International Journal of Research Studies in Science, Engineering and Technology
Volume 2, Issue 8, August 2015, PP 91-98
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

Security Enhanced Routing for Delay Tolerant Networks using Social Grouping

Jiji Soman[1], Devi Murali[2]

[1]Semester IV, M.Tech in Communication Engineering, Sree Buddha College of Engineering for Women, Pathanamthitta, Kerala, India
[2]Assistant Professor, Sree Buddha College of Engineering for Women, Pathanamthitta, Kerala, India

Abstract: *Delay tolerant networking (DTN) is a computer network architecture that seeks to address the technical issues in heterogeneous network that may lack continuous network connections. DTN overcome the frequent disconnections by storing data packets at the nodes for long periods of time until they come near other nodes. To increase the delivery probability, multiple copies of the same packet are spread on the network so that one of them reaches the destination. Given the limited storage and energy resources of many DTN nodes, there is a trade-off between maximizing delivery and minimizing storage and energy consumption. Protocol based on social grouping among the nodes will maximize data delivery and minimizing network overhead by efficiently spreading the packet copies in the network. The SGBR protocol achieves higher delivery ratio and less average delay compared to other protocols with significant reduction in network overhead. But using this protocol the security to data packets cannot be guaranteed. The security enhanced version of the SGBR protocol is proposed and simulated using Network Simulator Version-2 (NS2) to evaluate the performance of the modified protocol. The RSA algorithm is used to secure the data transmitted by the encryption and decryption of the packets at the source and destination respectively. The network parameters are improved by using these techniques and also ensured a reliable data network.*

Keywords: *DTN, AVG Delay, PDR, RSA, Packet Drop*

1. INTRODUCTION

Personal communication devices, such as cellular phones, have enabled voice and data communications to mobile users, achieving global connectivity via infrastructure networks (cellular, WLAN). Local connectivity among the devices may additionally be obtained by forming ad-hoc networks since the mobile devices are virtually always turned on and have the necessary radio interfaces, processing power, storage capacity, and battery lifetime to act as routers. However, such usually sparse ad-hoc networks generally cannot support the type of end-to-end connectivity required by the classic TCP/IP-based communications due to frequent topology changes, disruptions, and network partitions caused by the node movement. Instead, asynchronous message passing (store-carry-forward networking) has been suggested to enable communication over the space-time paths that exist in these types of networks (e.g., Delay-tolerant Networking).

Delay-tolerant Networking (DTN) enables communication in sparse mobile ad-hoc networks and other challenged environments where traditional networking fails and new routing and application protocols are required. Past experience with DTN routing and application protocols has shown that their performance is highly dependent on the underlying mobility and node characteristics. Applications of DTN have been found in many challenging environments such as providing delay-tolerant Internet services in suburban and rural areas. This has been implemented by first mile

solutions with a system called DakNet. Vehicular networking is a wide and growing field of DTNs, where many applications are being explored. One of these applications is the virtual warning sign that brings the hidden or unseen warning signs to the vehicle driver to be able to take the required precautions as early as possible. Another application is to provide Internet access to vehicles, by connecting to roadside wireless base stations. Non-commercial applications include monitoring and tracking wildlife animals and whales in oceans, and environmental monitoring, such as lake water quality monitoring and road-side noise monitoring.

The traditional routing protocols for wired and wireless networks fail to work in the DTN environment because they assume the existence of continuous end-to-end connections between sources and destinations. Routing protocols developed for DTN should be adapted to this challenging environment by sending multiple copies of data packets to increase the probability that one of the copies reaches the destination. Nodes receiving the packet copies store them until they meet other nodes or meet their destinations. A routing protocol that exploit the social grouping characteristic of DTN nodes will spreads a small number of packet copies to reduce network overhead, while guiding the packet copies using only local information to reach the destination. Consider two nodes to belong to the same social group if they contact each other frequently compared to their contacts with other nodes. All of the previous protocols are focused on social metrics, which predicts the path from source to destination by including nodes with strong social connections. The disadvantages of this approach are the need to collect network wide information to better predict the path to destination. But the social grouping based protocol propose an exclusive social metric, which sprays messages by excluding nodes that are not expected to add a significant value to the node carrying the message. Using exclusive metrics reduces the need to collect network wide information, while improving the performance metrics. Social groups-based routing (SGBR) is a multiple-copy routing protocol in DTN communication. The protocol exploits social grouping among network nodes to increase the packet delivery probability, without flooding the network with many redundant copies. The concern about a communication network is it's security and reliability of the packet data. In order to make the data secure, RSA algorithm is implemented to share the secret key between the source and destination. This enhanced version of SGBR is simulated and evaluated using Network Simulator Version-2 (NS2).

2. SOCIAL GROUP BASED ROUTING (SGBR) PROTOCOL

The SGBR protocol aims to utilize the grouping property of nodes. It is widely used the large and small communication networks. Consider the nodes that are frequently meeting each other, to belong to the same social group i.e., they are expected to meet each other again frequently. They are also expected to have around the same social relation with other nodes. Then each node may consider itself a representative of the group to distribute its packets to other groups. Therefore, a node that has a packet destined to other nodes outside its group tends to forward the packet copies to other groups. From this protocol perspective, it is useless to keep several copies of the same packet inside one social group.

2.1 The Protocol Design

To implementation of the protocol design, a node should know the nodes that belong to its group (frequently connecting) and those that are not. To measure how strong is the connection between two nodes, a parameter is used, the degree of connectivity, Γab, which is strengthened by frequent meetings between nodes considered, 'a' and 'b', and weakened by the time elapsed since the last meeting. Upon each meeting of nodes, their degree of connectivity, Γab, is updated using the

following equation:

$$\Gamma a,b = (\Gamma a,b)old\gamma^k + (1 - ((\Gamma a,b)old\gamma^k)\alpha \quad (1)$$

where:

Γab is the degree of connectivity between nodes a and b,

(Γa,b)old is the degree of connectivity before executing the equation,

α, α€(0,1], is the updating factor,

γ.γ€(0; 1], is the aging constant, and

k is the number of time units that have elapsed since the last time nodes a and b have met.

The protocol are explained using the following steps:

- Each packet generated is assigned with a unique ID. The list of all packet IDs in a node's buffer is called the Summary Vector.
- Each node 'a' has a degree of connectivity Γab to every other node 'b' that is strengthened by their frequent meetings, using. Based on the degree of connectivity, the two nodes decide to forward or not to forward their packets, except those that are destined to the other node as they should be delivered to the other node regardless of their degree of connectivity.
- Before two contacting nodes start transferring data packets, they exchange their Summary Vectors. Packets that are destined to the other node are put on the head of the transmission queue. Other packets that are not destined to the other node and are not in its buffer are sorted based on their traversed hop counts, so that packets with the minimum hop count will be transferred first.
- Packets that are not destined to the other node are transferred only if the degree of connectivity is less than a Connectivity Threshold, Cth, which indicates that these two nodes do not belong to the same group. In addition, each packet has a limited number of copies to be spread using the Binary Spray and Wait (SnW) mechanism. Packet transfer continues for the contact duration.
- After a packet is transferred, it may be dropped from the sender node if the degree of connectivity is greater than the dropping threshold Dth, which ensures that the receiving node is far from being in the same group.
- If the buffer of the receiving node is full, the packet with the largest hop count is dropped to create a space for the forwarded packet to be stored.

3. SECURITY ENHANCEMENT

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used

asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

3.1 The RSA Algorithm

- The RSA algorithm uses two keys, d and e, which work in pairs, for decryption and encryption, respectively.
- A plaintext message P is encrypted to cipher text by: C = Pe mod n.
- The plaintext is recovered by: P = Cd mod n.
- Because of symmetry in modular arithmetic, encryption and decryption are mutual inverses and commutative. Therefore, P = Cd mod n = (Pe)d mod n = (Pd)e mod n Thus, one can apply the encrypting transformation first and then the decrypting one, or the decrypting transformation first followed by the encrypting.

4. SIMULATION

The performance of SGBR protocol and it's security enhancement is evaluated using the NS2 simulator. The NS-2 simulation environment offer great flexibility in investigating the characteristics of sensor networks because it already contains flexible models for energy constrained wireless ad hoc networks. The wireless model also includes support for node movements and energy constraints. Consider a wireless network which will represent a real time environment. The wireless model essentially consists of the Mobile Node at the core with additional supporting features that allows simulations of multi-hop ad-hoc networks, wireless LANs etc. The Mobile Node object is a split object. The C++ class Mobile Node is derived from parent class Node. A Mobile Node thus is the basic Node object with added functionalities of a wireless and mobile node like ability to move within a given topology, ability to receive and transmit signals to and from a wireless channel etc. A major difference between them is that a mobile Node is not connected by means of Links to other nodes or mobile nodes. Mobile Node is the basic NS Node object with added functionalities like movement, ability to transmit and receive on a channel that allows it to be used to create mobile, wireless simulation environments. The class mobile node is derived from the base class Node. The entire processing steps can be categorized mainly into nine modules. The main modules in the simulation procedures are explained below:

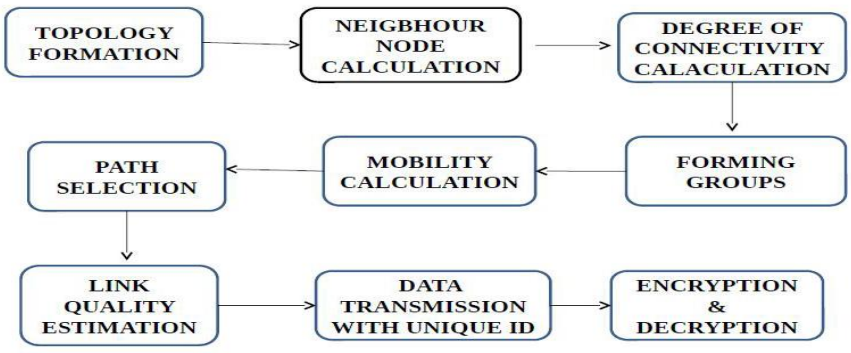

Figure1. *Block diagram of system model*

The wireless model essentially consists of the Mobile Node at the core, with additional supporting features. The ad-hoc routing protocols used here is Dynamic Source Routing (DSR). Initially the wireless nodes are created. This network model consists of 40 nodes. Before creating the mobile nodes, their topology has to be manually defined. The nodes are created using flat grid topology. When the topology of the network to be simulated is drafted, then the first step would be to create the mobile nodes. Then the node movement is set. The nodes will transmit the hello packets to indicate

the presence in the network. After this, the nodes will ready to transmit data packets. The Master key sharing is the important step in the encryption process. The nodes which will be an attacker cannot access this Master key shared in the network. The neighbour nodes are calculated in order to find the optimal path for the efficient routing. The nodes are grouped according to degree of connectivity and mobility calculation of each nodes in the network is done. Path selection between source and destination is done with respect to the DSR routing. Link quality between nodes is estimated. Data transmission is done by packet by packet and each packet provided with unique id from the source.

Below figures shows the network system and procedures developed for the simulation of the SGBR protocol using NS2.

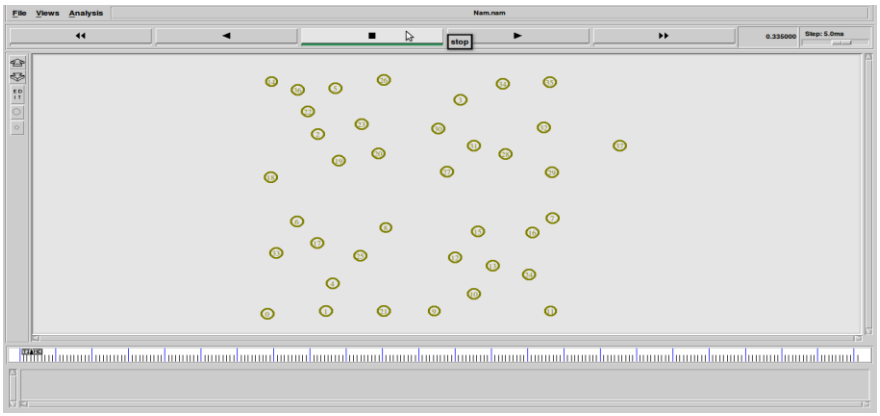

Figure2. *Node creation*

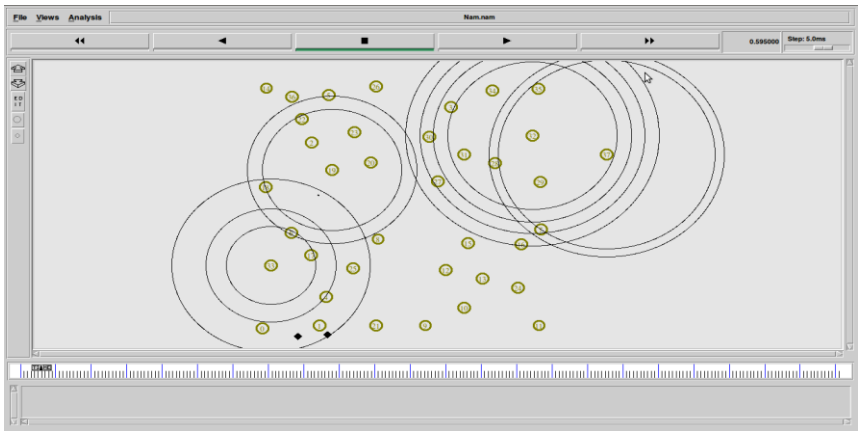

Figure3. *Master key sharing*

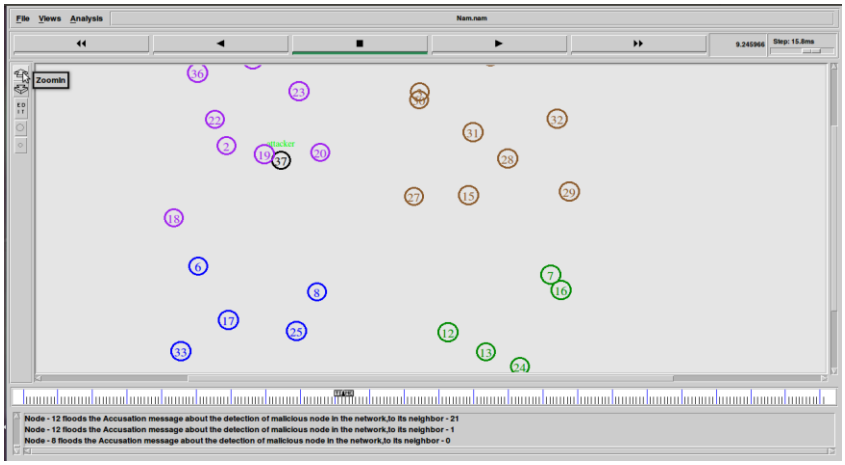

Figure4. *Attacker Detection*

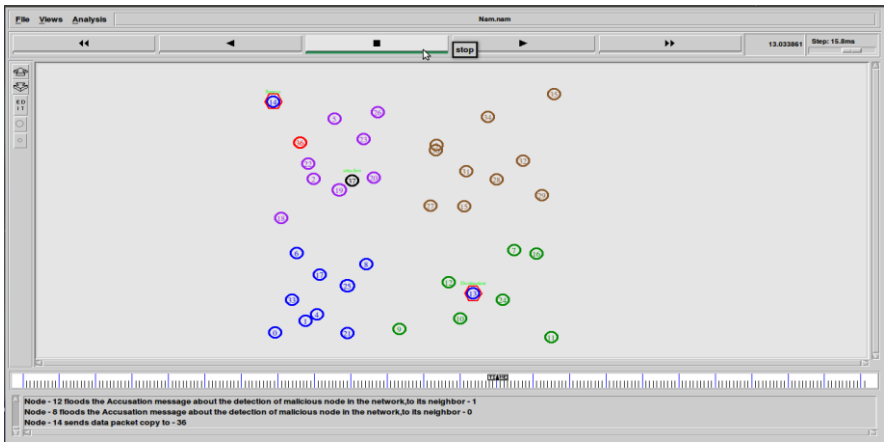

Figure5. *Data transmission*

5. RESULT

The parameters that considered to evaluate the performance of this protocol was Packet delivery Ratio (PDR), Packet Drop and Average Delay. These parameters' have been plotted and compared with other two DTN protocols- MAXPROP and Epidemic Routing Protocol.

- **PACKET DELIVERY RATIO**

  The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

  PDR = ∑ Number of packet receive / ∑ Number of packet send.

- **PACKET DROP**

  It is the total number of packets dropped during the simulation. The lower value of the packet drop means the better performance of the protocol.

  Packet Drop = Number of packet send – Number of packet received.

- **AVERAGE DELAY**

  It is defined as the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

  AVG Delay= ∑ (arrive time – send time) / ∑ Number of connections.

The results show that the enhanced SGR protocol shows better performance compared to the other existing protocols. The PDR have much improved and the attain a stable value. Also the AVG delay reduced compared to the other protocols that were considered. The resultant graphs are shown below:

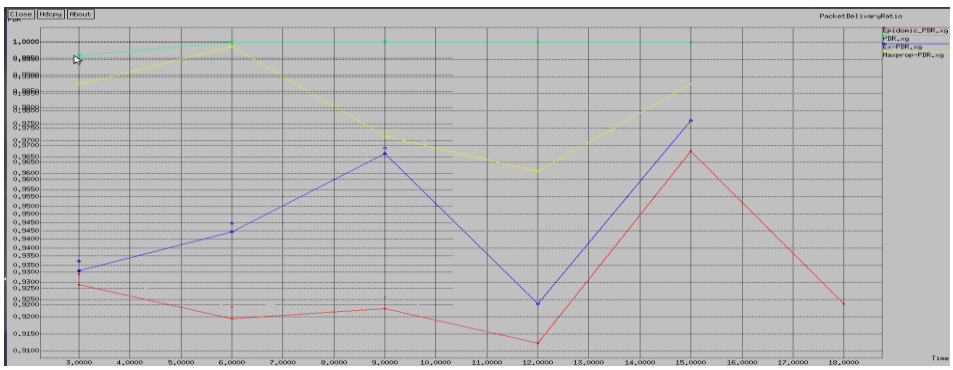

Figure6. *PDR*

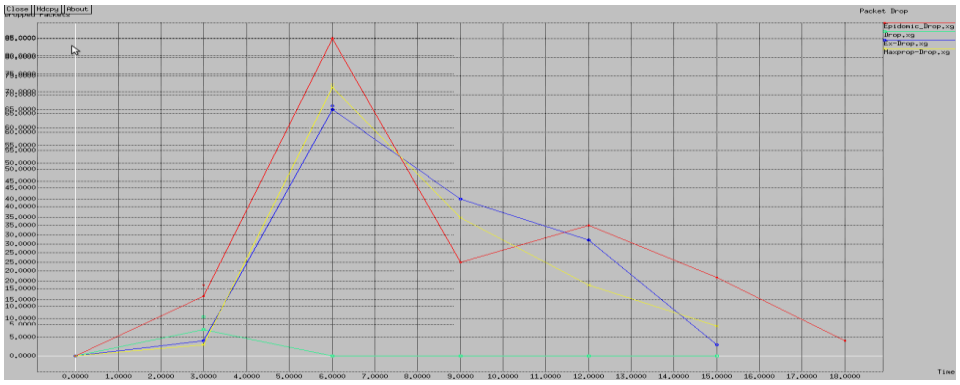

Figure7. *Packet Drop*

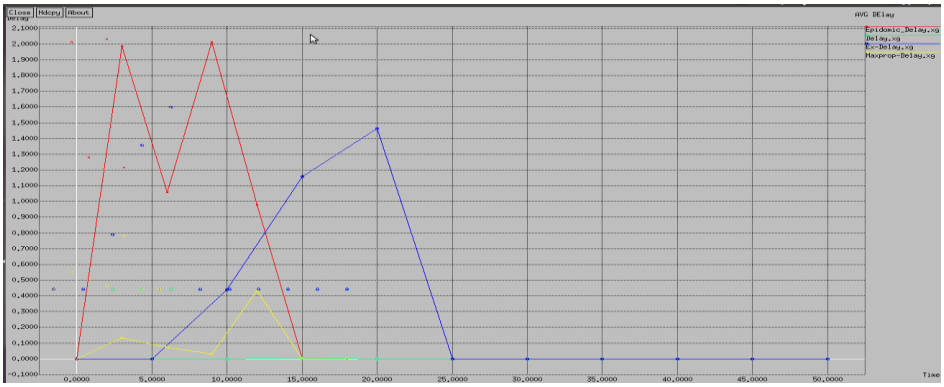

Figure8. *Average delay*

6. CONCLUSION

DTN are alternative structures to traditional networks facilitating connectivity of system and network regions with sporadic or unstable communication links. In networks with such circumstance mobile relay node are used to carry and forwarding message and make communication possible among other nodes. SGBR protocol utilizes the social relations between nodes to reduce redundant copying of packets is simulated using the network simulator. The network model using the enhanced version of this protocol significantly reduces number of transmissions leading to a considerable saving in energy consumption, while keeping same or higher delivery ratio. It also increase the delivery ratio, which causes an increase in the average packet delay which is acceptable in delay tolerant networks. This protocol system has number of procedures to deal the social grouping and several constraints to handle a packet in the network. Due to lack of end to end connection between the source and destination in DTN, the intermediate need to store data packets for a long period. This increases the buffer overhead. So the system reduces the need of long storage of data in the intermediates. Since the protocol, utilizes the social relations between nodes, it leads to a reduction in redundant copying of packets and search helps to identify the optimal path for every data. The spreading of data packets will cause an issue in the communication network system where security is an important concern. Cryptographic techniques allow a source node to disguise data so that an intruder can gain no information from the intercepted data. The receiver node must be able to recover the original data from the disguised data. The data is secured using an asymmetric key algorithm- RSA algorithm.

ACKNOWLEDGEMENT

This study was supported by the Department of Electronics and Communication Engineering, Sree Buddha College of Engineering for Women, Kerala. I would like to express my gratitude to my guide, coordinator and my friends whose expertise, understanding, and patience, added considerably to my post graduate experience.

REFERENCES

[1] Tamer Abdelkader, Kshirasagar Naik, Amiya Nayak, ”SGBR: A Routing Protocol for Delay Tolerantn Networks Using Social Grouping,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, December 2013.

[2] “Delay Tolerant Networking Research Group.” http://www.dtnrg.org, 2013.

[3] A. Pentland, R. Fletcher, and A. Hasson, “Daknet: Rethinking Connectivity in Developing Nations,” Computer, vol. 37, no. 1, pp. 78-83, Jan. 2004.

[4] A. Vahdat and D. Becker, ”Epidemic Routing for Partially Connected Ad Hoc Networks,” Technical Report CS-200006, Duke Univ., April, 2000.

[5] A. Lindgren, A. Doria, and O. Schelen, ”Probabilistic Routing in Intermittently Connected Networks,” SIGMOBILE Mobile Computing and Comm. Rev., vol. 7, no. 3, pp. 19-20, July 2003.

[6] J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine, ”Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks,” Proc. IEEE INFOCOM, pp. 1-11, April, 2006.

[7] E. Bulut, Z. Wang, and B. Szymanski, ”Impact of Social Networks on Delay Tolerant Routing,” Proc. IEEE GlobeCom, pp. 1-6, December, 2009.

[8] E.M. Daly and M. Haahr, ”Social Network Analysis for Routing in Disconnected Delay-Tolerant Manets,” Proc. ACM Eighth Intl Symp. Mobile Ad Hoc Networking and Computing, pp. 32-40, 2007.

[9] T. Abdelkader, K. Naik, A. Nayak, and N. Goel, ”A Socially-Based Routing Protocolfor Delay Tolerant Networks,” Proc. IEEE GlobeCom 10, 2010.

AUTHORS’ BIOGRAPHY

Jiji Soman is doing her final semester Master’s Degree in Communication Engineering at Sree Buddha College of Engineering for Women, Kerala, India. She has published two research papers in the field of Communication Networks during her academics. Her research interests include the areas of computer networking, wireless sensor networks, optical fibre communication, mobile ad hoc and sensor networks, dependable communication, intelligent transportation systems, and distributed systems, with 3 publications in refereed journals and conference proceedings.

Devi Murali has 5 years of experience in teaching and research in India. She is currently an assistant professor in the Department of Electronics and Communication at Sree Buddha College of Engineering for Women, Kerala, India. Her research interests include the areas of digital signal processing, computer networking, optical fibre communication, mobile ad hoc and sensor networks, with many publications in refereed journals and conference proceedings.