Cluster Computing
https://doi.org/10.1007/s10586-018-1703-4

A secure and efficient cluster based location aware routing protocol in MANET

S. Syed Jamaesha[1] · **S. Bhavani**[1]

Received: 11 December 2017 / Accepted: 3 January 2018

Abstract
Mobile adhoc network (MANET) is a collection of node under a communication with each other nodes in the network. They are mobile nodes which can change its location according to the requirement. So the location based routing is needed for transmission of packet. For the data packet security, the existing algorithm is enhanced as "A secure location aware routing protocol". In this nodes are arranged by means of a clustering technique. This protocol will predict the future location of node using particle swarm optimization. The link lifetime, speed, distance and position of node is calculated earlier to find the optimized route. The trust value of node is computed from neighbor node which helps in prediction of future location and also to find malicious node in network to reduce packet loss. To prevent data from malicious node, the packets are encrypted using elliptic curve cryptography. Due to trust value, the routing information can be updated for easily and also improve the network throughput.

Keywords Clustering · PSO · Link lifetime · Trust value · ECC

1 Introduction

Mobile adhoc wireless network [1] is a set of nodes which are linked through a links with some rules to transfer packet from one node point to another node. There are many protocols to design the structure of communication. The connections are managed using routing protocols for adhoc network. It has to handle various problems such as mobile handling and reduction of overhead meanwhile nodes have partial resources. Then the very important factor of protocol is to ease the influence of attacks on the protocol. Due to transmission natured networking, the attacker within the range of transmission will do eavesdrop on the traffic, drop of packets and tamper.

The three types of protocols are flat routing, hierarchical routing and geographical routing [2,3]. In geographical routing [4], the locations of nodes are considered for data forwarding toward destination node. So it looks like the adaptive method for transferring of data packets in wireless adhoc network. This geographic routing protocol route is the packet based on trustworthy and does not take account of security problem. And the degradation of performance in terms of delivery ratio will say the presence of malicious node in the network. An attacker may generate falsified fake beacon messages to make connection between the nodes with it for disruption of the routing scheme [5]. The attacks such as black hole and wormhole are created by malicious node in network system.

The existing method compared to this paper is highly secure geographic routing approach [6]. In that, geographical routing is enhanced with message authentication code (MAC) for security. This allows both source node and destination node to prove the authenticity and for acknowledgement with secret key exchange to protect data packets. Also the intermediate nodes have to send acknowledgement after forwarding of data packet. But in this method more energy is conserved and secret key also can be steal by the attacker when sharing process between source and destination. So in this paper, a secure location aware routing protocol is designed.

The proposed model is described in the Sect. 3, which contains clustering technique in Sect. 3.1, PSO in Sect. 3.2 and node status is explained in Sect. 3.3. The malicious node detection is detailed in Sect. 3.4 and trust computa-

✉ S. Syed Jamaesha
syedjamaesha@gmail.com

S. Bhavani
bhavanisridharan7@gmail.com

[1] Department of ECE, Karpagam Academy of Higher Education, Coimbatore, India

Published online: 20 January 2018

tion in Sect. 3.5. The encryption method ECC is explained in Sect. 3.6. The experimental result is given in Sect. 4 and conclusion at Sect. 5.

2 Literature review

Kaur and Kaur [7], developed a paper for an analyzation and implementation of cluster based routing protocol in MANET networks. MANET is a self-supporting adhoc networks with cellular nodes that can be migrate and connection between each nodes. Clustering structured methods are used to improve performance. The main purpose of cluster is to boost the routing protocols in the network and the clustering based routing protocol is developed [7].

Diwaker and Mehla [8], proposed a route optimization technique using PSO and DSDV protocols. This particle swarm intelligence based route optimization will enhance the life time of the network. It provides gateways and shortest path to find out the sent packets or to initialize the communication between the nodes. By this combinational method, optimized route is discovered by saving time and energy and also by managing delay [8].

Koul et al. [9], discussed link stability, frequency and distance of nodes in MANET. In this paper, link remains connected with neighboring nodes and the communication time is predicted. The next hop node is selected based on the time of link and not by the shortest distance. The stability of the route is increased based on the time period using the parameters like frequency, distance and signal quality to decide the best next hop neighbor [9].

Rahman and Akhtaruzzaman [10], proposed an efficient scheme depends on the speed, distance remaining battery of nodes for determination of route in wireless MANET. To increase the network lifetime and network performance, the difference in velocities and weight has to be balanced. The intermediate node velocities are encompasses by the load balancing issues using MRF method [10].

Khalili-Shoja et al. [11], proposed a method using secret mutual chanciness between two or more multiple nodes for communication security. In this paper, network routing metadata by achieving pure randomness generation and secret key agreement. Dynamic source routing protocol is used and it requires relatively little communication overhead [11].

Ertau and Chavan [12], explains the elliptic curve cryptography based on threshold, which provides promise of securing the network. MANET is a network; allow communication with each other without any infrastructure. ECC algorithm is more efficient when compared to RSA that gives result as ECC is most suitable method for MANET [12].

Radhika and Thejiya [13], proposed a MANET network which has improved security. Trust worthiness is used to avoid vulnerable attacks. Trust model is designed using adhoc on demand distance vector routing protocol. Instead of signature verification, cryptography is used [13].

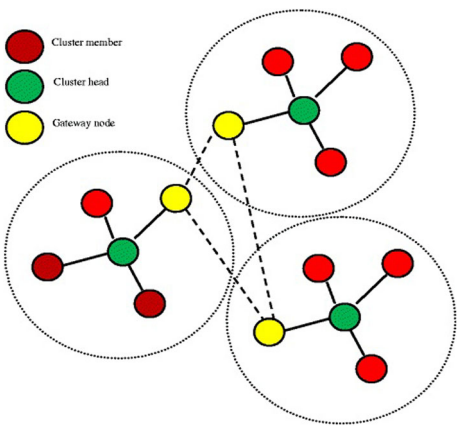
3 Proposed model

The protocol used to route the information based on location aware routing with trusted security is proposed in this paper. The nodes are communicated by clustering based routing between the boundaries of nodes. In MANET, to predict the future location of a cluster member, particle swarm optimization (PSO) method is used. Then the other parameters of node such as speed, position and distance has to be consider for the prediction of future location. Also it helps to find the shortest path easily and earlier. For transmission of packet between the nodes, check the node status for next-hop and reduce the packet delay. A random number is exchanged between the mobile nodes to predict the malicious node and also to prevent the loss of packets. Then trust value is calculated from its neighbor table for secure communication. For the data security, the packets are encrypted using elliptic curve cryptography (ECC) method. These methods are detailed in following sections.

3.1 Cluster based network model

In the adhoc network, the messages are transmitted in multihop method through various intermediate nodes from sender node to receiver node. The existing protocol sends data in peer to peer network without any centralized server and dynamically self-organization in adhoc topologies.

Clustering [14–17] is a method which means partitioning the whole network into smaller practical groups based on certain rules in order to distinguish the nodes in other sub networks. It is said that dissimilar nodes are grouped to form a structure; there every node is assigned different functions or status such as cluster head, gateway and member nodes. This partitioned area are called cluster that contains cluster head as a coordinator, which is elected by each cluster.



Cluster head is the nodes which acts as supervisor and do processes like management of cluster, updating routing table and finding new routes. The member nodes are the ordinary nodes in cluster and the nodes which have inter cluster communication link is called as gateway node. If the information transferred within the cluster, the data send to cluster head and it distribute the data to corresponding node. Otherwise the data can be forwarded by cluster head to gateway for communication between other clusters.

The process of clustering is each node of the cluster broadcast a HELLO message and its IP address is attached to it. Then cluster head adds IP address of its member, nodes to its own HELLO message. The cluster member will receive three HELLO messages from its cluster head during the cluster selection process. Otherwise it considers that the connection between them is broken. So, the node starts its searching of new cluster head. For conformation of its new cluster head, again it broadcast the Hello message that contains its IP address.

The node in cluster is a mobile node, so to predict the future location of nodes the following PSO method is used.

3.2 Particle swarm optimization

Particle swarm optimization (PSO) [18–20] is a modern and powerful method of optimization. This is based on group communication for sharing of individual knowledge. From the nature of the social behavior, a group of birds or insects search food or migrate to different space, although all that do not know where the best location is. The PSO algorithm learned basically from animal's activity or behavior for making solutions to optimization problems. In PSO, particles are referred as each member of group and the total population in group is called a swarm.

The process started with a random amount of populace and moving casually to chosen directions. Each unit drives through searching space and analyzes the memorized prior space of itself and its neighbor's. After finding good position the particles communicate the information to each other and then dynamically change their position and velocity accordingly. Next step begins when swarm has been moved completely. This method is faster, cheaper and more efficient implementation as compared to other optimization problems. PSO has the ability to swiftly coverage to a good solution.

The PSO has two algorithms, namely global best PSO (gbest) and local best PSO (lbest), with difference in size of their neighborhoods. The position of each particle influenced by best-fit particle in entire swarm is given by method global best. The global best PSO uses star topology where the social info can be gotten from all particles. The lbest method only allows all particles to chosen best-fit particle from neighborhood and uses ring social topology.

3.2.1 PSO algorithm parameters

In PSO algorithm there are some parameters that produce impact on efficiency of the PSO method. The basic parameters are swarm size, number of iterations, accelerations and velocity components.

1. Swarm size
   The number of units in swarm is called swarm size. Huge number of particles on swarm reduces the number of space covered per iteration for good optimization result. But it may lead to increase complexity per iteration and more time consuming.
2. Iteration numbers
   This parameter is defined as number of iterations which is a problem-dependent to obtain good result. Minimum number of iteration lead to stop the operation prematurely at the same time too large iteration will cause consequence of unnecessary computational complexity.
3. Velocity components
   The velocity of each particle has to be updated frequently. These velocity components will update particle's velocity and its three terms are,

1. The term which provides previous direction from memory that means movement in immediate past is called inertia component $\left(v_{ij}^{t}\right)$. It deals with a momentum that drastically changes the direction of particles and prediction towards the current direction.
2. The performance of particles relative to past performance is measured by the term called cognitive component $\left(c_1 r_{1j}^{t}\left[P_{best,i}^{t} - x_{ij}^{t}\right]\right)$. This is referred to as nostalgia of the particle. The position that was best for particle can be memorized in this term. Tendency of individuals to return to positions that satisfied them most in the past is represented.
3. The term social component $\left(c_2 r_{2j}^{t}\left[G_{best} - x_{ij}^{t}\right]\right)$ for gbest PSO or $\left(c_2 r_{2j}^{t}\left[L_{best,i} - x_{ij}^{t}\right]\right)$ for lbest PSO is used to measure the performance of particles that relative to a group of particles. It also determines the best position found by neighborhood particle.

4. Acceleration coefficient
   The stochastic effect of cognitive and social works of particles velocity can be maintained by random values r_1 and r_2 together with acceleration coefficients c_1 and c_2. In this c1 refers for confidence of particle itself and c2 express confidence of particle in its neighbors.

3.2.2 Mobility related information

The node has large impact on calculating mobility metrics like distance, speed and moving direction between nodes. This information will help the node to know its own position and also the position of destination. Let the location organizes of a node i is (x_i, y_i) and the position organizes of a source node s is (x_s, y_s), then the distance and average distance between nodes is calculated as,

$$D = \sqrt{(x_i - x_s)^2 + (y_i - y_s)^2}$$

$$D_{avg} = \frac{1}{n}\sum_{i=1}^{n}\sqrt{(x_i - x_s)^2 + (y_i - y_s)^2}$$

To make forwarding decision for sending the packets to the nodes that are moving towards the direction of destination geographical routing protocol source node consider the moving direction. Suppose the source nodes is at (x_0, y_0) and the destination node is at (x_d, y_d) and neighbor node i at (x_i, y_i) then moving angle between source and neighbor i toward the destination d can be calculated from,

$$A_{s,j}^{(d)} = arc\cos \frac{(x_d - x_0)(x_i - x_0) + (y_d - y_0)(y_i - y_0)}{\sqrt{(x_d - x_0)^2 + (y_d - y_0)^2}\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2}}$$

3.2.3 Calculation of link lifetime

The communication of nodes is done through the link between the nodes. The link life time is defined as the duration where communication between nodes can exist. It is important to maintain the link of nodes, which can breaks frequently due to some obstacles and varying speed of nodes. If break time of the nodes can predicted earlier then it can be used as one of the routing metric for next hop selection. The packet loss can be reduced by providing longer lifetime for link. The coordinates of source and destination node be (x_s, y_s), (x_i, y_i) and their velocities are v_s and v_i, where $v_s < v_i$ and range be R. the lifetime between this source and destination is calculated as,

$$L_{s,i} = R - \frac{\sqrt{(x_i - x_s)^2 + (y_i - y_s)^2}}{v_s - v_i}$$

After finding the mobility information and link life time of node then the node status is analyzed for the prediction of future location.

3.3 Node status

To determine the node status, the buffer queue length is beaconed before the next hop selection. For the network load analyzation, the buffer queue length is considered to avoid packet drops due to congestion at receiver node. The buffer size can be defined as number of packets in buffer queue. The average buffer capacity ($Q_i^{(t)}$) can be given as,

$$Q_i^{(t)} = \frac{Q_{\max} - Q_i^{(t)}}{Q_{\max}}$$

3.3.1 Calculation of one-hop node density

Routing metric includes traffic density as one of the important packets to determine the reliable routing path. The next hop selection in high node density without intermittent connectivity.by exchanging beacon packets of neighbor node table content the nodes can measure the one-hop node density based on number of neighbor nodes. It helps for stable routing path and reduces the risk of local maximum reaching of packet. The local node density of neighbor $T_i(t)$ given as,

$$T_i(t) = \frac{Neighbor\ table.size()}{R}$$

where the R is referred as radio range of node and $Neighbortable.size()$ will give the total number of neighbors in neighbor table at time t.

3.3.2 Speed, position and movement detection

The link between nodes is estimated for link stability. It is necessary to calculate for the prediction of link failure probability during a communication session. This can be used to detect the node that not in range for the next hop selection to forward/send the data. The link stability is appraised before selecting next hop for sending data to nearby nodes. The total link time can be calculated by estimating how long it takes for two neighbor nodes to move out of communication range. Communication lifetime by further divided as route validity time and link stability will give as result.

Assume that two nodes are moving in two different directions from time t_0 and t_1 with speed of v_1 and v_2.then the distance is D_0 and D_1 respectively. In that, D_0 represents their coordinates are A_0 (x_{i0}, y_{i0}) and B_0 (x_{i0}, y_{i0}) in t_0, while D1 denotes the distance in time t_1 with coordinates of A_1 (x_{j1}, y_{j1}) and B_1 (x_{j1}, y_{j1}). The estimated lifetime communication link is $\Delta t = t_1 - t_0$. The following equation can be used to predict future position (A_1 and B_1) of each vehicle from its current position (A_0 and B_0) and speed (v_1 and v_2).

$$\begin{cases} Bx_1 = Bx_0 + V_{bx}.\Delta t \\ By_1 = By_0 + V_{by}.\Delta t \\ Ax_1 = Ax_0 + V_{ax}.\Delta t \\ Ay_1 = Ay_0 + V_{ay}.\Delta t \end{cases} \quad (1)$$

Then the future distance can be calculated by getting the position of each node,

$$D_1^2 = |Ax_1 - Bx_1|^2 + |Ay_1 - By_1|^2 \tag{2}$$

By combining (1) and (2) equations,

$$D_1 = \sqrt{|(Ax_0 - Bx_0) + (V_{ax} - V_{bx})\,\Delta t|^2 + |(Ay_0 - By_0) + (V_{ay} - V_{by})\,\Delta t|^2} \tag{3}$$

In networks, there may be a malicious node to disrupt the process of communication. To prevent data loss and foe enhancement of security malicious node is detected and encryption of data is preferred. The trust value is calculated from neighbor table for trustworthy connection. The ECC method is used for encryption.

3.4 Malicious node detection

In the MANET network, malicious node detection is a problem that depends on network status and to discover drop data packets or route request packets. This problem happens due to intrusion of malicious node which attack is not the one that networks searches for. The other problem is huge amount of data exchange between the nodes that cause network traffic. Malicious node will lead to occupation of bandwidth and cause excessive resource consumption of nodes. Three types of attacks are data packet drop, drop of route request packets and changing the route request.

These three types of attacks are detected based on the presentation of each node within the network. For this, clustering technique is implemented. In clustering, each cluster selects cluster head and it will take decision about malicious node to find weather it is fake or not. Cluster head will introduce the malicious node to all nodes within the cluster by considering the info received from intrusion detection system. Packet loss is one of the parameter in performance of MANET. It occurs when the entire packet has dropped due to mobility, transmission error, congestion and the malicious node attack. If packet loss increases throughput will be decreased.so this packet loss can be reduced in this algorithm.

$$\text{Packet loss} = \text{Number of send packets} - \text{Number of received packets}$$

3.5 Trust computation

Trust can be defined as the level of confidence of one node about other node to be assigned for a work with in a time period. This trust value can be calculated [21] by one node against other node based on the past communication details or history. This value depends on time and it varies according to observations from trusted neighbor node.

The trust metrics is calculated using packet forwarding behavior to evaluate how packet forwarding is done by each neighbor. This can be the ratio between number of packets received and forwarded successfully by a node. Let assume i as sensing of nodes and j is the trust value and the equation be,

$$T_{i,j}(t) = \frac{F_{i,j}(t)}{R_{i,j}(t)}$$

where $F_{i,j}(t)$ represents at time t, number of packets promoted by node j and $R_{i,j}(t)$ represents number of packets received by node j. By this trust ratio, we can easily find the presence of malicious node. If malicious node is in the network its value gets decreased so it will be detected and removed from the route successfully.

3.6 Elliptic curve cryptography

Elliptic curve cryptography (ECC) [22,23] is one of a method of public key cryptography. In general, the public key cryptography each device or user taking part in communication, which working with pair of keys, a public key and a private key and operation needs for cryptographic process. When selecting public key schemes for specific operations, functionality, security and performance has to be considered. Public key processes such as signature verification and encryption are extra effectual in ECC. Private Key operations, such as signature generation and decryption for ECC are highly efficient. Advantages like processing power, storage, bandwidth, or power consumption are offered by ECC.

The elliptic curve cryptography consists of a finite field which represents field elements and algorithms for execution field arithmetic. Then an elliptic curve, that gives elliptic curve points and algorithms for elliptic curve arithmetic.

The elliptic curve in mathematical expression be like $\mathbf{y}^2 = \mathbf{x}^2 + \mathbf{ax} + \mathbf{b}$, in this each a and b values gives different elliptic curve. The public key is point on curve and private key is a random number. By multiplying private key with generator point G of curve the public key is obtained. The curve parameters and generator point G, together constitutes the domain parameters of ECC.

3.6.1 Finite fields

The elliptic curve operations on real number operations are slow and in accurate due to round off error. But this cryptographic process should be faster and accurate. So, it is defined over two finite fields,

- Prime field (F_p)
- Binary field (F_2^m)

In prime field, the equation of the elliptic curve is $\mathbf{y^2 \bmod p = x^3 + ax + b \bmod p}$, here elements of this finite field are integers between 0 and p-1. The prime number p is chosen such that to make more number of points on elliptic curve to make the cryptographic system secure.

In binary field, the elliptic curve equation is $\mathbf{y^2 + xy = x^3 + ax^2 + b}$, where $b \neq 0$. Here the elements of the finite field are integers of length almost m bits. These numbers can be considered as a polynomial of degree $m-1$. 0 and 1 be the binary polynomial coefficients. The operation such as addition, subtraction, division and multiplication involves polynomial of degree $m-1$. The m is chosen for large number of points on elliptic curve to make secure.

The working of ECC depends on efficiency of finite field computations and fast algorithms for elliptic scalar multiplication. Selection of specific underlying fields and elliptic curves can speed up the implementation.

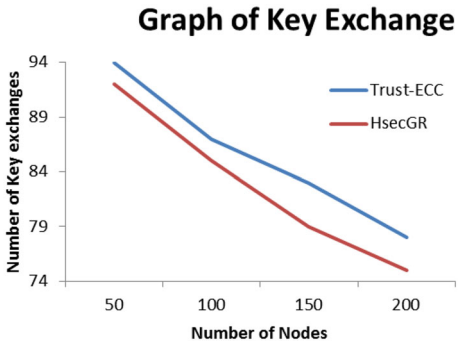
4 Experimental results

This new secure algorithm is implemented using ns2 simulator tool. The version used is ns2.34 and this tool is mainly applicable for the simulations of MANET, VANET, and WSN. The experimental result is shown in following figures.

The various graphs are drawn to analyze the performance of algorithm developed. The graphs such as key exchange, overhead, average delay, PDR, message drop and throughput.

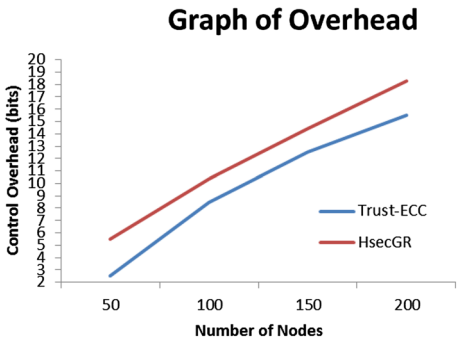
4.1 Key exchange

This is defined as the process, whereby a shared key becomes available to two parties for subsequent cryptographic use.



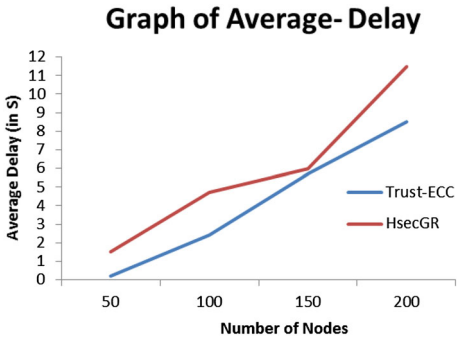
4.2 Overhead

It represents total number of forward in the network in terms of number of time it forwarded.



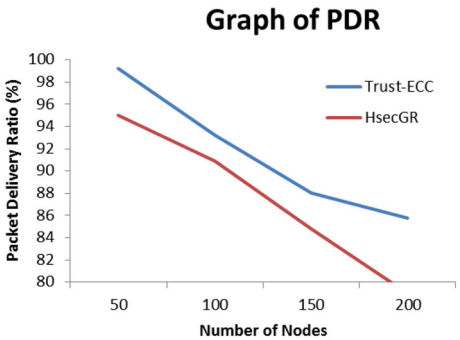
4.3 Average delay

It is the product of time taken to obtain public or private key to number of mobile nodes in network.



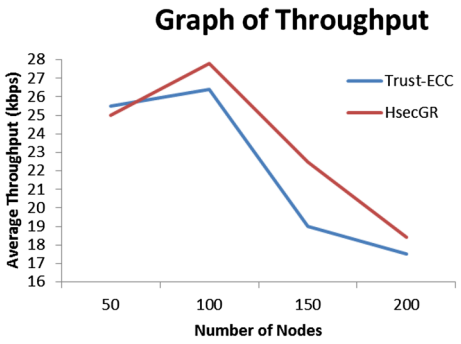
4.4 Packet delivery ratio

PDR defined as the fraction of packets sent which are actually received by destination node among all packets sent.



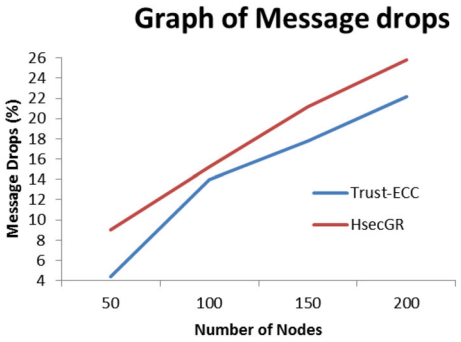
4.5 Throughput

Throughput is the arrival of completed data in time period to destination.



4.6 Message drop

The number of packets dropped not received by destination due to malicious node is called message drop.



5 Conclusions

In this paper, trusted ECC based "A secure location aware routing protocol" is proposed. The above experimental result shows that this protocol gives better performance than the existing method. The future location is predicted and so the link life time is calculated earlier. Due to PSO algorithm, all nodes are connected under a coordination, which helps to reduce the packet loss. The trust value also calculated to find weather malicious node intrusion occurs in network. For the data security, the packets are encrypted using the elliptic curve cryptography. Therefore overall performance of this algorithm has better efficiency.

References

1. Shanmugapriyan, D., Murugaanandam, S.: Secured and highly reliable data transfer in MANET using position-based opportunistic routing protocol. Int. J. Innov. Sci. Eng. Res. **1**(2), 69–74 (2014)
2. Panda, M.: Study of different routing protocols in wireless sensor networks. Am. J. Eng. Res. **5**(10), 19–23 (2016)
3. Gupta, A.K., Sadawarti, H., Verma, A.K.: Review of various routing protocols for MANETs. Int. J. Inf. Electron. Eng. **1**(3), 251–259 (2011)
4. Kaur, H., Singh, H., Sharma, A.: Geographic routing protocol: a review. Int. J. Grid Distrib. Comput. **9**(2), 245–254 (2016)
5. Sarika, S., Pravin, A., Vijayakumar, A., Selvamani, K.: Security issues in mobile adhoc networks. Procedia Comput. Sci. **92**, 329–335 (2016)
6. Boulaiche, M., Bouallouche-Medjkoune, L.: Hsecgr: highly secure geographic routing. J. Netw. Comput. Appl. **80**, 189–199 (2017)
7. Kaur, M., Kaur, S.: Analyze and implementation of cluster based routing protocol in MANETs. Int. J. Innov. Res. Sci. Eng. Technol. **5**(3), 3098–3107 (2016)
8. Diwaker, C., Mehla: Based route optimization technique to enhance network lifetime. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **6**(7), 205–210 (2016)
9. Koul, A., Patel, R.B., Bhat, V.K.: Distance and frequency based route stability estimation in mobile adhoc networks. J. Emerg. Technol. Web Intell. **2**(2), 89–95 (2010)
10. Rahman, M., Akhtaruzzaman: An efficient position based power aware routing algorithm in mobile ad-hoc networks. I. J. Comput. Netw. Inf. Secur. **7**, 43–49 (2016)
11. Khalili-Shoja, M.R., Amariucai, G.T., Wei, S., Deng, J.: Secret common randomness from routing metadata in ad-hoc networks. IEEE Trans. Inf. Forensics Secur. **11**(8), 1674–1684 (2016)
12. Ertau, L., Chavan, N.J.: Elliptic curve cryptography based threshold cryptography (ECC-TC) implementation for MANETs. IJCSNS Int. J. Comput. Sci. Netw. Secur. **7**(4), 48–61 (2007)
13. Radhika, N., Thejiya, V.: Trust based solution for mobile ad-hoc networks. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **4**(5), 73–82 (2014)
14. Rajasekar, S., Subramani, A.: Performance analysis of cluster based routing protocol For MANET using RNS algorithm. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **6**(12), 234–239 (2016)
15. Amine, D., Nassreddine, B., Bouabdellah, K.: Energy efficient and safe weighted clustering algorithm for mobile wireless sensor networks. Procedia Comput. Sci. **34**, 63–70 (2014)
16. Aissa, M., Belghith, A.: A Node quality based clustering algorithm in wireless mobile adhoc networks. Procedia Comput. Sci. **32**, 174–181 (2014)
17. Aissa, M., Belghith, A., Drira, K.: New strategies and extensions in weighted clustering algorithms for mobile ad hoc networks. Procedia Comput. Sci. **19**, 297–304 (2013)
18. Ali, H., Shahzad, W., Khan, F.A.: Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. Appl. Soft Comput. **12**, 1913–1928 (2012)
19. Mohammadi, A.O.K.: Particle swarm optimization in intelligent routing of delay-tolerant network routing. J. Wirel. Commun. Netw. **147**, 1–8 (2014)
20. Kumar, S., Mehfuz, S.: Intelligent probabilistic broadcasting in mobile ad-hoc network: a PSO approach. J. Reliab. Intell. Environ. **2**, 107–115 (2016)
21. Abinaya, S., Arulkumaran, G.: Detecting black hole attack using fuzzy trust approach in MANET. Int. J. Innov. Sci. Eng. Res. **4**(3), 102–108 (2017)
22. Sivamurugan, D., Raja, L.: Secure routing in MANET using hybrid cryptography. Int. J. Res. Granthaalayah **5**(4), 83–91 (2017)
23. Balamurugan, E.: Elliptic curve integrated encryption scheme using analysis vehicular ad-hoc network. Int. J. Innov. Sci. Eng. Res. **3**(5), 47–50 (2016)

S. Syed Jamaesha received his B.E. degree in 2007 from the Department of Electronics and communication Engineering, Anna University, Chennai, India and his M.E. degree in 2010 from the Department of Electronics and communication Engineering, Anna University, Coimbatore, India. He has been a faculty member in the Department of Electronics and communication Engineering, Karpagam Institute of Technology, Coimbatore. His research interests are mainly in cloud computing, network optimization, mobile adhoc network and wireless networks.

S. Bhavani received his B.E. degree in 1990 from the Department of Electronics and communication Engineering, Bharathiar University, Coimbatore, India and her M.E. degree in 2006 from the Department of Electronics and communication Engineering, Anna University, Chennai, India. She received her Ph.D. from Anna University, Chennai. She has been a Professor and Head in the Department of Electronics and communication Engineering, Karpagam Academy of Higher Education, Coimbatore. Her research interests are mainly in cloud computing, network optimization, mobile adhoc network, wireless networks, image processing and VLSI.