SECURITY ENHANCEMENT OF AODV PROTOCOL FOR MOBILE AD HOC NETWORK

Ms. Darshana Patel*

Ms. Vandana Verma**

Abstract

Here, authors presents a smart encryption algorithm integrated with existing AODV protocol that enhances the security of routing in MANET. Mobile Ad hoc Network's because of maliciousness that intentionally disrupts the network by using variety of attacks and due to routing protocols (e.g. AODV), which were already developed without considering security features to prevent the various kinds of attacks. And also there is infrastructure less environment, and having open peer-to-peer architecture, shared wireless medium and dynamic topology, MANETs are frequently established in insecure environments like disaster sites and military applications. Ad-hoc On-Demand Distance Vector (AODV) is widely used routing protocol. Author's strategy is to choosing one of the secure routing protocols among all according to its effectiveness. It is analyzed by its functionality and performance measurements. Then, the different existing security techniques (e.g. encryption algorithm.) were surveyed so that to come up with new algorithm to integrate with the basic AODV protocol. And fortunately, a scheme of integrating encryption algorithm with basic AODV routing protocol is found capable of handling both unauthorized and malicious nodes' attacks. The proposed security scheme was also simulated in the NS2.

***Keywords*— MANETs, Performance, Routing, Security.**

* M.Tech. student of RCEW, Jaipur, Rajasthan, INDIA.

** working with RCEW, Jaipur, Rajasthan, INDIA.

I. INTRODUCTION

MANET is a set of independent mobile nodes e.g. Laptops, tablets, pda etc. that communicate over relatively bandwidth and power constrained wireless links. My research strategy is to choosing one of the secure routing protocols among all according to its effectiveness, Authors have study it and analyze its functionality and performance measurements. Then, the different existing security techniques (e.g. encryption algorithm.) were surveyed so that to come up with new algorithm to integrate with the basic AODV protocol. And fortunately, a scheme of integrating encryption algorithm with basic AODV routing protocol is found capable of handling both unauthorized and malicious nodes' attacks.

In this work, Authors are presenting their own work with enhancing the security of AODV routing protocol that protects against a number of attacks carried out in packet routing mechanisms for MANETs. Authors would present their encryption algorithm to secure AODV messages which they have implemented on existing AODV protocol in NS-ALLINONE. Here authors are generating signature using their algorithm and concating it with AODV message formats, in addition they have applied encryption to safe the signature of destination node using public key and once again another signature is generated and also concated it along with AODV message formats for more security by various attackers.

II. AODV ROUTING PROTOCOL

AODV is a most widely used protocol and it is based on distance vector routing protocol that has been specially build for MANETs. AODV is an on demand protocol and reactive in nature as it finding the routes only when sender wants to send data. AODV makes widespread use of sequence numbers in control packets to avoid the problem of generation of routing loops. When a source node is interested to communicate with a destination node whose route is unknown for sender, it broadcasts a RREQ (Route Request) packet to all its neighbor nodes. Each RREQ packet contains a Request ID, source and the destination node IP addresses and sequence numbers along with a hop count and flags field in its packet format. The Request ID field uniquely identifies the RREQ packet; By observing sequence number field we can have information regarding how fresh the control packet is? And the hop-count maintains the number of intermediate nodes between the source and the destination. Recipient node of the RREQ

packet that has not find the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count.

When the RREQ packet arrived at the destination node a RREP (Route Reply) packet is generated and sent back to the source. RREP packet contains the destination node sequence number, the source and the destination IP addresses, route lifetime along with a hop count and flags. Intermediate node that receives the RREP packet, increments the hop count field, and it establishes a Forward Route to the source of the packet and transmits the packet on the Reverse Route. When a link failure 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.

III. Enhancing the Security of AODV in Mobile Ad-hoc Network using Encryption Algorithm

MANETs are frequently established in insecure environments like disaster sites and military applications. Ad-hoc On-Demand Distance Vector (AODV) is widely used routing protocol. AODV is based on distance vector routing, but here the updates are shared not on a periodic basis but on an as per on demand basis. For example, battle field ad hoc network, in such a network it would surely be first concerned with the efficient and in time delivery of the message but with this, we will have to be more concerned about the strong secrecy of the information also. These kinds of scenarios, where we want to transmit private and secure information very rapidly, motivate authors to make use of encryption algorithm with public key for security context. In this paper, author considers the advantage of encryption algorithm with public key to hide the information of all the fields of message by using an encryption algorithm.

Enhancing the Security of AODV in Mobile Ad-hoc Network using Encryption Algorithm

Here author have proposed an encryption algorithm with public key used 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 public key and then both signatures will be transmitted along with the AODV messages.

The Proposed Encryption Algorithm as follows:

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

- It uses secure hash algorithm (SHA) value to generate signature.
- Sets signature SHA value with the message format.
- Now for specially destination node sender uses public key to generate another signature and generate the same and also concate it with message.

2. Afterwards, each time an intermediate node receives sent message, it calculates the following calculations to verify the genuine 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.

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

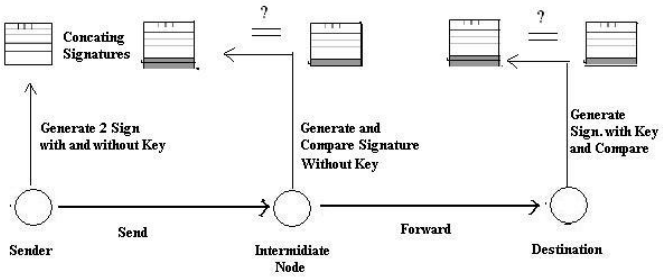


Figure 1: The proposed encryption scheme

The proposed scheme is explained using fig.1 and it fulfills all 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

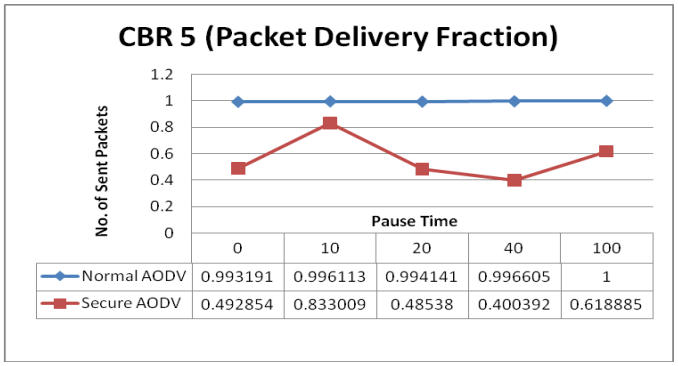
All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83GHz machine using Ubuntu 12.4.0 with 2 GB RAM and the network simulator NS2 version NS-2.34. Table.1 is summarized the different configuration values that were used in all the performed simulations.

Parameter	Value
MANET Area	500*500 sq. m.
Total number of nodes	25
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	100 sec
CBR Traffic	5-10-15-20
Pause Time	0-10-20-40-100

Table 1: General Simulation Parameters

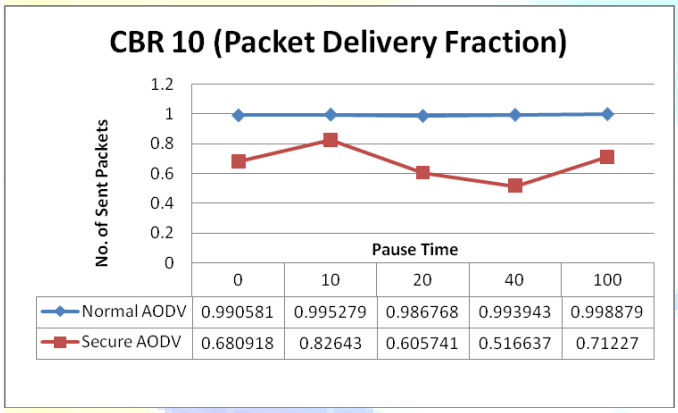
Experiment 1: Packet Delivery Fraction

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.



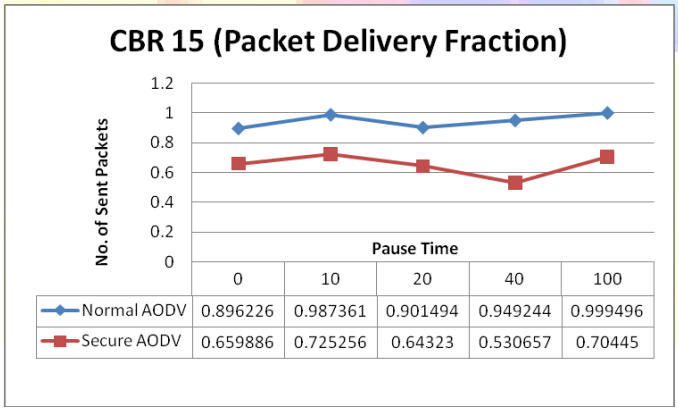
	0	10	20	40	100
Normal AODV	0.993191	0.996113	0.994141	0.996605	1
Secure AODV	0.492854	0.833009	0.48538	0.400392	0.618885

Figure 2: PDF values for CBR traffic 5 at different pause time



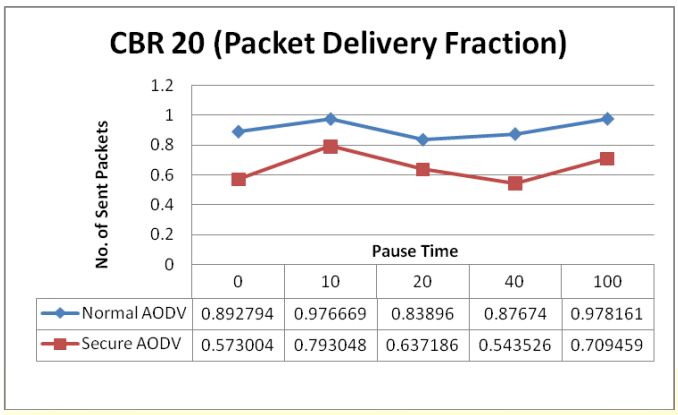
	0	10	20	40	100
Normal AODV	0.990581	0.995279	0.986768	0.993943	0.998879
Secure AODV	0.680918	0.82643	0.605741	0.516637	0.71227

Figure 3: PDF values for CBR traffic 10 at different pause time



	0	10	20	40	100
Normal AODV	0.896226	0.987361	0.901494	0.949244	0.999496
Secure AODV	0.659886	0.725256	0.64323	0.530657	0.70445

Figure 4: PDF values for CBR traffic 15 at different pause time



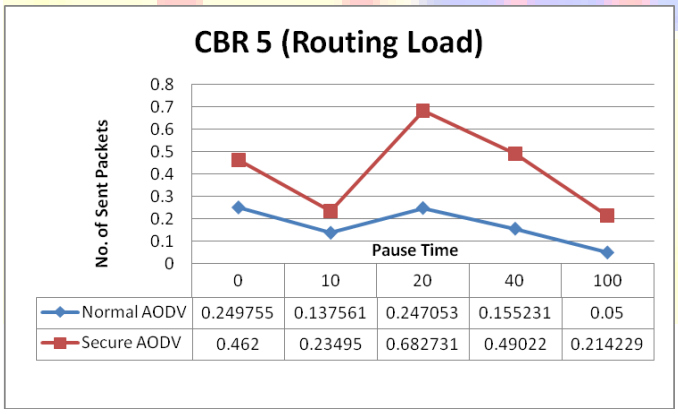
	0	10	20	40	100
Normal AODV	0.892794	0.976669	0.83896	0.87674	0.978161
Secure AODV	0.573004	0.793048	0.637186	0.543526	0.709459

Figure 5: PDF values for CBR traffic 20 at different pause time

In this experiment, the packet delivery ratio is being measured for the normal AODV and secure encrypted AODV. From the figure.2, 3, 4 and 5, it is clear that addition of security has not much effect (in fact good effect) on the efficient working of the MANET.

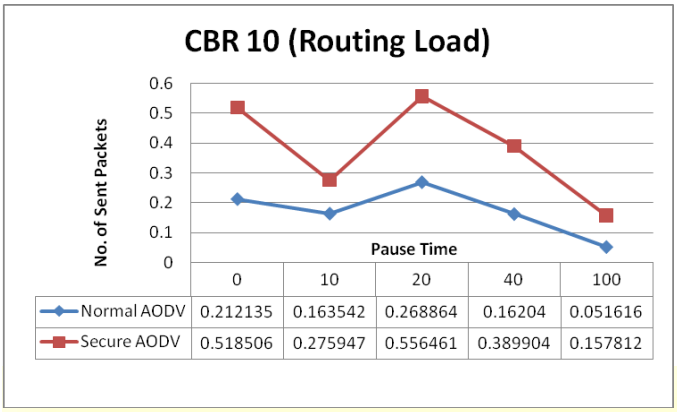
Experiment 2: Routing Load

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.



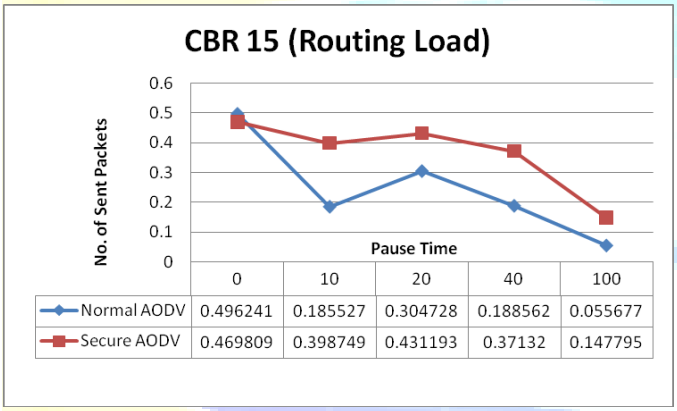
	0	10	20	40	100
Normal AODV	0.249755	0.137561	0.247053	0.155231	0.05
Secure AODV	0.462	0.23495	0.682731	0.49022	0.214229

Figure 6: RL values for CBR traffic 5 at different pause time



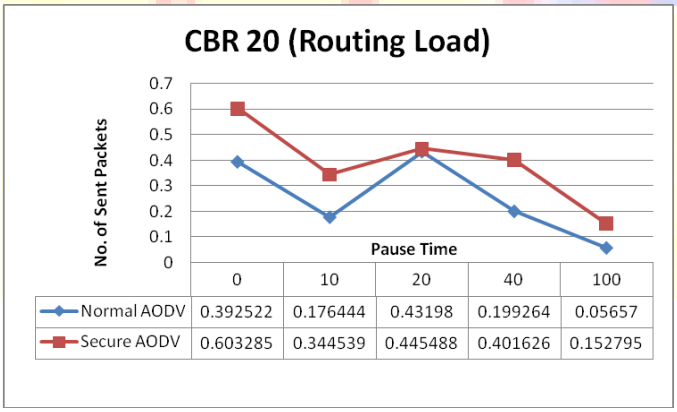
	0	10	20	40	100
Normal AODV	0.212135	0.163542	0.268864	0.16204	0.051616
Secure AODV	0.518506	0.275947	0.556461	0.389904	0.157812

Figure 7: RL values for CBR traffic 10 at different pause time



	0	10	20	40	100
Normal AODV	0.496241	0.185527	0.304728	0.188562	0.055677
Secure AODV	0.469809	0.398749	0.431193	0.37132	0.147795

Figure 8: RL values for CBR traffic 15 at different pause time



	0	10	20	40	100
Normal AODV	0.392522	0.176444	0.43198	0.199264	0.05657
Secure AODV	0.603285	0.344539	0.445488	0.401626	0.152795

Figure 9: RL values for CBR traffic 20 at different pause time

Figure. 6, 7, 8 and 9 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.

V. CONCLUSION

The proposed security scheme based on encryption algorithm defies various attacks possible in MANETs and satisfies the almost all the security requirements in routing protocol with using central authority and key management scheme which makes it more easily expandable and less complex in computation. As it generates very less overhead of calculations it saves power consumption of nodes significantly. According to the simulations that were performed, the newly proposed security scheme based on encryption algorithm, built on top of normal AODV routing protocol, achieves an overall good results.

The proposed encryption 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 message dropping attacks which very crucial to prevent. Thus, the proposed scheme proves to be more efficient and less power consuming in securing AODV routing protocol in defending against various attacks on AODV.

REFERENCES

[1] Vaidya, B.; Makrakis, D.; Mouftah, H. "*Provisioning secure on-demand routing protocol in mobile ad hoc network*" IEEE DOI: 10.1109/ AHICI.2011 .6113952, 2011

[2] Li-Li Pan, "*Research and simulation for secure routing protocol based on Ad hoc network*", DOI: 10.1109/ICETC.2010.5529947, 2010

[3] 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

[4] Hosseini, F.K., "*Dynamically Improve Throughput and Minimize End-to-End Delay in MANET*", DOI: 10.1109/MICCCA.2008.4669842, 2008

[5] Pirzada, McDonald, "*Secure Routing with the AODV Protocol*" IEEE pp.57-61, 2005

[6] Junaid Arshad, Mohammad Ajmal Azad, "*Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks*", IEEE, pp. 971-975, 2006

[7] Perkins, Royer, and Das, "Ad-*hoc On-demand Distance Vector (AODV) routing*", IETF RFC 3591, 2003.

[8] 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.

[9] L. Layuan, Y. Peiyan, and L. Chunlin, *"Performance evaluation and simulations of routing protocols in Ad hoc networks,"* Computer Communications, vol. 30, pp. 1890-1998, 2007.