Design and Implementation of Secure LAR Routing Protocol in MANETs

Y.V.S.Sai Pragathi[#1], S.P.Setty[#2]

[#1]*Associate Professor, Stanley College of Eng. & Tech. for Women, Osmania University, Hyderabad, Telangana, India*

[#2]*Professor, Andhra University, Vishakhapatnam, Andhra Pradesh, India*

***Abstract* —** *MANET is a collection of mobile nodes connected by wireless links without infrastructure. Due to inherent properties of MANETs like limited resources, dynamic topology, wireless medium, the possibility of attacks is more. So, there is a need for provisioning of security in Manets. Different cryptographic algorithms are investigated and Secure LAR is designed. From the results it is found that Secure LAR(S-LAR) with ECC provides security with minimum energy consumption.*

Keywords — *MANETs, LAR, ECC, RSA, Secure LAR, NS2, Encryption Algorithms.*

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure [1][2]. Location aided routing is one of the routing protocol where a source node estimates the current location range of the destination node based on last reported location information [3][4][5]. During the route discovery process, the route request messages are flooded in limited region known as expected zone which is expected to have the current location of the destination node.

The rest of the paper is organized as follows: Related work is discussed in section II, reactive routing protocol "LAR" is illustrated in section III, Cryptographic algorithms are discussed in section III-B, S-LAR is summarized in section IV, simulation environment is summarized in section VI, and results are presented in section VI and finally concluded with section VII.

.

II. LITERATURE REVIEW OF RELATED WORK

Vasil Hnatyshin, et al., in their paper "A Comparative study of Location aided routing protocols for MANET", examined and compared through simulation, the performance of AODV, LAR, and Geo AODV protocols under different environmental settings.

M.Uma and Dr.G.Padmavathi "A comparative study and performance evaluation of reactive quality of service routing protocols in mobile ad hoc networks" studied a comparison and performance evaluation of three reactive routing protocols AODV, DSR and LAR1 are done using qual net simulator to identify the protocol that is best suited for MANETs [6]. P.Channa Reddy et al., have analysed performance of Ad hoc network protocols in their paper and their results indicated that reactive routing protocols are more suitable for ad hoc networks [7].

III. ROUTING PROTOCOLS

A. LAR

The entire The Location-Aided Routing (LAR) protocol is a reactive routing protocol that utilizes geographical coordinates to direct route request messages to the previously known location of the destination. The protocol defines two areas: the expected zone and the request zone. The expected zone is the area in which the destination is most likely to be discovered. To calculate this area, the source must know a previous location of the destination at time t0, as well as an estimate of the velocity, v, at which the destination was travelling at t0. If the current time is t1, the expected zone can be calculated as a circle of radius v(t1 – t0) centred at D. The request zone is the area in which the route request for the destination should propagate. In order to have the greatest probability of finding the destination, the request zone is defined to be the smallest rectangle that contains both the expected zone and the source node.

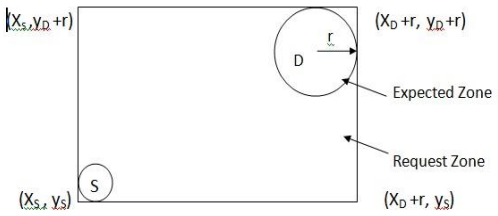

Fig. 1 LAR Request Zone

The route discovery procedure of LAR is when a source needs a route to a destination; it creates a route request (RREQ) message for that destination. If the source recently had a route to the destination, then the source calculates the expected zone and the request zone, and places the coordinates of the request zone boundary into the RREQ message. The node first determines whether it lies in the request zone defined in the RREQ. Because every node knows its current geographical coordinates, it can

easily make this determination. If the node does not lie within the request zone, then it does not process the packet. Otherwise, if it does lie within the request zone, it processes the packet and either rebroadcasts it or sends a reply, depending on whether it has a current route to the destination.

B. Cryptographic algorithms

RSA algorithm is one of the most popular and secure public-key encryption techniques. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers [8].

ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curve cryptography can obtain the same security as RSA with shorter keys and more efficient implementations [9].

IV. SECURE LAR

Secure Location aided routing protocol (S-LAR) has implemented ECC cryptography. It is observed that the energy consumption has been increased due to the increase in the control overhead.

```
LARPacketProcessor( LARRecievedPKT)
{
        IF( RecievedPKT == RouteRequestPKT)
        {
                IF( CurNodeID == DestID )
                {
                        Create ACK PKT
                        Free Current PKT
                }
                ELSE IF( In-Forwarding Zone )
                {
                        Update Route Table
                        Re-broadcast Packet
                }
                ELSE
                {
                        Drop Packet
                }
        }
        ELSE IF ( RecievedPKT == AckPKT )
        {
                IF( CurNodeID == SrcID )
                {
                        UpdateRouteTable
                        EncryptPath
                        Clear the Pending List of Packets
                }
        }
        ELSE IF ( RecievedPKT == DataPKT )
        {
                IF( CurNodeID == DestID )
                {
                        Decrypt Data
                        Dump Data
                        Free Data Packet
                }
                ELSE
                {
                        Decrypt Route
                        Send Data PKT DownStream
                }
        }
}

LARSendData( SrcID, DestID)
{
        IF ( No Route Found to DestID )
        {
                Create a Route Request ( LARPkt )
        }
        ELSE IF ( Route Request Initiated )
        {
                Add to the Pending List ( SRCID, DestID )
        }
        ELSE
        {
                Encrypt Route PATH
                Send Data ( LARPkt )
        }
}
```

Fig. 2 Pseudo code for Secure LAR Algorithm

V. RESEARCH METHODOLOGY

To evaluate the designs proposed in this paper, an effort is made to choose the most suitable evaluation methodology. Three evaluation methodologies are identified as simulation, experimental and mathematical. Of these three methods, Simulation method is chosen for the present study, as experimental method is not practicable, while mathematical method is highly restrictive.

VI. SIMULATION

NS-2 is an open simulation environment for computer networking research that is preferred in the research community. It is aligned with the simulation needs of modern networking research. It encourages community contribution, peer review, and validation of the software [10].

TABLE I
NS2 SIMULATION PARAMETERS

Simulation Parameters	Values
No. of Nodes	20,27,65,87,100
Area Size	200x200,500x500, 750x750,1000x1000
Routing Protocol	LAR, S-LAR
Simulation Time	1000 Sec
Propagation Model	Two Ray
Packet Size	512
Mobility Model	Random Way Point
Speed	5 m/s
Range	586,775,803,816,981,985,997,999

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

1) Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully to the total number of secure packets transmitted at each node.

2) Average Energy Consumed: Total energy consumed by all the nodes to the number of nodes.

3) Throughput: Total bytes received to the total bytes transmitted.

4) Overhead: Total protocol control bytes to the total data bytes transmitted.

5) Average End to end Delay: Average time take for the secure packets from send time to received time at the target node.

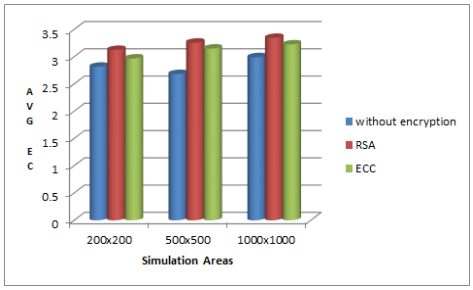

Fig. 3 Average Energy consumption for LAR, S-LAR with RSA and S-LAR with ECC in different sizes of simulation areas.

It is observed that ECC gives better energy saving than RSA by 5%.

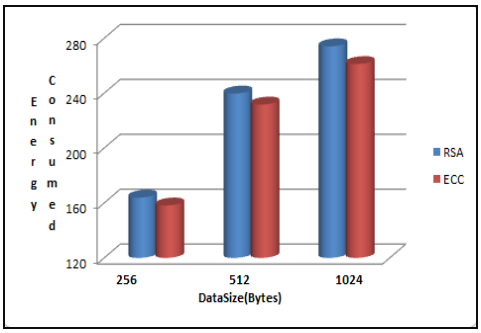

Fig. 4 shows the comparison of Energy consumed for RSA and ECC with different data sizes.

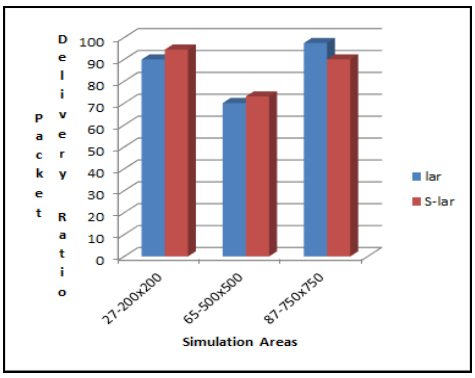

Fig.5 Comparison of PDR for LAR and S-LAR.

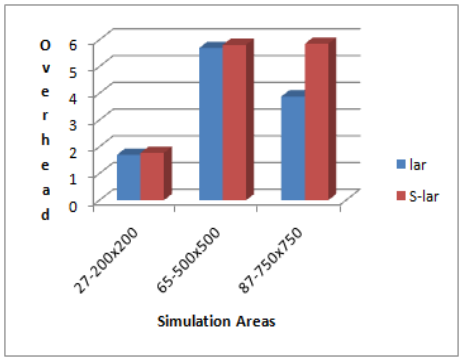

Fig. 6 Comparison of Overhead for LAR and S-LAR.

Overhead increases for S-LAR due to addition of security layer. It is observed average 2% increase in overhead due to security layer.

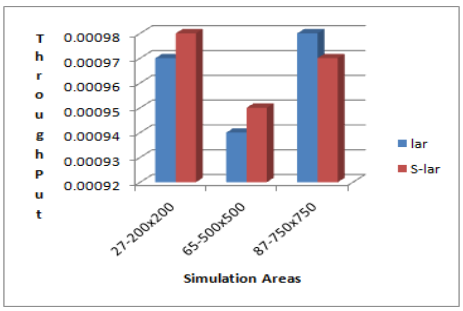

Fig. 7 shows the throughput comparison for LAR and S-LAR.

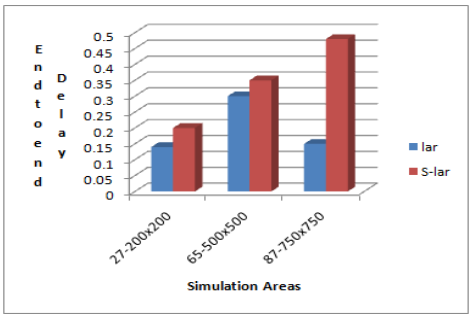

Fig. 8 shows End to End delay comparison for LAR and S-LAR.

End to end delay increases due to addition of security layer by S-LAR.

VII. CONCLUSIONS

From the Simulation results it is concluded that there is saving of energy by 5% with ECC compared to RSA. Further work can be done on optimizing the Energy consumption and End to End delay of S-LAR with soft computing techniques like Fuzzy and Artificial Neural Networks.

REFERENCES

[1] S.Giordan and W.W.Lu, "Challenges in mobile ad hoc networking", *IEEE Communications Magazine*, vol.39, no.6,pp. 129-181, June 2001.

[2] Book: Silvia Giordano, Stefano Basagni, Marco Conti and Ivan Stojmenovic, *Mobile adhoc networking*, Pg.no 286.

[3] Y.Ko and N.H.Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," in *Proc. of the ACM/ IEEE International Conference on Mobile Computing and Networking (Mobicom*), 1998, pp. 66–75.

[4] Vasil Hnatyshin and Malik Ahmed "A comparative study of location aided routing protocols for MANET", *IEEE*, 978-1-4577-2028-4/11 2011.

[5] Y.V.S.Sai Pragathi and S.P. Setty, "Hybrid anonymous location-aided routing protocol for privacy preserving and authentication in manet", *Journal of Theoretical and Applied Information Technology*, Vol.55, No.2, Sep.2013.

[6] M.Uma and Dr.G.Padmavathi, "A comparative study and performance evaluation of reactive quality of service routing protocols in mobile ad hoc networks" *JATIT*, Vol.6, No.2, 2009

[7] P.ChannaReddy, "Performance Analysis of Ad hoc network routing protocols, *IEEE 2006*", 1-4244-0731-1/06.

[8] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[9] https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[10] Network Simulator -2, http://www.isi.edu/nsnam/ns/.