ISSN 2047-3338

Providing Efficient Security in Multicast Routing for Ad-hoc Networks

Sejal Butani, Shivani Desai and Sharada Valiveti

***Abstract*— An Ad hoc Network consists of a set of autonomous mobile nodes that communicates via multi-hop wireless communication in an infrastructure-less environment. In such a network group communication takes place by implementing a multicasting technique. This multicasting technique is intended to provide energy and bandwidth efficiency with secure content delivery. The project concentrates on identifying such an efficient multicasting technique. On the basis of comparison of multicasting protocols, Protocol for Unified Multicasting through Announcement (PUMA) has been chosen for initial implementation. PUMA does not rely on any unicast routing approach. It delivers data at a higher efficiency, while also provides a tight bound for control overhead in a wide range of network scenarios. Secure communication is a major concern in PUMA, especially because multicasting protocols are applied in areas such as audio/ video conferencing, corporate communications, collaborative and groupware applications. For secure communication, the performance of RSA and ElGamal was examined; Findings say that RSA's execution time is comparatively less. To guarantee the data integrity in ad hoc networks, SHA-1 and MD5 are analyzed with RSA. Finally, the integration of PUMA has been done with RSA and SHA1 to guarantee more security.**

***Index Terms*— Ad hoc Network, Multicasting, Routing, Security and Data Integrity**

I. INTRODUCTION

AN Ad hoc Network consists of a set of autonomous mobile nodes that communicate via multi-hop wireless communication in an infrastructureless environment. It is an autonomous system in which mobile nodes connected by wireless links are free to move randomly and often act as routers at the same time. Ad hoc networks have become increasingly relevant in recent years due to their potential applications in military battlefield, emergency disaster relief, vehicular communications etc.

In ad hoc applications, collaboration and communication among a group of nodes are necessary. Instead of using multiple unicast transmissions, it is advantageous to use multicast in order to save network bandwidth and resources. Multicasting is a communication process in which the transmission of message is initiated by a single user and the message is received by one or more end users of the network. Under multicast communications, a single stream of data can be shared with multiple recipients and data is only duplicated when required. Main purpose of multicasting is to provide multiple packets to multiple receivers using bandwidth and energy efficiently. The Multicasting protocols can be classified into tree based and Mesh based protocols. The main objective of routing protocol structure is to efficiently deliver information to the members of the multicast group while avoiding non members. A tree based multicasting protocol maintains either shared based multicast tree or source based multicast tree to deliver information from senders to receivers of a multicast group. In a multicasting tree, there is usually only one single path between a sender and a receiver, while in a routing mesh protocol, there may be multiple paths between each sender-receiver pair. Routing meshes are thus more suitable than routing trees for system with frequently changing topology due to availability of multiple paths between a sender and a receiver. Example of tree based multicasting protocols are the multicast ad hoc on-demand distance vector protocol (MAODV) and AMRIS (Ad hoc Multicast Routing protocol). The well-known examples of mesh-based multicasting protocols are the Core assisted mesh protocol (CAMP), On-demand multicast routing protocol (ODMRP) and Protocol for unified multicasting through announcements (PUMA).

The rest of the paper is organized as follows. Section II shows the comparison between multicasting protocols. Section III presents an overview of the PUMA protocol. Section IV shows Simulation. Section V shows security requirements in multicasting ad hoc network. To secure communication using RSA and ElGamal is discussed in Section VI and integrity algorithms are also discussed in that section. Finally, Concluding remarks and future work are made in Section VII.

II. COMPARISON OF MULTICATING PROTOCOLS

In the following section we are going to compare different multicasting protocols in Ad- hoc network.

After comparison of protocols as shown in Table I, we select PUMA protocol because it does not rely on any unicast routing approach. Here, CAMP follows unicast routing approach and this may incur considerable overhead in a large ad hoc network. ODMRP is improved version in terms of control packet overhead as compared to DCMP and NSMP. MAODV and AMRIS, on the other hand, are tree based protocols and they provide only a single route between senders and receivers.

TABLE I
COMPARISON OF MULTICASTING

	ODMRP [4]	MAODV [3]	NSMP [7]	CAMP [2]	DCMP [7]	AMRIS [6]	PUMA [2]
N/w topology	Mesh	Tree	Mesh	Mesh	Mesh	Tree	Mesh
Initialization Approach by	Source	Source	Source	source & receiver	Source	Source	Receiver
Maintenance Approach	Soft State	Hard State	Soft State	Hard State	Soft State	Soft State	Soft State
Dependency	No	Yes	No	Yes	No	No	No
Loop Free	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flooding of control packets	Yes	Yes	Yes	No	Yes	No	No
Independent Routing Protocol	Yes	Yes	Yes	No	Yes	No	Yes
Periodic Control Msg	Yes	Yes	Yes	No	Yes	Yes	Yes

III. PUMA

PUMA (Protocol for Unified Multicasting through Announcement) uses a reactive routing protocol which discovers route only when it is required. It uses a receiver-initiated approach in which the receivers join the multicast group by using address of a special node, without the need for network-wide flooding of control or data packets from all the sources of the group. PUMA [1] uses the shared Mesh based Multicast topology and eliminate the need for a unicast routing protocol and pre-assignment of cores to multicast groups.

PUMA derives from its use of very simple signaling (Multicast Announcements) to accomplish all the functions needed in the creation and maintenance of a multicast routing structure in a MANET. Multicast announcements are used to elect cores dynamically, determine the routes for sources outside a multicast group to unicast multicast data packets towards the group, join and leave the mesh of a group, and maintain the mesh of the group. PUMA uses the soft state approach for Multicast group Maintenance where multicast group membership and its associated routes are refreshed periodically by flooding its Multicast Announcement (MA) packet. In PUMA, nodes maintain a packet ID cache to drop duplicate data packets.

A. Comparison of PUMA and ODMRP by structure

PUMA and ODMRP are both mesh-based protocols. However, every sender performs control packet flooding in ODMRP. Hence, depending on the number of senders there may be multiple nodes flooding the network periodically. In PUMA on the other hand, only one node, i.e., the core floods the network.

Fig. 1 and Fig. 2 illustrate the mesh established by ODMRP and PUMA respectively, where nodes R1, R2 and R3 are receivers and nodes S1, S2 and S3 are senders.

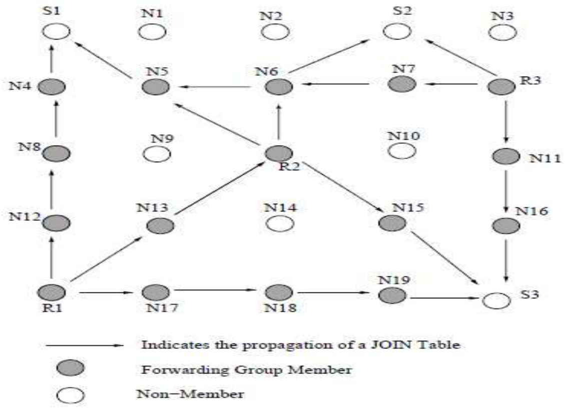

Fig. 1. Mesh structure of ODMRP [2]

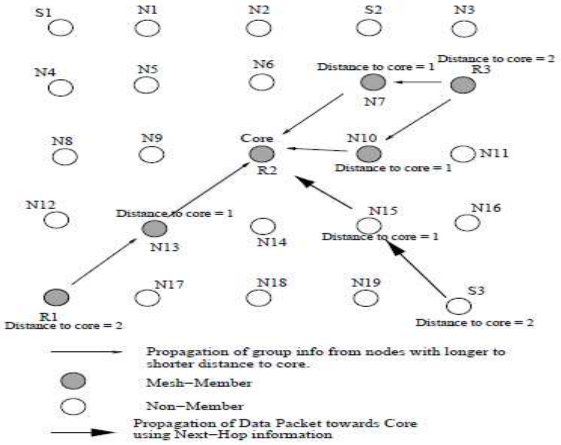

Fig. 2. Mesh structure of PUMA [2]

The forwarding group of ODMRP contains 16 nodes, whereas the mesh of PUMA contains only 6 nodes. Hence, a data packet sent by node S3 is retransmitted by 16 nodes in ODMRP, whereas in PUMA, it is retransmitted only by only 7 nodes. PUMA tends to concentrate mesh redundancy in the region where receivers exist by including all shortest paths from each receiver to the core, which is also a receiver. On the other hand, the mesh in ODMRP is simply the union of the shortest paths connecting all senders to all receivers. This can lead to a significant and unnecessary data packet overhead if all senders are also not receivers.

IV. SIMULATION

PUMA and MAODV are both receiver-oriented protocols. However, PUMA is a mesh-based protocol and provides multiple routes from senders to receivers. MAODV, on the other hand, is a tree based protocol and provides only a single route between senders and receivers.

A. Simulation Method and Environment

TABLE II
SIMULATION METHOD AND ENVIRONMENT

Simulator	NS 2.35
Total number of Nodes	25 to 175
Area	1000m × 1000m
Simulation Time	100 seconds
Mobility Model	Random Way Point Model
Minimum Speed	1 m/s
Maximum Speed	10 m/s
MAC layer	IEEE 802.11
Direction antenna model	OmniAntenna
Traffic Generator	CBR(Constant bit rate)
Data payload size	512 bytes

B. *Performance results*

We evaluated the performance of PUMA and compared it with MAODV in terms of routing overhead, throughput, packet delivery fraction and end-to-end delay in NS-2.35. The obtained results are illustrated in Fig. 3, Fig. 4, Fig. 5 and Fig. 6.

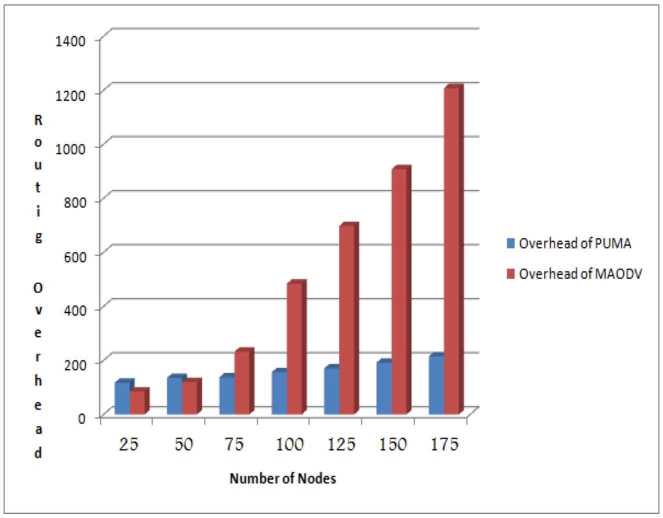

Fig. 3. Comparison of Routing Overhead

Based on the simulation results shown in Fig. 3 the routing overhead of PUMA is compared with MAODV for varying number of nodes. For increasing number of nodes, the routing overhead is increased in MAODV for varying number of nodes. So, MAODV incurs far more overhead compared to PUMA.

Fig. 4, shows the Throughput analysis. For increasing number of nodes the throughput of PUMA is higher than the MAODV.

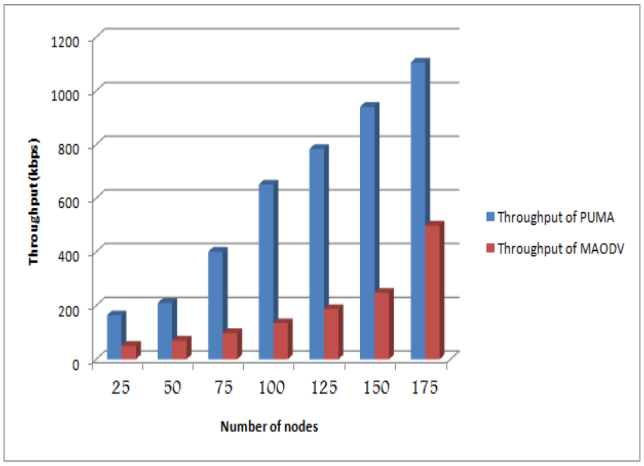

Fig. 4. Performance comparison of Throughput

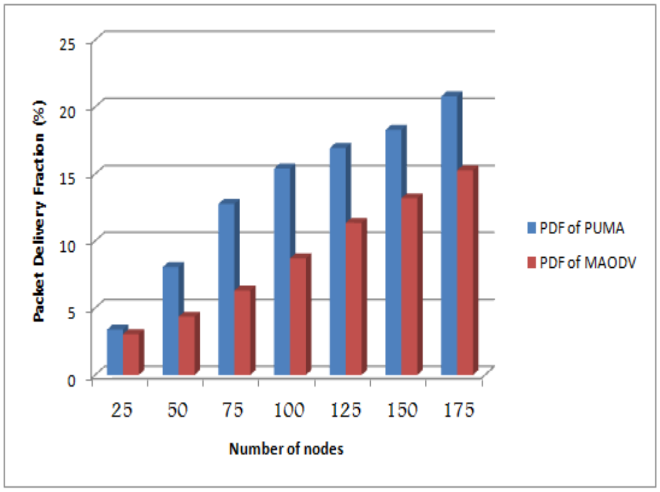

Fig. 5. Performance comparison of Packet Delivery

Based on the simulation results shown in Fig. 5, the packet delivery fraction of PUMA is higher than MAODV for varying number of nodes.

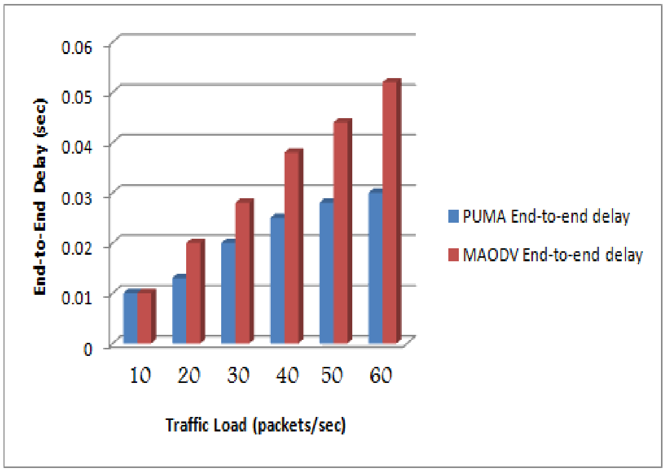

Fig. 6. Performance comparison of End-to-End Delay

Based on the results shown in Fig. 6, higher End-to-end delay values imply that routing protocol is not fully efficient and causes congestion in the network. As against the MAODV, PUMA exhibits lesser values of End-to-end delay.

C. *Performance Analysis*

PUMA incurs far less overhead as compared to MAODV. It has higher packet delivery fraction and throughput. The lesser values of End-to-end delay imply a better performance than other protocol. So, PUMA has been selected for further implementation.

V. SECURITY REQUIREMENTS

Secure communication [1] is a major concern in PUMA, especially because multicasting protocols are applied in areas such as audio/ video conferencing, corporate communications, collaborative and groupware applications.

To ensure secure communication, the selected cryptography algorithm must have following requirements [9]:

- Confidentiality
- Authentication
- Integrity
- Non repudiation

VI. CRYPTOGRAPHY

There are many types of Cryptography schemes to ensure security, such as symmetric key algorithms, asymmetric key algorithms and message digests. Symmetric and asymmetric key algorithms provide secrecy. Message digests are used for authentication. The purpose of this project was to determine which algorithm performs better for given input data. In public key algorithms, the encryption and decryption keys are different. As compared to symmetric cryptography, public key cryptography provides simplified key distribution. Public key space is larger and robust enough so no one can guess what they are. Public key cryptography also verifies the identity of sender using signature. From the Public key cryptography, we have implemented RSA and ElGamal algorithms.

A. *Performance Comparison of RSA and ElGamal*

We measured the encryption and decryption times of RSA and ElGamal on the client and server and graphs were plotted representing the measured times.

In Fig. 7 and Fig. 8, we see the encryption and decryption times increased with the varying number the nodes.

In ElGamal, the ciphertext is twice as long as the plaintext, which is a disadvantage as compared to RSA algorithm. From the figure we see, RSA takes less execution time as compared to ElGamal. So, here RSA is selected for further implementation.

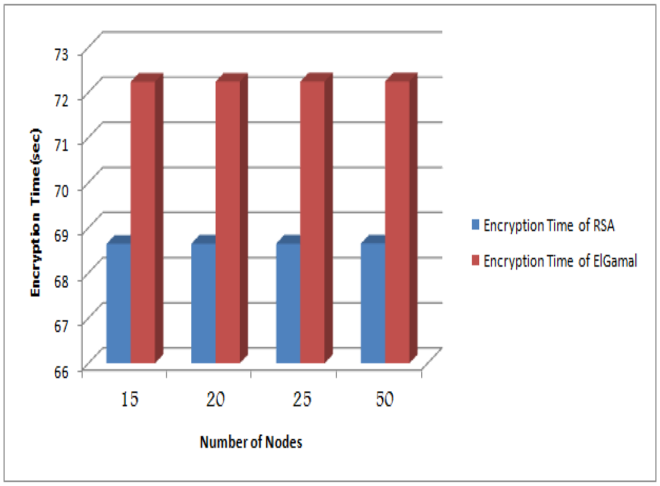

Fig. 7. Comparison of Encryption time

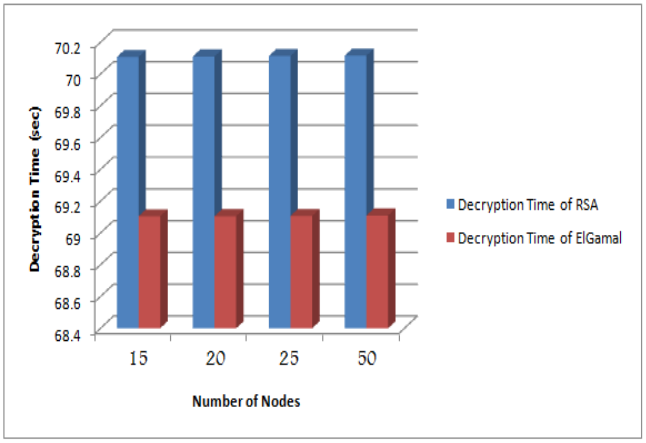

Fig. 8. Comparison of Decryption time

B. *Integrity in Multicast Ad hoc Network*

Integrity plays an important role in ad-hoc networks. To overcome man-in-the-middle attack in mobile-ad-hoc networks, SHA-1 and MD-5 algorithms are used. Secure hash functions or message digests work on an authentication scheme and do not require encrypting the entire message. SHA-1 [10] and MD5 [10], [11] are algorithms for computing a 'condensed representation' of a message or a data file. The 'condensed representation' is of fixed length and is known as a 'message digest' or 'fingerprint'. Here, SHA-1 generates 160 bits of message digest and MD5 generates 128 bits of message digest.

In further implementation, we have done the binding of SHA-1 and MD5 with RSA and measured the performance of RSA after binding.

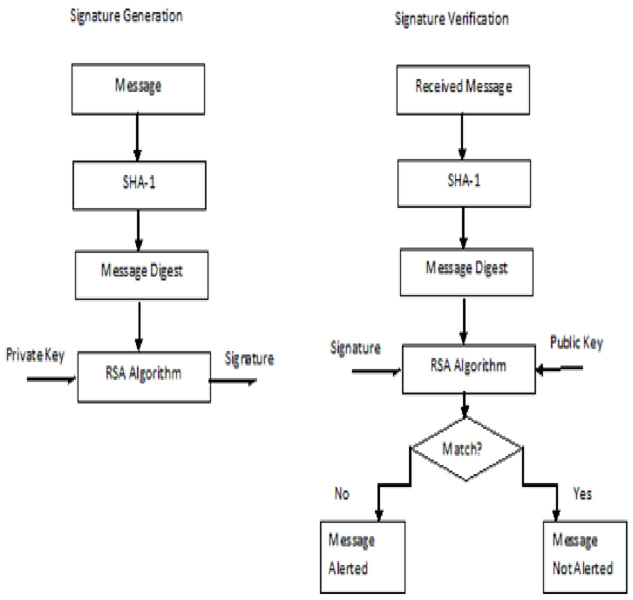

Fig. 9. Working of SHA-1 after binding with RSA algorithm

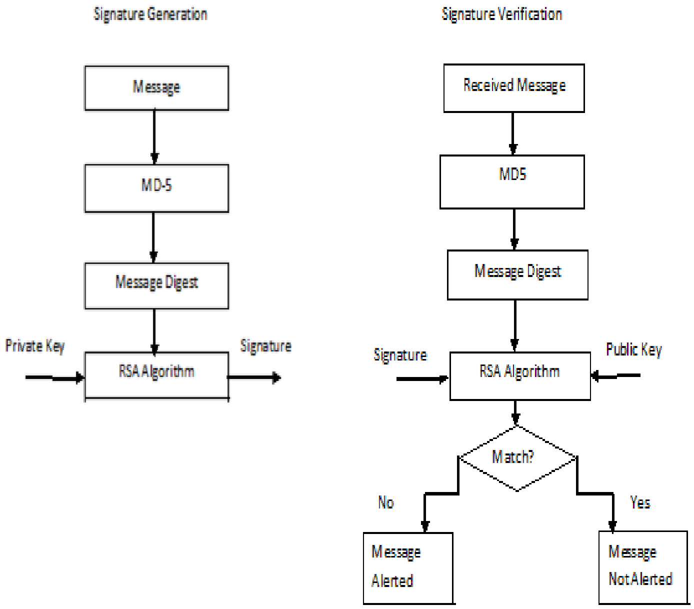

Fig. 10. Working of MD5 after binding with RSA algorithm

Here, the working of SHA-1 and MD5 after binding with RSA is shown in Fig. 9 and Fig. 10 respectively. Working of both the algorithms is similar. Basically the process can be implemented in two phases. First phase is signature generation, which is done on encryption side (sender side) and second is signature verification, which is done on decryption side (receiver side). In signature generation, first the message goes to SHA-1 or MD5 algorithm and then algorithm produces the message digest. After that, message digest goes to RSA algorithm and produces the signature using public key. In second phase signature verification, after receiving message from the sender side, the received message goes to again SHA-1 or MD5 algorithm and produces message digest. Then, message digest goes to RSA algorithm and produces another signature using public key. Now, if signatures at the sender and the receiver side are same, then message is not altered. But if signatures don't match, then the message is altered.

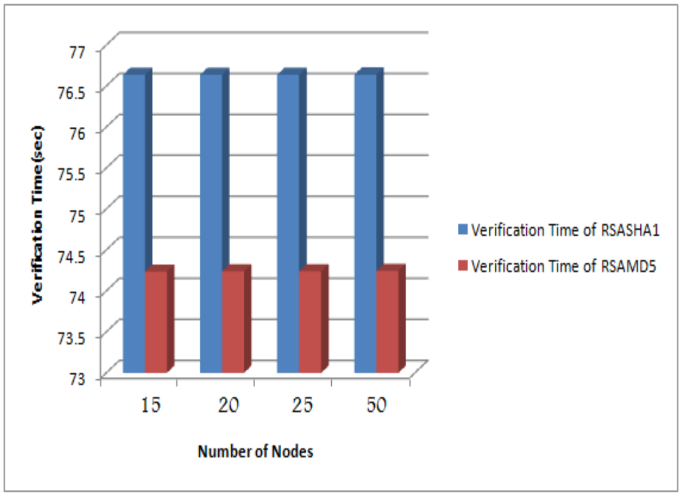

Fig.11. Comparison of Verification time

C. Security Analysis

The Verification time using RSA and SHA-1 is higher than RSA and MD5 as shown in Fig.11. Verification times for both RSA and SHA-1 and RSA and MD5 increased with increasing key size. This larger digest size of RSA and SHA-1 makes it stronger against attacks. These results suggest RSA and SHA-1 is more secure than RSA and MD5.

VII. CONCLUSION AND FUTURE WORK

PUMA is chosen for multicast ad hoc network based on comparison of various multicasting protocols. PUMA provides less routing overhead, high throughput and better PDF as compared to other protocols. RSA and SHA-1 is more secure as compared to RSA and MD5.

Future work will focus on the integration of PUMA and Security module.

REFERENCES

[1] Busola S. Olagbegi and Natarajan Meghanathan, June 2010, A Review of the Energy Efficient and Secure Multicast Routing Protocols for Mobile Ad hoc Networks - (GRAPH-HOC) Vol.2, No.2, Jackson State University.

[2] Ravindra Vaishampayan, March 2006, Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks University Of California Santa Cruz.

[3] Multicasting in Ad-Hoc Networks: Comparing MAODV and ODMRP - Thomas Kunz and Ed Cheng Carleton University

[4] E. Cheng, 2001, On-demand multicast routing in mobile ad hoc networks, Carleton University, Department of Systems and Computer Engineering.

[5] Brian Neil Levine, J.J. Garcia-Luna-Aceves, 1998, A comparison of reliable multicast protocols- Computer Engineering Department, School of Engineering, University of California, Santa Cruz, CA 95064 USA - Multimedia Systems c Springer-Verlag.

[6] Wu, C.W and Tay, Y.C., "AMRIS: A multicast protocol for ad hoc wireless networks", IEEE Proceedings of Conference on Military Communications, MILCOM 1999, Vol.1, pp. 25-29.

[7] Dewan Tanvir Ahmed, Multicasting in Ad Hoc Networks, University of Ottawa, Wireless Ad Hoc Networking , Ottawa, Ontario, Canada, Fall 2005.

[8] Osmah S. Badarneh and Michel Kadoch, Multicast Routing Protocols in Mobile Ad Hoc Networks: A Comparative Survey and Taxonomy, EURASIP Journal on Wirelesss Communication and Networking, Volume 2009(2009), Article ID 76047, 42 pages.

[9] Zhou, L. and Haas, "Securing Ad Hoc Network. IEEE Networks, Vol. 13, No. 6.

[10] Schneier Bruce, "Opinion:Cryptanalysis of MD5 ans SHA: Time for a new standard", April 19,2004.

[11] Den Boer B, Bosselaers A.,"Collisons for the compression function of MD5, Advances in cryptography",EUROCRYPT'93,p-293-304.

Sejal L. Butani B.Tech. Information and Technology Engineering from U.V. Patel college of Engineering ,Ganpat university , Mehsana, Gujarat, India, Year 2008. Working in the area of Wireless Ad hoc Network. Pursuing M.Tech from Nirma University, Ahmedabad, Gujarat, India. Field of research is Wireless Ad hoc Networks and Security.

Shivani Desai B.E in Computer Engineering from Government. Enginnering. College, Gandhinagar, Gujarat University, Gujarat, India, Year 2009. Working in area of Wireless Sensor Network. Pursuing M.tech from Nirma University, Ahmedabad, Gujarat, India. Field of research is Wireless Sensor Networks and Security.

Sharada Valiveti M.E. in Computer Engineering from ISTAR, SP University, Vallabh Vidyanagar, Gujarat, India in the year 2005. Working in the area of Ad Hoc Network Security. Pursuing Ph.D. from Nirma University, Ahmedabad, Gujarat, India. Field of research is Enhancing Security with Effective Routing Mechanisms for Ad Hoc Networks