International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Humming Bird (01st March 2014)

RESEARCH ARTICLE OPEN ACCESS

Misbehaviour Detection in Wireless Networks Of Selfish Individuals

An Sharmi.M

ME
Department of CSE, Loyola Institute of Technology and Science
[1]sharmi.m.rose@gmail.com

Mr.A.Arul Rex

Assistant Professor
Department of CSE, Loyola Institute of Technology and Science
[2]arulrx@gmail.com

Abstract —
Mobile opportunistic networks are characterized by unpredictable mobility, heterogeneity of contact rates and lack of global information. Successful delivery of messages at low costs and delays in such networks is thus challenging. Based on these observations we develop a new strategy for forwarding, which we refer to as Epidemic Forwarding and Delegation Forwarding, the Epidemic forwarding protocol for packet forwarding in a social mobile setting that leverage on the social aspects of the network to tolerate selfish behaviour friend nodes meet with high frequency. This protocol maintains unlimited buffer and the user can make them selfish choices. The selfish node drops the redundant message. This helps us showing formally that no rational node has any incentive to deviate. The second protocol Delegation protocol which is used to find the hackers in the network using HF (Hacker Finding)Algorithm and also which is used to check the forwarding quality by reducing the number of replicas using RR(Replica Reduction)Algorithm In other words, our two protocols are strategy proof, i.e., the strategies of following the protocols are Nash Equilibrium. Nodes that is selfish with outsiders and faithful with people from the same community. My protocols are shown to be very efficient in detecting possible misbehaviour. All the nodes are selfish and show formally that both protocols are strategy proof that is, no individual has an interest to deviate. Extensive simulations show that our protocols introduce an extremely small overhead in terms of delay.
Index Terms- strategy proof, social mobility, selfishness, forwarding protocols, Nash Equilibrium.

I. I NTRODUCTION

Now a day's peoples are using Smart phones to communicate, to use applications, and to organize their life. But forwarding in the selfish individuals is difficult. Our project proposes two forwarding protocols for mobile wireless networks of selfish individuals. I assume that all the nodes are selfish and show formally that both protocols are strategy proof that is, no individual has an interest to deviate. Pocket Switched Networks (PSN), can be key technology to provide innovative services to the users without the need of any fixed infrastructure.

Introducing two forwarding protocols Epidemic Forwarding [2] and Delegation Forwarding [4] for mobile wireless networks of selfish individuals, Extensive simulations with real traces show that our protocols introduce an extremely small overhead in terms of delay, while the techniques I introduce to force faithful behaviour have the positive and quite surprising side effect to improve performance by reducing the number of replicas and the storage requirements. I test our protocols also in the presence of a natural variation of the notion of selfishness nodes that are selfish with outsiders and faithful with people from the same community.

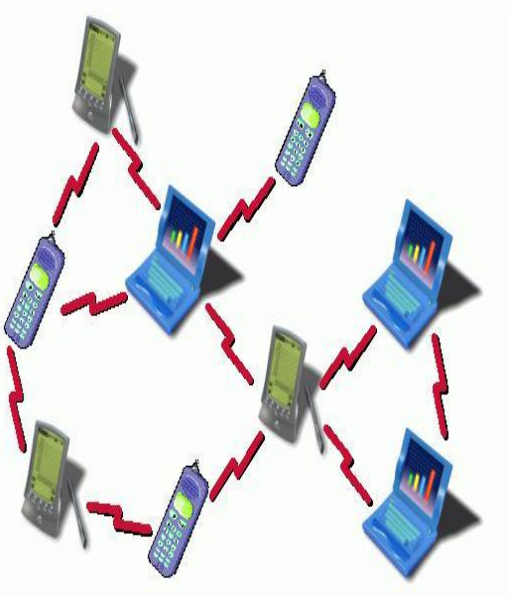


Fig no 1: Communication Network

Network security consists of the provisions and policies adopted by unauthorized users by a network Administrator to prevent and monitor unauthorized access, misuse,modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by Epidemic Protocol.

Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. But in our proposed system there is two forwarding protocols are used to tolerate the selfishness and to identify the intruders in the network .Which also reduce the replicas and storage requirements.

2. METHODOLOGY

Lot of work has been done in building efficient forwarding protocols for Pocket Switched Networks [1], [4]. The problem of building mechanism and protocols that can tolerate selfish behaviour is an important and modern issue in the design of networking protocols and distributed systems. Earlier work has been done to mitigate the impact of selfish behaviour in mobile ad hoc networks as well. The solutions can be classified into two main approaches: reputation-based schemes and credit based schemes. The application of mobile ad hoc networks (MANETs)[3] for the support of open communities has emerged recently. In this scenario, open MANETs will likely resemble social environments. A group of persons can provide benefits to each of its members as long as everyone provides his contribution. For our particular case, each member of a MANET [12] will be called to forward messages and to participate on routing protocols.

A selfish behaviour[9] threatens the entire community. Optimal paths may not be available. LoCom[5] is an interesting mechanism to enforce cooperation among nodes in wireless networks. Schemes that suffer from the lack of fairness guarantees or the reliance on costly mechanisms such as tamper proof hardware or the requirement for Trusted Third Parties (TTPs) that are not suitable for ad-hoc networks. Optimistic fair exchange for secure forwarding[2] solves the fairness problem that is inherent to peer rewarding schemes. The protocol achieves total fairness with the help of a TTP and is optimistic in that the TTP is only involved in case of conflict between peer nodes. It is more applicable and useful network for the file transaction and message transaction in real world applications. The files which are forwarded are double checked. It can forward only after the proof of the relay is received. Pocket Switched Networks (PSN)[4], can be key technology to provide innovative services to the users without the need of any fixed infrastructure. Delay-Tolerant Networking techniques address these issues for systems that lack continuous network connectivity. The 'bundle' protocol has been developed in a co-operative research effort to support continuous communications across disrupted links. DTN is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space

3. THE SYSTEM MODEL

3.1 System and Node Properties

In our system model, every node is selfish. This is a realistic scenario, if people can get the same level of service without using part of their battery or part of their wireless uptime or memory without any consequence, they will. And as soon as the first user finds a way to get more (or the same) while paying less, and publishes the patch of the system software, everybody will download the patch and use it. The dotted circle around each entity represents the wireless transmission range of each node any entity colored in dark represents a misbehaving entity.

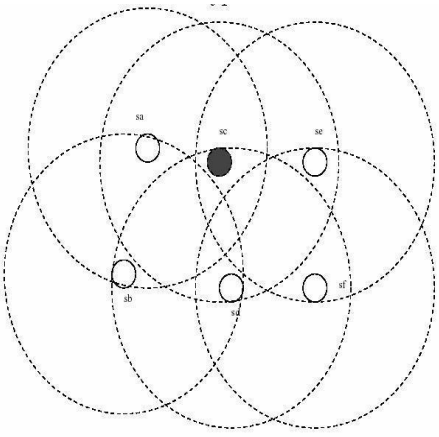


Fig no 2: Typical Scnario

3.2 System and Key Revocation

In our system nodes that join and leave are handled by a central authority. The authority handles new nodes joining the network in a standard way: It identifies the new node and it signs the new node's certificate (or the master public key is handed out to the node in case of an identity-based public key system). More authorities can coexist, as long as they exchange information on nodes that enter and exit the system in real time. To communicate with the nodes, we assume that the authority can use the cellular infrastructure or wireless technology like, e.g., GSM. This technology is very expensive compared with Bluetooth communication used by our forwarding protocols. We can reasonably expect that this event is rare. In three types of selfish nodes related to routing such as Dynamic Source Routing (DSR) [7] are defined:

3.3 Types Of Selfish Nodes

There are three types of selfish nodes are available
in the communication network.

3.3.1 Selfish Nodes Type 1 (SN1)

These nodes participate in the DSR Route Discovery and Route Maintenance phases, but refuse to forward data packets (which are usually much larger than the routing control packets);

3.3.2 Selfish Nodes Type 2 (SN2)

These nodes participate in neither the Route Discovery phase, nor forwarding data packets. They only use their energy for transmissions of their own packets.

3.3.3 Selfish Nodes Type 3 (SN3)

These nodes behave (or misbehave) differently based on their energy levels. When the energy lies between full energy *E* and a threshold *T*1, the node behaves properly. For an energy level between *T*1 and another lower threshold *T*2, it behaves like a node of type SN1. Finally, for an energy level lower than *T*2,it behaves like a node of type SN.

3.4 System Architecture

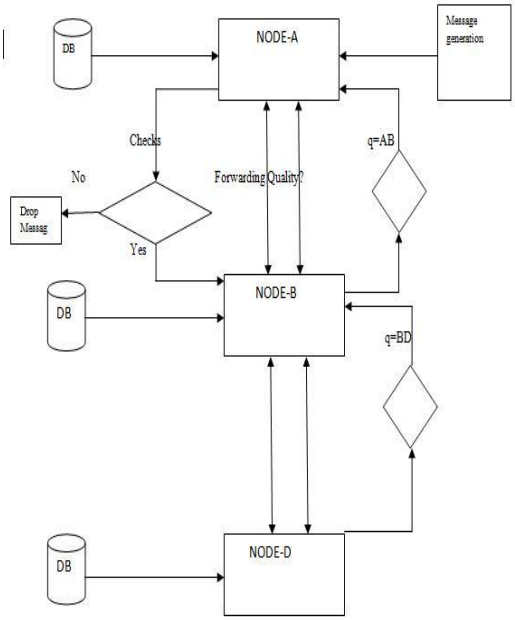


Fig no 3: System Architecture

Source node A will generate the message to forward to the destination then it will asks the node-b to show its proof, because it is in the need to forward a message via node-b to the destination node. Then node-b will send its proof node-checks the proof and forwards the corresponding message to it. Source node and the destination node will check the forwarding quality of the relay node. And the message will be double checked for its quality

4. PERFORMANCE EVALUATION

4.1 Security analysis*:*

We analyse the global scheme with respect to the security requirements defined in section II-B. We assume that nodes are uniquely identified by a certificate issued by a TTP and that there exists an underlying authentication mechanism. To ensure the proper security measures the copy of the data is verified with the previous data of the node.

Here i and j are considered as a two nodes in the communication network. Here each and every nodes are maintaining separate database to store the of the data. During the exchange of the data the copy of the data is stored in the data base of the node . To ensure the proper security measures the copy of the data is verified with the previous data of the node.

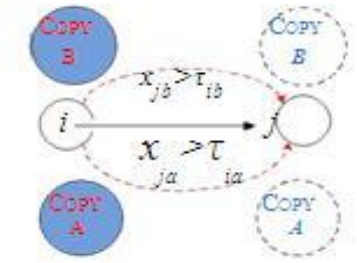
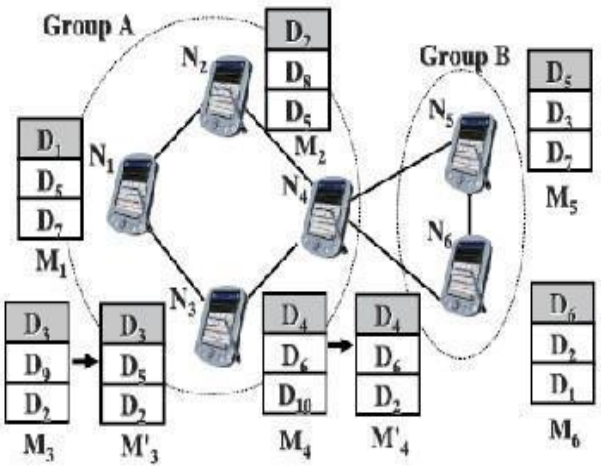


Fig no 4: Data Verification

4.2 Cooperation enforcement:

First of all, we showed that thanks to the proposed protocol, cooperation is mandatory because of the underlying rewarding mechanism. Nodes have no Choice but to receive all incoming packets if they want to be sure to receive packets that are intended to them. Once they received packets, they must forward those that are not intended to them in order to recover rewards spent before the reception. If packets are not forwarded, then they simply lose some rewards and thus are immediately punishing themselves. Moreover, intermediate nodes that participate in the forwarding of packets are rewarded more than they are charged and therefore compensate the energy they deploy to perform such operations

Wireless networks rely on node cooperation to perform and support basic functions like packet forwarding, routing and network management. In general, nodes' misbehaviour can significantly degrade the performance of the network. Cooperation enforcement schemes are seen as a lightweight alternative to conventional security techniques, providing a "softer" security layer to protect basic networking operations.



4.3 Protection against attackers:

Thanks to the rewarding mechanism whereby only the source is charged for sending the packet, a node will not have incentive to send bogus messages for the purpose of poisoning. If packets are not forwarded, then they simply lose some rewards and thus are immediately punishing themselves.

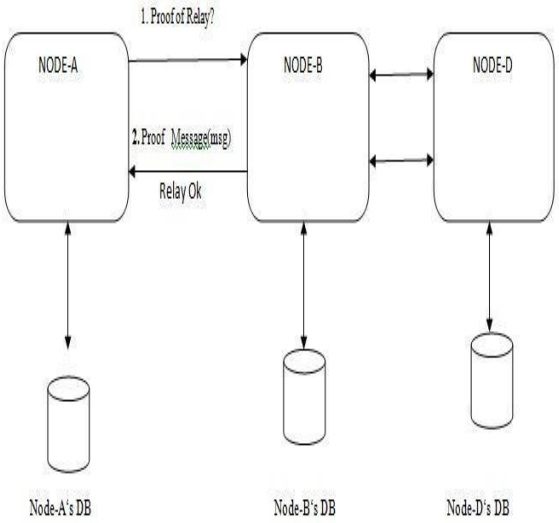


Fig no 5: Showing Proof of Relay

4.4 Protection against cheating actions:

In order to maximize their payoff, nodes might forward a packet to several other nodes in order to receive multiple rewards. If a node requires to transform two rewards that both depend on the same message, the TTP will not credit this particular node and will punish it by debiting it for an amount that is proportional to the replay frequency. Therefore, a cheating node will lose both in terms of resources that are consumed by forwarding the packets several times and in terms of losses due to the punishment.

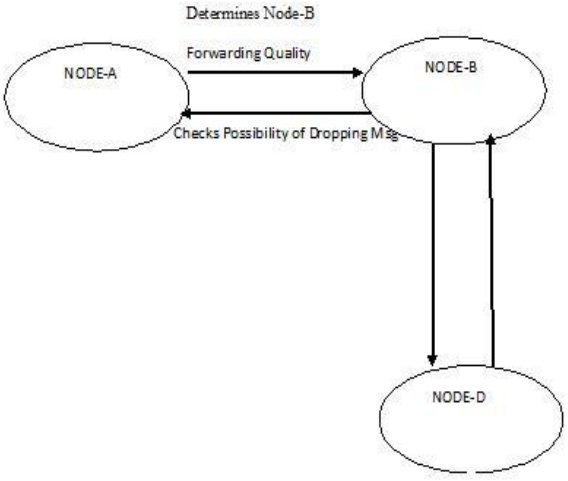


Fig no 6: Protection of cheating actions

4.5 Fairness:

Protocol. The exchanged is defined to be fair if at the end of the protocol, node A receives its reward and node B receives the message. As described in section III-C, nodes A or B contact the TTP only if a problem occurs during the exchange.

5 EXPERIMENTS

5.1 Epidemic Forwarding

In Epidemic Forwarding , every contact is used as a

opportunity to forward messages. social network properties are observed in many DTNs and tend to be stable over time. A distributed algorithm, which only utilizes local information, is then applied to detect communities and the formed communities have strong intra-community connections. We also present two schemes to first select and then prune gateways that connect communities to control redundancy and facilitate efficient intercommunity packet forwarding. Extensive real-trace-driven simulation results are presented to support the effectiveness of our scheme.
There are three phases in Epidemic Forwarding

- Relay phase
- Test Phase

1) During message generation the message is modified so that a relay candidate has no interest in not accepting it;
The relay phase "forces" nodes to collect the so-called proof of relay to show to previous relays (or source), during the test phase,

3) That they have correctly behaved with the original message.

We now evaluate the fairness of the exchange message—this is to make it impossible to relays to drop messages. The details of each phase will be given in the remaining of the section

5.2 Delegation Forwarding

Message generation is just like message generation and in Epidemic Forwarding. Thus, in the next sections, we will describe only the phases that are substantially different from Epidemic Forwarding. As in Epidemic, the relay and the test phases are based on the idea of making nodes collect proofs of relay and to check relays about their behaviour with the message.

In the test by the sender phase the sender will check the forwarding quality of the relay node. And in the test by the destination phase the destination will check the forwarding quality of the received message that has forwarded by the relay.

When a message is generated, it is associated with the forwarding quality of the sender. Then, the message is forwarded from node to node, creating a new replica of the message at each step, according to the following protocol: When a relay node A gets in contact with a possible further relay B, node A checks whether the forwarding quality of B is higher than the forwarding quality of the message. If this is the case, node A creates a replica of the message, labels both messages with the forwarding quality of node B, and forwards one of the two replicas to B. Otherwise, the message is not forwarded.

Algorithm 1: Delegation Forwarding

1:There are N nodes in the network. 2.Thre are D destination.

3. Node n has quality x_{nd} and level τ_{nd} for destination d. INITIALIZE $\forall n, d : \tau_{nd} \leftarrow x_{nd}$.

4. On contact between node i, which is the message holder for destination a and node j:

5. : **if** $x_{ja} > \tau_{ia}$ **then**
6. $\tau_{ia} \leftarrow x_{ja}$
7. **if** node j does not have the message for destination a **then**

8. replicate a message to node j.

9 **end if**

10 else
11 : **if** node j is the destination a **then** 13: replicate a message to node j.
12.
end if
end if

Delegation Forwarding consists of four phases:

- Message generation
- Relay
- Test by the sender
- Test by the destination
- Message generation like epidemic forwarding
- The relay phase "forces" nodes to collect the so-called quality of message to show to previous relays (or source).
- Test by the sender, that they have correctly behaved with the message—Is there any deviation in the message drop messages. If there is no deviation respond with ms Test by the destination, which checks the messages with source messages ok.

5.3 HF algorithm

Hacker finding (HF) algorithm is used to find the hackers in the network. Which allows the secure communication among the nodes .

Algorithm 2: Hacker Finding

1.Create the peer to peer network.
2. Update all authorized users into the router monitor.
3. Initiate the communication among the authorized users.
4**. If** any unauthorized node enters into the network which is

considered as a hacker.
5**. else**
6. Allow the node to communicate.
7. **end if.**

5.4 RR algorithm

During the communication among the nodes in the network the copy of the data is create and stores in the nodes DB's .When the copy of the data is increased the storage requirement will be high and the performance will be reduced .Thus Replica Reduction algorithm is used to remove the redundant copy of the data.

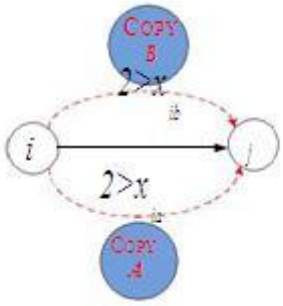
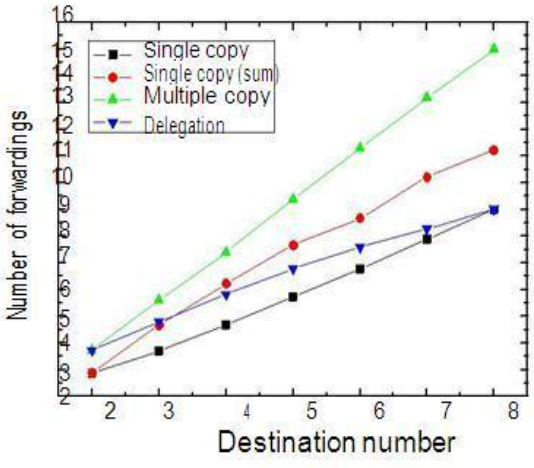


Fig no 7:cheking the number of copy

5.5 Selfishness and Selfishness with Outsiders

selfishness- Nodes that can deviate from the protocol with the goal of maximizing their personal interest.
selfishness- With outsiders nodes that can deviate from the protocol for their personal interest only when this does not damage people from the same community.

This notion is natural since it comes from our personal experience: Some people can tend to be truthful with those they care about, and selfish with outsiders. Formally, it is just vanilla selfishness with a different objective function. However, it is useful to define it as an independent notion. A set of messages is generated with sources and destinations chosen uniformly at random, and generation times from a Poisson process averaging one message every 4 seconds



(a) Number of forwardings in Intel

6. CONCLUSION

The files which are forwarded are double checked, it can forward only after the proof of the relay is received. So there no chance for data loss. Pocket Switched Networks (PSN), can be key technology to provide innovative services to the users without the need of any fixed infrastructure. It is efficient to implement in the large scale peer to peer network by using the relay node. No possible way to hack the data transferred.

7. FUTURE ENHANCEMENTS

In future, our project will improve the performance by reduce the delay overhead. This will lead to the efficient detection of misbehaviour in selfish networks. So the relay nodes can't do the any changing inside the network. The delay overhead will be reduced.

REFERENCES

[1.] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot,"Pocket Switched Networks and Human Mobility in Conference Environments," Proc. ACM SIGCOMM Workshop Delay-Tolerant Networking (WDTN '05), 2005.

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

[3.] V. Erramilli, M. Crovella, A. Chaintreau, and C. Diot, Delegation Forwarding," Proc. ACM MobiHoc '08, 2008.

[4.] E.M. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant Manets," Proc. ACM MobiHoc '07, 2007.

[5.] F. Li and J. Wu, "LocalCom: A Community-Based Epidemic Forwarding Scheme in Disruption- Tolerant Networks," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09), 2009.

[6.] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in Delay Tolerant Networks: A Social Network Perspective," Proc. ACM MobiHoc '09, 2009.

[7.] A.Mei, G. Morabito, P. Santi, and J. Stefa, "Social-aware Stateless Forwarding in Pocket Switched Networks," Proc. IEEE INFOCOM '11, 2011.

[8.] Q. Li, S. Zhu, and G.Cao, "Routing in Socially Selfish Delay Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.

[9.] P. Hui, K. Xu, V. Li, J. Crowcroft, V. Latora, and P.Lio, "Selfishness, Altruism and

Message Spreading in Mobile Social Networks," Proc. First IEEE Int'l Workshop Network Science for Comm.2006.

[10.] R. Janakiraman, M. Waldvogel, and Q. Zhang, "Indra: A peer-to-peer approach to network intrusion detection and prevention," in Proc. IEEE WETICE, Jun. 2003, pp. 226–231.

[11.] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00, 2000.

[12.] S. Buchegger and J.-Y.L. Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes Fairness in Dynamic Ad-Hoc NeTworks," Proc. IEEE/ACM MobiHoc '02, June 2002.

[13.] K. Balakrishnan, J. Deng, and V. Varshney, "Twoack: Preventing Selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Comm. And etworking Conf., vol. 4, Mar. 2005.

[14.] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security, 2002.

[15.] L. Buttya´n and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc Wans," Proc. ACM MobiHoc '00, 2000.

[16.] J.-P. Hubaux, T. Gross, J.-Y. LeBoudec, and M. Vetterli, "Towards Self-Organized Mobile Ad Hoc Networks: The Terminodes Project," IEEE Comm. Magazine, vol. 39, no. 1, pp. 118-124, Jan. 2001.

[17.] M. Jakobsson, J.-P. Hubaux, and L. Buttya´n, "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Net-works," Proc. Int'l Conf. Financial Cryptography '03, Jan. 2003.

[18.] M. Onen, A. Shikfa, and R. Molva, "Optimistic Fair Exchange for Secure Forwarding," Proc. Fourth Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous '07), 2007.

[19] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks," Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.

[20] M. Grossglauser and D. Tse, "Mobility Increases the Capacity of Ad Hoc Wireless Networks," IEEE/ACM Trans. Networking, vol. 10, no. 4, pp. 477-486, Aug. 2002.

[21] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.

[22] P. Hui, K. Xu, V. Li, J. Crowcroft, V. Latora, and P. Lio, "Selfishness, Altruism and Message Spreading in Mobile Social Networks," Proc. First IEEE Int'l Workshop Network Science for Comm. Networks (NetSciCom '09), Apr. 2009.

[23] G. Palla, I. Dere´nyi, I. Farkas, and T. Vicsek, "Uncovering the Overlapping Community Structure of Complex Networks in Nature and Society," Nature, vol. 435, no. 7043, pp. 814-818, 2005.

[24] J. Leguay, A. Lindgren, J. Scott, T. Friedman, and J.Crowcroft, "Opportunistic Content Distribution in an Urban Setting," Proc. SIGCOMM Workshop Challenged Networks (CHANTS '06), 2006.

[25] J. Leguay, A. Lindgren, J. Scott, T. Riedman, J. Crowcroft, and P. Hui, "CRAWDAD Trace upmc/content/imote/cambridge (v. 2006-11-17)," Downloaded from http://crawdad.cs.dartmouth. edu/upmc/content/imote/cambridge, 2006.

[26] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "CRAWDAD Trace Cambridge/haggle/imote/infocom (v. 2006-01-31)," Downloaded from http://crawdad.cs.dartmouth.edu/ cambridge/haggle/imote/infocom, Jan. 2006.

[27] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "CRAWDAD Trace Cambridge/haggle/imote (v. 2009-05-29).