Performance Evaluation of Mobile Ad Hoc Networks In the Presence of Energy-based Selfishness*

Ehsan Ataie
Department of Computer Engineering
Sharif University of Technology
ataie@mehr.sharif.edu

Ali Movaghar
Department of Computer Engineering
Sharif University of Technology
movaghar@sharif.edu

Abstract

Cooperation of nodes for routing and packet forwarding is inevitable in a mobile ad hoc network. Selfishness in such networks is a significant challenge and can cause network performance to noticeably degrade. In this paper, we propose some new selfishness models elicited from psychological behavior of human beings. We also evaluate performance of MANET in the presence of different percentages of selfish nodes that act based on our selfishness models. Results show that energy-based selfishness is a serious problem that could affect performance depends on mobility of nodes, density of network, and time of simulation. This kind of selfishness needs a comprehensive mechanism to cope with and we have planned to publish such mechanism in early future.

Key words

Mobile Ad Hoc Network, Routing, Security, Selfishness, Malice

1. Introduction

An ad hoc network is a group of wireless mobile nodes, in which nodes cooperate by forwarding packets for each other to allow communication beyond their direct wireless transmission range. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed.

In such networks, cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding, i.e. relaying packets for other nodes.

Misbehavior means aberration from normal routing and forwarding behavior. It arises from several reasons. When a node is faulty, its erratic behavior can deviate from the protocol and thus produce non intentional misbehavior. Intentional misbehavior aims at providing an advantage for the misbehaving node [1]. An advantage for a malicious node arises when misbehavior enables it to mount an attack [2]. An example for an advantage gained by misbehavior is power saved when a selfish node does not forward packets for other nodes. The latter misbehavior is called selfishness [3].

Depending on the proportion of selfish nodes and their specific strategies, network throughput can be severely degraded, packet loss increases, nodes can be denied service, and the network can be partitioned. These detrimental effects of misbehavior can endanger the functioning of the entire network [4].

Early routing protocols in mobile ad hoc networks such as DSR [5], AODV [6], DSDV [7], and ZRP [8] did not have any mechanism for coping with security threats and specially selfishness. Later protocols like SRP [9], ARAN [10], SEAD [11] and ARIADNE [12] could not still withstand selfishness even though they introduced some security features to older basic protocols.

Buttyan and Hubaux in [13] proposed two nugget-based approaches to encourage and motivate nodes in order to perform routing and packet forwarding functions.

Later, Michiardi and Molva [14] introduced a mechanism in which each node monitors its neighbors' behavior and deprives selfish nodes of routing services. Alarm messages also are broadcasted to inform other nodes of misbehavior observations.

Yang and Meng in [15] made use of a token-based technique to enforce cooperation among nodes.

Nevertheless, proposed mechanisms have weak spots, like false recognition of selfishness behavior or propagation

* This material is based upon work supported, in part, by Iran Telecommunication Research Center under contract number T500/6379

of alarm messages all over the network, and coping with selfish nodes is still an open subject.

Furthermore, manifestation modality of selfishness behavior and effects of this behavior on the overall network performance is an open discussion topic that needs presenting new and more accurate models of selfishness and investigating their effects and then introducing more comprehensive techniques that can contend with such selfishness.

Most mobile nodes in a typical MANET are controlled by humans either directly or indirectly. So, selfishness in ad hoc networks rises from human being tendency to keep resources for his/her own use and do not waste them for helping other nodes. But as a human behavior, it is more likely that selfishness depends on node's instant energy level. In other words, as node's energy decreases along the time, its sensitivity respect to its energy exhaustion may increase.

Based on this psychological principle, we present a series of nondeterministic and probabilistic selfishness behaviors. These behaviors are modeled by some linear and non-linear functions which define different types of selfish nodes. We evaluate performance of MANET in the presence of different percentages of selfish nodes that act based on our selfishness models and finally propose a general solution. In this way, we also measure the impact of parameters like density and mobility on network packet delivery ratio. Furthermore, performance degradation over time is measured and analyzed.

The remainder of the paper is organized as follows: Section 2 discusses about assumptions and backgrounds of our research. In section 3 models of energy-based selfishness are introduced. Section 4 includes results of simulation about network throughput in different conditions of mobility, density, and time. Finally, in section 5 we discuss about our current future works.

2. Assumptions and Background

This section outlines the assumptions that were made regarding the properties of the physical and network layer of the MANET and includes a brief description of the Dynamic Source Routing (DSR), the routing protocol that has been used for our simulations.

2.1 Physical Layer Characteristics

Throughout this paper, we assume bi-directional communication symmetry on every link between the nodes. This means that if a node B is capable of receiving a message from a node A at time t, then node A could instead have received a message from node B at time t. This assumption is valid because the protocol selected for the simulations is the MAC 802.11 that provides bi-directional communications.

2.2 Dynamic Source Routing (DSR)

DSR is an on-demand, source routing protocol [5]. Every packet has a route path consisting of the addresses of nodes that have agreed to participate in the routing of the packet. The protocol is referred to as "on-demand" because route paths are discovered at the time a source sends a packet to a destination for which the source has no path. The DSR routing process includes two phases: the Route Discovery phase and the Route Maintenance phase. When a source node (S) wishes to communicate with a destination node (D) but does not know any path to D, it invokes the Route Discovery function. S initiates the route discovery by broadcasting a ROUTE REQUEST packet to its neighbors that contains the destination address D. The neighbors in turn append their own addresses to the ROUTE REQUEST packet and re-broadcast it. This process continues until a ROUTE REQUEST packet reaches D. D must now send a ROUTE REPLY packet to inform S of the discovered route. Since the ROUTE REQUEST packet that reaches D contains a path from S to D, D may choose to use the reverse path to send back the reply. The second main function of the DSR is Route Maintenance, which handles link outages.

3. Selfishness Models of Nodes

Selfishness in mobile ad hoc network has a significant importance, since harms it causes can not be alleviated by general security mechanisms like symmetric and asymmetric cryptography. On the other hand, it is almost probable in such networks that nodes act selfishly when they have limited energy power i.e. each node try to consume its energy just when it needs to send its own packets.

If a selfish node does not cooperate in any route discovery process, it is implicitly eliminated from network, because it will come in no source route of a packet. Effect of such selfishness is approximately equal to effect of eliminating all selfish nodes form the network and just lowering network density.

So we assume that a selfish node acts the same in route discovery and packet forwarding according to probabilistic and nondeterministic selfishness models we introduced in the following sections.

3.1. Linear Selfishness Model

According to sensitivity of mobile nodes to their energy consumption, it is reasonable and logical to suppose probability of selfishness behavior as a function of node's energy level.

If we define S_i as probability of selfishness in behavior of node i (i.e. probability that node i drops a data packet), then a simple model can be declared as following linear function:

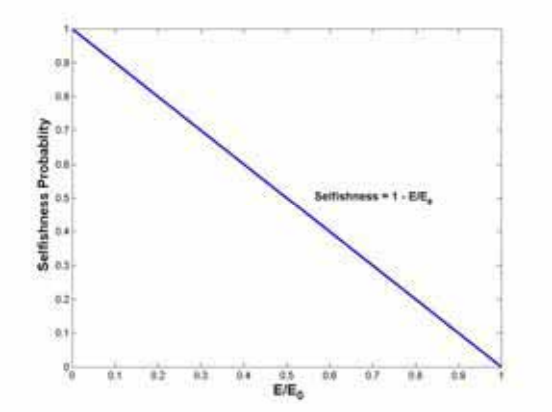

Figure 1: Linear Selfishness Function

$$S_i(E, E_0) = 1 - \frac{E}{E_0}$$

in which E and E_0 are current and initial energy of node i respectively. The probability is zero at first; but it increase linearly and when node's energy reaches zero, node will naturally forward no packet. Figure 1 shows this function.

3.2. Hyperbolic Selfishness Behavior

It is more probable that nodes show nonlinear selfishness behavior. At first, node is somehow indifferent to its energy consumption. But over the time, node's sensitivity to its energy reduction appears more and more. In other words, this behavior function has a positive second derivation. An interesting model we have proposed comes below:

$$S_i(E, E_0) = \left(\frac{1 - E/E_0}{1 + E/E_0} \right)^k$$

where k is a positive integer. Figure 2 shows this function for k equals to 1 and 2.

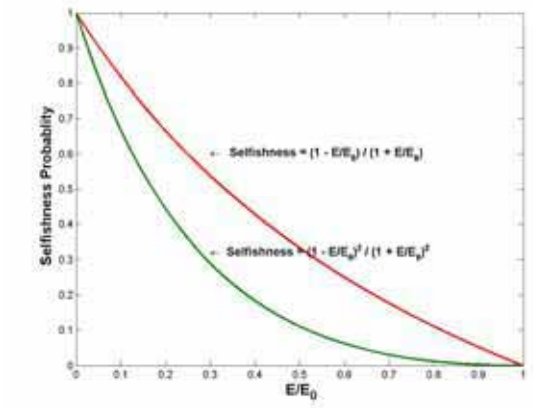

Figure 2: Hyperbolic Selfishness Functions

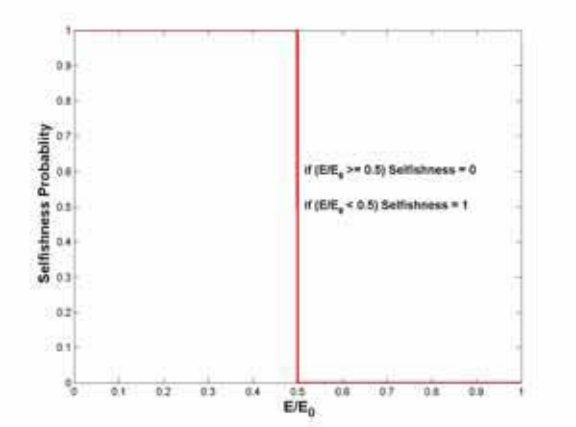

Figure 3: Step Selfishness Function

3.3. Step Selfishness Behavior

In the third model, the node is a benign one as long as its energy is more than or equal to a predefined threshold. But as soon as its energy reaches below the threshold, the node will refuse to forward others' packets. This type of selfishness can be described by following formula:

$$if \;\; E/E_0 \geq 1/k \;\; S_i(E, E_0) = 0$$

$$if \;\; E/E_0 \prec 1/k \;\; S_i(E, E_0) = 1$$

where k is a positive integer. Figure 3 shows this behavior for threshold value of 0.5.

4. Simulation Results

In this section, we show simulation results of energy-based models introduced before and absolute selfishness for comparison. An absolute selfish node is one who drops data packets and forwards request packets, but do not reply these requests. The criterion for measurement and analysis of network performance is network throughput defined as ratio of received packets at destination nodes to sent packets.

The software we have used to simulate the MANET is a version of the Berkeley's Network Simulator (ns-2) that includes wireless extensions made by the CMU Monarch Project. We have also modified DSR protocol to model selfishness.

The nodes communicate using 10 constant bit rate (CBR) sources that are randomly bound to a subset of all the nodes forming the MANET.

In all our node movement scenarios, the node chooses a destination and moves in a straight line towards it at a speed uniformly distributed between 0 meters/seconds (m/s) and some maximum speed. This is called the *random waypoint* model. Once the node reaches its destination it waits for a pause time before choosing a random destination and repeating the process.

4.1. Effect of Mobility on Throughput

In order to compare effect of mobility on network throughput, we have considered two groups of scenarios: low mobility scenarios and high mobility scenarios. Details of simulation characteristics are shown in table 1.

Figure 4 shows network throughput for low mobility scenarios for different selfishness functions.

Table 1: Variant Mobility

Variable	*Value*
Size of Environment	1000^{m} x 1000^{m}
Number of Nodes	30
Speed	$2^{m/s}$ for Low Mobility $20^{m/s}$ for High Mobility
Pause Time	Uniform [0^{s}, 20^{s}]
Initial Energy	100^{J}
Simulation Time	500^{s}

Each point on the figure is average throughput of seven different simulation runs in each on them selfish nodes are selected randomly. As it can be seen, when no selfish node exists, network throughput is about %95. This means that probability of link breakage is low when mobility is low.

It is obvious that gradually reduction of throughput in energy-based models is because of more packet droppings when percentage of selfish nodes increases. But since energy level of nodes at the end of simulation time just decreases slightly compared to their initial energy, reduction of throughput is not very substantial.

Network throughput curves for high mobility scenarios can be seen in figure 5. In these groups of scenarios, throughput is about %87 when all nodes are benign.

The difference between this value and corresponding one in low mobility scenarios is the result of nodes' speed that increases broken links and causes throughput to recede.

An interesting point when comparing figures 4 and 5 is divergence of curves of each energy-based model in figure 4 and its correspondent in figure 5. In other words, curves at high mobility scenarios subside faster when percentage of selfish nodes increases.

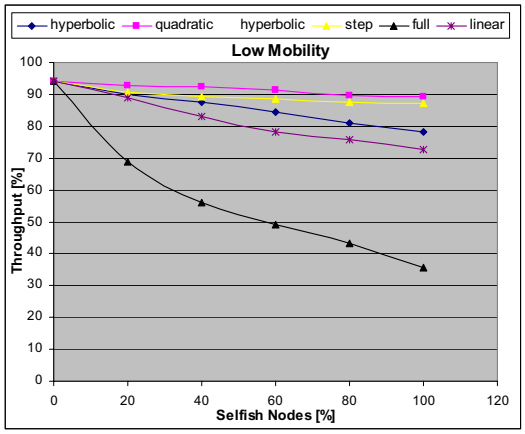

Figure 4: Low Mobility Scenarios

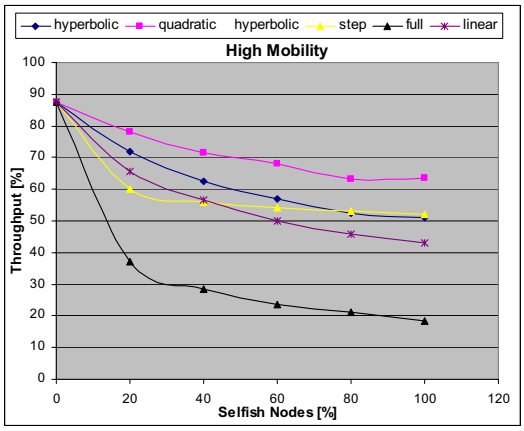

Figure 5: High Mobility Scenarios

Since in higher mobility more link breakage occurs, more route request and reply packets are propagated all over the network which results in more energy consumption in nodes. Thus selfishness of these nodes increases and network throughput dies down much faster.

4.2. Effect of Density on Throughput

In the second research, we have measured throughput changes for two groups of scenarios: high density scenarios and low density scenarios

Characteristics of these two sets of simulation are shown in tables 2. Figure 6 and 7 show result curves.

Table 2: Variant Density

Variable	*Value*
Size of Environment	1000^{m} x 1000^{m}
Number of Nodes	15 for Low Density 50 for High Density
Speed	Uniform [$2^{m/s}$, $20^{m/s}$]
Pause Time	Uniform [0^{s}, 20^{s}]
Initial Energy	100^{J}
Simulation Time	500^{s}

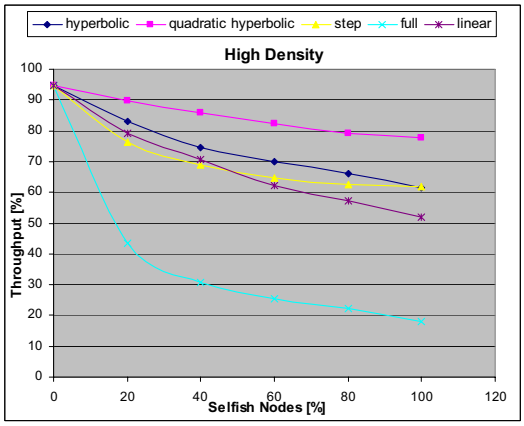

Figure 6: High Density Scenarios

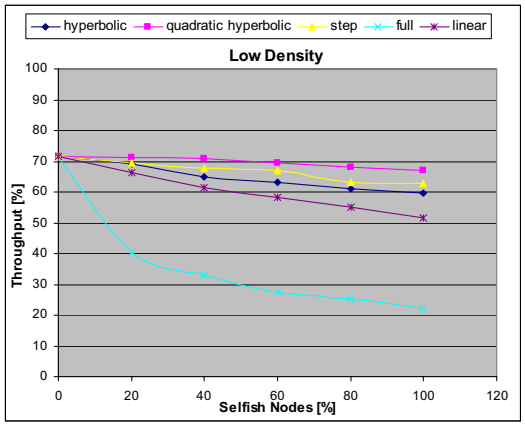

Figure 7: Low Density Scenario

When all nodes cooperate for route discovery and packet forwarding in high density scenarios, network throughput is almost %94. But the corresponding throughput in low density scenarios is %71. The difference between these two values is caused from longer paths between sources and destinations when density is low.

More density results in more probability of finding shorter path between a pair of source and destination. So, in low density scenarios probability of link breakage is greater and as a result throughput subsides. Let's illustrate this subject. Assume S and D are connected via node A in a high density scenario. It is more probable that corresponding S and D in low density scenario are connected via more nodes e.g. A, B, and C. We define P(XY) as probability of availability of connection between nodes X and Y. when a packet is traversing toward destination, then P(SD) can be approximately defined as:

P(SD) = P(SA) P(AD) in high density

P(SD) = P(SA) P(AB) P(BC) P(CD) in low density

If we suppose that P(XY) for an adjacent pair of X and Y is a constant in both scenarios, it is clear that P(SD) in low density is smaller than P(SD) when density is high.

In addition to link breakage problem, it is common in lower densities that a source waits a long time for receiving first route reply, or even sends several route requests before establishing a connection to a destination. All of the above reasons cause such a reduction in throughput when density is low.

A point that can be mentioned is that slope of energy-based selfishness curves in high density scenarios is more than the slope of their corresponding curves in low density scenarios. This fact can be justified as follows: when density is high, each node has more neighbors. So average number of route requests a node receives, replies, or forwards is much more than this number in corresponding low density scenarios. This is also true for number of data packets a node should receive and process even if the node is not in source route of packets.

When number of packet receipts increases, energy level decreases and probability of selfish behavior increases: the result is throughput reduction.

Our studies show that average value of nodes' energy in high density scenarios is much less than nodes' energy in low density scenarios and so our above justification is true.

4.3. Effect of time on Throughput

Last study shows effects of time on network throughput. Simulation characteristics are shown in table 3. Results can be seen in figure 8. As it can be seen, network throughput reduces gradually when simulation time increases. This reduction is about 5 percent for absolute selfishness when simulation time changes from 100^{s} to 1000^{s}.

But the throughput decrease will be between 45-55 percent for energy-based selfishness curves. This proves that reduction of energy level has what a corruptive effect on network throughput.

Table 3: Time

Variable	*Value*
Size of Environment	1000^{m} x 1000^{m}
Number of Nodes	30
Speed	Uniform [$2^{m/s}$, $20^{m/s}$]
Pause Time	Uniform [0^{s}, 20^{s}]
Initial Energy	100^{J}

Since energy of most nodes reaches the threshold when 200-300 seconds of simulation time passes, curve of step selfishness has a different behavior from other energy-based functions in the shape.

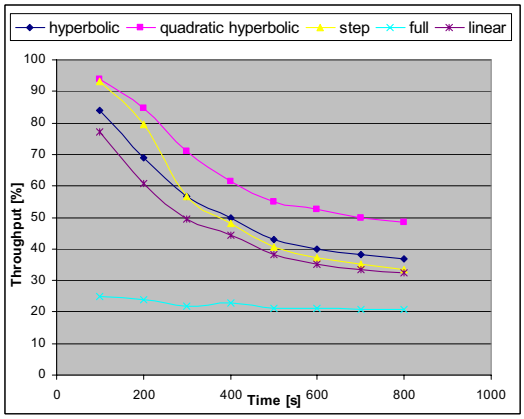

Figure 8: Time Scenarios

5. Conclusions and Future Works

In this research, we propose nondeterministic and probabilistic models of selfishness in mobile ad hoc networks which are dependent on node's instantaneous energy level. Since selfishness usually arises form node's interest in its survivability, these models seem to be tangible and completely probable. Applying these models to

MANETs shows that in the presence of energy-based selfishness when density is high, network throughput degrades faster than when density is low.

We also conclude that mobility has a strong effect on network performance and throughput degradation is much faster when mobility is high.

Other result of our simulation is corresponding to effect of time on throughput. Unlike absolute selfishness, energy-based selfishness models causes network throughput to gradually decrease over time.

The results prove that we should design a mechanism for coping with selfishness that encourages nodes to cooperate and deprives selfish nodes of routing services. When nodes show energy-based selfishness, this mechanism should have additional and strong features.

Currently, there are some unti-selfishness mechanisms like watchdog/pathrater [16], nugget-base mechanism [13], token-based mechanism [15], CORE [14], and CONFIDANT [4] [17].

A point in case regarding deficiency of existed protocols for copping with energy-based selfishness is incorrect accusation and reputation improvement. There are always benign nodes which may be incorrectly accused to be malicious or selfish because of link breakages.

Some of the above mechanisms do not handle to exculpate these benign nodes. Some others usually use techniques to allow nodes to improve their reputation. These techniques allow such nodes to not permanently be recognized as selfish nodes.

Since our selfishness models are nondeterministic, finding a real selfish node is much harder. In these models a selfish node may not forward a packet for the time being and then may immediately forward another one. So, it can improve its reputation and never be recognized as a selfish node if we use above techniques.

In addition, propagation of alarm messages in the network as is done in some previous mechanisms will consume energy of sender, intermediate, and receiver nodes and thus will increase overall selfishness behaviors.

Our next plan has being to design a mechanism which can cope with these several problems of energy-based selfishness. The result protocol, called "Cooperation Enforcement, Malice Detection, and Energy Efficient Mechanism" (CEMDEEM) will be published in the near future.

Reference

[1] L. Zhou and Z. J. Haas, *Securing Ad Hoc Networks,* IEEE Network Magazine, Vol. 3, NO. 6, Nov-Dec. 1999.

[2] H. Deng, Wei Li and D. P. Agrawal, *Routing Security in Wireless Ad Hoc Networks,* IEEE Communication Magazine, Vol. 40, NO. 10, Oct. 2002, pp. 70-75.

[3] P. Michiardi and R. Molva, "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks", in proceedings of European Wireless Conference, 2002.

[4] S. Buchegger, *Coping with Misbehavior in Mobile Ad Hoc Networks*, PhD thesis, EPFL, 2004.

[5] D. B. Johnson and D. A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks,* Mobile Computing, Chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996.

[6] C. Perkins, *Ad hoc On Demand Distance Vector (AODV) Routing,* Internet draft, draft-ietf-manet-aodv-02.txt, November 1998.

[7] C. E. Perkins and P. Bhagwat, *Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,* In Proceedings of the SIGCOMM 94 Conference on Communications Architectures, 1994.

[8] Z. J. Hass and M. R. Pearlman, *The Zone Routing Protocol (ZRP) for Ad Hoc Networks,* Internet draft, draft-ietf-manet-zone-zrp-01.txt, Aug. 1998.

[9] P. Papadimitratos and Z. J. Haas, *Secure Routing for Mobile Ad Hoc Networks,* in Proceedings of CNDS2002.

[10] K. Sanzgiri, et al, *A Secure Routing Protocol for Ad Hoc Networks,* Proceedings of the 10th IEEE International Conference on Network Protocols, 2002.

[11] Y-C Hu, D. B. Johnson and A. Perrig, *SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,* in the Fourth IEEE Workshop on Mobile Computing Systems and Applications, 2002.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, *Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks,* in proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom), Sept. 2002.

[13] L. Buttyan and J. P. Hubaux, *Nuglets: a virtual currency to stimulate cooperation in selforganized ad hoc networks,* Technical Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne, 2001.

[14] P. Michiardi and R. Molva, *Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks,* IFIP - Communication and Multimedia Security Conference, 2002.

[15] H. Yang, X. Meng and S. Lu, *Self-Organized Network-Layer Security in Mobile Ad Hoc Networks,* WiSe 2002.

[16] S. Marti, et al., *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*, Proceeding of 6th Annual International Conference on Mobile Computing and Networking (MOBICOM 2000), ACM Press, 2000, pp. 255–265.

[17] S. Buchegger and J. Y. Boudec, *Performance analysis of the CONFIDANT protocol: Cooperation Of Nodes: Fairness In Distributed Ad-hoc NeTworks*, in Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, Switzerland, June 2002.