Multicast and Multipath Based on Batch Signature Scheme on Adhoc Networks

Satish K, Anand R, Jitendranath Mungara

Abstract*— Adhoc Networks are becoming a very important tool for many nonconventional civil and military applications. In this adverse environment it is very difficult for the source to send the information to the destination in multicasting style. The main requirement of the network is to provide the security and promising the message integrity. To solve the various problems in the multicasting style for very large adhoc networks a Modified Tiered Authentication Multicast scheme is developed. This scheme has two steps, the first step includes generation of keys and these keys are used to form the Message Authentication Code for every packet sent to the receiver. The second step includes the Message Digest Algorithm 5 is used for message integrity. The movement of nodes in the mobile adhoc network quickly changes the topology resulting in the increase of the overhead message in topology maintenance. There are many clustering schemes are proposed for many adhoc networks. This paper presents on the performance of the Modified TAM protocol in different clustering schemes such as Distance Based Clustering and Weighted Based Clustering. Comparing the generated results from various clustering schemes by using Modified TAM protocol and decide which clustering scheme is better for implementing the Modified TAM protocol.

Index Terms*— Authentication, Clustering, Mobile Adhoc Networks.

I. INTRODUCTION

The continuous growth in wireless technologies has enabled networked-solutions for many nonconventional civil and military applications. The modern ad-hoc networks have been captivated from the research and engineering community. The solutions must be scalable to support networks covering vast areas with a large set of nodes that communicates over many hops. These characteristics make the design and management of ad-hoc networks significantly challenging in comparison to contemporary networks. In addition, the great flexibility of ad-hoc networking comes at the price of an increased vulnerability to security attacks and trade-off would be unavoidable at the level of network management and services.

Aggregation connection is considered a captious service in adhoc networks due to their genetically collective operations, where the nodes advance in network management and attempt to achieve common missions autonomously in highly unreliable environment without reliance on infrastructure equipment. For example, in a military operation the soldiers report their status and share observed data in order to become aware of the overall situation and coordinate their actions.

Manuscript received July, 2013.

Mr. Satish K, Pursuing MTech (CNE) Final Year in CMR Institute of Technology, Bangalore, Visveswaraiah Technological University, Belgaum, India

Mr. R.Anand, Associate Professor, CMR Institute of Technology, Bangalore, India

Dr. M. Jitendranath, working as Professor & Dean of Research in Computer Science Engineering department in CMRIT, Bangalore, India

In addition, it is common for ad-hoc networks to rely on multicast for management-related control traffic such as neighbor/route discovery to setup multi-hop paths, the establishment of time synchronization, etc. Such multicast traffic among the nodes has to be delivered in a secure and trusted manner. In particular the provided network services need to achieve the following security goals: Confidentiality, Message integrity and Source Authentication [5], [6], [7]. Confidentiality is achieved by encrypting the transmitted data [9]. This paper aims at addressing the message integrity and source authentication. Providing an efficient multicast message and source authentication security service that can easily scale for large networks is an important capability for the operation and management of the underlying network. Source and message authentication is the corroboration that a message has not been changed and the sender of a message is as claimed to be. This can be done by sending a (1) Cryptographic digital signature, or (2) Message Authentication Code (MAC).

II. RELATED WORK

We focus with the study of number of clustering schemes for MANETs. Mohamed Younis, Osama Farrag, Bryan Althouse [1] presents a new Tiered Authentication scheme for Multicast traffic (TAM) for large scale dense ad-hoc networks. Intra-Clustering source authentication nodes will synchronize every time and Inter-Clustering uses secret information asymmetry. Ismail Ghazi Shayeb, AbdelRahman Hamza Hussein and Ayman Bassam Nasoura [2] is a a survey of clustering schemes for Mobile Ad-Hoc Network (MANET). [3] Mohamed Elhawary and Zygmunt J. Haas, Fellow proposed an Energy-Efficient Protocol for Cooperative Networks. [4] Adrian Perrigy, Ran Canetti, Dawn Song, J. D. Tygar, UC Berkeley, Digital Fountain, IBM T.J. Watson proposed an Efficient and Secure Source Authentication for Multicast. This paper proposes several substantial modifications and improvements to Timed Efficient Stream Loss-tolerant Authentication.

III.MODIFIED TIERED AUTHENTICATION OF MULTICAST TRAFFIC SCHEME

The Modified Tiered Authentication Multicast pursues a two-tier process for authenticating multicast traffic in ad-hoc networks. The Modified Tiered Authentication Multicast uses clustering schemes for partition a network, and then it authenticates the multicast traffic by using symmetric keys. Clustering is a very popular scheme for supporting scalable network operation and management.

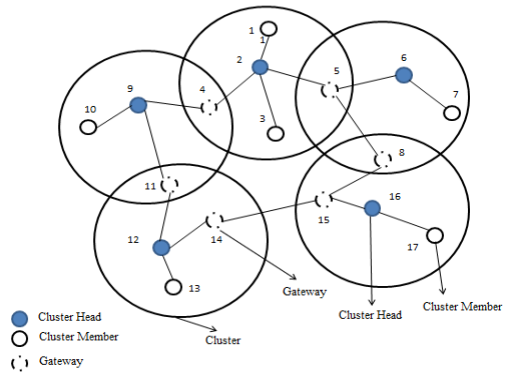

Fig. 1 An example clustered ad-hoc network.

In the Fig. 1 cluster-head controls the cluster, the cluster-head is reachable to all nodes in its cluster, either by single-hop or multi-hop paths. The Fig. 1 is also a very good example for clustered adhoc network. In a clustered adhoc network the nodes that are having the links in other clusters, it will acts as a gateway. The nodes that are serving as gateways between the clusters, so that the heads of the other clusters should be reachable to each other over multi-hop path and these clusters are considered as neighbors.

In the clustered adhoc network, if a node moves out from its parent cluster and joins another cluster, it is assumed that the associated cluster-heads will conduct a handoff to update each other about the change in membership of their clusters; other cluster-heads will not be involved in the handoff events outside their clusters.

A. Modified Tiered Authentication Multicasting approach.

The proposed approach includes the modification of the Tiered Authentication Multicast Protocol. The modified Tiered Authentication Multicast Protocol includes:

- AES symmetric key algorithm to generate the keys and forms the message authentication code for every packet sent to the receiver through the network and these keys are shared by all the nodes in the network.
- Message Digest (MD5) Cryptographic Hash Function is used to attach to the message to check for Message Integrity at the receiver.

The Modified Tiered Authentication Multi-cast Scheme Algorithm as shown below:

Step 1: Let G be the network.
Step 2: Let N be the total number of nodes.
Step 3: Assign key(i) -> n(i) // for every n(i) € N, by using AES Symmetric Key Algorithm.
Step 4: Assign the message(i) -> n(i) by using MD5 cryptographic hash function
Step 5: If n(i) -> send(data) -> n(j) then
Step 6: If message(n(i)) == message(i) && message(n(j)) == message(j)
then Data_transmission(ni,nj) = true;
else
Data_transmission(ni,nj) = false;
Step 7: End

B. Different clustering schemes to implement Modified TAM protocol

There are many kind of algorithms are available for clustering [8]. In this paper we are using two different kind of clustering algorithms, one is Distance based and the other one is weighted based.

1) Distance Based Algorithm

In this algorithm we initially elect a node which is far from the base station and near to the cluster nodes in a particular region. Also all the nodes are clustered due to the distance initially from the base station and region wise. Fig. 2 shows an example for Distance Based Clustering. Every cluster might have k number of node and the total network has N number of nodes and m number of clusters [10]. Since it is MANET all the nodes has mobility, the distance may change after some time [12], [13], [15]. So we are electing the next CH by applying the same distance condition.

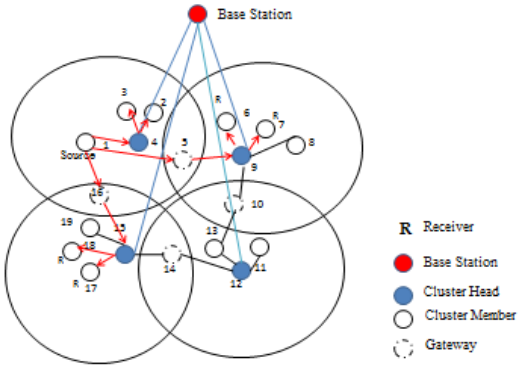

Fig. 2 An example for Distance Based Clustering.

The complete pseudo code of the clustering approach is given in below.

Step 1: Let G be the Mobile Adhoc network
Step 2: Set of nodes n [¥ n N]
Step 3: Let BS be the Base station
Step 4: Initialize the location of the nodes from the BS $N_i(x,y) < - N_i(rand(x), rand(y))$.
Step 5: Calculate the Inter and Intra distance of the nodes from the BS. (by using distance formula Euclidean).
Step 6: For I = 1 to numberClusters
Elect n_i as CH where n_i member(cluster) && dist(CH,BS) <- max(dist(n_i,BS))
Step 7: End for
Step 8: $N_i(x,y) <- N_i(rand(x), rand(y))$
Step 9: Since all nodes are relocated
Step 10: Goto step 6.

2) Weighted Based Clustering

Fig. 3 shows the initial setup of the network for Weighted Based Clustering where every node and the Base-Station has equal amount of energy (E_i) [16]. In the Weighted Based Clustering method, initially we elect any node as CH as shown in the Fig. 4, because all the nodes are has same weight and same energy level and BS is the Base-Station. Due to data transmission the nodes will lose its energy and weight. Fig. 5 shows the multicasting of data from source to number of destinations in the Weighted Based Clustering. At each time the nodes will communicate with the neighbor nodes, so that every node in the network should be synchronized. In the Weighted Based Clustering after completion of the node energy levels the node is considered as dead node. The node currently acting as cluster-head,

when energy level is goes down then it should hand over cluster-head membership to the node which is having more energy level among the cluster. So we re-elect the CH by calculating the energy and weight by taking the maximum value of the energy, weight of the particular node.

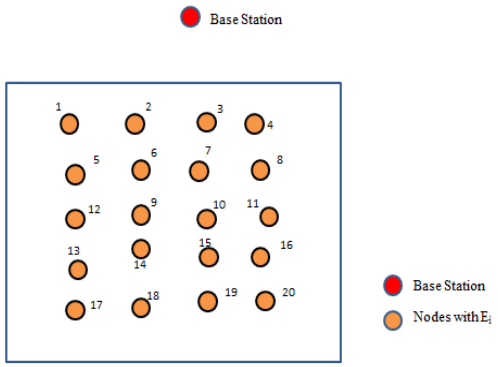

Fig. 3 Initial setup of the network for Weighted Based Clustering where every node and the Base-Station has equal amount of energy (E_i).

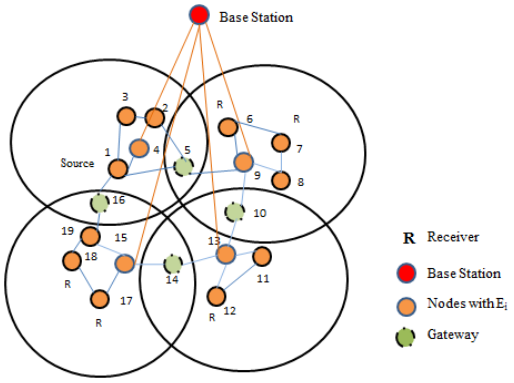

Fig. 4 Base-Station selects any node as CH because every node has equal energy and the CH will broadcast the Hello Packets to all Nodes using the AODV Routing protocol.

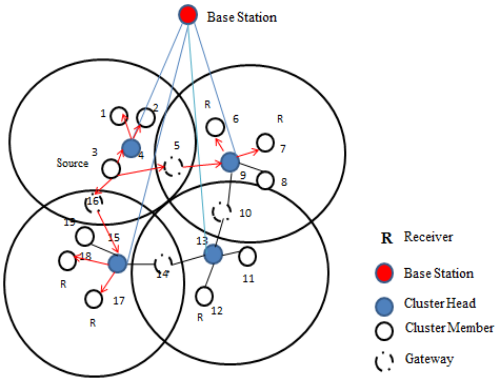

Fig. 5 shows the multicasting of data from source to number of destinations in the Weighted Based Clustering.

The weighted based clustering algorithm is as shown below:

Step 1: Let G be the Mobile Adhoc network
Step 2: Set of nodes n [¥ n N]
Step 3: Let BS be the Base station
Step 4: Initialize the location of the nodes from the BS $N_i(x,y)$ <- N_i(rand(x), rand(y)). //Initialize energy value for all the nodes in the network
Step 5: Let $Energy_i$ = 100J; // for all the nodes
Step 6: Initial phase all nodes should send hello packet to all the nodes.
Step 7: So energy gets vary.
Step 8: For I = 1 to numberClusters
Elect n_i as CH where n_i member(cluster) && energy(CH) <- max(energy(n_i,n_j)).
Step 9: End for
Step 10: Data transmission is happening within the Inter, and Intra clusters.
Step 11: Since all nodes energy get changed, re-elect the CH.
Step 12: Goto step 8.

VI. IMPLIMENTATION

In the implementation phase we have mentioned the details about the implementation of the proposed algorithm and the results found after the implementation. The implementation of the project includes proposed Modified Tiered Authentication Multi-casting Scheme and Distance Based Clustering and Weighted Based Clustering. The simulation parameters include 23 mobilenodes for Distance Based Clustering and 101 mobilenodes for Weighted Based Clustering. The simulation area 1200 X 1000, the channel type is Channel/WirelessChannel, radio-propagation model is Propagation/TwoRayGround, network interface type is Phy/WirelessPhy, MAC type is Mac/802_11, interface queue type is Queue/DropTail/PriQueue, link layer type is LL, antenna model is Antenna/OmniAntenna, max packet in ifq is 50, routing protocol is AODV, Transmission Model is RadioModel, Initial Energy is EnergyModel, Initial energy in Joules is 100 [11].

V. PERFORMANCE ANALYSIS

I. Analysis for Modified TAM

In Modified TAM, the multi-cast involves distinct procedures for intra and inter-cluster operations. For the intra-cluster multi-cast, the cluster head forwards the packet over a tree and employs a symmetry key based authentication protocol that requires only a single MAC per packet. Assuming the network again, the bandwidth overhead with exception that the number of nodes is a fraction of the network population and the fact that the bit overhead per packet is much smaller. For a multi-cast that extends outside the source's cluster, an inter-cluster procedure is invoked to deliver the packet to the cluster heads of the participating receivers. Each cluster-head will then locally multi-cast the packet within its cluster [14]. Thus, the number of transmissions is the sum of all local (intra-cluster) multi-casts inside the individual clusters and the multi-cast from the source node to the other cluster-heads in the network. Before deriving the equation, estimates of the number of clusters N_{ch} and the size of the node population per cluster N_c are needed.

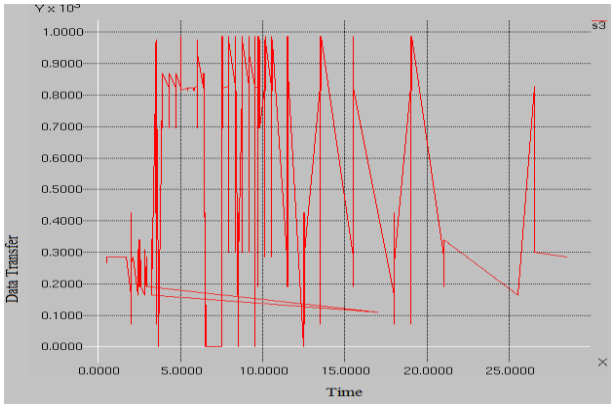

Fig. 6 The graph represents the data transmission vs time for Distance Based Clustering.

The graph which is shown in the Fig. 6 is the data transmission versus time delay for the distance based clustering. The graph which is shown in the Fig. 7 is the data transmission versus time delay. When comparing the two graphs Fig. 6 and Fig. 7 the data transmission is low in the Weighted Based Clustering. The graph which is shown in the Fig. 8 is the data transmission versus time delay in the intra-clustering in the Distance based clustering. And finally the graph which is shown in the Fig. 9 is the data transmission versus time delay for one node in the Weighted based clustering. The packet loss is more in the Weighted based Clustering because of nodes losing the energy in the network and the maximum energy of the nodes in the network is used for selecting the cluster-head and the main concept of the Weighted based Clustering is whenever the node comes to the act it will losses its energy. The node may act as the router or it may act as gateway or it may act as cluster-head or it may act as ordinary node it will losses its energy.

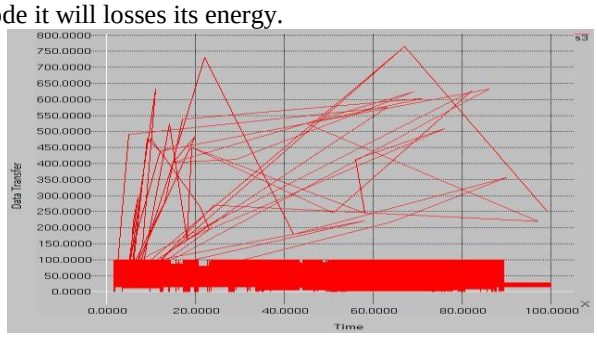

Fig. 7 The graph represents the data transmission vs time for Weighted Based Clustering.

The graph shown in the Fig. 11 is the packet loss versus number of nodes for the distance based clustering. The graph shown in the Fig. 10 is the packet loss versus time for the Weighted based clustering. When comparing the Fig. 10 and Fig. 11, the packet loss is more in the Weighted based clustering.

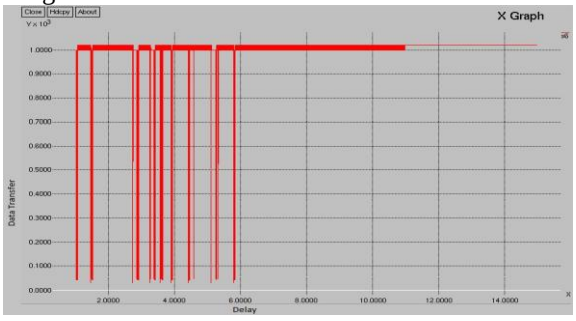

Fig. 8 The graph represents the data transmission vs time for Intra-Clustering in Distance Based Clustering.

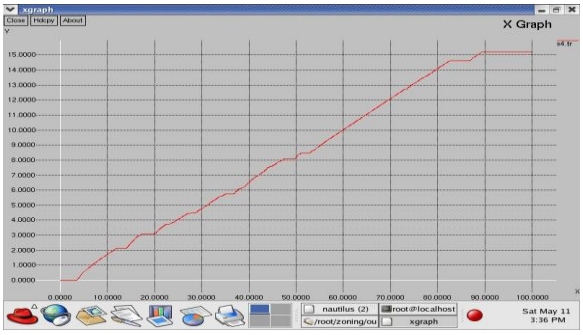

Fig. 9 The graph represents the data transmission vs time for Weighted Based Clustering for one node.

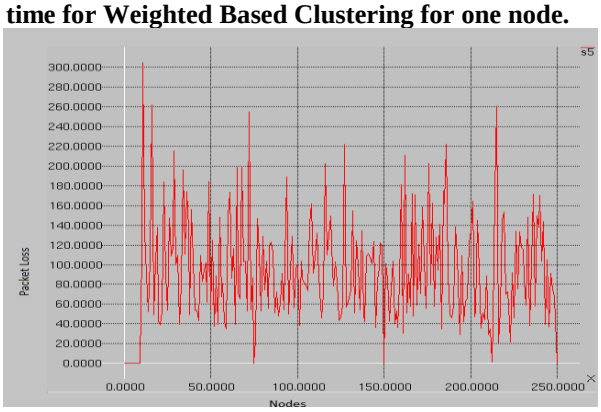

Fig. 10 The graph represents the packet loss vs number of nodes for Weighted Based Clustering.

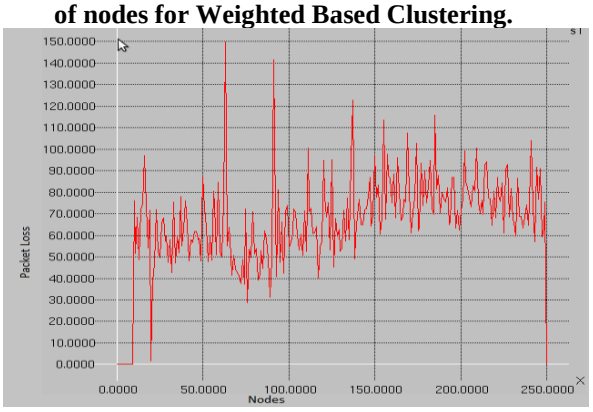

Fig. 11 The graph represents the packet loss vs number of nodes for Distance Based Clustering.

VI. CONCLUSION

The proposed system as modified tiered authentication multicast protocol which improves the authentication and the message integrity than the existing tiered authentication multicast protocol. The proposed system has an improved weighted clustering algorithm based on the Weighted Clustering Algorithm and Distance based Clustering Algorithm. Both the clustering schemes are implemented by using Modified tiered authentication multicast protocol. The simulation results show the Distance Based Clustering is better than the Weighted Based Clustering.

ACKNOWLEDGMENT

The present work is part of Mobile Ad hoc communication Network. The authors wish to thank their parents for supporting and motivating for this work. And a special thanks to Mr. Eswaraiah Korapati and Mrs. Krishna Veni Korapati because without their blessings and supports this was not possible.

REFERENCES

1. Mohamed Younis, Senior Member, IEEE, Osama Farrag, Senior Member, IEEE, and Bryan Althouse, "A Tiered of Multicast Protocol for Ad-Hoc Networks", 2012.
2. Ismail Ghazi Shayeb, AbdelRahman Hamza Hussein and Ayman Bassam Nasoura, "A Survey of Clustering Schemes for Mobile Ad-Hoc Network (MANET)", 2011.
3. Mohamed Elhawary and Zygmunt J. Haas, Fellow proposed an "Energy-Efficient Protocol for Cooperative Networks".
4. Adrian Perrigy, Ran Canetti, Dawn Song, J. D. Tygar, UC Berkeley, Digital Fountain, IBM T.J. Watson, "Efficient and Secure Source Authentication for Multicast", 2009 IEEE Symposium on Security and Privacy, May 2009, pp. 56-73.
5. P. B. Velloso, *et al.*, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Trans. Network Service Management*, vol. 7, no. 3, Sep. 2010.
6. F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Trans. Netw. Service Management*, vol. 7, no. 4, pp. 258–267, Dec. 2010.
7. A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 8, no. 3, pp. 48–66, Dec. 2006.
8. J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 1, no. 1, pp. 31–48, 2005.
9. H. Yang, *et al.*, "Security in mobile ad-hoc wireless networks: challenges and solutions," *IEEE Wireless Commun. Mag.*, vol. 11, no. 1, pp. 1536– 1284, Feb. 2004.
10. A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. 2000 IEEE Symposium Security Privacy*.
11. The Network Simulator - ns-2. Available: http://www.isi.edu/nsnam/ns/
12. L. Wang and F. Gao, "A secure clustering scheme protocol for MANET," in *Proc. 2010 International Conf. Multimedia Inf. Netw. Security*.
13. L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile ad-hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 1, pp. 78–91, first quarter 2009.
14. M. Younis, O. Farrag, and S. Lee, "Cluster mesh based multicast routing in MANET: an analytical study," in *Proc. 2011 IEEE International Conf. Commun.*.
15. G. Angione, P. Bellavista, A. Corradi, and E. Magistretti, "A *k*-hop clustering protocol for dense mobile ad-hoc networks," in *Proc. 2006 IEEE International Conf. Distrib. Computing Systems Workshop*.
16. "A Load-balancing and Energy-aware Clustering Algorithm in Wireless Ad-hoc Networks" Wang Jin, Shu Lei, Jinsung Cho, Young-Koo Lee, Sungyoung Lee, Yonil Zhong.

AUTHORS PROFILE

Mr. Satish K has completed his B.E (CSE) from Rao Bahadur Y Mahabaleshwarappa Engineering College, Bellary, Visveswaraiah Technological University, Belgaum in 2011 and Pursuing MTech (CNE) Final Year in CMR Institute of Technology, Bangalore, Visveswaraiah Technological University, Belgaum.

Mr. R.Anand has completed his M.E (CSE) from Jayam College of Engineering & Technology, Anna University Coimbatore in 2009 and B.E (CSE) from Adhiyamaan College of Engineering, University of Madras in 2001. He is presently working as Associate Professor, CMR Institute of Technology, Bangalore. He presented nearly 10 papers in national and international conferences. His research areas include Wireless Adhoc networks and QOS for MANETS.

Dr. M. Jitendranath is double doctorate in Electronics and Computer Science Engineering and working as Professor & Dean of Research in Computer Science Engineering department in CMRIT, Bangalore. He has published 35 papers in the area of Mobile ad hoc Networks international journals.