International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Security for enhancing routing mechanism in Mobile Ad-hoc Network with Elliptic curve algorithm

[1] *Mrunali Meshram ,Electronics and tele-communication , D.Y.Patil college of engg. Akurdi Pune, Maharashtra , India*
[2] *Sayali N. Mane, Electronics and tele-communication , D.Y.Patil college of engg. Akurdi Pune, Maharashtra , India*

Abstract – Security is considered to be an important issue in any wireless network. Many protocols are being designed for providing security in mobile ad-hoc network to protect the data or network from various threads and attacks. Another important factor for ad-hoc network is path optimization with less delay and energy consumption. In this paper, along with security path is optimized based on minimum delay and link quality of ad-hoc network. For optimizing path, Adaptive Node Stability (ANS) mechanism is used which makes the routing strategy in the network. Estimation of path is based on the delay, link quality and energy of the neighboring nodes that are closer to each other. Thus, ANS helps to select the efficient path from source to destination. Security is being provided by Secure Elliptic Curve Routing Algorithm (SECRA) which consumes less energy and provides greater security over the network. NS2 simulator shows the comparison of proposed and existing protocol such as AODV and DECRP present in the network.

Keywords— Mobile Ad-Hoc Network; Delay; Link Quality; Secure Elliptic Curve Routing Algorithm

1. Introduction

Ad-hoc network consist of mobile nodes without the requirement of any centralized access point or existing structure. Ad-hoc network is wireless network which has ability to establish network anytime and anywhere. Security in ad-hoc network has become more challenging task for researchers. Security must be provided in ad-hoc network, thus to provide security in this network various routing protocols has been introduced. Due to repetitive changes in route several problems occur while implementing ad-hoc networks owing to the mobility of the nodes and intrusion between nodes. The high packet loss rates and recurrent topological changes lead to unbalanced transport layer and constrained amount of traffic being carried out by the network. The three eminent problems in ad-hoc networks are the lack of constant packet delivery due to the intrusion and movement of nodes, incomplete bandwidth owing limitations to channel and restrained node life span causes an outcome of small battery size. A major challenge in mobile ad-hoc network is to maximize data packet delivery in rapidly changing network topology without obtaining excess of energy [1].

In recent years, several routing protocols have been proposed for mobile ad-hoc network in [1] and [3]. QoS is considered to be an important factor for designing a network. Thus, S.Venkatasubramanian and Dr. N.P. Gopalan introduced a QoS-based Robust Multipath Routing (QRMR) protocol for mobile ad hoc networks which is used to allot weights to individual links depending on the metrics quality of link, channel and delay. The selection of the proportion of traffic to be routed to each neighbor is made to perform routing such that the weight of the node is a possibly minimum. But TORA simulations are not carried out successfully in this paper.

Geeta jayakumar and Gopinath ganapathy introduced that AODV and DSR use reactive On-demand routing strategy. AODV and DSR both perform better under high mobility simulations. High mobility results in frequent link failures and the overhead involved in updating all the nodes with the new routing information as in DSDV is much more than AODV and DSR where the routes are created when required. The poor performances of DSR are mainly attributed to aggressive use of caching and lack of any mechanism expire stale routes or determine the freshness of routes when multiple choices are available. DSR is more effective for lower loads while AODV is more effective for higher loads in [4].

Monitoring node selection with high battery is considered by Marjan Kuchaki Rafsanjani in [5]. To exchange information between the nodes, the nonreactive technique for authentication is applied. As several tasks are performed by monitoring nodes more energy is consumed. Secured Reliable Multipath Routing Protocol

(SRMRP) using Distributed Trust Computation and Carrier Sense Multiple Access with Collision Intimation for Distributed Heterogeneous Mobile Ad-hoc Networks is given in [6]. As compared to other protocols it achieves better performance than existing protocol. Slow detection and periodic exchange does not perform well in hybrid and proactive dynamic topologies.

Arafat S. M. Qaed and T Devi proposed a novel delay and energy conscious routing approach is based on ant colony optimization. The estimated delay and residual energy of the nearby nodes, "Delay and Energy Conscious Routing Protocol (DECRP)" finds the efficient node and sends the data packets through that node. In simulation results it is proved that DECRP reduces delay and energy consumption and increases packet delivery ratio than that of the "Ad-hoc on Demand Distance Vector (AODV)" in [9]. Link quality, delay and energy conscious routing approach based on ant colony optimization and estimated link quality, delay and residual energy of the nodes which are close to each other. Adaptive node stability (ANS) mechanism is mathematically modeled to make the routing strategy. LQDEARP selects the efficient node based on the ANS mechanism and sends the data packets through that node. Simulation results shows that LQDEARP reduces delay and energy consumption and increases packet delivery ratio than that of the AODV and DECRP protocol but they does not provide security while sending data through the network. Data is sent to destination at higher risk in [10].

This paper uses the idea from [9] [10] and introduces secured routing mechanism to provide security in mobile ad-hoc network and determine a solution for the problems related to ad-hoc network. For providing security several parameters such as link quality, delay, and energy aware routing are considered. Adaptive node stability mechanism is used to make the routing strategy and to estimate the nearby nodes based on estimation of respective parameters. This secured routing protocol is used to prevent the network from various attacks. This routing protocol selects the efficient node and sends the packet through that node which is based on adaptive node stability mechanism. Use of secured routing protocol with security algorithm makes the transmission more secure [2]. Secured transmission over ad-hoc network provides security using elliptic curve routing Algorithm. The encryption and decryption mechanisms present in this algorithm are used to achieve higher security.

2. Estimation of link quality, delay and residual energy

Secured routing protocol is on demand unipath routing protocol. This protocol takes the various features of AODV and estimates certain parameters such as link quality, delay and cost for selecting the path towards destination node. It first estimates link quality based on signal strength and then estimates the cost and delay. If more than one node has same mobility then node having least delay and energy is selected.

2.1. Estimating link quality:

As nodes are mobile and route is about to break in mobile ad-hoc network it is necessary to consider quality of link in the network. This information which is identified by the physical layer is sent to the upper layer when packets are received from a node and then indicate that node is in less link eminent zone [9]. Less link-eminent zone is the region where the signal strength is weaker which leads to the link failure. Thus, using the received signal strength from physical layer, the quality of the link is predicted and then the links which are having low signal strength will be discarded from the route selection.

When a sending node broadcasts RTS packet, it piggybacks its transmission power. While receiving the RTS packet, the projected node quantifies the strength of the signal received [10].

$$\left.\begin{aligned} \mathrm{Pwr}_{\mathrm{Rvr}} &= \mathrm{Pwr}_{\mathrm{Ttr}}(\lambda / 4\prod \mathrm{d})^2 * (\mathrm{AUG}_{\mathrm{T}}) * (\mathrm{AUG}_{\mathrm{R}}) \\ \mathrm{Lq} &= \mathrm{Pwr}_{\mathrm{Rvr}} \end{aligned}\right\}$$

where, $\mathrm{Pwr}_{\mathrm{Rvr}}$ is power of receiving node, $\mathrm{Pwr}_{\mathrm{Ttr}}$ refers power of transmitting node, λ stands for wavelength carrier, d is distance between sending and receiving node, $\mathrm{AUG}_{\mathrm{T}}$ is average unity gain of omni-directional transmitting antenna, $\mathrm{AUG}_{\mathrm{R}}$ is average unity gain of omni-directional receiving antenna.

2.2. Estimating delay:

For path optimization, delay estimation is important. The data packets or RREQ packets arrive the buffer with passion distribution referred by λ. Hence the delay of node is calculated as

$$\mathrm{Delay} = \frac{\lambda T_2}{2(1-\sigma)} + T_1 \qquad (2)$$

Here, λ is the arriving rate of data packets to the buffer. T_1 is the mean service time required to transfer a data packet with success (which also includes retransmission delays). σ is the rate occupation which is equal to λT_1. T_2 is the second moment of service time distribution [10].

2.3. Estimating residual energy:

The information about the residual energy of the neighbor nodes is stored by every node throughout requesting the other nodes about their residual energies. The residual energies at a node is calculated as

$$\begin{pmatrix} \text{Re}\,sidual \\ energy \end{pmatrix} = \begin{pmatrix} Initial \\ energy \end{pmatrix} - \begin{pmatrix} Consumed \\ energy \end{pmatrix} \quad (3)$$

2.4. Adaptive Node Stability (ANS) mechanism:

By estimating the three parameters adaptive node stability is calculated in equation 4. The node with ANS is selected and link is established

$$\text{ANS} = \max\left(LQ\left[\text{energy} * \left(\frac{1}{delay} \right) \right] \right) \quad (4)$$

3. Proposed routing protocol:

3.1. Secure elliptic curve routing algorithm:

Elliptic curve in MANET is used to provide higher security with smaller key size and less energy consumption. Smaller key size is sufficient to provide more security in message.

A. Encryption:

In encryption process, the algorithm consists of combination of public key infrastructure for hybrid system and elliptic curve algorithm for confusion and diffusion operations as shown. The proposed encryption algorithm is shown in Figure 1. Hexadecimal numbers which is being used is arranged in the form of matrixes i.e. 8*8 in public position. Elliptic curve algorithm helps to generate a private position based to the secrete value from public key.1024 bits are divided into two parts of 512 bits . The last step is inserting the key inside the Cipher data based on the private position.

B. Elliptic Curve Security Algorithm:

SECRA Key Generation: An entity M key pair is associated with a particular set of EC domain parameters such as key k, secure key s, public key p and data to be secured is considered.

1. Select a random integer d in the interval [1, n- 1].

2. Compute Q = dp.

3. M's public key is p, M's private key is s.

Algorithm:

The elliptic curve algorithm shows the process which describes security using public and private key. This algorithm is described in following steps:

- Public position of A, B, C, D taken.
- Public key infrastructure is given to generate secrete key value
- The secrete key of value is been considered as S[0,....,2r+3]
- Certain value of B and D is taken with addition of secrete key i.e.
  B = B + S [0] and D = D + S [1]

Algorithm is performed such that after addition of secrete key there will be data generated at private position is (B, C, D, A) which is equal to the data generated at public position.

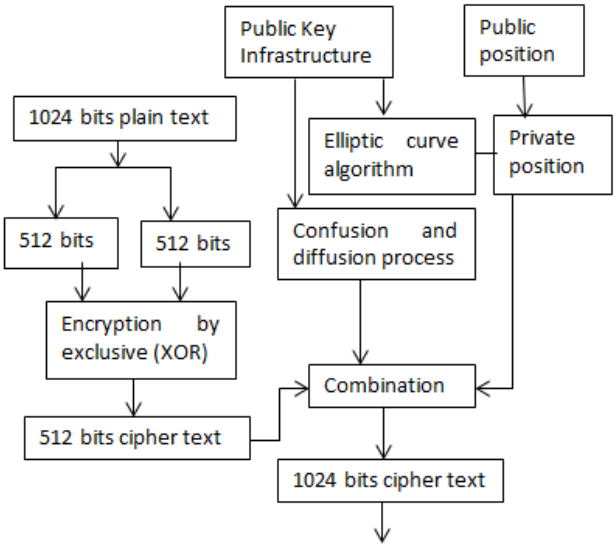

Fig1: Encryption Process

A. Decryption:

Exactly reverse of the encryption is the decryption process. Figure 2 describes the proposed decryption algorithm consists of vice versa of elliptic curve

algorithm. This decryption process involves converting the encrypted data back to its original form which can be understand by the receiver. Same as that of process at the beginning of encryption at the start, decryption process is described at the sender side to generate the same private position at the receiver side to eliminate the key from the cipher text.

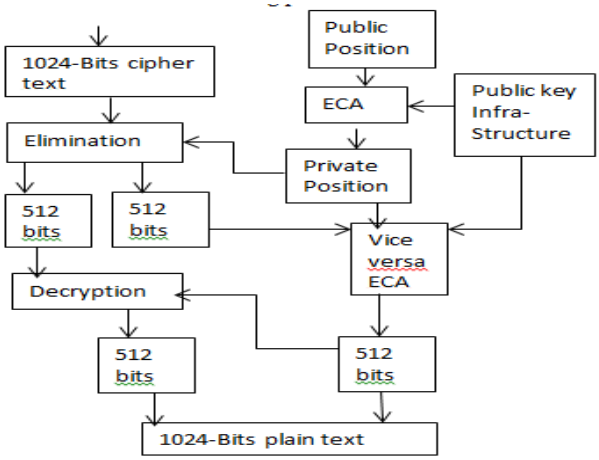

Fig2: Decryption Process

4. Simulation results:

NS2 is used to simulate proposed protocol. The channel capacity of mobile host is set to 2Mbps. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In simulation, 50 to 200 mobile nodes move in a 1000 meters x 1000 meters rectangular region for 100 seconds simulation time. Here it is assume that simulation each node move independently at the same average speed. All nodes have the same transmission range of 250 meters. Simulation setting parameters are described in table1.

Table1: Simulation parameters

No. of Nodes	50, 75, 100, 125, 150 and 200
Area Size	1000m x 1000m
MAC	802.11b
Radio Range	250 meters
Traffic Source	CBR
Mobility Model	Random Waypoint
	Model

Performance metrics are calculated between numbers of nodes and routing overhead, delay, packet delivery ratio and average energy consumption are shown in figures. Fig. 3 shows that the packet delivery ratio is constant from 50 to 75 nodes. The security mechanism will take some more additional number of packets for encryption and decryption of data sent over the ad-hoc network. It slightly decreases due to complexity of proposed mechanism.

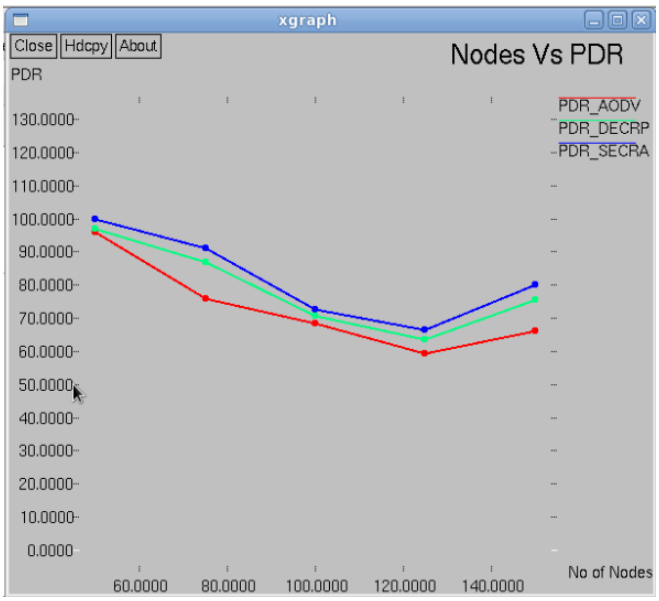

Fig3: Number of Nodes vs Packet Delivery Ratio

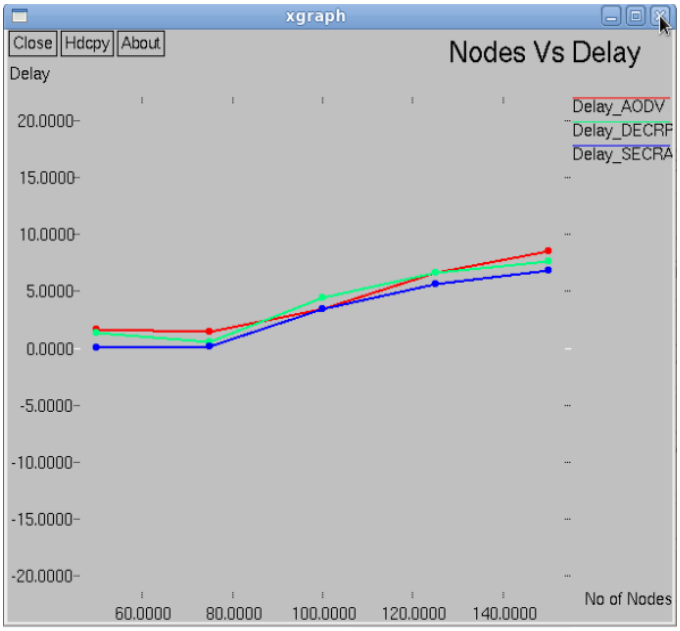

Fig4: Number of Nodes vs Delay (sec)

Fig.4 delay slightly gets increased after 75 nodes and eventually decreases as there is increase in number of nodes in the network. These changes occur because of security algorithm and it performs better than AODV.

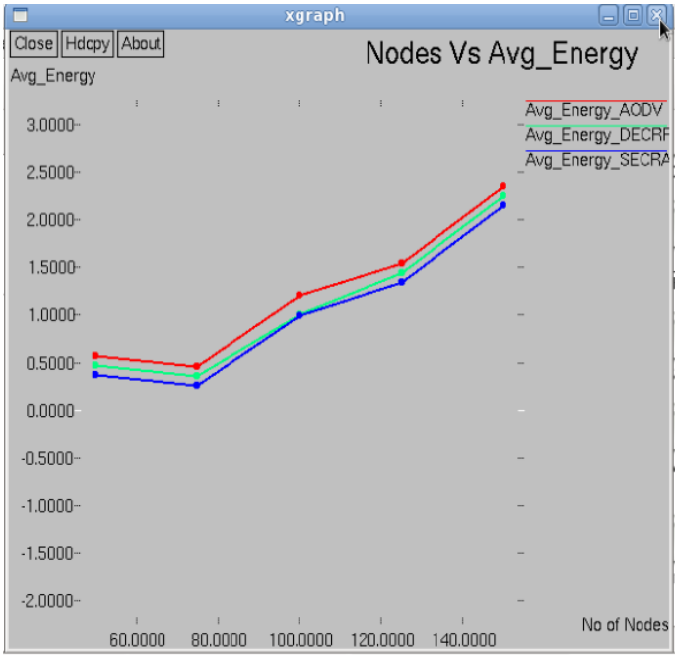

Fig5: Number of Nodes vs average energy

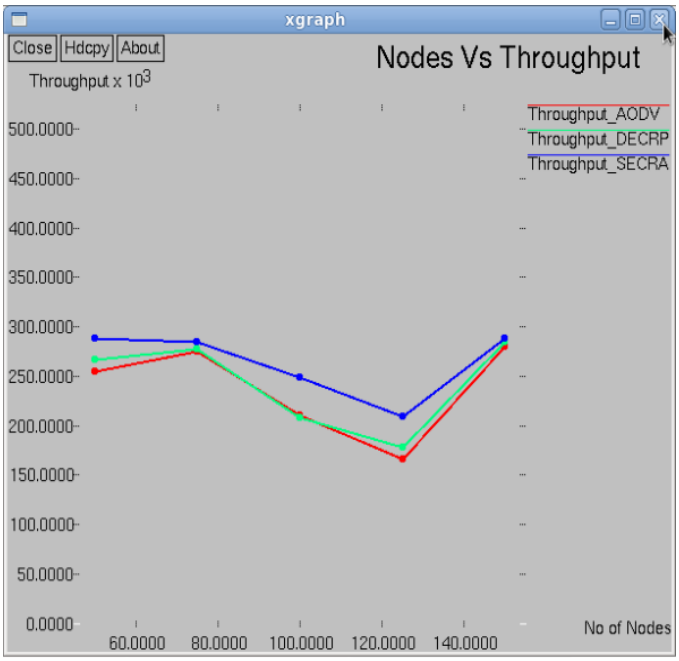

Fig6: Number of Nodes vs throughput

Fig. 5 shows that energy consumption increases but after 120 nodes it start decreasing. The comparison graphs shown specify that proposed routing protocol performs better as compared to AODV by providing security in the network. Fig. 6 shows the throughput performance maximum the throughput maximum the performance of the network. Here, the throughput gets slightly decrease for 120 nodes but as the no of nodes increases it again gets increased but as compared to other protocol it achieves maximum throughput than the others.

5. CONCLUSION

This paper presents secured ad-hoc routing algorithm based on adaptive node stability mechanism. By estimating the parameters such as link quality, delay and energy of nearby nodes secured routing protocol finds the efficient node between the neighboring nodes so that the data packets can be send over that node. Also, elliptic curve algorithm is used in this paper which provides secure transmission in the network. The performance graph shows that as the number of nodes increases drastic changes occurs due to security mechanism. As compared to other protocols proposed SECRA performs better by achieving security.

REFERENCES

[1] Xiaobing Hou and David Tipper, "Impact of Failures on Routing in Mobile Ad-hoc Networks Using DSR", IEEE Journal on Selected Areas in Communications vol. 8, no. 9, pp. 1696-1708, 1990.

[2] Charles E.Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing", IEEE Workshop on Mobile Computing Systems and Applications, vol.4, pp-90-100, 1999.

[3] S.Venkatasubramanian and Dr. N.P. Gopalan, "A QoS based robust Multipath Routing Protocol for Mobile Ad-hoc Networks", IACSIT International Journal of Engineering and Technology, vol.1, pp-391-396, 2009.

[4] Geetha Jayakumar and Gopinath Ganapathy, "Performance Comparison of Mobile Ad-hoc Network Routing Protocol", International Journal on Computer Science and Network Security, vol. 7, pp-77-84, 2007.

[5] Marjan Kuchaki Rafsanjani et al, "Identifying Monitoring Nodes with Selection of Authorized Nodes in

Mobile Ad Hoc Networks", World Applied Sciences Journal vol.4, pp-444-449, 2008.

[6] B Narasimhan, R Vadivel, "Secured Reliable Multipath Routing Protocol (SRMRP) using Trust Computation and Carrier Sense Multiple Access with Collision Intimation (CSMA/CI) for Heterogeneous IP-based Mobile Ad-hoc Networks", International Journal of Computer Applications, vol. 60, pp:12-16, 2012.

[7] Ms. Reshna Wilson A, Mr. Biju Balakrishnan, "Securing Location and trust extended authentication in mobile ad hoc network" International Journal of Innovative Research in Computer and Communication Engineering, vol.2, special issue 1, pp: 4103 – 4108, 2013.

[8] Jianbo Xue, Patrick Stuedi and Gustavo Alonso, "ASAP: An Adaptive QoS Protocol for Mobile Ad Hoc Networks", 14th IEEE proceedings on Personal, Indoor and Mobile Radio Communications, vol. 3, pp: 2616- 2620, 2003.

[9] Arafat S. M. Qaed and T Devi, "Ant Colony Optimization based Delay and Energy Conscious Routing Protocol for Mobile Ad hoc Networks", International Journal of Computer Applications, vol. 41, pp:1-5,2012.

[10] Arafat S.M. Qaed and T Devi, "Link Quality, delay and energy Aware Routing Protocol (LQDEARP) for Mobile AD HOC Networks", International Journal of Computer and Communication Technology, vol. 4, pp: 49-54, 2013.

BIOGRAPHIES

Mrunali Meshram received B.E degree from of electronics and telecommunication branch in 2012 and M.E. degree from university of Pune. I m student of last year of college D.Y.Patil college of engineering,pune

