Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Mobile Ad hoc Routing Using Clusters Confrontations (SMARUC^2) with Genetic Algorithm (GA)

[1]S. R. M.Krishna, [2]Dr. M. N. Seeta Ramnath, [3]Dr. V. Kamakshi Prasad, [4]B. Manju Kumari

[124] Computer Science & Engineering, G.V.P College of Engineering, Visakhapatnam, India

[3]Computer Science & Engineering, JNTU, Hyderabad, India

Abstract— Data Routing among nodes in a wireless network is pretty complex when compared to traditional centralized network architecture. The wireless networks face quite a lot of threats due to open medium. The genuinity of the neighboring nodes must be known a priori to the transmission or routing of data packets. So, there is a need to address two issues posed by these self organizing architectures. One is to perform a genuine check before routing and the other is to find a shortest path among those trusted nodes. First issue (genuinity) can be addressed by generating dynamic topology with secure routing using "SMARUC^2". Clusters are formed through"CCAM" (Classification Based Clustering Algorithm for Mobile Ad Hoc Networks). The second issue (Dynamic Traffic Assignment or routing) is addressed by using Genetic Algorithm (GA) in combination with dynamic allocation of costs among different nodes through measurement of latitudes and longitudes. Efficient utilization of resources like battery power and signal strength can also be achieved by "classification with ROSETTA". Finally, secure communication is provided among trusted nodes through enhanced Open SSL-DES96.

Keywords — Dynamic Traffic Assignment, Genetic Algorithm, ROSETTA, DES96, Open SSL.

I. INTRODUCTION

A mobile ad hoc network (MANET)[1] is an autonomous system of mobile nodes, mobile hosts (MHs), or MSs (also serving as routers) connected by wireless links, the union of which forms a network in the form of a dynamic communication graph.

MANETs are basically peer-to-peer (p2p) multi-hop mobile wireless networks where information packets are transferred in a store-and-forward method from a source to Destination, via intermediate nodes, as shown in Fig1. As the nodes move, the resulting change in network topology must be made known to the other nodes so that prior topology information can be updated. Such a network may operate in a stand-alone fashion, or with just a few selected routers communicating with an infrastructure network.

A. Characteristics of MANETs

- No integrated control and administration is done
- Communication through the various nodes in a network
- Alteration of the topology and frequent breakage of links once the connection is proven
- Can be set up anywhere, in any situation
- Limited security

B. Security issues in MANETs

1) Easier to hit: Since the broadcasting is nothing but air, it can be tapped easily.

2) Quality of Service: The different QoS metrics include throughput, packet loss, delay, and jitter and error rate. The dynamically changing topology, limited bandwidth and quality makes the difficulty in achieving the desired QoS guarantee for the network.

C. Objective

The main objectives of this paper are

- To generate dynamic topology with secure routing using SMARUC2
- Formation of clusters through CCAM in generating Dynamic topology
- Efficient utilization of resources like battery power, Signal strength with classification using ROSETTA
- To Avoid Dynamic Traffic Assignment (routing) problem using Genetic Algorithm with dynamic Allocation of costs among different nodes through latitude and longitude measurements
- To provide secure communication among trusted nodes using Open SSL-DES96

D. Overview

The proposed SMARUC algorithm carries out establishment of companion networks in MANETs. In the same way as in real life situations.

SMARUC2 algorithm is divided into four stages,

1. Confrontation Your Neighbor
2. Scale Companions
3. Share Companions and
4. Route through Companions.

Dynamic Traffic Assignment (routing) is one of the most important issues that have a significant impact on the network's performance. An ideal routing algorithm should strive to find an optimum path for packet transmission within specified constraints. Previously different statistical routing algorithms are proposed to find the optimal path from the source to destination, but the major problems with these algorithms are if the size of the network is huge in number, it is very difficult to find out the optimal solution and also it takes a huge amount of time to execute the system. In order to overcome these problems Genetic Algorithm is proposed.

In order to determine the quality of a node, the parameters like battery power and signal strength are compared for each and every node to elect the cluster head. This classification among the nodes is done using ROSETTA through Naive Bayesian Classification method.

Finally secure communication among the nodes can be achieved using enhanced Open SSL-DES96.

II. RELATED WORK

Summary of MANET Protocols and Clustering Algorithms:

MANET Protocols	
1. 1. DSDV (Destination Sequenced Distance Vector) Protocol	**DSDV** [2] is a hop-by-hop distance vector routing protocol that in each node has a routing table that for all reachable destinations stores the next-hop and number of hops for that destination.
2. AODV **(**Ad Hoc On-Demand Distance Vector Routing) Protocol	**AODV** [3] protocol belongs to the class of distance vector routing protocol. In distance vector routing protocol, every node knows its neighbour node and the costs to reach the neighbour node. Every node maintains its own routing table by storing all the nodes in the network, the distance and the next best hop(node).
2. 3. ARAN 3. (Authentic ated 4. Routing Protocol 5. for Ad Hoc **6.** Networks)	**ARAN** [6] is most recent Ad Hoc network research has focused on providing routing services without considering security. ARAN deals with security threats against ad hoc routing protocols, specifically examining AODV and DSR. ARAN[6], detects and protects against malicious actions by third parties and peers in one particular ad hoc environment.
4. ARIADNE: A Secure On-Demand Routing Protocol for Ad Hoc Networks	**ARIADNE** is an Ad Hoc Network is a group of wireless mobile computers (or nodes), in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. ARIADNE [7] prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks.

CLUSTERING ALGORITHMS	
1. LCC	**LCC** is the clustering algorithm is divided into two steps:cluster formation and cluster maintenance. Initially mobile nodes with the lowest ID in their neighbourhoods are chosen as cluster heads [9].
2. WCA	**WCA** selects the cluster heads **according to the weight value of each node**. The weight associated to a node v is defined as: **Wv=w1△ v +w2Dv+w3Mv+w4Pv** **----------> (1)** **The node with the minimum weight is selected as a cluster hed. [10]**
3. Lo west ID cluster algorithm (LIC)	**LIC is an algorithm in which a node** with the minimum id is chosen as a cluster head. Thus, the ids of the neighbours of the cluster **head will be higher than that of the cluster head. [11]**
4. Hig hest Degree Clustering	The degree of nodes is computed based **on its distance from each other. All nodes flood their connectivity value within their** transmission range. Thus, a node decides to become a CH or remain as CN by comparing the connectivity value of its neighbours with its own value. Node with **highest connectivity value in its vicinity will** become CH.
5. Max-Min Cluster algorithm	**If a node A is the largest in the d-neighbourhood** of another node B then node A, **A will be elected a cluster head even though node A may not be the largest in its d-neighbourhood.[12]**
6. Distributed Scenario Based clustering algorithm for Mobile Ad Hoc Netwoks (DSCAM)	While selecting the dominating nodes, redundancy is achieved by choosing the value of parameter K greater than one ana parameter r allows increasing local availability. These two parameters can be convinently set depending on the eqirement. Dominating nodes are potential nodes to become cluster heads and during the cluster formation phase, the ordinary nodes elect their best as the cluster head.[13][14].

III. PROPOSED WORK

In this segment, we deliberate our proposed work

A. SMARUC^2 Algorithm Description

Secure Mobile Ad Hoc Routing using clusters Confrontations (SMARUC^2) accomplishes establishment of companion networks in MANETs in the same way as in real life scenarios. We apply the same idea to develop the SMARUC^2 algorithm. The proposed SMARUC^2 algorithm is **divided into four stages Confrontation your neighbour, Scale** companions, Share companions and Route through companions.

1. Confrontation Your Neighbour: Confrontation is a mechanism to validate nodes initially when no condition is present. It is a basic test which a node has to complete in order to verify its honesty and integrity. Let us assume that the node A confronts its neighbour node B.

Step 1) When a new network is initialized, each node is a stranger to another. Thus each node sends its neighbours in the unsubstantiated list.

Step 2) The node A picks one of the neighbours B and performs the usual Share Friends Stage.

Step 3) As a response the neighbour node B either sends its friend list or the nodes from its unsubstantiated list if the companion list is empty.

Step 4) On receiving the list, the node A picks up a node which can reach on its own and in the most efficient way. Let us say that this node is C.

Step 5) Now the node A has two ways to reach the node one through B and another through a route already known to it.

Step 6) Each node is initialized with a pair of large prime numbers. (Let us Suppose A(a, b), B(c,d) and E(e,f)).

Step 7) Node A wants to confront node B. Then it sends one of his random prime number as the confront. (Here we send first prime number as the confront i.e. 'a')

Step 8) Here we use public key cryptography algorithm known as RSA. (It uses 2 keys for encryption and decryption)

Step 9) Node A sends 'a' as the confront to node C

Step 10) In node C we apply RSA algorithm for key generation (public key, private key)

Step 11) N ode C sends public key to node A

Step 12) Node A encrypts 'a' with public key of node C.
Then we get some 'k'. Then node A sends 'k' to node C

Step 13) Node C receives & decrypts 'k' with C's private key. Then we get some 'n'

Step 14) Then node C computes ' c^d mod n' & sends result to
Node A

Step 15) Now node A sends 'a' as the confront to node B

Step 16) In node B we apply RSA algorithm for key generation (public key , private key)

Step 17) node B sends public key to node A.

Step 18) node A encrypts 'a' with public key of node B. Then we get some 'k'. Then node A sends 'k' to node B

Step 19) node B receives & decrypts 'k' with B's private key.
Then we get some 'n'

Step 20) Node B sends 'n' to node C

Step 21) Node C receives 'n' & computes ' c^d mod n' & sends result to Node A

Step 22) Since n, c and d are all very large prime numbers it is unfeasible to determine c and d from the result of the *mod* Function as that is known to be a tough problem

Step 23) Node A compares both results. If they are equal node B is added at the bottom of the A's friend list otherwise it is placed in unauthenticated list.

B. Classification Based Clustering Algorithm for Mobile Ad Hoc Networks (CCAM) is a clustering algorithm for providing guaranteed QoS. Best quality nodes are potential nodes to become cluster heads and during the cluster formation phase, the ordinary nodes select their best node as cluster head. This selection is done by Classification through Rosetta Tool, based on signal strength and battery power. Selection of cluster head based on these parameters help in maintaining the structure of the cluster stable by minimizing the topology changes and associated overheads during cluster head changes.
Cluster Classification is done through Rosetta based on battery power and signal strength. When the battery power is low and the signal strength is high then the quality of the nodes is low, when both battery power and signal strengths' are low

then the node quality is also low. Thus due to this classification we can easily detect the quality of the node. This classification helps in identifying the cluster head. Our approach focuses on the elimination of the redundant attributes in order to generate the effective reduct set (i.e., reduced set of necessary attributes) and formulating the core of the attribute set.

ROSETTA is a toolkit for analyzing tabular data within the framework of rough set theory. ROSETTA is designed to support the overall data mining and knowledge discovery process: From initial browsing and preprocessing of the data, via computation of minimal attribute sets and generation of if-then rules or descriptive patterns, to validation and analysis of the induced rules or patterns.

Node	Battery Power	Signal Strength	Decision
N1	High	Low	Low
N2	High	High	High
N3	Low	High	Low
N4	Low	Low	Low

C. Distance

In dynamic topology, the distance between two nodes is calculated using '**haversine**' formula

Haversine formula:

$$a = \sin^2(\Delta\varphi/2) + \cos(\varphi_1).\cos(\varphi_2).\sin^2(\Delta\lambda/2)$$

$$c = 2.\text{atan2}(\sqrt{a}, \sqrt{(1-a)})$$

$$d = R.c$$

Where φ is latitude, λ is longitude, R is earth's radius (mean radius = 6,371km)

note that angles need to be in radians to pass to trig functions!

D. Route Evaluation through Genetic Algorithm:

*I*nitially the network contains 'n' number of nodes together with source and destination; here the shortest path can be found between source and destination based on the networks nodes that are in the creation state. If any node in the communication line got deactivated or failed then the traffic should be dynamically assigned to a new path that has shortest distance among all possible paths. The underlying topology of multi hop networks can be specified by the directed graph G

(N, A), where 'N' is a set of nodes (vertices), and 'A' is a set of its links (arcs or edges). There is a cost C (i, j) associated with each link (i, j). S and D denote source and destination nodes, separately. Each link has the link connection display denoted by I (i, j), which plays the role of a chromosome map (masking) providing information on whether the link from node 'i' to node 'j' is included in a routing path or not.

It can be defined as follows: if the link from node to node exists in the routing path

I (i, j)=1 ---□ if the link from node 'i' to node 'j' exists in the routing path

I (i, j)=0 ---□ if there is no link exist in between node 'i' to node 'j'

It is observable that all the diagonal essentials I (i,j) of must be zero. From the above data the shortest path can be formulated as

Minimize

$\sum\sum C(i, j)*I(i, j)$ Subjected to

I (i, j)=1 where i, j are nodes in the communication path. And first and last nodes should be source and destination.

For the above methodology genetic operator have been designed and represented below.For Elaboration of these following Genetic operations [15][16].

Genetic Representation

a) Population Initialization
b) Selection Operator
c) Crossover Operator
d) Mutation Operator
e) Fitness Operator [15][16]

A. Open SSL

The openssl program provides a rich variety of commands each of which often has a wealth of options and arguments.

The pseudo-commands list-standard-commands, list-message-digest-commands, and list-cipher-commands output a list of the names of all standard commands, message digest commands, or cipher commands, respectively, that are available in the present openssl utility.

enc.sh

```
#$1 = filename

openssl enc -aes-256-cbc -salt -in $1 -out y.txt -pass #pass:"sirkrs123"
```

dec.sh

```
openssl enc -d -aes-256-cbc -in y.txt -out y.dec -pass #pass:sirkrs123
```

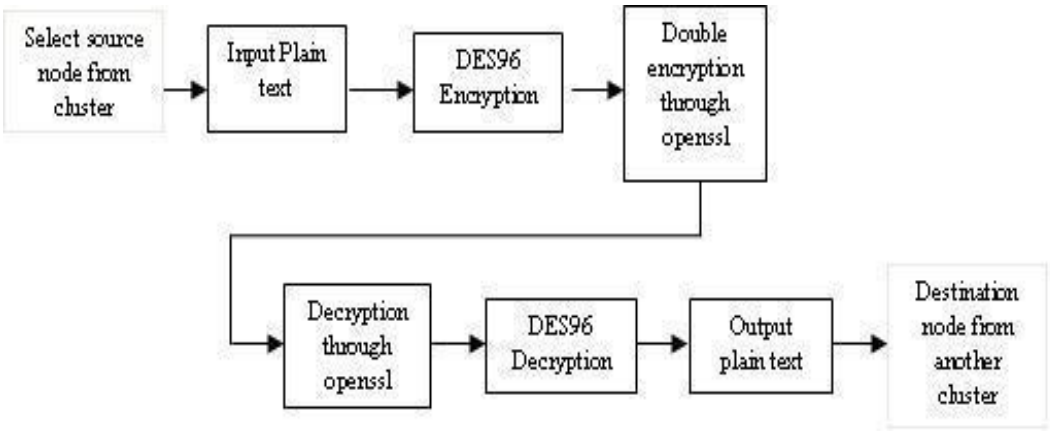
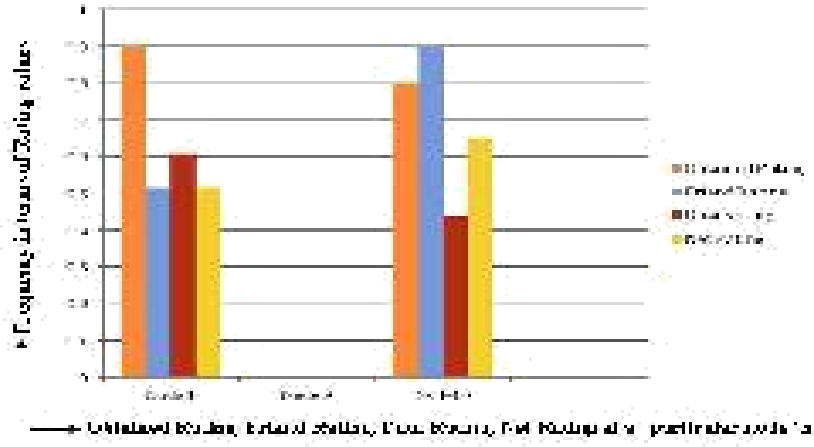


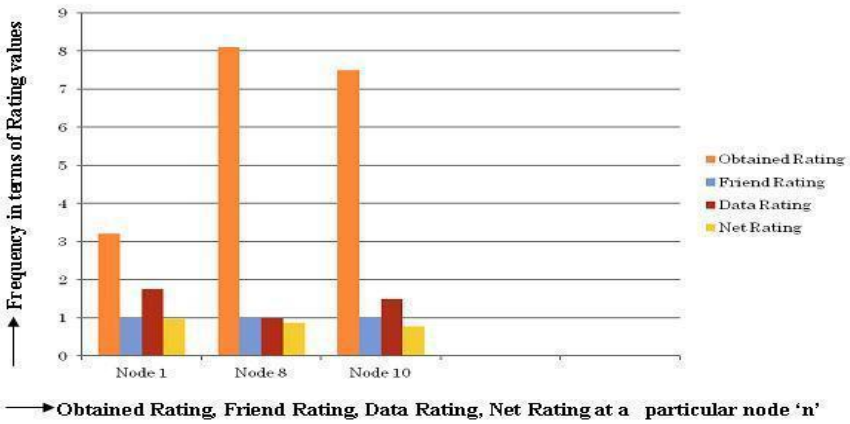
Figure 5: Block Diagram of open SSL Cryptography

IV . EXPERIMENTAL RESULTS

1. Graph representing ratings/ scalings when malicious node is being detected

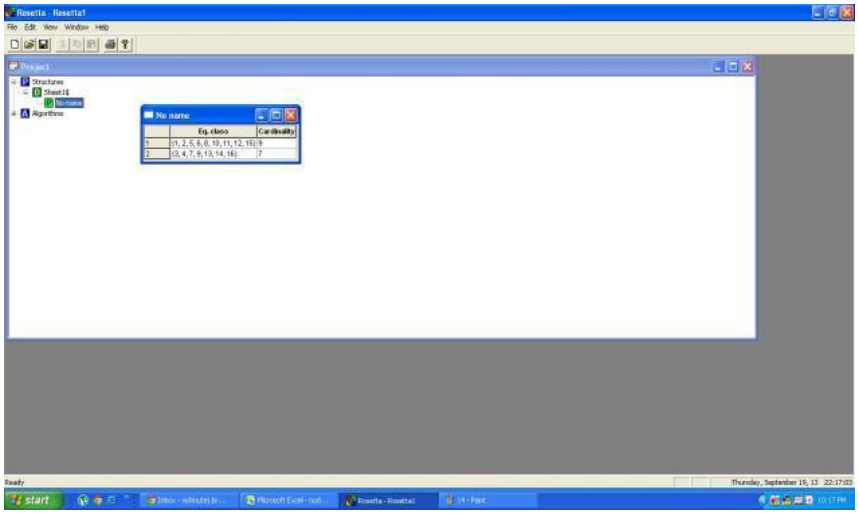


2. Graph representing ratings/ scalings when malicious node is not being detected

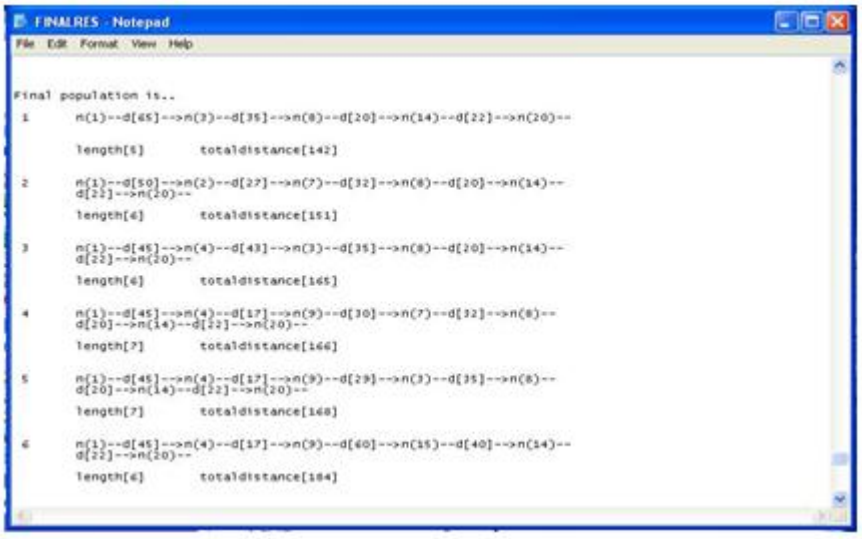


3. Classification using ROSETTA:

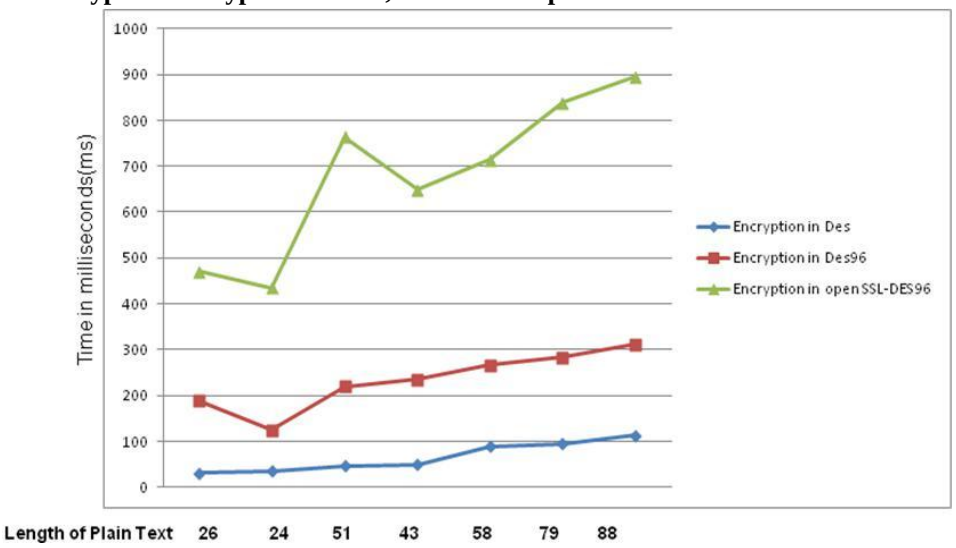
	Battery Power	Signal strength	Quality
N1	**High**	**High**	**High**
N2	**High**	**Low**	**High**
N3	**Low**	**High**	**Low**
N4	**Low**	**Low**	**Low**
N5	**High**	**High**	**High**
N6	**High**	**Low**	**High**
N7	**Low**	**High**	**Low**
N8	**High**	**Low**	**High**
N9	**Low**	**High**	**Low**
N10	**High**	**Low**	**High**
N11	**High**	**High**	**High**
N12	**High**	**Low**	**High**
N13	**Low**	**High**	**Low**
N14	**Low**	**High**	**Low**
N15	**High**	**Low**	**High**
N16	**Low**	**Low**	**Low**



4. Genetic Algorithm with Dynamic Traffic Assignment:



5. Time Taken for Encryption/Decryption in DES, DES96and Open SSL-DES96



V. CONCLUSION

This paper put forward on enhancing the security in MANETs by generating secured dynamic network topology through SMARUC[2] and avoids Dynamic Traffic Routing problem using Genetic Algorithm by comparing the other clustering and maliciou detection protocols. This proposal also incorporates secure communication between trusted nodes among clusters using OpenSSL-DES96. It is observed that which we obtained from the above results, increases the quality of the services among MANETs.

REFERENCES

[1] D. P. Agrawal and Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*. Pacific Grove, CA: Brooks/Cole, Thomson, 2002.

[2] Charles E. Perkins and Pravin Bhagwat, "*Highly dynamic Destination-Sequenced Distance-Vector(DSDV) routing for mobile computers*", Conference on Communication Architecture, pp 234-244,August 1994.

[3] C. Perkins, E. Royer, and S. Das, "*Ad Hoc on Demand Distance Vector(AODV) Routing",* Internet experimental RFC 3561, Jul. 2003.

[4] D. Johnson and D. Maltz, "*Dynamic source routing in ad hoc wireless networks*," in Book Chapter inMobile Computing, T. Imielinski andH. Korth, Eds. Dordrecht, The Netherlands: Kluwer, pp. 131–181, 1996.

[5] Mingliang Jiang, Jinyang Li and Yong Chiang Tay, "*Cluster Based Routing Protocol (CBRP) Functional specification*", August 1998.

[6] K. Sanzgiri, B. N. Levine, C. Shields, B. Dahill, and E. M. Belding-Royer, "*A secure routing protocol for ad hoc networks*," in Proc. 10th IEEE Int. Conf. Network Protocols (ICNP), Paris, France, pp. 78–89, Nov. 12–15,2002.

[7] Y. Hu, A. Perrig, and D. B. Johnson, "*Ariadne: A secure on-demand routing protocol for ad hoc networks*," Wireless Netw., vol. 11, no. 1–2,pp. 21–38, Jan. 2005.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "*Mitigating routing misbehavior in mobile ad hoc networks*," in Proc. MobiCom 2000, Boston, MA, pp. 255–265, Aug. 2000.

[9] C.-C. Chiang et al., "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," in proceedingsof IEEE SICON'97, 1997

[10] M. Chatterjee, S. K. Das, and D. Turgut, "An On-Demand Weighted Clustering Algorithm (WCA) for Ad hoc Networks," in proceedings of IEEE Globecom'00, pp. 1697–701, 2000

[11] M. Gerla and J. T. Tsai, "Multiuser, Mobile, Multimedia Radio Network," Wireless Networks, vol. 1, pp. 255–65, Oct. 1995

[12] A.D. Amis, R. Prakash, T.H.P Vuong, D.T. Huynh. "Max-Min D-Cluster Formation in Wireless Ad Hoc Networks". In proceedings of IEEE Conference on Computer Communications (INFOCOM) Vol. 1. pp. 32-41, 2000 G. Chen, F. Noc

[13] Anitha, V.S., M.P. Sebastian, "*Scenario-based Diameter-bounded Algorithm for Cluster Creation and Management in Mobile Ad hoc Networks*,"13th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications, pp. 97-104, 2009.

[14] Anitha, V.S. and M. P. Sebastian, "*SCAM: Scenario-based Clustering Algorithm for Mobile Ad hoc Networks,"* Proc. First International Conference on Communication Systems and Networks, 2009.

[15] Shengxiang Yang, Hui Cheng and Fang Wang, "*Genetic Algorithms With Immigrants and Memory schemes for Dynamic Shortest Path Routing Problems in Mobile Ad Hoc Networks*" *IEEE Trans.*,vol.40,No.1,Jan. 2010

[16] R.sivaraj, Dr.T.Ravichandran, "*A review of selection methods In genetic algorithm*", International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462 Vol. 3 No. 5, May 2011.

BIOGRAPHY

S.R.M.Krishna received M.Tech degree in Computer Science & Engineering from JNTU-Hyderabad, pursuing Ph.D in JNTU-Hyderabad, India.

Dr. M.N.Seetha Ramnath received Ph.D in JNTU-Hyderabad and working as a Professor in department of Computer Science & Engineering in Gayathri Vidya Parishad college of Engineering (Autonomous), Visakhapatnam, Affiliated to JNTU-Kakinada, India.

Dr.V.KamakshiPrasad presently serves as Professor of Computer Science & Engg JNTUH College of Engineering Hyderabad.He received his masters degree (M.Tech) in ComputerScience from Andhra University in the year 1992 and Ph.D from IIT Madraa, India.

B.Manju Kumari received B-Tech degree in Computer Science & Engineering from Kaushik College of Engineering, Affiliated with JNTU-Kakinada in 2012 and completed M-Tech (2012-2014) in Gayathri Vidya Parishad college of Engineering (Autonomous), Visakhapatnam, Affiliated to JNTU-K, India.

