ISSN: 2229-6948 (ONLINE)
DOI: 10.21917/ijct.2013.0108

S-SPRAY ROUTING PROTOCOL FOR INTERMITTENTLY CONNECTED MOBILE NETWORKS

S. Ramesh[1], R. Indira[2], R. Praveen[3] and P. Ganesh Kumar[4]
[1,2,3]*Department of Computer Science and Engineering, Anna University Regional Centre, Madurai, India*
E-mail: [1]itz_ramesh87@yahoo.com, [2]indi_cse@yahoo.co.in, [3]pravvin.it@gmail.com
[4]*Department of Electronics and Communication Engineering, KLN College of Engineering, India*
E-mail: ganesh_me@yahoo.com

Abstract
The Intermittently Connected Mobile Networks (ICMN) is a disconnected mobile network where a complete connectivity never exists. The intermittent connectivity is due to the dense nature of the network. The dense nature is mainly due to the high mobility of the nodes in the network. Routing in such a sparse network is arduous. Due to the disconnected attribute of the network, the encounter of the suspicious nodes in the network also remains a tedious task. In this paper, we put forward a secure routing that aids in detecting and preventing intrusion of malicious nodes. The routing process is made adorable through Spray and Wait (SNW). Since ICMN is prompt to higher delays certain authentication series are used to enable secure communication within the network. The amalgamation of SNW with authentication series leads a novel routing protocol named S-Spray (Secured-Spray) which is highly secure.

Keywords:
Mobile Network, ICMN, Delay Tolerant Network, S-Spray, Spray and Wait, Authentication Series

1. INTRODUCTION

The era of network started with the traditional wired networks that is lasting from many decades that communicate through physical medium. It leads to Wireless Networks where communication does not enfold the physical medium. Another form of network evolved where nodes are intended to move within the network named Mobile networks. Subsequent to which is the Wireless Sensor Networks (WSN) where the communication channels operate through the inbuilt wireless sensor devices within the nodes. A new form of network raised as a challenge for routing called Ad hoc network with a special feature of dynamically changing topology. Mobile Ad hoc Network (MANET) [9], [13]-[14], [28] run through into existence where the topology keeps changing frequently in addition to the mobile nature of nodes. At present, the Intermittently Connected Mobile Ad hoc Networks (ICMANET) [27] explored a new era where the connectivity between nodes never occurs with high density of nodes resulting in spasmodic environment.

The routing in all forms of networks is possible through traditional routing schemes like Distance Vector Routing, Link State Routing, Open Shortest Path First (OSPF), Opportunistic Adaptive routing, Distance Source routing (DSR) [10], Ad hoc On demand Distance Vector (AODV) [11], Destination-Sequenced Distance Vector (DSDV) [12]etc. But these schemes are not applicable for Intermittent Connected Network.

In general ICMN is a Delay tolerant Network (DTN) [8], [18] capable of holding larger delays. It is designed to operate effectively over extreme distances such as those encountered in space communications or an interplanetary scale. The sparse or dense nature of intermittent network is mainly due to high mobility of the nodes. The nodes stir within fractions of time and hence their topology changes in a dynamic way. Typical examples of intermittent network are wild life tracking, habitat monitoring sensor networks, military networks, nomadic community networks, vehicular networks etc. Due to typical distorted nature of the network, routing becomes an onerous task.

Many routing algorithms are proposed for efficient routing in the intermittent network namely flooding [1], epidemic [2], direction based routing, adaptive routing, utility based routing, probabilistic routing, copy case routing, spray and wait [5] routing etc. These algorithms furnish a proficient channel for data transmission. But they do not clear out a way for efficient secure routing.

The target of secure routing is to prevent malicious attacks by the intruders. This also prevents unwanted attacks or threats of data in the network. The secure routing should be provided in an efficient manner such that they should not degrade the normal performance of data routing in the networks i.e. increase in delay, higher overhead and maximum storage capacity, invariant bandwidth should not occur. In this paper, we put forth a technique called S-Spray that aims at providing a high range of security without deteriorating the periodic behaviour of data transmission.

In the proposed S-Spray, routing is done by splitting the network into 'n' regions. Source and destination regions are chosen. The data are transmitted through relay nodes using Spray and Wait routing protocol. In prior to transmitting the data, a neighbour challenge method is implemented in which each node maintains a list of associated nodes. When a node wants to transmit a data, it imposes a few authentication series to estimate whether the node is a trusted node. It initially enacts neighbour challenge followed sharing the lists, identity tracking and code generation. When all these terminologies are completed successfully, the node is assumed to be a trusted node in the network and hence the data transmission occurs. In this way, an efficient secure communication is proposed.

The paper is organized as the following sections. Section 2 describes the related work of intermittent mobile network. Section 3 portrays the basic mechanism of SNW. Section 4 depicts the principle of S-Spray. The simulation results are shown in the Section 5.

2. RELATED WORK

The Intermittently connected network is a new form of emerging network where routing data packets is seemed to be

monotonous task. Many research works have proved the possibility of routing in ICMN. This section provides an overview of routing techniques applicable in the intermittent network. The routing techniques vary at a larger rate from the traditional routing protocols. The routing protocols of ICMN should include the main feature of tolerating higher delays as the connectivity is transient in nature. Some of the intermittent routing protocols are described as follows.

The age old technique for routing in intermittent network is the flooding [1] based routing. In this, one node sends packet to all other nodes in the network. Each node acts as both a transmitter and a receiver. Each node tries to forward every message to every one of its neighbours [1]. The results in every message eventually delivered to all reachable parts of the network.

The Epidemic routing oeuvres on the basis of the traditional flooding based routing protocol, which states that periodic pair – wise connectivity is necessitate for message delivery [2]. The protocol banks on immediate dissemination of messages across the network. Routing occurs based on the node mobility of carriers that are within distinctive position of the network.

The Single Copy Case routing [3], from its nomenclature it postulates that only a single copy of message packet is carried to destination. The routing scheme includes direct transmission, randomized routing, utility based routing, seek and focus and Oracle based routing.

The Multiple Copy Case [4] scheme deals with the mechanism of spraying a few copies of message and then routing each copy in isolated manner to the destination. The algorithm that holds multiple copy case routing are Spray and Wait and Spray and Focus.

A Probabilistic Routing protocol encompasses the history of encounters and transitivity. Every node A calculates the Probabilistic metric called delivery predictability [6] for the destination. The assessed predictability is used to regulate the willingness of any particular node to convey the message towards destination. The Summary vectors [6] are interchanged, when two nodes meet, that includes the delivery predictability information stored at the nodes. By considering this information the internal predictability is updated and the forwarding strategy will be used to request the messages from other nodes.

The Semi Probabilistic Routing (SPR) [7] algorithm considers that the network is partitioned into tiny portions that have a stable topology. The protocol upholds the information about host mobility and connectivity changes for more accurate message forwarding.

This routing technique does not have a way for secure communication. To enhance the mode of secure communication, in this paper we proposed a new routing scheme called S-Spray. The security in network plays an imperative role in preventing threats or data theft by the intruders. The privation for security is essential in network communication.

3. SPRAY AND WAIT ROUTING (SNW)

The Spray and Wait routing (SNW) protocol [5] oeuvres in core of spraying a few message copies into network and then waiting for them to get in contact with target node in concord to its name. In general, the Spray and Wait spreads a scarce amount of message packets into the network and waits for a bounded amount of time until one of the nodes in the network get in contact with the destination node.

The SNW outstrips the other traditional routing schemes with its average message delivery ratio, the total number of transmission hops to reach the destination on packet delivery and the overall routing performance. The implementation complexity of SNW [5] is undemanding and it also can be heightened to pull off the performance in certain. It is palpable that this routing scheme limits the amassed number of transmissions per message packet without conciliation with the performance.

The SNW protocol holds two phases namely the Spray phase and Wait phase.

3.1 SPRAY PHASE

For every message originating at a source node, L message copies are initially spread forwarded by the source and possibly other nodes receiving a copy – to L distinct "relays".

The Fig.1 depicts the L message copies initially spread to L distinct nodes. The spray scheme is done in two ways as source spray and binary spray and wait.

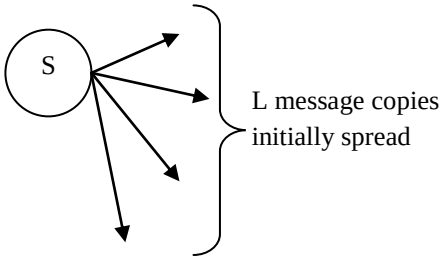

Fig.1. L message copies

3.1.1 Source Spray:

Source spray is the simplest approach in which the source node forwards all L copies to the first L distinct nodes it encounters.

It means that the source node hand over all the packets that were generated in it to the node that it has encountered within its radio range. This is clear from Fig.2.

3.1.2 Binary Spray and Wait:

The source of a message initially starts with L copies; any node A that has n > 1message copies (source or relay), and encounters another node B (with no copies), hands over B n/2 and keeps n/2 for itself; when it is left with only one copy, it switches to direct transmission.

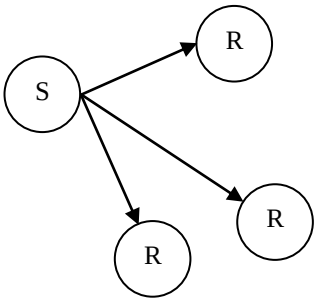

Fig.2. Source Spray

3.2 WAIT PHASE

If the destination is not found in the spraying phase, each of the L nodes carrying a message copy performs direct transmission (i.e. will forward the message only to its destination).

Once during spraying phase [3] if the destination node is not found, each of the L node that holds the copy of message packet performs the direct transmission as it encounters the destination and to any other relay nodes in the network.

4. S-SPRAY ROUTING PROTOCOL

The S-Spray is designed to ensure secure routing in ICMN. The network topology into n x n regions, where n is any positive integer. The network region is partitioned to entitle that the network is intermittent in nature. By means of SNW, initially the data packets are sprayed across the network using binary spray. The process of spraying continues until a single copy of data is left. With a single copy of data the wait phase starts where the node waits by itself until the destination node is encountered. The data transmission is possible with the help of the relay nodes.

Following the general process of the routing protocol, the authentication series [20]-[24] are induced on each handover of data packet to the relay node. The initial step in the series is the identity tracking. The sender node requests for the IP address of the node it has currently encountered. The relay node replies the sender with its IP address. If the received IP address matches with the one in buffer maintained by sender, the relay node is assumed to be the trusted node. Each node maintains a trustee list, a list that contains details about the entire trusted node in the network and an untrustee list, a list that maintains information about all the malicious or suspicious nodes of the network. A buffer at each node holds the IP address of all the other nodes in the network, from its initial placement and also its public key.

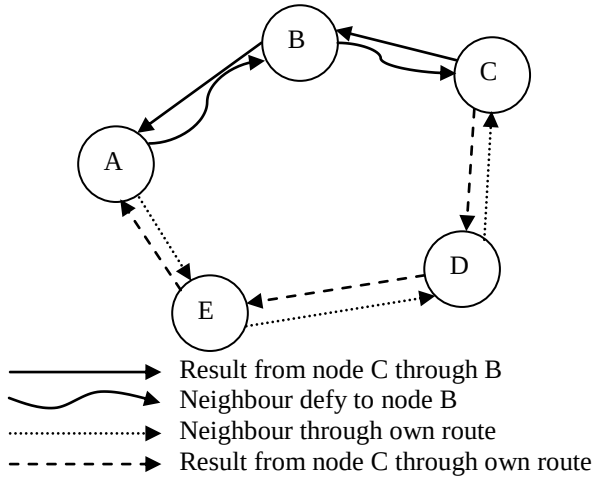

Fig.3. Process of Neighbour Challenge

A neighbour challenge is passed to estimate whether the primary relay node is a trusted node or a malicious node. It includes transmitting any of the pair of positive prime integers (a, b) available to it. The data is encrypted before forwarding it to the relay node. The neighbour challenge is forwarded through two possible routes, one holding the test node and the other is the known node. On receiving the challenge, secondary relay node computes cd mod n [20] and sends back the result to the sender through the two paths defined. The sender compares the result received from two paths. If both are same, the test node is assured to be a trusted node. The sender adds the test node to the trustee list, if the results differ sender appends it to the untrustee list. The challenge process is initiated only if the sender node doesn't find the relay node currently it has encountered in its trustee list.

As a sequence the trustee and untrustee lists are shared between the nodes, to have a history about all the trusted nodes in the network. During sharing process, the nodes compare the lists and they append the nodes that are found to be absent in it. The authentication series involves a pair code generation test. In this the sender node generates a random code and forwards it to the relay node in an encrypted form. If the relay node decrypts and sends back the same code, it is assured to be the trusted node. When these authentication series are passed by the encountered node, it is assured to be fully trusted and the data transmission is allowed. The SNW along with authentication series enables S-Spray efficient. S-Spray ensures secure data transmission in ICMN.

The Fig.3 depicts the overview of neighbour challenge scheme. Initially node A wants to test whether node B is a trusted or malicious node. Node A transmits challenge to node B. On receiving it, node B just forwards it towards node C. Node A also sends a copy of challenge towards C through its own path. C computes the challenge and replies through B and also through its own path to A. Node A evaluates the result arrived from two paths. If they are found to be same, Node A assumes that node B is one of the trusted node in the network.

5. SIMULATION RESULTS

This section describes the simulation results of the proposed S-SPRAY. It is compared with the previous routing techniques namely Epidemic routing and Spray and Wait routing. Varieties of network parameters are used for evaluating the routing protocols. Section 5.1 clearly shows the scenario setup for evaluation. Section 5.2 depicts the comparative performance of S-SPRAY with SNW by varying the number of nodes with respect to delivery ratio and latency.

5.1 SCENARIO SETUP

The parameters set are the basic One Simulator [15]-[17] environ parameters and are given in Table.1.

The One Simulation [25]-[26] for S-SPRAY in this paper uses the random waypoint model. The nodes move in an area of 2000 x 2000 m with a speed limit within bounds 0.5 to 1.5 m/s. The radio range is set to 250 m. The efficiency of any routing protocol is determined by the node density i.e. the total number of nodes within the set network. The packets are generally generated with the initial setup of the simulation and holds through the overall simulation time. The time to live (TTL) or the packet life time is set as 600s initially that are varied lately on consideration to the performance criterion. When evaluating, the simulation is run for 3000s.

5.2 PERFORMANCE COMPARISON OF SNW AND S-SPRAY

To show the pro of SNW, we compared the simulated result of both SNW and S-Spray. SNW is an efficient routing algorithm with good delivery probabilities. In order to mark the outperformance of S-Spray, a comparative analysis is made between SNW and S-Spray grounded on some basic network parameters.

We have made the comparison using various metrics as follows:

i. Number of nodes vs Delivery Ratio
ii. Number of nodes vs Latency

Table.1. Basic Simulation Parameters

PARAMETERS	One Simulator
Area	2000 × 2000 m
Mobility Model	Random Waypoint
Node Density	50 nodes
Node Speed	1.5 m/s
Radio Range	250 m
Packet Life Time	600 s

5.2.1 Number of Nodes Vs Delivery Ratio:

Comparing the delivery ratio i.e. the probability to deliver the message, initially SNW provides an optimal delivery ratio. On setting of agent, it provides considerably slight higher ratio. Both SNW and S-Spray vary with slight variation in delivery ratio and are shown in Fig.4 with respect to the number of nodes.

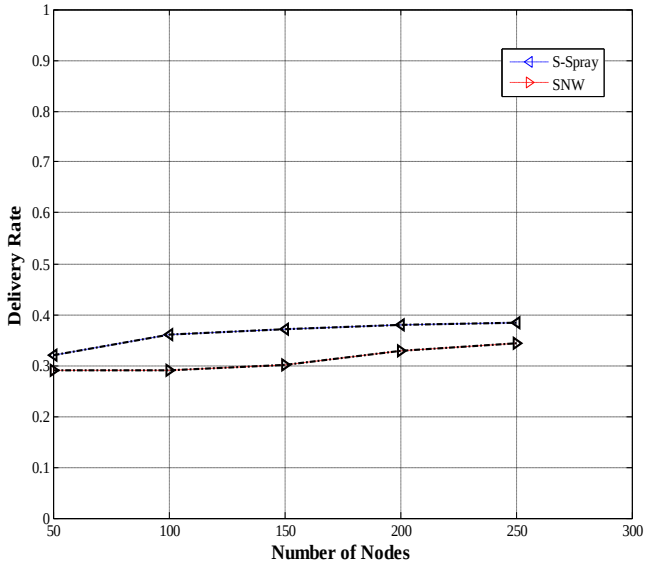

Fig.4. Delivery Ratio for various numbers of nodes

The Fig.4 shows that on setting of agent, SNW has slight modification in its performance. The S-Spray exerts a minimum of 20% (approx.) higher delivery probability than SNW protocol. Both schemes deliver with the average probability that is required for an efficient routing whereas S-Spray provides higher delivery ratio and ensures secure routing.

5.2.2 Number of Nodes Vs Delivery Latency:

The time criteria once again stand forth as an important aspect during the measure of latency. The setting of agent takes a few milliseconds less to route. This is because of the basic nature of agent to use lesser time. Figure 5, shows the comparative analysis of latency in both SNW and S-Spray and the analysis is made over average latency with respect to the number of nodes set in the network.

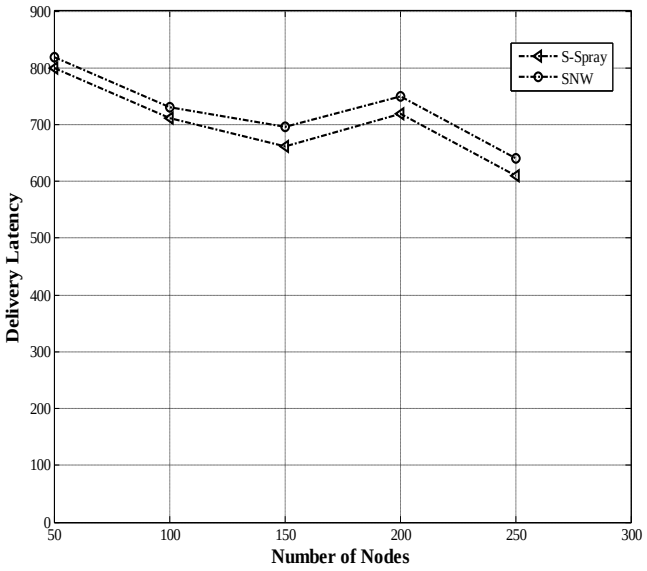

Fig.5. Delivery Latency for various numbers of nodes

The delay in S-Spray is 4% lesser than SNW and shows a better performance. This variation in delay is mainly due to the time reduction characteristic of agents. With lesser delay S-Spray renders secure message transfer. The secure and efficient transmission is evident from the Fig.5.

6. CONCLUSION

In this paper, we have demonstrated the efficient secure routing S-Spray. The proposed routing protocol provides a higher degree of security in the intermittently connected mobile networks. The routing performance metrics are not degraded with the implementation of the security mechanism. Neighbour challenge provides an integrity check among the available network groups. S-Spray paves a better way delivering data towards destination without degrading the routing performance. S-Spray varies at 35% from SNW and 17% from ER with respect to overhead. It also varies at an approximate rate of 70% and 93% with respect to delivery latency. In regard to delivery rate, S-Spray varies approximately in the range of 82% and 76% respectively. As an extension to the work, in future certain optimization techniques and computing techniques will be used. The work will be progressed as, (i) hard computing technique with agent setup and (ii) soft computing technique with cryptographic algorithms. This paper proves the efficiency of secure routing in ICMN.

REFERENCES

[1] D. Cokuslu and K. Erciyes, "A Flooding based Routing Algorithm for Mobile Ad Hoc Networks", *Proceedings of IEEE 16th Signal Processing, Communication and Applications Conference*, pp. 1-5, 2008.

[2] wwwA. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks", Technical Report CS-200006, Duke University, 2000.

[3] T. Spyropoulos, K. Psounis and C. S. Ragavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case", *IEEE/ACM Transactions on Networking*, Vol. 16, No. 1, pp. 63–76, 2008.

[4] T. Spyropoulos, K. Psounis and C. S. Ragavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case", IEEE/ACM Transactions on Networking, Vol. 16, No. 1, pp. 77-90, 2008.

[5] T. Spyropoulos, K. Psounis and C. S. Raghavendra, "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks", *Proceedings of the ACM SIGCOMM Workshop on Delay - Tolerant Networking*, pp. 252-259, 2005.

[6] A. Lindgren, A. Doria and O. Schelen, "Probabilistic routing in intermittently connected networks", *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 7, No. 3, pp. 19-20, 2003.

[7] K. Shi, "Semi-Probabilistic Routing in Intermittently Connected Mobile Ad Hoc Networks", *Journal of Information Science and Engineering*, Vol. 26, No. 5, pp. 1677-1693, 2010.

[8] Delay Tolerant Networking Research Group. http://www.dtnrg.org.

[9] Z. Zhang, "Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges", *IEEE Communications Surveys and Tutorials*, Vol. 8, No. 1, pp. 24–37, 2006.

[10] S. Basagni, I. Chlamtac and V. R. Syrotiuk, "Dynamic Source Routing for Ad Hoc Networks Using the Global Positioning System", *Proceedings of the IEEE Wireless Communications and Networking Conference*, Vol. 1, pp. 301-305, 1999.

[11] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, 1999.

[12] C. E. Perkins and Pravin Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", *Proceedings of the Conference on Communications Architectures, Protocols and Applications*, Vol. 24, No. 4, pp. 234–244, 1994.

[13] A. Boukerche, "*Algorithms and Protocols for Wireless Mobile Ad Hoc Networks*", Wiley-IEEE Press; 1st edition, 2008.

[14] W. Hsu, T. Spyropoulos, K. Psounis and A. Helmy, "Modeling Timevariant User Mobility in Wireless Mobile Networks", Proceedings of the 26th IEEE International Conference on Computer Communications, pp. 758–766, 2007.

[15] A. Keranen, J. Ott and T. Karkkainen, "The One Simulator for DTN Protocol Evaluation", *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, pp. 1-10, 2009.

[16] A. Keranen, T. Karkkainen and J. Ott, "Simulating Mobility and DTNs with the ONE", *Journal of Communications*, Vol. 5, No. 2, pp. 92-105, 2010.

[17] D. Gorgen, H. Frey and C. Hiedels, "JANE – The Java Ad Hoc Network Development Environment", Proceedings of the 40th Annual Simulation Symposium, pp. 163-176, 2007.

[18] S. Jain, K. Fall and R. Patra, "Routing in a Delay Tolerant Network", *ACM SIGCOMM Computer Communication Review*, Vol. 34, No. 4, pp. 145-158, 2004.

[19] H. Wen, J. Liu, C. Lin, F. Ren, P. Li and Y. Fang, "A Storage Friendly Routing scheme in intermittently connected Mobile networks", IEEE Transactions on Vehicular Technology, Vol. 60, No. 3, pp. 1138 – 1149, 2011.

[20] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta and P. Dhurandher, "FACES: Friend – Based Ad Hoc Routing using Challenges to Establish security in MANETs systems", *IEEE Systems Journal*, Vol. 5, No. 2, pp. 176-188, 2011.

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

[22] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644-654, 1976.

[23] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols", *Proceedings of the 1st ACM Workshop on Wireless Security*, pp. 1-10, 2002.

[24] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Securing mobile ad hoc networks with Certificateless public keys", *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, No. 4, pp. 386-399, 2006.

[25] A. Keranen, "Opportunistic Network Environment Simulator", Special Assignment report, Helsinki University of Technology, Department of Communications and Networking, 2008.

[26] TKK/COMNET, 2009, Project page of the ONE simulator. http://www.netlab.tkk.fi/tutkimus/dtn/theone.

[27] S. Ramesh, R. Praveen, R. Indira and P. Ganesh Kumar, "A Survey of Routing Methodologies in Intermittently Connected MANETs", Proceedings of the International Conference on Advanced Computing, 2012.

[28] Hui Xu, Xianren Wu, Hamid R. Sadjadpour and J. J. Garcia-Luna-Aceves, "A Unified Analysis of Routing Protocols in MANETs", *IEEE Transactions on Communications*, Vol. 58, No. 3, pp. 911-922, 2010.