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 path delivery rate based on enhanced metrics that capture the quality of wireless links. 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 and two further refinements that reduce the network overhead and improve security. Our solutions combine, 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 metrics with a well-known routing protocol for wireless mesh networks, OLSR, and evaluated it using both the NS2 simulator and the real-life ORBIT wireless testbed. The results show that our cross-layer metric and its refinements accurately capture the paths reliability, even when a high percentage of network nodes misbehave, considerably increasing the WMN performance.

***Index Terms*—Wireless Mesh Networks, Selfish Nodes, Data Dropping, Routing Metrics, Experimental Testbed.**

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 the wireless links in order 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 [4]. 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 [5], [6]. These metrics, tailored for reactive routing protocols like AODV [7] and DSR [8], 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 previous metrics do not accurately model the quality of the wireless links. As a result, the community network is left with several link-layer metrics that fail to accurately choose high-throughput paths between a source and a destination in the presence of selfish nodes dropping packets at the network layer.

In this paper we propose a cross-layer metric to select the path with the highest packet delivery rate considering both the quality of the wireless links and the reliability of the 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 routing and MAC layers to cope with the problem of selfish behavior (i.e., packet dropping) of mesh routers in a WMN. Our metric combines direct observation of routing-layer forwarding behavior of neighbors with the MAC-layer quality of the wireless links in order to allow a routing protocol to select the most reliable and high-performance path.
- The proposal of two variants of EFW, in order to reduce the complexity of the network topology representation and secure the transmission of the information representing the forwarding behavior of neighbor nodes. The two

variants penalize a communication link considering either the worst or the joint dropping behavior, respectively.
- The integration of the proposed metrics with OLSR[9], a well-known routing protocol for WMNs, and the extension of the MAC layer through the implementation of a forwarding probability estimation technique that evaluates the network nodes reliability in a distributed fashion.
- A thorough evaluation of the three metrics using the NS2 simulator and the real-life wireless testbed composed of 40 machines provided by ORBIT [10], using a customized version of *olsrd*[1] and *madwifi* driver.

Numerical results show that the proposed metric improves the network performance with respect to the baseline approach more than 200% when several selfish mesh routers are placed inside the network. Moreover, the two refined optimizations perform closely to the proposed metric, thus representing an effective yet feasible solution for reliable routing in WMCNs.

The rest of the paper is structured as follows: Section II discusses related work. Section III presents the network and adversary models considered in our work. Section IV illustrates the proposed metrics as well as the monitoring mechanism that we use to evaluate the forwarding behavior of neighbor nodes. Section V provides a numerical evaluation of the proposed framework, while Section VI illustrates the results obtained testing our solution on the ORBIT testbed. Finally, conclusions and directions for future work are presented in Section VII.

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 in the recent years based on *detection techniques* or *incentives*.

The former approach that comprises works like [6], [11], [12], [13] deals with detecting the dropping actions and, if necessary, excluding the guilty nodes from the network.

ODSBR [6] 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 [11] is an opportunistic routing protocol that uses both flooding and unicast transmission techniques to deliver reliably the message to the destination. Sprout [13] is a routing protocol that probabilistically generates a multiplicity of link-disjoint paths to reach other network nodes and deliver the messages using the most reliable route. The secure message transmission (SMT) protocol proposed in [12] 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 reliability of the set of paths used to deliver the packets to the destination 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 players whose decisions are mainly driven by selfish interests. The routing task is modeled as a game, defining the utility perceived by a network node as a function of the cost incurred in packet relaying and the reward obtained from the devices interested in the node collaboration (whether source or destination nodes).

SPRITE [14] 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 the forwarding nodes on the basis of the collected receipts. The authors of [15] 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 the packets, and that behaves according to the protocol specifications. Commit [16] further develops this approach to enforce the truthful property even when the source node behaves strategically.

Note that in all incentive-based approaches, the cooperation is the rational and best strategy only considering the costs that are modeled by the utility function. However, these approaches do not capture the dropping behavior caused by side effects, like temporarily malfunctions or rate limiting techniques that prevent the starvation of a relaying node.

Other protocols not designed specifically using a game theoretical approach, but that define a rewarding mechanism to foster node cooperation are proposed in [17], [18]. In [17] 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 [18] 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. System Model and Assumptions

This section presents the communication and threat models considered in our architecture, as well as the definitions and assumptions we adopt in the design of our detection technique.

A. Network Model

This work considers a wireless mesh community network composed of two different types of devices: *mesh routers* that form the infrastructure of the WMCN and are maintained by different community users, and *customer devices* that are only interested in the services provided by the WMCN (e.g., Internet access).

We assume that all mesh routers communicate with each other using the wireless medium; in particular they use the IEEE 802.11 MAC protocol to coordinate access to the channel. All mesh routers are equipped with at least one omni-directional antenna for backbone communications.

[1] Available on-line at http://www.olsr.org/

The mesh router owners can connect to the backbone network with their wireless devices, whereas the customers can only access the WMCN services through the mesh routers. Mesh routers can be equipped with an auxiliary wireless interface and operate like access points of a WLAN in order to provide access to generic customers that do not participate to the community.

Community users may be charged different fees to access the WMCN services. As a consequence, these services must satisfy Quality of Service (QoS) requirements, and penalties can be envisaged if QoS requirements are violated.

B. Security and Adversary Models

We assume that there exists a public key infrastructure managed by a trusted Certification Authority (CA). For each new mesh router that a community user wants to add to the WMCN, the CA generates a unique public/private key pair and issues a certificate that binds the identity of the mesh router to its public key. The private key is used to sign the topology information contained in the routing messages that each node disseminates inside the network. Routing messages whose signature cannot be verified are silently discarded by the receiving nodes.

We assume that the mesh routers managed by the users of the WMCN may exhibit a selfish behavior, i.e. they selectively discard the packets that they should forward. Specifically, mesh routers owned by community users perform all the procedures required by network protocols, but some of them behave selfishly towards the traffic of the nodes they serve. All community users have two opposed interests: on the one hand, they compete against the customer devices which they serve for the available network bandwidth provided by the mesh routers, since they share the capacity of their outgoing wireless links established with other mesh routers. On the other hand, mesh routers have an incentive to serve a large number of users in a fair way, since we assume they are rewarded by the community network considering both the number of served customers and the quality of service they perceive. The rewarding policy applied by the community network is out of the scope of this paper, and can be obtained applying, for example, mechanisms like those proposed in [19].

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

This section presents our proposed metric, the Expected Forwarding Counter (EFW), and two alternative refinements that combine 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 and that motivate the utilization of our proposals. 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 necessity to avoid the selection of unreliable network paths due to the presence of lossy wireless links that are prone to transmission errors. However, in the presence of selfish mesh routers that drop the packets sent by other network nodes, these metrics fail to select the network path with the highest delivery rate and thus with the highest end-to-end throughput. Specifically, even the presence of only one selfish mesh router that drops almost all traffic on a path composed of highly reliable wireless links can lead to serious unfairness and throughput degradation.

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. In order to compute the ETX it is necessary to estimate the packet loss probability in both directions, since in wireless networks based on the IEEE 802.11 protocol the destination must acknowledge each received data frame. 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 [2]. 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 the transmission of the data packet and the successive acknowledgment, can be evaluated according to expression (1):

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

Despite the purpose of selecting the most reliable network paths, ETX does not model accurately the delivery rate of a network link since, as explained above, 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 a rational and selfish node 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

[2] $(1 - p_{ij})$ and $(1 - p_{ji})$ are called link qualities in forward and reverse direction, respectively.

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 node j is identified both by the sending node i and the relying 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:

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

In equation (2) the first part, which coincides with the *ETX*, 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.

B. Maximum and Joint Selfishness Metrics

The EFW metric requires the representation of the network topology with a directed graph, since the forwarding probabilities of any two neighbor nodes i and j are different. More specifically, because $p_{fwd,ij} \neq p_{fwd,ji}$, the communication link that these two nodes can establish has to be represented using two different arcs: (i, j) and (j, i), whose weights are equal to EFW_{ij} and EFW_{ji}, respectively. However, this representation increases the memory required to store the network topology and can lead to select two different paths for the packets of closed loop connections, like TCP. Moreover, the internal representation of the network topology used by routing protocols deployed in WMCNs hinders its implementation on a real-life testbed.

To address this limitation, we design the Maximum Expected Forwarding Counter (MEFW) that penalizes a communication link considering the worst dropping behavior, yet allowing a simpler representation of the network topology using only one arc. Specifically, for each link (i, j) that a node i can establish with each neighbor j, we consider the maximum among the dropping probabilities of the two end nodes of the link, according to equation (3):

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

Even though the MEFW metric simplifies considerably the topology representation, capturing the worst link value measured by the EFW, it requires the exchange of the forwarding probabilities related to the nodes that have established the communication link, in addition to the forward and reverse loss probabilities. This information might induce a node whose forwarding behavior has been rated with a low value to misbehave, providing false information about the forwarding rate of its neighbors.

To avoid the transmission of the forwarding probability estimates in the routing messages, we further refine the EFW metric, proposing the Joint Expected Forwarding Counter (JEFW), where both the two forwarding probabilities are multiplied to take into account the cumulative effect of the selfish behaviors, according to equation (4). Indeed, the link quality transmitted in the routing messages can be replaced by the product of the link quality $(1 - p_{f,ij})$ and the forwarding rate of the corresponding neighbor node $(1 - p_{d,ij})$. This improvement increases the security of the proposed metric, since a node cannot distinguish between the two factors (i.e., link quality and its forwarding rate) that contribute to the link cost.

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

Even though these metrics approximate the network topology representation, they do not reduce the chances to select a path with an honest node (i.e., with a high forwarding probability), since they affect differently and independently the weights assigned to the wireless links that a node establishes with its neighbors. In particular, the first metric tries to prevent the selection of a link with a low network reliability caused by the most dishonest node on that link, whereas the second metric penalizes a link considering the joint selfishness.

C. Forwarding Probability Estimation

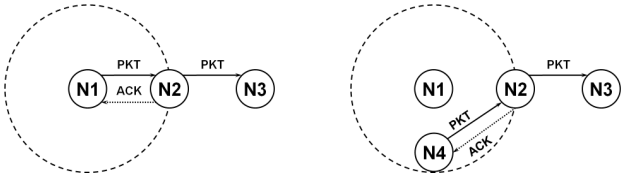
The routing metrics that we proposed in the previous sections require the estimation of the dropping probability, or equivalently the forwarding probability, of the relaying nodes. In this section we present the mechanism operating at the MAC layer that evaluates the forwarding behavior of the network 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 packets transmission of its neighbors, we assume that the wireless interface of each network node is in monitoring mode [20]. Each node maintains for each neighbor the number of successfully received packets, that is, the number of frames to which it has replied with an acknowledgement, 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 forwarding probability of the neighbor node, $p_{fwd} = \frac{c_{fwd}}{c_{ack}}$.

To illustrate how the forwarding probability is evaluated by a mesh router, let us refer to the example network scenario shown in Figure 1, where solid and dotted lines represent the transmission of packets and acknowledgments, respectively. When mesh router $N1$ receives from $N2$ the acknowledgment for a previously sent packet, $N1$ monitors the wireless channel until it hears the transmission of the same packet performed by $N2$ (towards $N3$, see Figure 1(a)). If such transmission does

not occur before a timeout expires, $N1$ will conclude that $N2$ has not forwarded its packet and increment only the counter of the number of acknowledged packets, c_{ack}; otherwise it will increment also the number of forwarded packets, c_{fwd}. The *timeout* parameter is tuned to take into account processing and transmission delays.

To increase the opportunity to detect the forwarding behavior of the mesh routers, the monitoring mechanism considers all the packets sent by the nodes inside the transmission area of the node on which it is installed, in addition to those that the node has directly transmitted to its neighbors (i.e., the packets of which it is the source). As shown in Figure 1(b), $N1$ considers also the packets transmitted by $N4$. If $N1$ does not hear the retransmission of the acknowledged packet sent by $N4$ before the timeout expires, it will conclude that $N2$ has dropped it and it will update only the number of packets acknowledged by $N2$.



(a) (b)

Fig. 1: Example of forwarding probability estimation performed by node $N1$.

Note that the described monitoring technique might underestimate the neighbor forwarding probability, since traditional medium access protocols, such as the IEEE 802.11 CSMA/CA, guarantee the absence of collisions only at the receiver side, while the nodes that are overhearing the transmission, can still be involved in collisions, due to for example the Hidden Terminal problem. Even if these collisions do not affect the correct reception of a packet, they may prevent the correct estimation of the forwarding probability, since the monitoring node may not decode the packet. However, we can assume that such error affects quite uniformly the forwarding probability estimate of all neighbor nodes.

V. Simulation Results

This section presents and discusses the numerical results obtained testing the proposed routing metrics with the NS2 simulator [21].

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 [22], since it models both layers more accurately than the basic version provided by NS2, including the cumulative SINR computation, the preamble and PLCP header processing, and a more realistic frame body capture.

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 [22]. We compare the proposed metric and the two refinements, namely (1) EFW, (2) MEFW, and (3) 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, though assuring the network connectivity.

Attack Scenarios. In our simulations, 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*: the adversary nodes can vary the rate with which they drop the packets they should forward.

In the simulations we vary the percentage of traffic that an adversary node drops (i.e., its drop rate) from 0% to 100%.

Adversary Nodes Placement. To provide a more complete comparison, we also evaluate two different placements of the adversary nodes. Specifically, we consider the following configurations:

- *Anywhere Placement*: all network nodes can be selected as selfish nodes.
- *Central Placement*: only nodes placed in the middle of the network topology can be selected to act selfishly.

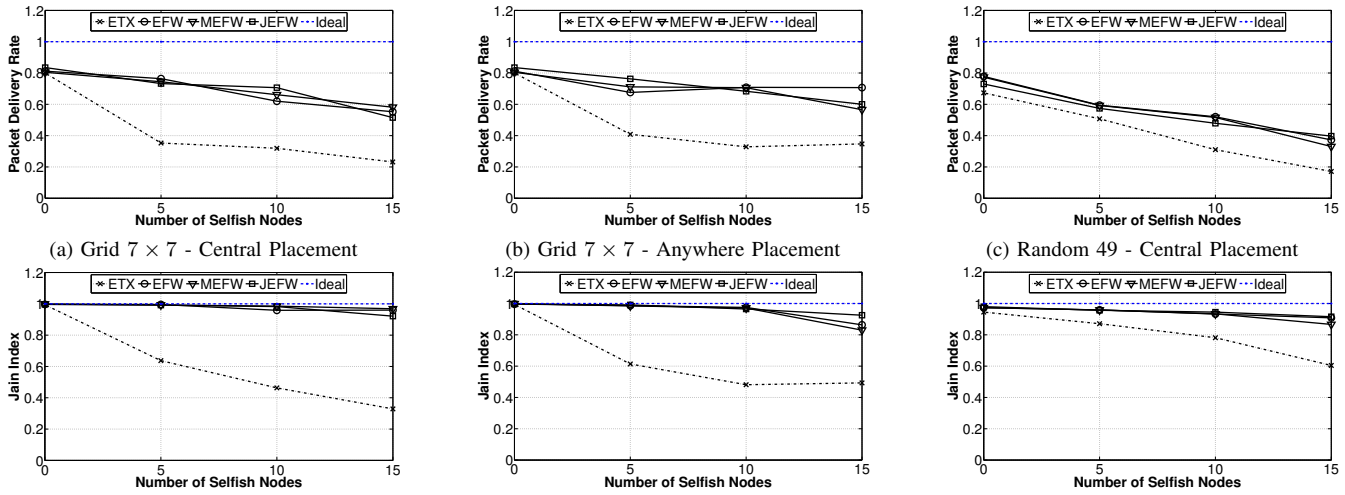
Data Traffic Pattern. In the *Grid* scenario, each node on the first column generates a CBR traffic with a rate equal to 100 kbit/s towards the corresponding destination node at the right end of the same row. The packet size is equal to 1000 bytes. The number of CBR connections is therefore equal to 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 the network topologies. However, due to the random selection of the source and destination nodes of the CBR connections, only the *Central* placement attack is evaluated in the *Random* topology.

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 handled by the network.

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

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

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.



(a) Grid 7 × 7 - Central Placement (b) Grid 7 × 7 - Anywhere Placement (c) Random 49 - Central Placement

(d) Grid 7 × 7 - Central Placement (e) Grid 7 × 7 - Anywhere Placement (f) Random 49 - Central Placement

Fig. 2: **Effect of adversary size**. Average PDR and Jain Fairness Index measured in the *Grid* and *Random* network scenarios as a function of the number of adversary nodes.

B. Network Performance Analysis

Effect of adversary size. We first evaluate the effect of the number of the 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 number of adversary nodes, considering three different percentages, 10%, 20%, and 30%. The mesh routers selected as adversaries drop all the traffic sent by other nodes, therefore their forwarding rate is equal to 0%.

Figures 2(a) and 2(b) show the average PDR as a function of the number of adversary nodes in the *Grid* topology considering the *Central* and *Anywhere* placements, respectively. As expected, the *Central* placement causes a more serious performance degradation than the *Anywhere* placement. However, the performance gap becomes evident only for a high number of adversary nodes, since as the number of these nodes increases, the probability that at least one node on any path connecting a source and a destination is an adversary increases as well. For example, when OLSR uses the ETX metric and 15 nodes are selected as dropping nodes, the PDR decreases by 72% and 60% for the *Central* and *Anywhere* scenarios, respectively.

It can be further 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 the 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 *Central* placement, that represents the worst case scenario, 15 adversary nodes (30% of the overall number of network nodes) cause an average PDR drop of 72%, 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 the relying 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.

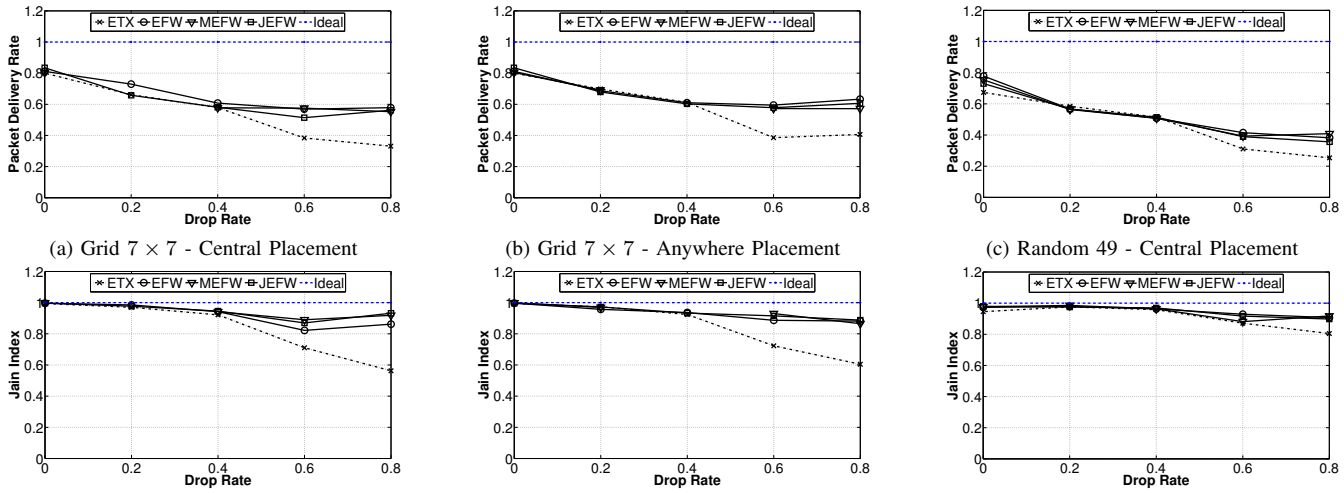
On the other hand, in the *Random* topology, whose results are illustrated in Figure 2(c), the PDR obtained using the ETX metric decreases almost linearly, since in this case the network presents a higher connectivity that, in turn, increases the number of available paths and thus the survivability to the attack. However, the higher proximity of the network nodes reduces the spatial reuse of the channel 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 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 considering the *Central* and *Anywhere* placements are illustrated in Figures 2(d) and 2(e), respectively; whereas Figure 2(f) shows the performance in the *Random* network.

The *Central* placement represents even in this case the most effective strategy for a selfish community user, when the routing protocol uses the ETX metric. As shown in Figure 2(d), the fairness keeps decreasing as long as the number of adversary mesh routers increases (it falls under 40% when there are 15 adversary nodes), whereas in the *Anywhere* placement it remains around 50%.

As discussed above, the lower vulnerability of the *Random* network to the considered attack reduces also the network unfairness. Figure 2(f) shows that 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



(a) Grid 7 × 7 - Central Placement (b) Grid 7 × 7 - Anywhere Placement (c) Random 49 - Central Placement

(d) Grid 7 × 7 - Central Placement (e) Grid 7 × 7 - Anywhere Placement (f) Random 49 - Central Placement

Fig. 3: **Effect of drop rate**. Average PDR and Jain Fairness Index measured in the *Grid* and *Random* network scenarios as a function of the drop rate (the number of adversary nodes is fixed and equal to 30%).

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 illustrated in Figure 3, 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 network 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 experimental 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 a heavily loaded network, 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 (see Figure 3(a)), the PDR obtained using ETX decreases by as much as 61%, 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 a *Central* placement of the adversary nodes, as highlighted in Figures 3(a) and 3(b), whereas the higher connectivity of the *Random* topology increases its robustness against the packet dropping attack. As illustrated in Figure 3(c), 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 27% and 30% in the *Grid* network (51% and 60% using ETX), considering the *Anywhere* and *Central* placement, respectively, whereas in the *Random* topology the performance degradation is equal to 51% (67% with ETX).

Figures 3(d) and 3(e) show the network fairness in the *Grid* topology considering the *Central* and *Anywhere* placements of the adversary nodes, respectively. We observe that the Jain Fairness Index drops quickly to 60% when the routing protocol uses the ETX metric, whereas with the EFW and its derived metrics (i.e., MEFW and JEFW) the fair allocation of the network resources is guaranteed even for high drop rates, since the Jain Fairness Index is always above 85%.

As illustrated in Figure 3(f), in the *Random* topology the network fairness is less affected by the packet dropping attack performed by the adversary nodes. 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%. As explained above, these results reflect the intrinsic resilience of the *Random* topology to the packet dropping attack.

In addition to confirming the validity of the proposed approaches, Figure 2 and 3 shows also an interesting phenomenon: in a heavily loaded network, installing a relatively high number of adversary nodes that drop less than 40% of the data traffic represents a better strategy for a selfish community user than installing a low number of adversary nodes that drop all the data traffic. In the presence of adversary nodes with a high dropping rate, the proposed metrics restore the network fairness, distributing the damage among all network connections, and thus reducing the effectiveness of the attack,

since the decision of the routing algorithm is mainly influenced by the forwarding behavior of intermediate nodes.

VI. Experimental Study

In order to further evaluate the effectiveness of the proposed metrics, we implemented the entire solution and evaluated its performance using the wireless mesh network testbed developed under the ORBIT project [10].

A. Prototype Implementation

Monitoring Mechanism. In order to use the same wireless interface both for monitoring and communication purposes, we implemented the monitoring mechanism as an extension of the *madwifi* driver. To this end, we have modified both the receiving and transmission code of the driver, adding the necessary control structures and functions to estimate the forwarding rate of every neighbor node.

The numerical results obtained testing the solution on the wireless testbed deployed at the department of Computer Science of Purdue University, that we omit for the sake of brevity, show that the driver implementation provides high detection accuracy, even for traffic loads that saturate the network capacity. In such extreme conditions, the error performed by the monitoring mechanism is lower than 8%.

Routing Protocol. The three proposed metrics were developed as a loadable plug-in of *olsrd*, the most widely deployed OLSR implementation in WMCNs. The forwarding rates of the neighbor nodes are disseminated through the network exploiting two unused bytes of the HELLO and Topology Control (TC) messages, so that no network overhead is introduced by our implementation. In our architecture, the monitoring mechanism collects the IP-MAC bindings inspecting the ARP messages that are exchanged by neighbor nodes before the transmission of the first data packet. Finally, an hysteresis scheme is used to prevent the route flapping (i.e., the periodic route changes) and thus stabilize the routing protocol.

B. Performance Evaluation on ORBIT Testbed

The experiments that we perform on the ORBIT testbed aim to evaluate the effectiveness and the scalability of the proposed solution.

Testbed Setup. The ORBIT testbed is an open access indoor radio grid testbed for controlled experimentation consisting of 200 wireless nodes equipped with IEEE 802.11a/g wireless cards laid out in a 20×20 grid with 1 meter spacing between nodes.

Due to wireless card requirements and the high interference generated by the proximity of the wireless nodes, the network scenario employed in our experiments was composed of 40 nodes placed to form a grid topology 5×8, as illustrated in Figure 4.

Since all nodes of the ORBIT testbed are in the same radio range, we forced the grid topology both by using orthogonal channels and filtering rules. Specifically, we split the group composed of 40 devices in 4 subsets, each composed of at most 15 nodes using orthogonal channels (i.e., we split the entire grid into smaller grids of 5×3). The second interface

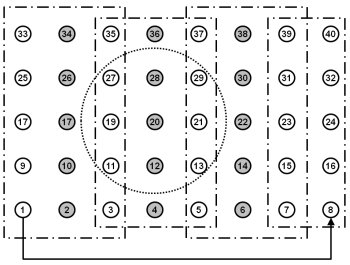


Fig. 4: **ORBIT Topology**. Network topology used for the experiments performed on the ORBIT testbed. The gray circles represent the nodes that can be selected to act selfishly.

of the nodes that belong to the first and last column of each subset was configured to ensure the complete connectivity of the network. We select as selfish nodes only the mesh routers with one active wireless interface in order to evaluate also the monitoring mechanism and thus have a complete picture of the effectiveness of the proposed solution. In Figure 4 the dotted circle represents the set of nodes whose routing messages are not filtered by a sample node (node 20) and that can establish a symmetric communication link with this node. The 4 subgroups of nodes obtained using orthogonal channels are identified by the 4 dashed boxes. The overlapped boxes identify the nodes that connect two adjacent groups using two radio interfaces, thus acting as bridges.

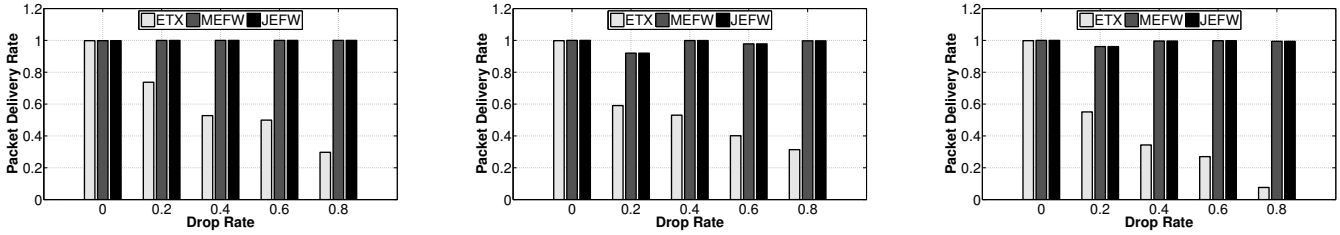
Experimental Methodology Similarly to the grid scenario presented in Section V, we measured the *Average Packet Delivery Rate* (PDR) achieved by 5 CBR connections established between the nodes on the two sides of the grid topology illustrated in Figure 4. The transmission rate and the packet size of each CBR connection were fixed to 50 kbit/s and 1470 bytes, respectively. The CBR traffic was generated using the traffic generator *iperf*.

We consider as attack scenarios the *No Attack* and the *Data Dropping Attack*. However, in the experiments we vary the percentage of traffic that an adversary node drops from 0% and 80%, since *iperf* uses the first and last packets to establish the data connection and transmit the measured statistics (throughput, PDR, etc.) that would be discarded by an adversary node that drop all traffic, causing the impossibility to set up the data connection or estimate its performance.

We evaluate the effectiveness of the proposed metrics against the data dropping attack varying both the number of selfish nodes and their drop rates. Specifically, we select randomly 4, 8, and 12 nodes (equivalent to 10%, 20% and 30% of the overall number of network nodes) placed in the central area of the grid to act selfishly.

For each scenario we performed 10 independent measurements, as in the simulation analysis. The total time on which we evaluated the performance of a CBR connection was equal to 600 seconds.

Results. Figure 5 shows the average PDR measured as a function of the drop rate considering the attack and placement scenarios presented above. The results confirm the effectiveness of the proposed metrics to model the expected number of transmissions necessary to have the packet successfully forwarded.



(a) PDR with 10% Selfish Nodes (b) PDR with 20% Selfish Nodes (c) PDR with 30% Selfish Nodes

Fig. 5: **Impact of dropping attack on ORBIT testbed**. Average PDR measured in the grid scenario illustrated in Figure 4 as a function of the number of selfish nodes and the drop rate.

In a real scenario, the performance degradation caused by a selfish node is more serious than in the simulated scenario, due to the increased stability of the routes obtained using the hysteresis technique. It can be observed that even a small fraction of adversary nodes with a relatively low drop rate can drastically reduce the end-to-end throughput. For example, when OLSR uses the ETX metric and 10% of nodes drop 20% of the traffic that they should forward, the PDR decreases by 24%. This performance is halved when the drop rate increases from 20% to 40%. Furthermore, as the number of adversary nodes increases, the impact on the PDR becomes more evident. As Figure 5(c) illustrates, when 30% of network nodes are selfish, they can seriously affect the network performance and cause unfairness among the data connections. In this case, the PDR quickly decreases to less than 10% of the performance obtained using the proposed metrics. On the other hand, the monitoring mechanism coupled with the proposed routing metrics select the most reliable network paths resulting in no evident performance degradation even considering severe attack scenarios.

VII. Conclusion

The routing metrics proposed in recent years for wireless multi-hop networks fail to select the routing paths with the highest delivery rate when the forwarding behavior of intermediate nodes 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 the wireless links and the forwarding behavior of the nodes that belong to a network path. 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.

Interestingly, simulation results show that in heavily loaded networks, where the high channel contention causes a degradation of the link quality due to the numerous collisions, installing a relatively high number of adversary nodes with a low dropping rate (less than 40%) represents the best strategy to greedily consume the available bandwidth. However, as long as the dropping rate keeps increasing, the proposed metrics permit the selection of the most reliable path, reducing the throughput degradation and restoring the network fairness. We can therefore conclude that the proposed metric and its refinements represent an effective solution for achieving highly resilient routing and thus high delivery rates in WMCNs.

References

[1] P. Antoniadis, B. Le Grand, A. Satsiou, L. Tassiulas, R.L. Aguiar, J.P. Barraca, and S. Sargento. Community Building over Neighborhood Wireless Mesh Networks. *IEEE Technology and Society*, 2008.

[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*, 2005.

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

[4] 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*, 14(4):79–89, 2007.

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

[6] 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 Transactions on Information and System Security (TISSEC)*, 10(4):6, 2008.

[7] M. Ad, E.M. Royer, C.E. Perkins, and S.R. Das. Ad Hoc On-Demand Distance Vector (AODV) Routing. *IETF RFC 3561*, 2000.

[8] D.B. Johnson, D.A. Maltz, J. Broch, et al. DSR: The Dynamic Source Routing Protocol for Multi-hop Wireless Ad Hoc Networks. *Ad Hoc Networking*, 2001.

[9] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR) RFC 3626. *http://www.ietf.org/rfc/rfc3626.txt*, 2003.

[10] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H. Kremo, R. Siracusa, H. Liu, and M. Singh. Overview of the ORBIT Radio Grid Testbed for Evaluation of Next-Generation Wireless Network Protocols. *IEEE WCNC*, 2005.

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

[12] P. Papadimitratos and Z.J. Haas. Secure Message Transmission in Mobile Ad Hoc Networks. *Ad Hoc Networks*, 2003.

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

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

[15] 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.

[16] 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.

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

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

[19] X. Ai, V. Srinivasan, and C.K. Tham. Wi-Sh: A Simple, Robust Credit Based Wi-Fi Community Network. *IEEE INFOCOM*, 2009.

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

[21] S. McCanne, S. Floyd, and K. Fall. Vint project U.C. Berkeley, ns-2 network simulator. *URL: http://www.isi.edu/nsnam/ns/*.

[22] 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.