Evaluating the Effect of Selfishness on Flooding Based DTN Routing Algorithms

Sobin C C
Dept. of Computer Science and Engineering
IIT Roorkee, Uttarakhand, India - 247667
Email: sobincc@gmail.com

Vaskar Raychoudhury
Dept. of Computer Science and Engineering
IIT Roorkee, Uttarakhand, India - 247667
Email: vaskar@ieee.org

***Abstract*—Delay Tolerant Networks (DTNs) are sparse mobile networks in which a complete end-to-end path may not exist. Routing is challenging in such networks, because of the frequent network disconnections, which will result in frequent change in network topology. Most of the existing DTN routing algorithms consider that all the nodes are honestly participating in message delivery. But in many real scenarios, nodes are selfish, and not willing to forward the message further in the network. We observed that in many real scenarios, neither all nodes are altruistic nor selfish, and classified the selfishness present in the network into individual selfishness and social selfishness. In case of individual selfishness, a node may behave selfishly because of some external reason, such as limited buffer space, limited power, etc. A node will forward the message only to nodes, who are friends, or having similar interests, or belongs to same community, etc., in case of social selfishness, In this paper, we have analyzed the impact of both individual and social selfishness on exiting flooding based routing algorithms such as Epidemic routing and Spray and Wait routing and proposed a method to detect and resolve selfishness to improve their routing performance.**

I. Introduction

Delay Tolerant Networks (DTNs) are sparse wireless networks where mobile nodes work in an ad-hoc manner and forward data opportunistically upon contacts. DTNs allow communication between nodes in the absence of network infrastructure and continuous network connectivity. Therefore, they are widely used in many applications like social networking [1] [2], wildlife tracking [3] [4], remote village networks [5] [6], vehicular communication [7] [8] and underwater networks [9], etc.

In DTNs, different types of user behavior will result in different network conditions. DTN based short message service has become very popular these days because it offers a more convenient way to exchange information in a mobile way. DTNs are marked by their mobile nodes with their contact sequences in order to exchange the packets. DTN Routing can be divided into opportunistic routing, social based routing and incentive based routing. In opportunistic routing, the relay node is selected based on its opportunity of meeting the destination node. In social based routing, the relay is selected based on social relationship with the destination node. In incentive based routing, credits are given to the relay node for forwarding the message.

A node in a DTN is considered as selfish when that node is not willing to forward the packet further in the network. There can be various scenarios present in which few nodes in a network can act selfishly. The nodes in DTN can act individually or socially selfish. Nodes show individual selfishness because of the small buffer space and less battery power and they act socially selfish because they do not want to act as a relay for the nodes with which it does not have social ties with it or does not belong to same communities, etc. For successful working of DTNs there is a need that all nodes in the network communicate honestly, but in reality nodes are not willing to participate in the network which hinders the performance of the network.

In this paper, we have discussed two types of selfishness, individual and social, that can be present in the network. We then analyze the effects of these two types of selfishness on flooding based DTN routing algorithms such as Epidemic routing and Spray and Wait routing, and proposes a technique to improve the packet delivery ratio of the existing algorithms by mitigating the selfishness involved.

II. RELATED WORKS

The routing in DTN can be done with the help of the social characteristics of the nodes, like friendship, community, etc.; or by forcing the nodes to participate in the routing process by giving credit to them; or it can be done just by mere exchanging the packets when encountered with other nodes. Selfishness can be divided as individual selfishness and social selfishness. In individual selfishness the nodes behave selfishly because of its own interest, the nodes in this category are only interested in forwarding their own packets. In the social selfishness, the nodes do they not forward the packet to the nodes with which they do not have any social connection.

Three types of individual selfishness are considered in the previous works. In the first category, non-participation, there are two types of nodes present in the network, the one who explicitly do not take part in the routing process and the other one, who after accepting the packet drops it from the network. In the second category, energy-preservation, the nodes do not participate to save their device energy. In the last category, storage-preservation, the nodes act selfishly even when the storage space is available to save their buffer space for their own use.

Chen, et al. [10] proposed a trust management protocol in which, not only the quality of service is considered, but, also considers the social properties of the network. The social properties include the honesty and unselfishness of the nodes.

They propose two models, equal weight QoS and also the social trust management protocol. When compared with epidemic routing, the trust based protocol gave a higher delivery ratio than epidemic routing.

Wu, et al. [11] uses a theoretical framework to analyze the effect of the social selfishness. A social graph is considered as an overlay above the actual physical graph. A social graph is a graph in which two nodes are connected if they are friends with each other. It is then assessed that the links of a node in the social graph follow a power law distribution. A relation between nodes can be of strong link and weak link as nodes are more willing to help their friends. The system is modeled as a Markov process. The results of the analysis show that the different degree of social selfishness has different performance of the routing algorithm.

Miao, et al. [12] calculates the effect of binary Spray and Wait protocol when selfish nodes present in the network. Two types of nodes are assumed to be present in the network, the nodes which specifies explicitly for non participation and the nodes which drops the packet after receiving the same. They calculated that the delivery probability of the routing algorithm reduced to 40 % when all the nodes are selfish with the help of Random Way Point Model.

Wu, et.al. [13] gives a theoretical model to simulate the presence of individual and social selfishness in Epidemic Routing. The model was based on Markov process. Their simulation results show that the presence of selfish nodes reduces the performance of epidemic routing significantly, also, if there are nodes which are present in two or more communities which in turn improves the delivery performance of the same.

III. Epidemic Routing

Vahdat, et al. [14] have proposed a flooding based forwarding approach, called as Epidemic routing with an aim to maximize the delivery rate while minimizing the delivery delay. For reducing the total network resources consumed while routing the message from source to destination, they suggest to put a limit on either the message hop count or the buffer space allocated at each node. Therefore, the message will be dropped after its TTL (Time-To-Live) expires or if the buffer at the peer is full. This scheme is based on the idea that the message will eventually find its destination through transitive exchanges between nodes, if they are spread in the connected portion of the network.

The primary goal of epidemic routing is to deliver messages with high delivery probability to the destination node. As it can be seen from figure 1, that the source of the message floods the message to C_1 and C_2, which are in its range; C_2 then stores the message till it meets another node C_3. Then C_3 stores the message and finally deliver it to the destination D. So, the overall goal of epidemic routing is to escalate the delivery rate and minimize the delivery latency.

All nodes are assigned a unique node identifier. Every node stores a summary of the messages it has cached locally in a summary vector. Whenever some node *A* comes in the communication range of node *B*, the node with smaller identifier, say node *A*, starts an anti-entropy session with the node *B*, as shown in figure 2. During this, *A*, provides its summary vector to *B*. Node *B*, finds which messages present in *A*s cache are not present locally and makes a request for them. Then, the initiator of the anti-entropy session, here node A, provides the requested messages to node *B*. Some messages may find their destination in this step only (i.e., messages destined to *B*), while others have to be similarly relayed across the network.

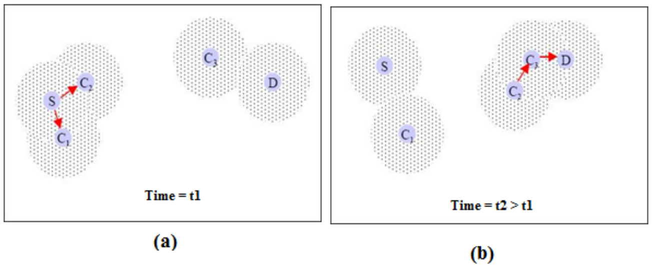


Fig. 1. Epidemic Routing

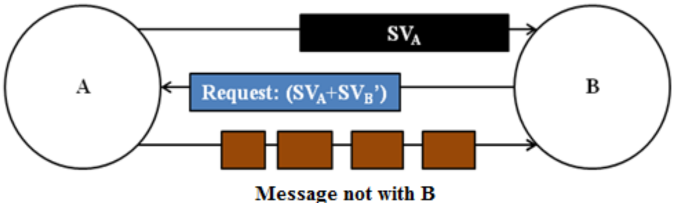


Fig. 2. Summary vector exchange in Epidemic Routing

Flooding results in high resource consumption in terms of both power and storage. Hop count can be set to lower values to avoid this. By setting a low value of hop count, the delivery ratio will decrease and average delivery time will increase. On the other hand, if hop count is high, messages will be dispersed in the network more quickly, resulting in a higher delivery ratio and lower average delivery time. Bounding the buffer space at every node is another trick to reduce resource consumption. Epidemic routing can have a delivery rate of 100% in partitioned networks where ad-hoc routing protocols fail entirely.

A. *Epidemic Routing With Selfishness*

Epidemic routing is the flooding based algorithm, no decision making scheme is required while choosing the relay, to decrease the resource consumption. Whenever node *A*, meets a peer *B*, all the messages which node *A*, have, are forwarded to node *B*. As the contact time is small in these types of networks and when the nodes in the network are showing the selfish behaviors, the packets should be sent to those nodes first who does not show the selfishness property. Every node in the network maintains a table *R*, which is used to store history of receipt of messages from its neighbors. Suppose, a source node *S*, wants to send a message to destination node *D*. Let *X*, be the set of neighbors of the node *S*, then the node *S*, sorts the list its neighbors in increasing order with respect to the value of corresponding *R*, as shown in equation 1. Then a node sends the messages to the connections in order according with the sorted list.

$$\underset{i \in X, i \neq S}{\forall} Sort_{ascending}(X, R) \tag{1}$$

IV. Spray and Wait Routing

Spray and Wait is a limited flooding-based approach [15], a betterment of Epidemic Routing. It is also a multi-copy scheme where the message is replicated with encountered nodes for routing to the destination. The strength of this scheme is that it is simple, does not require any knowledge about the network and does not even use the past encounter records.

Whenever a node has a message to send to some other node, it replicates the message into *L* different nodes. This is called as the spray phase, because the source node, without any network information, copies its message to other nodes. If the destination of the message is not met during the spraying process, these *L* nodes transmit a single copy directly to the destination node. Transmitting the message directly means that the nodes will buffer the message till they see its destination or its TTL expires. This is the wait phase of the algorithm.

There may be different variations of the algorithms based on the distribution of initial *L* copies on the network. In the simplest form, *L* copies can be distributed to first *L* distinct nodes the source encounters. Another variation of the algorithm, called Binary Spray and Wait, is to distribute half of the copies to the encountered node and keeping the remaining half at every step of relaying. This means, if a node A has *n* copies of the message and encounters a node B, it sprays *n/2* copies to B and keeps the remaining *n/2* copies with itself and repeats this until it is left with just a single copy when it switches to direct transmission. Spray and Wait is a ticket-based forwarding scheme, in which, every message is assigned logical tickets. Tickets depict the number of relays the message is to be forwarded.

We have worked on Binary Spray and Wait algorithm, in which, if a node have multiple copies of a packet and if it has a connection with node B, then the former node gives half of the copies to the later node and keeps half of it. And when a node is left with one instance of the packet, it can do only transmission to the destination node.

We can see an example, in figure 3, in which node *S*, sprays, 3 copies to node 1, 2 and 3 respectively. Node 7 sprays 2 copies to node 11 and 8 and is left with half of the copies. Nodes 11 and 8 send their copies to node 10 and so on. Node 14 and 16 is the nodes who were finally left with only one copy and they send it directly to the destination, *D*.

The advantages of this algorithm are :

• It has less number of transmissions when compared with other flooding-based schemes

• When the load is high in the network, it gives less delivery delay

• It is scalable, as the number of nodes in the network increases, the number of transmissions per node decreases

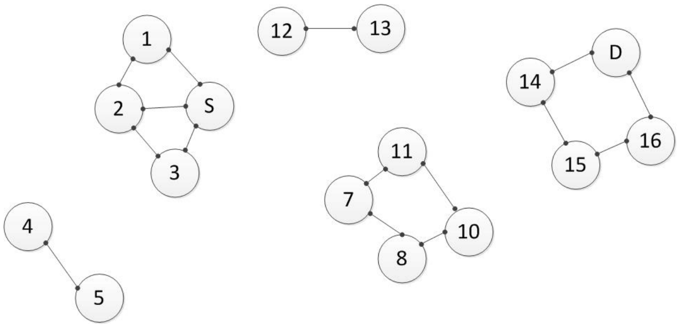


Fig. 3. Spray and Wait Routing

• It is a very simple algorithm and requires no knowledge of the network

A. Spray and Wait With Selfishness

As Spray and Wait routing is the modified version of epidemic routing, it is also a type of flooding based technique. The only difference lies in the fact that instead of disseminating the message to all the connections, it sprays or sends only L copies to all the active connections it has. Similar to epidemic routing, the method sort all its neighbors, *X*, in the increasing order of table *R* as in equation 1, where *S* is the node who is seeking the next relay.

V. Results

Evaluating the various DTN protocols requires some proper tool and the ONE simulator [16] is one such tool. The ONE simulator is mainly used for the modeling of the nodal movement, inter node contacts, message handling and routing. We have done the empirical analysis for Epidemic Routing and Spray and Wait with the help of ONE Simulator.

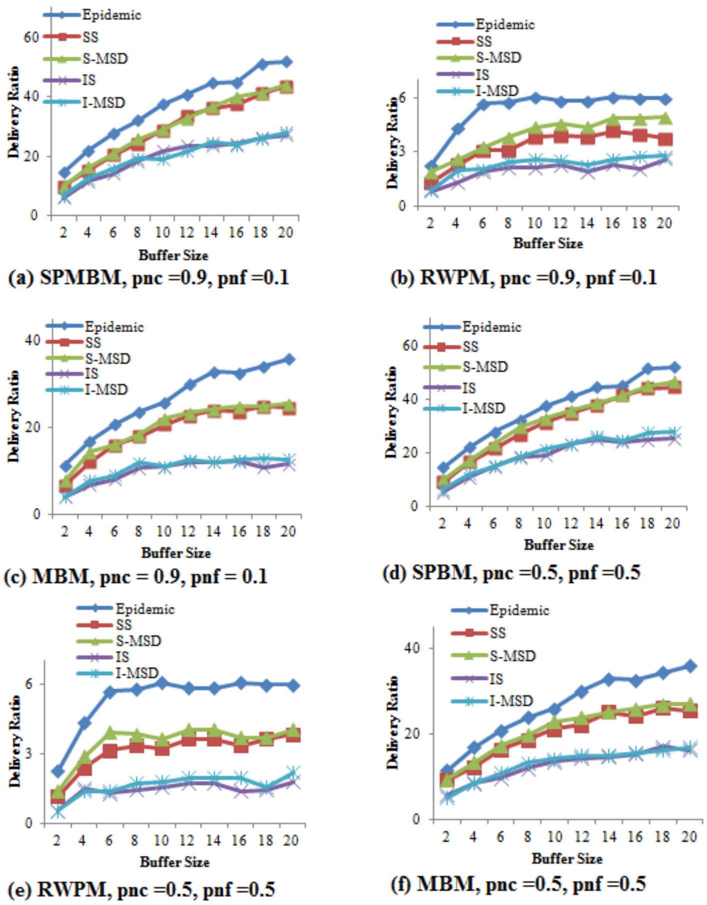
We have considered that there are three types of nodes present in the network, vehicular nodes, pedestrian nodes and tram nodes. The simulation time is the total number of time span which have considered for node communication. The transmission speed of the node is the data rate at which the packets are transmitted from one node to another. Time to live is the total number of seconds after which the packet will get dropped from the network. A message creation interval is the time range in which the nodes creates packet for each other. Wait time is the time for which each node waits before moving to the next location.

TABLE I. Simulation Settings

Parameters	Values
Simulation time	43200s=12h
Transmission Speed of nodes	250kBps
Number of nodes	125
Time To Live (TTL) of a message	300 minutes
Message Creations Interval	25-30 Seconds
Wait Time	10-30 seconds
Interface	Bluetooth and high speed interface

To model the real-world mobility, we have used two types of map based mobility and random movement models for simulation.

TABLE II. Epidemic Routing Results



(a) SPMBM, pnc =0.9, pnf =0.1

(b) RWPM, pnc =0.9, pnf =0.1

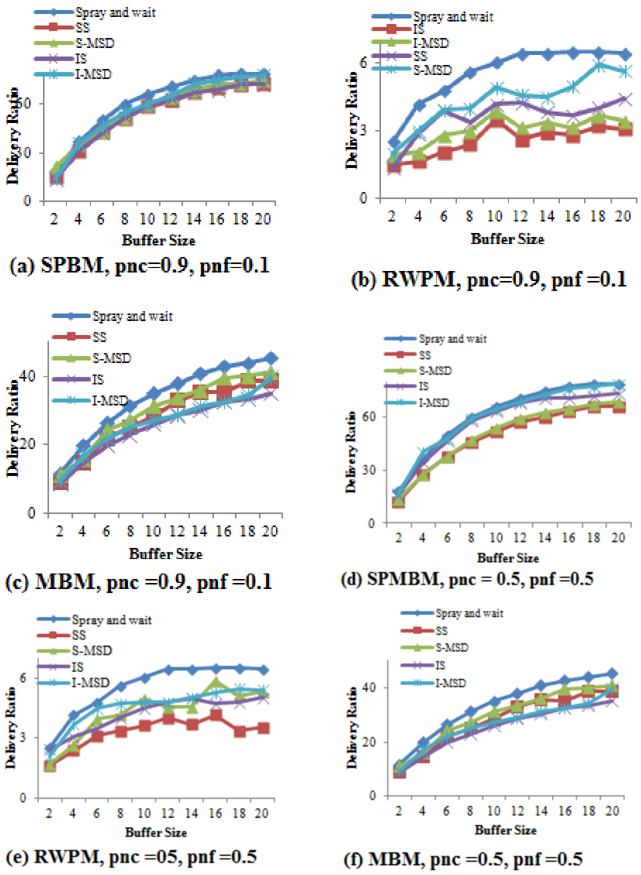
(c) MBM, pnc = 0.9, pnf = 0.1

(d) SPBM, pnc =0.5, pnf =0.5

(e) RWPM, pnc =0.5, pnf =0.5

(f) MBM, pnc =0.5, pnf =0.5

TABLE III. Spray and wait Routing Results



(a) SPBM, pnc=0.9, pnf=0.1

(b) RWPM, pnc=0.9, pnf =0.1

(c) MBM, pnc =0.9, pnf =0.1

(d) SPMBM, pnc = 0.5, pnf =0.5

(e) RWPM, pnc =05, pnf =0.5

(f) MBM, pnc =0.5, pnf =0.5

- Random Movement Mobility Model: In this type of models the nodes move randomly and freely without restrictions, and their location, velocity and acceleration changes with time. It is a famous model because of its simplicity. The destination for a node, its speed and direction are all chosen randomly. The drawback with this type of model is that, it is not close to the real world movement.

- Map-Based Movement Mobility Model: This mobility model is different from the random movement model in a way that all the node movement is confined to the underlined paths of the graph. We have used Helsinki downtown area, both roads and pedestrian walkways.

Figure (a) to (c) in Table II shows the performance of Epidemic Routing when the buffer threshold is 30% and the value of pnc=0.9 and pnf=0.1 with ShortestPathMapBased Movement (SPMBM), Random Waypoint Movement (RWPM) and MapBasedMovement (MBM). Figure (d)-(f) shows the same but with variation with probabilities, pnc=0.5 and pnf=0.5.

It can be concluded from the above results that the effect of social and individual selfishness is different on the delivery probabilities of the Epidemic routing. I-MSD and S-MSD gives good performance with SPMBM and RWPM model and, I-MSD does not gives good results with MBM model, as this mobility model does not follow any path property and the relations between the nodes could not be created. Whereas S-MSD gives better results with MBM because the friends of a node does not change and is irrespective of the node mobility.

Figure (a)-(c)in Table III shows the performance of Spray and Wait Routing when the buffer threshold is 30% and the value of pnc=0.9 and pnf=0.1 with ShortestPathMap-Based Movement (SPMBM), Random Waypoint Movement (RWPM) and MapBasedMovement (MBM). Figure (d)-(f) shows the same but with variation with probabilities, pnc=0.5 and pnf=0.5.

It can be seen from the above results that the effect of social and individual selfishness is different on the delivery probabilities of the Spray and Wait routing. The effect of social selfishness on the delivery performance is more than individual selfishness which is not the case in epidemic routing. I-MSD and S-MSD gives good performance with SPMBM and RWPM model and, I-MSD does not gives good results with MBM model as this mobility model does not follow any path property and the relations between the nodes could not be created. Whereas S-MSD gives good results with MBM, because no matter the mobility, the friend in the network does not change.

VI. Conclusion

In many real scenarios of DTN applications, selfishness may be present in the network. In such cases, a node will not forward the packet to ray node or to the destination. There can be various scenarios present in which few nodes in a network can act selfishly such as individual selfishness and node selfishness. Individual selfishness is when selfish nodes do not want to store messages of other nodes because of their limited buffer space. Social selfishness is when a node acts selfishly towards another node only if the latter is not a friend of the former. In this paper, we have evaluated the impact of both individual selfishness and social selfishness on flooding based DTN routing algorithms such as Epidemic routing and Spray and Wait and proposed a technique to improve the packet delivery ratio of the existing algorithms by mitigating the selfishness involved. As part of future work, we would like to conduct the empirical and real test bed analysis of the proposed method.

REFERENCES

[1] H. Ntareme, M. Zennaro, and B. Pehrson, "Delay tolerant network on smartphones: applications for communication challenged areas," in *Proceedings of the 3rd Extreme Conference on Communication: The Amazon Expedition*, p. 14, ACM, 2011.

[2] S. M. Allen, G. Colombo, and R. M. Whitaker, "Uttering: Social micro-blogging without the internet," in *Proceedings of the Second International Workshop on Mobile Opportunistic Networking*, pp. 58–64, ACM, 2010.

[3] P. Zhang, C. M. Sadler, S. A. Lyon, and M. Martonosi, "Hardware design experiences in zebranet," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 227–238, ACM, 2004.

[4] R. C. Shah, S. Roy, S. Jain, and W. Brunette, "Data mules: Modeling and analysis of a three-tier architecture for sparse sensor networks," *Ad Hoc Networks*, vol. 1, no. 2, pp. 215–233, 2003.

[5] A. S. Pentland, R. Fletcher, and A. Hasson, "Daknet: Rethinking connectivity in developing nations," *Computer*, vol. 37, no. 1, pp. 78–83, 2004.

[6] A. Doria, M. Uden, and D. Pandey, "Providing connectivity to the saami nomadic community," *generations*, vol. 1, no. 2, p. 3, 2009.

[7] A. Balasubramanian, Y. Zhou, W. B. Croft, B. N. Levine, and A. Venkataramani, "Web search from a bus," in *Proceedings of the second ACM workshop on Challenged networks*, pp. 59–66, ACM, 2007.

[8] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden, "Cartel: a distributed mobile sensor computing system," in *Proceedings of the 4th international conference on Embedded networked sensor systems*, pp. 125–138, ACM, 2006.

[9] T. Small and Z. J. Haas, "The shared wireless infostation model: a new ad hoc networking paradigm (or where there is a whale, there is a way)," in *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pp. 233–244, ACM, 2003.

[10] R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Trust management for encounter-based routing in delay tolerant networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1–6, IEEE, 2010.

[11] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks," *Communications Letters, IEEE*, vol. 14, no. 11, pp. 1026–1028, 2010.

[12] J. Miao, O. Hasan, S. B. Mokhtar, L. Brunie, and K. Yim, "An investigation on the unwillingness of nodes to participate in mobile delay tolerant network routing," *International Journal of Information Management*, vol. 33, no. 2, pp. 252–262, 2013.

[13] Y. Wu, S. Deng, H. Huang, and Y. Deng, "Performance analysis of epidemic routing in delay tolerant networks with overlapping communities and selfish nodes," *International Journal of Computers Communications & Control*, vol. 8, no. 5, pp. 744–753, 2013.

[14] A. Vahdat, D. Becker, *et al.*, "Epidemic routing for partially connected ad hoc networks," tech. rep., Technical Report CS-200006, Duke University, 2000.

[15] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, pp. 252–259, ACM, 2005.

[16] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*, p. 55, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.