EFW: A Cross-Layer Metric for Reliable Routing in Wireless Mesh Networks with Selfish Participants

Stefano Paris*, Cristina Nita-Rotaru†, Fabio Martignon‡ and Antonio Capone*
*Dip. di Elettronica e Informazione
Politecnico di Milano
{paris, capone}@elet.polimi.it
†Dep. of Computer Science
Purdue University
crisn@cs.purdue.edu
‡Dep. of Inf. Technology
and Math. Methods
University of Bergamo
fabio.martignon@unibg.it

***Abstract*—Wireless mesh networks (WMNs) have emerged as a flexible and low-cost network infrastructure, where heterogeneous mesh routers managed by different users collaborate to extend network coverage. Several routing protocols have been proposed to improve the packet delivery rate based on enhanced metrics that capture the wireless link quality. However, these metrics do not take into account that some participants can exhibit selfish behavior by selectively dropping packets sent by other mesh routers in order to prioritize their own traffic and increase their network utilization.**

This paper proposes a novel routing metric to cope with the problem of selfish behavior (i.e., packet dropping) of mesh routers in a WMN. Our solution combines, in a cross-layer fashion, routing-layer observations of forwarding behavior with MAC-layer measures of wireless link quality to select the most reliable and high-performance path.

We integrated the proposed metric with a well-known routing protocol for wireless mesh networks, OLSR, and evaluated it using the NS2 simulator. The results show that our cross-layer metric accurately captures the path reliability, even when a high percentage of network nodes misbehave, thus considerably increasing the WMN performance.

***Index Terms*—Wireless Mesh Networks, Selfish Nodes, Packet Dropping, Routing Metrics.**

I. Introduction

Wireless Mesh Networks (WMNs) have emerged as a technology for next generation wireless networking, fostering the development of new network paradigms such as wireless mesh community networks (WMCNs) [1]. Since many applications envisioned to run on WMCNs have high-throughput requirements, recent research [2], [3] has introduced several link layer metrics that capture the quality of wireless links to select the network paths with the highest delivery rates.

However, most of the proposed metrics have been designed assuming that each wireless mesh router participates honestly in the forwarding process. While this assumption may be valid in a network managed by a single network operator, it is not necessarily met in a network where the participants are managed by different entities that may benefit from not forwarding all the traffic. Specifically, in a WMCN, a selfish user that provides connectivity through his own mesh routers might try to greedily consume the available bandwidth by favoring his traffic to the detriment of others, by selectively dropping packets sent by other nodes [1]. Tools like *iptables* can be used to easily implement packet dropping at the network layer even by inexpert users. Such selfish behavior can cause unfairness and severe performance degradation, since periodic dropping at relaying nodes decreases the throughput of closed loop connections (such as TCP) established by other nodes, even when the fraction of dropped packets is small.

Previous works focused mainly on the detection of nodes that exhibit selfish behavior and their exclusion from the network. To the best of our knowledge, only two routing metrics have been proposed in the research literature to consider the selfish behavior of network nodes [4], [5]. These metrics, tailored for reactive routing protocols like AODV and DSR, increase the hop count of a network path proportionally to the number of selfish nodes that belong to that path. However, the hop count and the above cited metrics do not model accurately the wireless link quality. As a result, the community network is left with several link-layer metrics that fail to choose high-throughput paths between a source and a destination in the presence of selfish nodes which drop packets at the network layer.

In this paper we propose a cross-layer metric that selects the path with the highest packet delivery rate considering both the quality of wireless links and the reliability of network nodes. While many factors contribute to the former, like interference and received signal strength, the latter is mainly influenced by the selfishness of the users that control and manage the network devices. Our contributions are:

- The design of EFW (Expected Forwarding Counter), a new reliability metric that combines information across the routing and MAC layers to cope with the problem of selfish behavior (i.e., packet dropping) of mesh routers in a WMN.
- The integration of the proposed metric with OLSR, a well-known routing protocol for WMNs, and the extension of the MAC layer through the implementation of a forwarding probability estimation technique.
- A thorough evaluation of the metric using the NS2 simulator in several realistic network and attack scenarios.

Numerical results show that the proposed metric improves the network performance with respect to existing approaches more than 200% when several selfish mesh routers are placed inside the network.

The rest of the paper is structured as follows: Section II discusses related work. Section III illustrates the proposed metric as well as the monitoring mechanism used to evaluate the forwarding behavior of neighbor nodes. Section IV provides a numerical evaluation of the proposed framework. Finally, conclusions are presented in Section V.

II. Related Work

Several research works deal with reliable data transmission in wireless multi-hop networks with selfish participants. In particular, two different approaches have been proposed to address this problem, namely *detection techniques* and *incentives*.

The former approach deals with detecting the dropping actions and, if necessary, excluding the guilty nodes from the network. ODSBR [5] leverages on an active probing technique to detect unreliable links controlled by adversary nodes, and defines an innovative route discovery mechanism to avoid network paths containing such links. Castor [6] is an opportunistic routing protocol that uses both flooding and unicast transmission techniques to deliver reliably the message to the destination. Sprout [7] is a routing protocol that probabilistically generates a multiplicity of link-disjoint paths to reach other network nodes and deliver messages using the most reliable route. The secure message transmission (SMT) protocol proposed in [8] exploits multiple node disjoint paths to increase the end-to-end delivery rate using a message dispersion scheme that enables the destination to recover the information contained in data packets by increasing its redundancy. All previous solutions measure the path set reliability using an end-to-end acknowledgment mechanism. However, this active detection technique results in an increased network overhead and thus in a lower available bandwidth for data connections.

On the other hand, incentive-based approaches propose solutions in which the collaboration emerges as the best strategy for rational and selfish players. SPRITE [9] defines a rewarding mechanism which enforces forwarding as the best strategy. The proposed solution is based on a centralized trusted third party that charges or rewards intermediate nodes collecting receipts that prove their forwarding behavior. The authors of [10] design Ad Hoc-VCG, a routing protocol based on the well-known Vickrey, Clarke, and Groves auction, to guarantee that each intermediate node is refunded at least the cost incurred to relay packets, and that it behaves according to the protocol specifications. Commit [11] further develops this approach to enforce the truthful property even when the source node behaves strategically.

Other protocols that define a rewarding mechanism to foster node cooperation are proposed in [12], [13]. In [12] the authors propose a distributed algorithm based on the concept of reciprocity among nodes, where credit is represented by the amount of traffic directly or indirectly forwarded by other network nodes. In [13] the authors propose two forwarding approaches, the Packet Purse Model (PPM) and the Packet Trade Model (PTM), through which the intermediate nodes trade in packets.

III. Cross-Layer Routing Metrics for Wireless Mesh Community Networks

This section presents our proposed metric, the Expected Forwarding Counter (EFW), which combines the link quality measured by the Expected Transmission Counter (ETX) [2] with the forwarding behavior of relaying nodes. We first review the problems that ETX and its derived metrics do not address, which motivate the utilization of our proposal. Then, we show how to combine data-link and network layer measures to strengthen the overall routing reliability. Finally, we describe the mechanisms designed to estimate the dropping probability and thus the forwarding rate of neighbor nodes.

A. Expected Forwarding Counter Metric

Several routing metrics have been proposed in recent years to select the path with the highest delivery rate in wireless multi hop networks. The essence of all these metrics lies in the selection of reliable network paths, avoiding lossy wireless links prone to transmission errors.

Routing metrics for wireless multi hop networks like ETX adopt a probabilistic model to represent the transmission reliability of a wireless link. Specifically, ETX measures the expected number of transmissions, including retransmissions, needed to correctly send a unicast packet over a wireless link. Let (i, j) be a wireless link established between node i and j; p_{ij} and p_{ji} denote the packet loss probability of the wireless link (i, j) in forward and reverse directions, respectively [1]. The probability of a successful transmission on the wireless link (i, j) can therefore be computed as $p_{s,ij} = (1-p_{ij})\cdot(1-p_{ji})$.

Then, the expected number of transmissions necessary to deliver the data packet, considering both its transmission and the successive acknowledgment as required by the IEEE 802.11 protocol, can be evaluated according to expression (1):

$$ETX = \frac{1}{p_{s,ij}} = \frac{1}{(1-p_{ij})\cdot(1-p_{ji})}. \quad (1)$$

Despite the purpose of selecting the most reliable paths, ETX does not model accurately the delivery rate of a network link, since it does not consider the forwarding behavior of the nodes that have established that link. In particular, ETX and its derived metrics do not take into account that a selfish node might discard the packet after its correct reception, if it benefits from not forwarding it.

Note that the best strategy for a rational, selfish node is to drop data packets sent by other nodes at the *network* layer, after the reception of the data frame and the successive transmission of the acknowledgment. If the selfish node does not send the acknowledgement after the reception of the data frame, the sending node will increase the packet loss probability in the reverse direction, $p_{r,ij}$, and thus this selfish action will be considered in the ETX metric by lowering the data-link layer reliability.

To address the problem caused by the dropping behavior of selfish participants, we combine the link quality measured by the ETX routing metric with the forwarding reliability of a relaying node j by improving the probabilistic model on which ETX is based. Let $p_{d,ij}$ be the dropping probability of a network node j ($(1 - p_{d,ij})$ represents its forwarding probability). Since a network node can drop selectively the traffic sent by its neighbors, the dropping probability of any

[1] $(1 - p_{ij})$ and $(1 - p_{ji})$ are called *link qualities* in forward and reverse direction, respectively.

node j is identified both by the sending node i and the relaying node j. The probability that a packet sent through a node j will be successfully forwarded can be computed as $p_{fwd,ij} = p_{s,ij} \cdot (1 - p_{d,ij})$.

Then, the expected number of transmissions necessary to have the packet successfully forwarded (Expected Forwarding Counter, EFW) can be measured according to the following equation:

$$EFW = \frac{1}{p_{fwd,ij}} = \frac{1}{(1-p_{ij}) \cdot (1-p_{ji})} \cdot \frac{1}{(1-p_{d,ij})} \quad (2)$$

The first part of equation (2), which coincides with the *ETX* metric, considers the quality of the physical and MAC layers, whereas our contribution takes into account the *network* layer reliability. Therefore, EFW represents a cross-layer metric that models both the physical conditions of the wireless medium and the selfishness of the node with which the link is established.

The EFW metric requires the representation of the network topology with a directed graph, since the forwarding probabilities of two neighbor nodes i and j may differ (i.e., $p_{fwd,ij} \neq p_{fwd,ji}$).

To address this limitation, we propose two further refinements that penalize a communication link considering the worst and the joint dropping behavior. Specifically, for each link (i, j), the Maximum Expected Forwarding Counter (MEFW) considers the maximum among the dropping probabilities of nodes i and j, whereas the Joint Expected Forwarding Counter (JEFW) takes into account the cumulative effect of the selfish behavior by multiplying the forwarding probabilities of the two end nodes, according to the following equations:

$$MEFW_{ij} = \frac{1}{p_{fwd,ij}} = \frac{1}{p_{fwd,ji}} = MEFW_{ji} = \\ = \frac{1}{(1-p_{ij}) \cdot (1-p_{ji})} \cdot \frac{1}{(1-\max\{p_{d,ij}, p_{d,ji}\})} \quad (3)$$

$$JEFW_{ij} = \frac{1}{p_{fwd,ij}} = \frac{1}{p_{fwd,ji}} = JEFW_{ji} = \\ \frac{1}{(1-p_{ij}) \cdot (1-p_{ji})} \cdot \frac{1}{(1-p_{d,ij}) \cdot (1-p_{d,ji})} \quad (4)$$

B. Forwarding Probability Estimation

The routing metrics we proposed in the previous section require the estimation of the dropping probability, or equivalently the forwarding probability, of relaying nodes. In this section we present the mechanism operating at the MAC layer that evaluates the forwarding behavior of the network nodes in a distributed fashion.

Our approach relies on the broadcast nature of the wireless channel, which enables a network node to overhear the transmissions of any device within its radio range. In order to overhear the packet transmissions of its neighbors, we assume that the wireless interface of each network node is in monitoring mode [14]. Each node maintains for each neighbor the number of successfully received packets, that is, the number of frames for which it has received an acknowledgement from the neighbor, c_{ack}, and the number of forwarded packets with the same source address of the acknowledged packets, c_{fwd}. The ratio between these two values represents the estimated forwarding probability of the neighbor node, $\hat{p}_{fwd} = \frac{c_{fwd}}{c_{ack}}$.

IV. Simulation Results

This section discusses the numerical results obtained testing the proposed routing metrics with the NS2 simulator [2].

A. Experimental Methodology

Nodes Configuration. All nodes employ the IEEE 802.11a MAC protocol and use the same wireless channel. We use as MAC and physical layers the implementation proposed in [15], since it models both layers more accurately than the basic version provided by NS2.

Network Topologies. In our simulations, we consider typical WMCN topologies composed of 49 mesh routers placed over a $1000\ m \times 1000\ m$ area. The maximum channel capacity is 6 Mbit/s, while the transmission range is set to $90\ m$, as suggested in [15]. We compare the proposed metric and the two refinements, namely EFW, MEFW, and JEFW, to the standard ETX metric, considering the two following network topologies:

- *Grid Scenario*: the mesh routers form a square grid topology.
- *Random Scenario*: the nodes are randomly placed over the square area, forming a connected network.

Attack Scenarios. We consider the two following attacks:

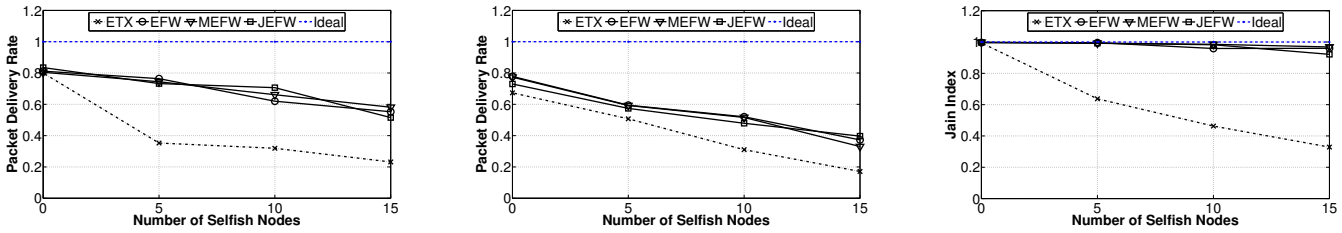
- *No Attack*: there are no adversaries in the network. This scenario represents the ideal case and provides an upper bound on network performance for our scheme.
- *Data Dropping Attack*: in this scenario, the adversary nodes vary their packet drop rate in the 0% to 100% range.

Data Traffic Pattern. In the *Grid* scenario, each node on the first column generates a CBR traffic with a rate equal to 100 kbit/s towards the corresponding destination node at the right end of the same row. The packet size is equal to 1000 bytes. The number of CBR connections is therefore equal to the 7 rows in the grid. On the other hand, in the *Random* scenario, the source and destination nodes of the CBR connections are randomly selected among all network nodes. For a fair comparison of the two scenarios, we set up the same number of CBR connections in both network topologies.

Performance Metrics. We consider as performance metrics the *Average Packet Delivery Rate* (PDR) achieved by the 7 CBR connections and the network fairness measured using the *Jain's Fairness Index*, defined according to equations (5) and (6), respectively. In these equations x_i and y_i represent the PDR and the average throughput of the i^{th} connection, whereas n represents the number of connections established in the network.

$$\text{Average PDR} \triangleq \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \quad (5)$$

[2] Available on-line at http://www.isi.edu/nsnam/ns/



(a) Grid 7×7 (b) Random 49 (c) Grid 7×7

Fig. 1: **Effect of adversary size**. Average PDR and Jain's Fairness Index as a function of the number of adversary nodes.

$$\text{Jain's Fairness Index} \triangleq \frac{(\sum_{i=1}^{n} y_i)^2}{n \cdot \sum_{i=1}^{n} {y_i}^2} \tag{6}$$

For each scenario we performed 10 independent measurements, achieving very narrow 95% confidence intervals that we do not show for the sake of clarity. The simulation time on which we evaluated the performance was equal to 300 seconds.

B. Network Performance Analysis

Effect of adversary size. We first evaluate the effect of the number of adversary nodes on the network performance using the three proposed metrics, in terms of packet delivery rate and fairness of the established CBR connections. We vary the percentage of adversary nodes in the 10 to 30% range. The mesh routers selected as adversaries drop all the traffic sent by other nodes; therefore their forwarding rate is null.

Figure 1(a) shows the average PDR as a function of the number of adversary nodes in the *Grid* topology. It can be observed that the three proposed metrics (i.e., EFW, MEFW, JEFW) increase the resilience against the considered attack, since the delivery rate experienced by all CBR connections is enhanced with respect to the baseline approach (ETX metric). In particular, the PDR using the ETX metric decreases quickly in the presence of adversary nodes. In the *Grid* topology, 15 adversary nodes (30% of the overall number of network nodes) cause an average PDR drop of 70%, considerably greater than the delivery degradation experienced using our proposed metrics, whose PDR reduction is less than 35%. This reflects both the inability of ETX to model the dropping behavior of relaying nodes and the inherently uniform structure of the *Grid* topology, where even a low number of dropping mesh routers placed in sensitive positions can partition the network and cause a severe throughput degradation.

On the other hand, in the *Random* topology, whose results are illustrated in Figure 1(b), the PDR obtained using the ETX metric decreases almost linearly, since in this case the network presents a higher connectivity that, in turn, increases the number of available paths and thus the survivability to the attack. However, the higher proximity of network nodes reduces the spatial reuse and increases the network interference, since all nodes periodically broadcast their topology information. This leads to a lower PDR as well as a lower performance gain in the *Random* topology with respect to the *Grid* network (we measured a maximum performance gain with respect to the ETX approach of 250% in the *Grid* topology and 230% in the *Random* scenario).

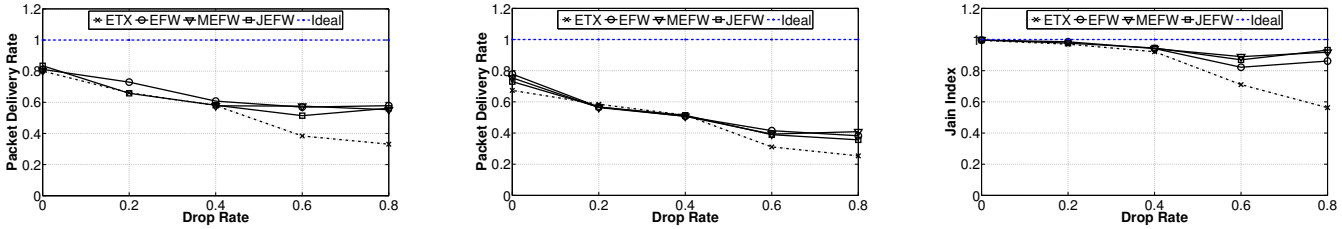
To provide a more in-depth comparison, we also measured the Jain's Fairness Index, which provides an indication of the variance of the delivery rate, and thus the throughput, of the CBR connections. The corresponding results measured in the *Grid* topology are illustrated in Figure 1(c), whereas for the sake of brevity, we do not show this performance metric in the *Random* network.

The results confirm the high vulnerability of the *Grid* topology. As shown in Figure 1(c), the fairness keeps decreasing as long as the number of adversary mesh routers increases (it falls under 40% when there are 15 adversary nodes). We notice that similar results has been obtained in the *Random* scenario. However, due to the lower vulnerability of the *Random* network, the fairness drops to only 60% when there are 15 adversary nodes inside the network.

All previous figures highlight that the proposed metric and its refinements improve the network fairness, reducing the convenience of the dropping attack as a means to greedily consume the available network bandwidth. Specifically, even in the presence of a high number of adversary nodes, the routing algorithm coupled with our metrics is able to restore the network fairness among all data connections.

Effect of drop rate. The second set of simulated scenarios, whose results are depicted in Figure 2, aims to evaluate the effectiveness of the three proposed metrics when the nodes selected to act selfishly drop only some traffic that should be forwarded. In the following simulations, the number of adversary mesh routers is fixed and equal to 30% of the total number of nodes (i.e., 15 nodes are selected randomly as adversaries), while their drop rates vary between 0% and 80%.

It can be observed that in all these simulation scenarios, the three proposed metrics (EFW, MEFW, JEFW) outperform the baseline metric (ETX) only when the drop rate is higher than 40%. This is due to the cross-layer nature of these metrics, which model both the data-link and the network layer reliabilities in the computation of the cost assigned to each network link. In fact, in heavily loaded networks, where the high channel contention causes a degradation of the link reliability, the routing decision is mainly driven by the cost that models the quality of the wireless link. However, as the dropping attack becomes more severe, the PDR obtained using the ETX metric keeps decreasing, whereas our proposed metrics improve significantly the performance. For example, when the adversary nodes are placed in the central area of the *Grid* network and they drop 80% of the data traffic



(a) Grid 7×7 (b) Random 49 (c) Grid 7×7

Fig. 2: **Effect of drop rate**. Average PDR and Jain's Fairness Index as a function of the drop rate (the number of adversary nodes is fixed and equal to 30%).

(see Figure 2(a)), the PDR obtained using ETX decreases by as much as 60%, whereas with the proposed metrics the performance degradation is only 30% with respect to the PDR experienced when there exists no adversary node.

It can be further observed that these results confirm the trends obtained under the attack described above. Specifically, the *Grid* topology is more vulnerable to adversary nodes, as highlighted in Figure 2(a), whereas the higher connectivity of the *Random* topology increases its robustness against the packet dropping attack. As illustrated in Figure 2(b), however, in this latter topology the interference due to the higher proximity among network nodes causes a lower PDR as well as a lower performance gain with respect to the *Grid* topology. For a drop rate equal to 80%, the PDR decreases by 30% in the *Grid* network (60% using ETX), whereas in the *Random* topology the performance degradation is equal to 50% (65% with ETX).

Figure 2(c) shows the network fairness in the *Grid* topology. We observe that the Jain's Fairness Index drops quickly to 60% when the routing protocol uses the ETX metric, whereas with the EFW and its derived metrics the fair allocation of the network resources is guaranteed even for high drop rates, since the Jain's Fairness Index is always above 85%. The results measured in the *Random* scenario confirm the intrinsic resilience of this latter topology to the packet dropping attack. When the adversary nodes discard the 80% of the traffic that they should forward, the CBR connections experience an overall fairness equal to 80% when the network nodes use ETX as metric to select the best network paths, whereas with the proposed metrics the performance is increased to 90%.

In addition to confirm the validity of the proposed approaches, Figure 1 and 2 shows that in heavily loaded networks, installing a relatively high number of adversary nodes that drop less than 40% of the data traffic represents a better strategy for selfish community users than installing a low number of adversary nodes that drop all the data traffic. In the presence of adversary nodes with high dropping rates, the proposed metrics restore the network fairness, distributing the damage among all data connections, and thus reducing the effectiveness of the attack.

V. Conclusion

Routing metrics proposed in recent years for wireless multihop networks fail to select the network paths with the highest delivery rate in the presence of intermediate nodes whose forwarding behavior is driven by selfish interests. To overcome this problem, we propose a cross-layer routing metric, EFW, and two alternative refinements (MEFW, JEFW) to select the most reliable path by considering both the quality of wireless links and the forwarding behavior of network nodes. We evaluate the effectiveness and the scalability of the proposed metrics through simulations in typical network scenarios. Our results show that the proposed solutions increase considerably both the network throughput and fairness with respect to the baseline approach that takes into account only the successful transmission of a wireless link.

References

[1] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D.P. Agrawal. Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky. *IEEE Wireless Communications*, 2007.

[2] D.S.J. De Couto, D. Aguayo, J. Bicket, and R. Morris. A High-Throughput Path Metric for Multi-Hop Wireless Routing. *Wireless Networks*, 11(4):419–434, 2005.

[3] S. Roy, D. Koutsonikolas, S. Das, and Y.C. Hu. High-Throughput Multicast Routing Metrics in Wireless Mesh Networks. *Ad Hoc Networks*, 6(6):878–899, 2008.

[4] F. Oliviero and S.P. Romano. A Reputation-Based Metric for Secure Routing in Wireless Mesh Networks. *IEEE GLOBECOM*, 2008.

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks. *ACM Transaction on Information and System Security*, 10(4):6, 2008.

[6] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer. Castor: Scalable Secure Routing for Ad Hoc Networks. *IEEE INFOCOM*, 2009.

[7] J. Eriksson, M. Faloutsos, S.V. Krishnamurthy, and C. MIT. Routing Amid Colluding Attackers. *IEEE ICNP*, 2007.

[8] P. Papadimitratos and Z.J. Haas. Secure Message Transmission in Mobile Ad Hoc Networks. *Ad Hoc Networks*, 1(1):193–209, 2003.

[9] S. Zhong, J. Chen, and Y.R. Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. *IEEE INFOCOM*, 2003.

[10] L. Anderegg and S. Eidenbenz. Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents. *ACM MobiCom*, 2003.

[11] S. Eidenbenz, G. Resta, and P. Santi. The COMMIT Protocol for Truthful and Cost-Efficient Routing in Ad Hoc Networks with Selfish Nodes. *IEEE Transactions on Mobile Computing*, 7(1):19–33, 2008.

[12] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos. Stimulating Participation in Wireless Community Networks. *IEEE INFOCOM*, 2006.

[13] L. Buttyan and J.P. Hubaux. Enforcing Service Availability in Mobile Ad Hoc WANs. *ACM MobiCom*, 2000.

[14] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *ACM MobiCom*, 2000.

[15] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein. Overhaul of IEEE 802.11 Modeling and Simulation in ns-2. *ACM MSWiM*, 2007.