Evaluating Selfishness Impact on MANETs

Dimitra G. Kampitaki, Eirini D. Karapistoli and Anastasios A. Economides
Interdepartmental Program of Postgraduate Studies on Information Systems
University of Macedonia
Thessaloniki, 54006 Greece
{kampitaki, karapis, economid}@uom.gr

***Abstract*—Mobile Ad Hoc Networks (MANETs) use many different routing protocols to route data packets between nodes. These routing protocols are designed taking for granted that all nodes are cooperative and willing to forward control and data packets from and to other nodes. However, when selfish nodes exist in the network, the network performance may degrade significantly. In previous research, selfish nodes are predetermined, meaning that a node is either selfish or not from the beginning (i.e., when deployment takes place) and retains that behavior over time. However, in reality selfishness is not static, but an outcome of restricted energy. In this paper, we investigate the operation of Dynamic Source Routing (DSR) protocol, as selfish behavior emerges in a MANET due to energy depletion. We define different levels of selfishness, and we investigate the protocol performance when the nodes inside the network exhibit different levels of selfishness.**

***Keywords*—Mobile Ad Hoc Networks; routing protocols; DSR; selfish nodes; simulation;**

I. Introduction

Mobile Ad Hoc Networks (MANETs) [1] are networks that have no predefined infrastructure. Many routing protocols are currently being used for routing in MANETs, and are categorized under different criteria [2]. The most general distinction of MANET routing protocols is proactive and reactive, with hybrid protocols using principles from both of these categories. Dynamic Source Routing (DSR) protocol is an on-demand or reactive routing protocol that uses flat network topologies [3].

Nodes participating in a MANET behave cooperatively obeying the routing protocol that is used. In fact, routing protocols are designed taking for granted that all nodes participating in the network are cooperative. In some cases though, nodes might deviate from that behavior causing problems to the network. There are various types of misbehavior of a MANETs nodes. Some of them occur when specific circumstances exist, while others are the outcome of security attacks. The most common cause of unintentional misbehavior is the shortage of energy resources. When a nodes battery level gets low, that node might not cooperate as expected by the routing protocol. Instead, it may save energy resources to serve its own communication needs, and to prolong its own lifetime, regardless of the common welfare of the network.

In this paper, we contribute to the area of routing for MANETs by investigating the impact of the presence of selfish nodes in the network when the DSR protocol is employed. We provide a more realistic definition of the selfish behavior distinguishing it from intentional misbehavior. We also define various types of selfish nodes and extensively examine their impact on the network by simulating several scenarios.

The rest of the paper is organized as follows. Section II provides an overview of related work as well as existing definitions of selfishness. Section III provides an overview of the simulation environment and the parameters used, and analyzes the obtained simulation results. Section IV concludes the paper with some insightful discussion and future research directions.

II. Related Work

There have been several performance evaluation studies of MANET routing protocols under various scenarios [4]–[12]. In many cases, researchers compare different types of routing protocols [4]–[11] while in others, they compare protocols of the same type [12] in order to identify the best performing protocol under certain circumstances and with respect to various metrics. Other studies test the performance of routing protocols when the nodes follow different mobility models [13], [14], or even when there are obstacles in the field [15]. Other approaches to routing protocol evaluation consider heterogeneous networks and examine the network performance when nodes of different types exist [16].

The performance of routing protocols when selfish nodes exist in the network has attracted several research studies, but in all cases, selfishness is considered as a threat or an attack instead of an expected behavior of the network nodes. Thus, research focuses on detection and suppression of selfish nodes by employing watchdogs or other central or distributed authorities. These kinds of solutions are characterized as reputation-based [17]–[20]. Other approaches, characterized as credit-based, provide incentives to cooperate in the form of virtual currency [21], [22]. There are also game theoretic approaches [23]–[25] that utilize Game Theory to model and explain selfish behavior. There is a comprehensive overview of selfishness management schemes in [26].

One of the initial definitions of node misbehavior in MANETs can be found in [17]. There, a misbehaving node is one that agrees to participate in forwarding packets (/) but then indiscriminately drops all packets that are routed through it. Following that definition, the network performance is evaluated by modifying the percentage of selfish nodes in the network (out of 50 nodes). DSR is the routing protocol used. Other researchers mostly use the above definition of node misbehavior.

In [27], the nodes selfish behavior is categorized into four different types depending on the way the various control and data packets are handled. Various scenarios with varying number of selfish nodes are examined based on the Ad hoc On-demand Distance Vector (AODV) routing protocol. The same approach is followed in every comparative simulation that is presented in [17]–[25] disregarding the cause of selfishness which is the depletion of energy resources.

In [28], a more formal approach to categorize and investigate node behavior is attempted, forming four main categories: cooperative, inactive, selfish and malicious nodes. The most important difference between selfish and malicious nodes, is that the first category of nodes do not wish to harm the network, while the second category of nodes intentionally aim to harm the network and disrupt its protocols.

In this work, we examine the performance of the DSR routing protocol considering selfishness as an expected behavior of the nodes. We define four levels of selfishness to describe selfish behavior, with each level depending on the nodes residual energy. Our simulations begin with nodes having different initial energy levels, so their expected selfishness level is different. In this way, we approach the problem of selfishness in MANETs more realistically.

III. Simulation Setup and Results

In this section, we first present the simulation configuration and then analyze the obtained results. For the purposes of our analysis, we used the OMNeT++ 4.4.1 [29] with the addition of the inetmanet-2.0 framework [30]. We used the dsr-uu implementation provided by the inetmanet-2.0 framework in order to simulate the DSR protocol. Several modifications were conducted to this model mainly concerning the statistics collection. The AdhocHost node module implementation and the Battery module implementation included in inetmanet-2.0 framework are also modified to serve our needs.

A. Simulation Parameters

In Table I, the general simulation parameters are denoted. All the simulations are averaged over 10 runs. Each simulation runs until the energy of at least one node is completely depleted. The simulation area is 1500m x 500m and the nodes move inside this area following a Random Way Point mobility model with a speed ranging between 0-2m/s (low mobility scenario). The transmission range for each node is set to 250m. To avoid congestion, we use 64B packets that are sent with a rate of 4 packets/sec.

We examine four cases that are summarized in Table II. In Case A (No Selfishness), nodes act cooperatively and there is no selfish behavior. This case is used as a reference and comparison measure for better understanding.

TABLE I. Simulation Scenarios Parameters

Parameter	Value
Simulation Time	Time until the first node's energy runs off
Simulation Area	1500 m x 500 m
Number of Nodes	10-20-30-40-50
Transmission Range	250 m
Mobility Model	Random Way Point
Node Speed	0-2 m/s
Traffic Generator	CBR
Packet Bytes	64 bytes
Data Rate	2 MBps

In case B (Constant Selfishness), we examine the impact of selfishness in a way that it has been examined in previous research studies, i.e., by specifying at the beginning of the simulation a percentage of selfish nodes. This percentage remains constant all the time and does not change according to the energy depletion of the nodes. To compare this case with the other cases, we set a 20% of the total nodes to be selfish. As stated in [17], considering 40% of the total nodes to be selfish seems unrealistic, so we selected a more realistic scenario with 20% of the total nodes to be selfish for our simulations, which is about equal to the time-averaged percentage of selfish nodes present in the network at simulation Cases C and D.

In Case C (Single Threshold Selfishness), time is considered as a new parameter. As time progresses and the nodes energy gets below a specific percentage of their nominal energy, they instantly become selfish dropping all data packets that arrive to them. This should be the case for all similar evaluations, as selfishness emerges when the residual energy levels are low. We name nodes that behave in this manner as Threshold Selfish nodes. The threshold can take any desired value depending on the nodes needs. We arbitrarily set that threshold at 20% for the purpose of our study.

Finally, in Case D (Multi-Threshold Selfishness) the nodes act more selfishly as their energy dissipates, dropping packets with some probability. We define the Residual Energy Percentage $RE\%$ as follows:

$$RE\% = \frac{\text{Residual Battery Capacity}}{\text{Nominal Battery Capacity}} \quad (1)$$

Then, we define four Selfishness Levels (SL) based on three energy thresholds T_1, T_2, T_3 where $T_1 > T_2 > T_3$, that orientate the behavior of the nodes, as follows:

$$SL = \begin{cases} \text{Always Altruistic (AA)}, & \text{if } RE\% \geq T_1, \\ \text{Sometimes Selfish (SS)}, & \text{if } T_1 > RE\% \geq T_2, \\ \text{Often Selfish (OS)}, & \text{if } T_2 > RE\% \geq T_3, \\ \text{Always Selfish (AS)}, & \text{if } T_3 > RE\%. \end{cases} \quad (2)$$

Each Selfishness Level corresponds to a Packet Drop Probability (PDP), which is defined by the individual nodes needs, with $\text{PDP}_{AA} = 0\%$ and $\text{PDP}_{AS} = 100\%$. The PDP_{SS} and PDP_{OS} can take any value that suits the nodes needs, as long as $\text{PDP}_{SS} > \text{PDP}_{OS}$. In our simulation, we define the thresholds and the PDP for each SL as declared in Table II.

TABLE II. Selfishness Types and Packet Drop Probability

Case	Residual Energy (%)	Selfishness Type	Packet Drop Probability
A	Not Important	Not Applicable	0%
B	Not Important	Selfish (constant number of selfish nodes)	100%
C	<20	Selfish	100%
D	80-100	Always Altruistic (AA)	0%
	50-80	Sometimes Selfish (SS)	10%
	20-50	Often Selfish (OS)	50%
	<20	Always Selfish (AS)	100%

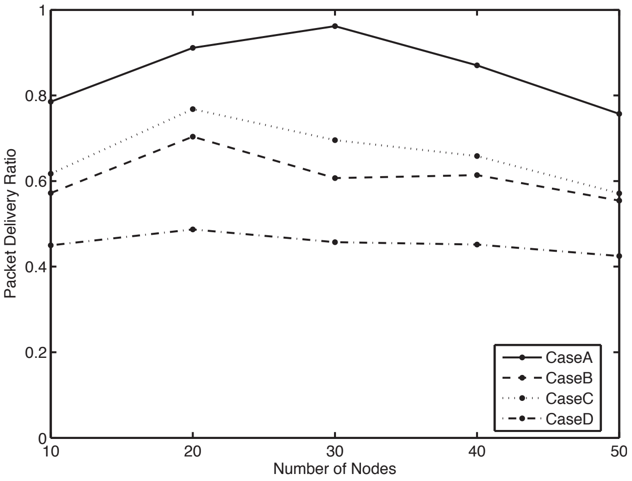

Fig. 1. Average Packet Delivery Ratio vs Number of Nodes

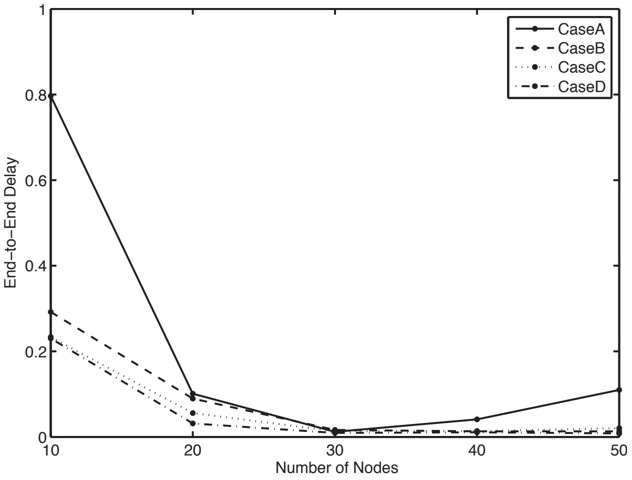

Fig. 2. Average End-to-End Delay vs Number of Nodes

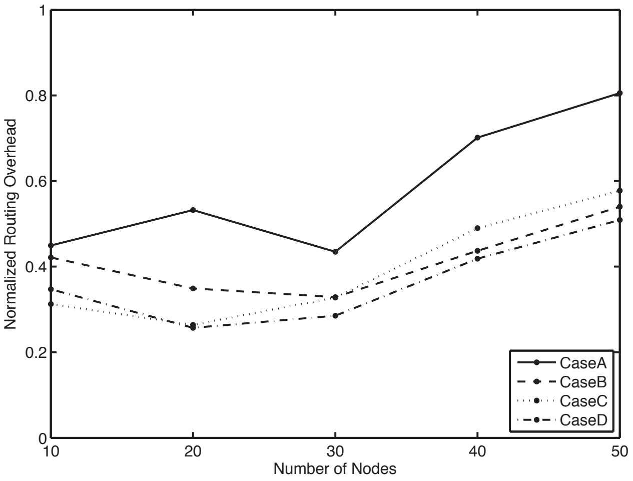

Fig. 3. Average Normalized Routing Overhead vs Number of Nodes

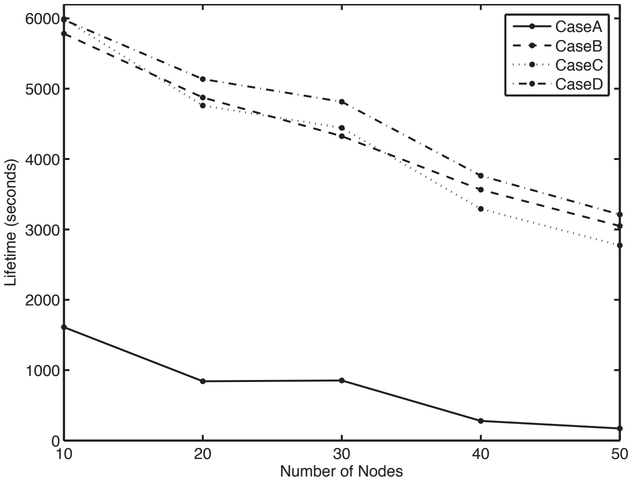

Fig. 4. Average Network Lifetime vs Number of Nodes

B. Simulation Metrics

In order to investigate the impact of selfishness on the network performance, we used the following metrics:

1) Average Packet Delivery Ratio (PDR): This metric is computed by dividing the total number of packets received by destination nodes with the total number of packets sent from the source nodes.

2) Average End-to-End Delay (AEED): This metric is computed by averaging the end-to-end delay of all successfully delivered packets in the network.

3) Average Normalized Routing Overhead (NRO): This metric is computed by dividing the total control packets with the total packets received in the network.

4) Network lifetime: This is the lifetime of the network, until at least one nodes energy is depleted.

Additionally to the metrics that consider routing protocol performance, we also recorded the percentage of selfish nodes versus time during our simulations for better understanding of the underlying mechanisms of Single- and Multiple-Threshold Selfishness.

C. Simulation Results

In this section, we present our simulation results. In Figures 1-4 the Average PDR, the AEED, the Average NRO and the Average Network Lifetime respectively, versus the number of nodes are presented for all four cases.

As expected, the best performance for all metrics is recorded when no selfish nodes exist in the network, i.e., in Case A. The PDR is close to 100% when the nodes are 30 with less values for less nodes, due to restricted connectivity and reachability. For more nodes, the PDR drops again due to the high node density of the network that leads to more interference between the nodes.

Cases B, C and D have similar results in all metrics except for the PDR, which in Case D seems to be more affected than in the other two cases. Generally, case D, i.e. Multiple-Threshold Selfishness seems to affect all metrics more than all the other cases, so we can assume more strain is put on the routing protocol when that kind of model is used. Additionally, in Case D nodes do not become suddenly selfish, but go through multiple levels of selfishness before they become completely selfish. Therefore, this information can be passed

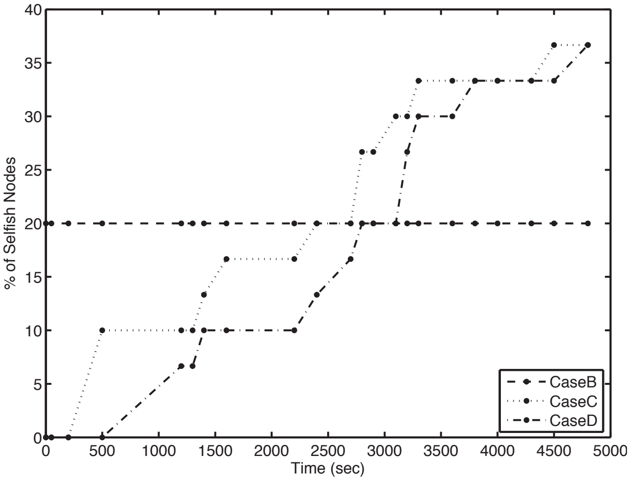

Fig. 5. Percentage of Selfish Nodes vs Time

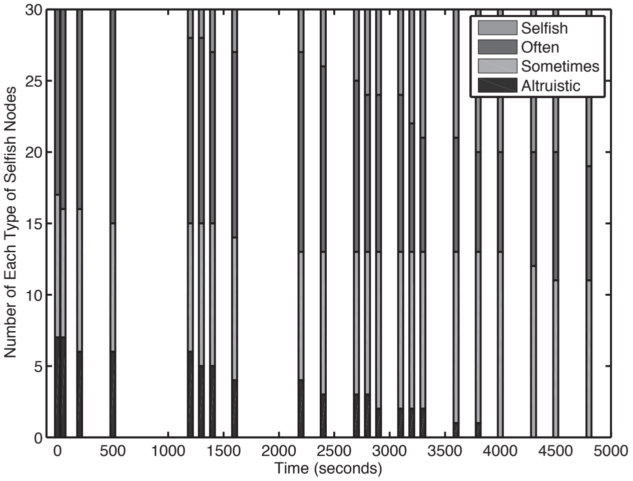

Fig. 6. Number of Selfish Nodes vs Time

towards the routing protocol to be able to distinguish which nodes are going to be selfish soon and to avoid them during the routing process.

In Fig. 5 the percentage of selfish nodes over time is presented for Cases B, C and D for a representative case. In Case B the percentage of selfish nodes is constant throughout the simulation. In Case C the percentage of selfish nodes gets bigger sooner than in Case D. This happens because in Case D there are multiple levels of selfishness, which help sustain nodes with lower energy for more time.

Finally, in Fig. 6, the total number of nodes that correspond to each level of selfishness is illustrated for one representative simulation of Case D. Initially, there are no selfish nodes at all (AS), while many altruistic nodes exist (AA). In addition, nodes with SS and OS selfishness levels exist, depending on the initial energy of each node. As time progresses, the residual energy of the nodes decreases and their selfishness level increases, as defined in Eq. (2). After some time, no AA nodes remain, and solely selfish nodes of various levels of selfishness emerge. Finally, just before the simulation halts, more than 1/3 of the nodes become of AS selfishness level.

Summarizing the results, we assume that the model of Multiple-Threshold Selfishness is more appropriate for routing protocol evaluation purposes than the other two, since it highlights the increased effect of selfishness on the routing process in a more prominent way. Therefore, it can be used for performance evaluation studies of proposed selfishness suppression protocols, instead of the standard Constant Selfishness model (i.e. Case B), that is used until now.

IV. Conclusions and Future Work

As expected, the impact of the presence of selfish nodes in a MANET is small when there are few selfish nodes present, and gets higher the more they become. When the available energy is restricted, and as time passes by, more nodes adopt selfish behavior, affecting more the network performance metrics. The most affected metric seems to be PDR followed by AEED and NRO. We proved by simulation that by defining multiple levels of selfishness we are able to extend nodes and consequently network lifetime in comparison to defining only two levels for selfishness, selfish or not selfish.

In the future, we intend to utilize the aforementioned analysis in order to design and implement a routing protocol based on DSR that will minimize the effect of the presence of selfish nodes on the network performance, concentrating our efforts to ensure high PDR and low AEED and NRO. Another interesting approach is the development of an analytical model to describe selfishness over time when battery resources are constrained.

References

[1] C. S. R. Murthy and B. Manoj, *Ad hoc wireless networks: Architectures and protocols*. Pearson education, 2004.

[2] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad hoc networks*, vol. 2, no. 1, pp. 1–22, 2004.

[3] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile computing*. Springer, 1996, pp. 153–181.

[4] C. Samara, E. Karapistoli, and A. A. Economides, "Performance comparison of manet routing protocols based on real-life scenarios," in *Ultra Modern Telecommunications and Control Systems (ICUMT), 2012 4th International Congress on*. IEEE, 2012, pp. 870–877.

[5] D. Kampitaki and A. A. Economides, "Simulation study of manet routing protocols under ftp traffic," in *Conference on Electronics, Telecommunications and Computers (CETC)*, 2013.

[6] F. Diamantopoulos and A. A. Economides, "A performance study of dsdv-based clusterpow and dsdv routing algorithms for sensor network applications," in *Wireless Pervasive Computing, 2006 1st International Symposium on*. IEEE, 2006, pp. 1–6.

[7] P. Karavetsios and A. A. Economides, "Performance comparison of distributed routing algorithms in ad hoc mobile networks," *WSEAS Transactions on communications*, vol. 3, no. 1, pp. 317–321, 2004.

[8] F. Diamantopoulos and A. A. Economides, "Performance evaluation of power control routing for ad-hoc networks," in *Wireless Conference 2006-Enabling Technologies for Wireless Multimedia Communications (European Wireless), 12th European*. VDE, 2006, pp. 1–6.

[9] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1998, pp. 85–97.

[10] C. Mbarushimana and A. Shahrabi, “Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks,” in *21st International Conference on Advanced Information Networking and Applications AINAW’07*, vol. 2. IEEE, 2007, pp. 679–684.

[11] N. Bilandi and H. K. Verma, “Comparative analysis of reactive, proactive and hybrid routing protocols in manet,” *International Journal of Electronics and Computer Science Engineering (IJECSE)*, vol. 1, no. 03, pp. 1660–1667, 2012.

[12] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, “Performance comparison of two on-demand routing protocols for ad hoc networks,” *Personal Communications, IEEE*, vol. 8, no. 1, pp. 16–28, 2001.

[13] F. Maan and N. Mazhar, “Manet routing protocols vs mobility models: A performance evaluation,” in *Ubiquitous and Future Networks (ICUFN), 2011 International Conference on*. IEEE, 2011, pp. 179–184.

[14] F. Bai, N. Sadagopan, and A. Helmy, “Important: A framework to systematically analyze the impact of mobility on performance of routing protocols for adhoc networks,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 2. IEEE, 2003, pp. 825–835.

[15] Y. H. Ho, A. H. Ho, and K. A. Hua, “Routing protocols for intervehicular networks: A comparative study in high-mobility and large obstacles environments,” *Computer Communications*, vol. 31, no. 12, pp. 2767–2780, 2008.

[16] H. A. Amri, M. Abolhasan, and T. Wysocki, “Scalability of manet routing protocols for heterogeneous and homogenous networks,” *Computers & Electrical Engineering*, vol. 36, no. 4, pp. 752–765, 2010.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000, pp. 255–265.

[18] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the confidant protocol,” in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2002, pp. 226–236.

[19] P. Michiardi and R. Molva, “Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” in *Advanced Communications and Multimedia Security*. Springer, US, 2002, pp. 107–121.

[20] K. Balakrishnan, J. Deng, and P. K. Varshney, “Twoack: preventing selfishness in mobile ad hoc networks,” in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 4. IEEE, 2005, pp. 2137–2142.

[21] S. Zhong, J. Chen, and Y. R. Yang, “Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1987–1997.

[22] L. Anderegg and S. Eidenbenz, “Ad hoc-vcg: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents,” in *Proceedings of the 9th annual international conference on Mobile computing and networking*. ACM, 2003, pp. 245–259.

[23] V. Srinivasan, P. Nuggehalli, C.-F. Chiasserini, and R. R. Rao, “Cooperation in wireless ad hoc networks,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 2. IEEE, 2003, pp. 808–817.

[24] D. Hales, “From selfish nodes to cooperative networks-emergent link-based incentives in peer-to-peer networks,” in *Peer-to-Peer Computing, 2004. Proceedings. Proceedings. Fourth International Conference on*. IEEE, 2004, pp. 151–158.

[25] M. Naserian and K. Tepe, “Game theoretic approach in routing protocol for wireless ad hoc networks,” *Ad Hoc Networks*, vol. 7, no. 3, pp. 569–578, 2009.

[26] Y. Yoo and D. P. Agrawal, “Why does it pay to be selfish in a manet?” *Wireless Communications, IEEE*, vol. 13, no. 6, pp. 87–97, 2006.

[27] S. Yokoyama, Y. Nakane, O. Takahashi, and E. Miyamoto, “Evaluation of the impact of selfish nodes in ad hoc networks and detection and countermeasure methods,” in *Mobile Data Management, 2006. MDM 2006. 7th International Conference on*. IEEE, 2006, pp. 95–95.

[28] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz, “On the effect of node misbehavior in ad hoc networks,” in *Communications, 2004 IEEE International Conference on*, vol. 6. IEEE, 2004, pp. 3759–3763.

[29] A. Varga and R. Hornig, “An overview of the omnet++ simulation environment,” in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, ser. Simutools ’08. Brussels, Belgium, Belgium: ICST, 2008, pp. 60:1–60:10.

[30] A. Ariza-Quintana. (2014, Apr.) Main download page. [Online]. Available: https://github.com/aarizaq/inetmanet-2.0/tree/inetmanet-2.2