward the message to the next node.
- But before rebroadcasting a message it will check the index of upcoming node to check whether it is destination or not.

Step3. When a destination node receives a message, it will calculate the signature with using secret key for more security purpose and compare it with concated special signature with key.

The proposed secure algorithm fulfills almost all major security requirements. As it generates very less overhead for computation, it saves power consumption of nodes significantly that is most important aspect of the mechanism.

IV. Simulation and Results

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83GHz machine using Ubuntu 12.4.0 with 2 GB RAM and the network simulator NS2 version NS-2.34.

Table.1 is summarized the different configuration values that were used in all the performed simulations.

Parameter	Value
MANET Area	750*750 sq. m.
Total number of nodes	40
Movement Pattern	Non-random
Node Speed	0 up to 20 m/s
Application	Constant Bit Rate (CBR)
No. of generated Packets	10000 packets per CBR
Size of Packet	512 bytes
Simulation Time	200 sec
CBR Traffic	5-15-25-35
Pause Time	0-50-100-150-200

Table 1: General Simulation Parameters

Experiment 1: Packet Delivery Fraction

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

In this experiment, the packet delivery ratio is being measured for the normal AODV and secure encrypted AODV. From the figure.1, 2, 3 and 4 it is clear that when traffic connections are increasing; proposed algorithm has larger PDF value than normal AODV which is really a good result.

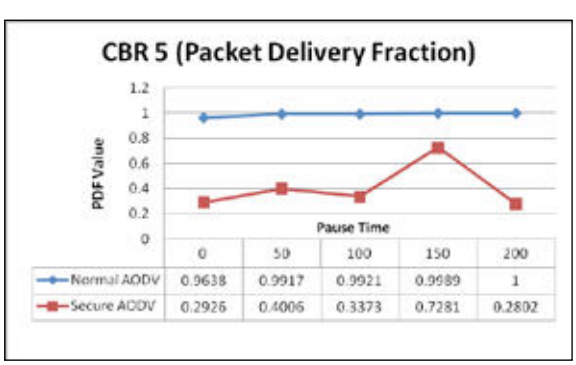

Figure 1: PDF values for CBR traffic 5 at different pause time

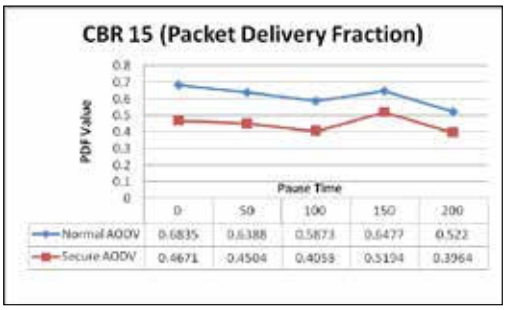

Figure 2: PDF values for CBR traffic 15 at different pause time

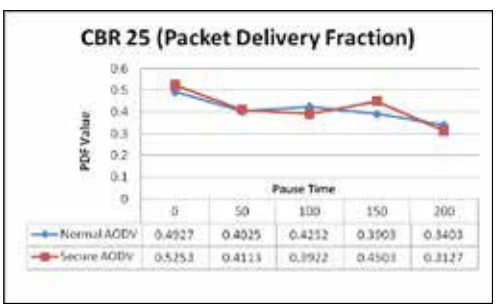

Figure 3: PDF values for CBR traffic 25 at different pause time

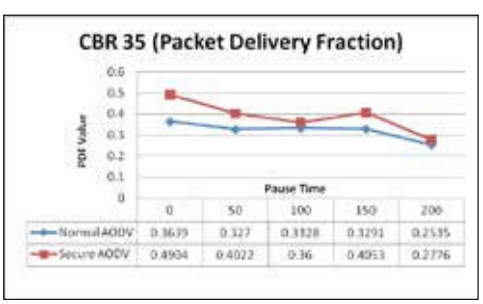

Figure 4: PDF values for CBR traffic 35 at different pause time

Experiment 2: Routing Load

It is the number of routing packets required to be sent per data packet delivered. It is given by routing packets/received packets. In this experiment, the routing load is being measured for the normal AODV and secure encrypted AODV.

Figure. 5, 6, 7 and 8 shows the dramatic fall of RL in secure encrypted AODV. It is also found that secure version of AODV has less routing load than normal AODV. It is also concluded by many researchers that less RL is indication of good performance.

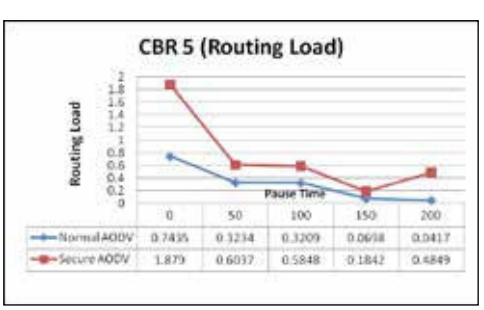

Figure 5: RL values for CBR traffic 5 at different pause time

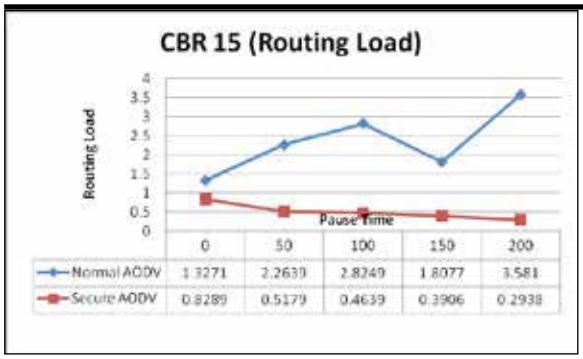

Figure 6: RL values for CBR traffic 15 at different pause time

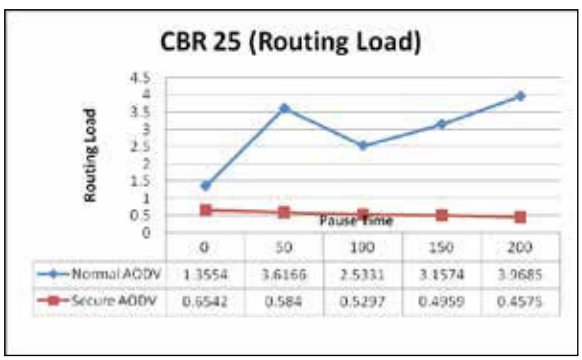

Figure 7: RL values for CBR traffic 25 at different pause time

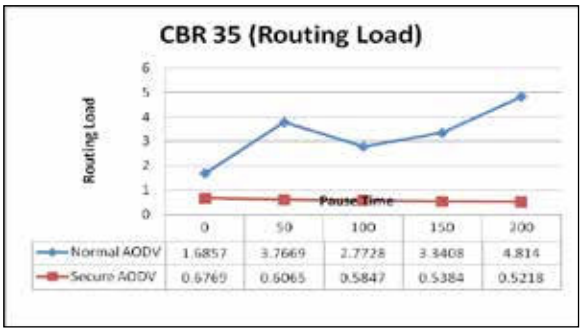

Figure 8: RL values for CBR traffic 35 at different pause time

V. Conclusion

According to the simulations that were performed, the newly proposed security scheme based on double signature security scheme achieves overall good results.

The proposed algorithm also assures that if any malicious node drops invalid messages to the destination between the route intermediated node, it can be easily detected; so proposed security scheme prevents black hole attack also

REFERENCES

[1] Li-Li Pan, "Research and simulation for secure routing protocol based on Ad hoc network", DOI: 10.1109/ICETC.2010.5529947, 2010 | [2] Irshad, A.; Gilani, S.M.; Khurram, S.; Shafiq, M.; Khan, A.W.; Usman, M., "Hash-chain based peer-peer key management and establishment of security associations in MANETS ", DOI: 10.1109/ICIET.2010.5625727, 2010 | [3] Hosseini, F.K., "Dynamically Improve Throughput and Minimize End-to-End Delay in MANET", DOI: 10.1109/MICCCA.2008.4669842, 2008 | [4] Pirzada, McDonald, "Secure Routing with the AODV Protocol" IEEE pp.57-61, 2005 | [5] Junaid Arshad, Mohammad Ajmal Azad, "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", IEEE, pp. 971-975, 2006 | [6] Perkins, Royer, and Das, "Ad-hoc On-demand Distance Vector (AODV) routing", IETF RFC 3591, 2003. | [7] R. Kumar, C. L. Reddy, and P. S. Hiremath, "A Survey of Mobile Ad hoc Network Routing Protocols", Journal of Intelligent System Research, vol. 1, pp. 49-64, Jan.-June, 2008. |