MobiCom 2010 Poster: A Cross-Layer Reliability Metric for Wireless Mesh Networks with Selfish Participants

Stefano Paris, Antonio Capone[a] **Cristina Nita-Rotaru**[b] **Fabio Martignon**[c]
{*paris, capone*}*@elet.polimi.it* *crisn@cs.purdue.edu* *fabio.martignon@unibg.it*
[a]Dep. of Electronics and Information, Politecnico di Milano, Italy
[b]Dep. of Computer Science, Purdue University, Indiana, USA
[c]Dep. of Information Technology and Mathematical Methods, University of Bergamo, Italy

I. Introduction

Wireless Mesh Networks (WMNs) have emerged as a technology for next generation wireless networking. Many of the applications envisioned to run on WMNs have high-throughput requirements.

Several routing metrics have been proposed in recent years to select the path with the highest delivery rate in wireless multi hop networks in order to improve the throughput experienced by network terminals. The essence of all these metrics lies in the necessity of avoiding 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.

In this paper we propose a new cross-layer 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 and select the path with the highest packet delivery rate considering both the quality of the wireless links and the reliability of the nodes. Our metric combines routing-layer direct observation of forwarding behavior of neighbors, with MAC-layer quality of the wireless links in order to allow a routing protocol to select the most reliable and high-performance path. We integrated the proposed metric with a well-known routing protocol for mesh networks, OLSR [1], and evaluated it using the NS2 simulator using the physical layer extension from [2]. Our preliminary 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.

II. Expected Forwarding Counter

In this section we present the Expected Forwarding Counter (EFW), our cross-layer routing metric which combines the link reliability measured by the Expected Transmission Counter (ETX) [3] with the forwarding behavior of relaying nodes. We first provide an overview of ETX, then we describe our scheme, and finally, we illustrate the distributed mechanism designed to estimate the forwarding probability of the network nodes.

ETX Overview. 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 needed to 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 the 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 the forward and reverse directions, respectively. The probability of a successful transmission on the wireless link (i, j) can be therefore computed as:

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

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 (2):

$$ETX = \frac{1}{p_{s,ij}} = \frac{1}{(1 - p_{ij}) \cdot (1 - p_{ji})} \tag{2}$$

EFW Description. Despite the purpose of selecting the most reliable network paths, ETX does not model accurately the delivery rate of a network link in a network with selfish nodes because it does not consider the forwarding behavior of the nodes that have established that link. In particular, ETX and its variants do not take into account that a selfish node might

discard a packet after its correct reception if it benefits from not forwarding it. Specifically, if a selfish node drops the data packets sent by other nodes at the network layer, after the reception of the data frame and the successive transmission of the acknowledgment, it will not be detected by ETX, since at the data link layer the packet was reported as being successfully transmitted and received.

We propose to combine the link quality measured by the ETX routing metric with the forwarding reliability of a relaying node j at the routing layer. Let $p_{d,ij}$ be the dropping probability of a network node j ($(1-p_{d,ij})$ represents its forwarding probability). The probability that a packet sent through a node j will be successfully forwarded can be computed as:

$$p_{f,ij} = p_{s,ij} \cdot (1 - p_{d,ij}) \tag{3}$$

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:

$$EFW = \frac{1}{p_{f,ij}} = \frac{1}{(1-p_{ij}) \cdot (1-p_{ji})} \cdot \frac{1}{(1-p_{d,ij})} \tag{4}$$

In equation (4) the first part, i.e. the *ETX*, considers the reliability 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.

Forwarding Probability Estimation. The routing metric that we propose requires the estimation of the dropping probability, or equivalently the forwarding probability, of the relaying nodes. The mechanism operating at the MAC layer, which evaluates the forwarding behavior of the network nodes, relies on the broadcast nature of the wireless channel. This property 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 [4]. 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 estimate of the neighbor node, $\hat{p}_f = \frac{c_{fwd}}{c_{ack}}$.

The number of forwarded packets is incremented only if the monitoring node hears the transmission of a packet previously acknowledged. If the neighbor node does not forward the packet before a *timeout* expires, the monitoring node will conclude that the packet has been discarded and increment only the counter of the number of acknowledged packets. 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).

III. Simulation Results

In this section we present and discuss the numerical results by before testing the proposed routing metric and the monitoring mechanism with the NS2 network simulator [5].

Experimental Methodology. In our simulations all nodes use the IEEE 802.11a MAC protocol and the same wireless channel. Specifically, we employ as MAC and physical layers the implementation developed by Daimler-Chrysler Research and University of Karlsruhe [2], since it models accurately the effects occurring in a real wireless network, including the cumulative SINR computation, the preamble and PLCP header processing, and a more realistic frame body capture.

We compare the proposed metric to the standard ETX, considering a typical network scenario composed of 49 mesh routers placed over an area of $1000\ m \times 1000\ m$ to form a grid topology 7×7. The maximum channel capacity is set to 6 Mbit/s, while the transmission range is set to $90\ m$. To this end we use the parameters suggested in [2].

We set 7 CBR connections between the nodes placed on the first and last column of each row of the grid. Each source node 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.

We evaluate the effect of the number of selfish nodes on the network performance in terms of packet delivery rate and fairness of the established CBR connections. More specifically, we vary the number of selfish 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%.

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.

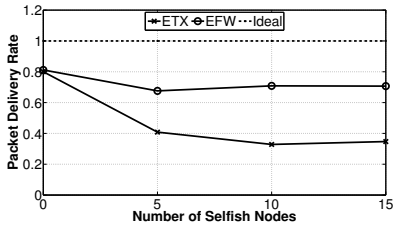
$$\text{Average PDR} \triangleq \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \tag{5}$$

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

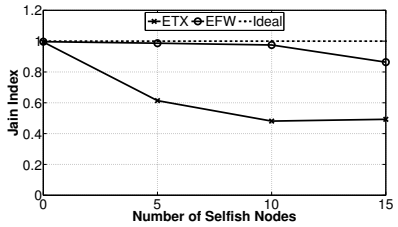
For each scenario we performed 10 independent measurements, achieving very narrow 0.95 confidence intervals, which we do not show for the sake of clarity. The simulation time on which we evaluated the performance was equal to 300 seconds.

Performance Evaluation. Figure 1(a) shows the average PDR as a function of the number of selfish nodes in a grid topology. As expected, the dropping behavior causes a severe performance degradation when the routing protocol exploits the ETX metric to select the best path. In particular, the PDR using the ETX metric decreases quickly with respect to the value experienced when there are no selfish nodes. It can be further observed that the proposed metric (i.e. EFW) increases the resilience against the dropping behavior, since the delivery rate experienced by all the CBR connections is enhanced with respect to the baseline approach (ETX metric). As the number of selfish nodes increases, the performance gap becomes evident, since the probability that at least one dropping node is on any path connecting the source and the destination increases as well. For example, when 15 nodes are selected as dropping nodes (30% of the overall number of network nodes), the PDR decreases by 64%, considerably greater than the delivery degradation experienced using our proposed metrics, whose PDR reduction is less than 35%.

To provide a more in-depth comparison, we also measured the Jain Fairness Index to evaluate the variance of the delivery rate, and thus the throughput, of the CBR connections. As illustrated in Figure 1(b) the dropping attack causes an unfair allocation of the available bandwidth when the OLSR exploits the ETX metric. The fairness measured using the Jain Index keeps decreasing as long as the number of selfish mesh routers increases, falling under 50% when 15 mesh routers are selected as selfish nodes. On the contrary, the proposed metric improves the network fairness, reducing the variance of the delivery rate. More specifically, in the network scenario illustrated in the figure the Jain Fairness Index remains very close to 1, that is, all CBR connections are fairly served by the network.



(a) Average PDR



(b) Jain's Fairness Index

Figure 1: **Effect of adversary size**. Average PDR and Jain Fairness Index measured in a grid network scenario as a function of the number of adversary nodes.

IV. Conclusion and Ongoing Work

We have proposed a new cross-layer routing metric that mitigates the effect of the dropping behavior on the throughput experienced by end to end data connections. Moreover, the proposed solution reduces the convenience of this selfish action as a means to greedily consume the available network bandwidth, since as illustrated in the simulation results, the routing algorithm coupled with our metric is able to restore the network fairness among all the data connections. Our ongoing work consists of further evaluation through simulations in different network topologies and adversarial placement strategies, and experimental results in a wireless mesh testbed.

References

[1] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (RFC 3626). *IETF Internet Draft*, 2003.

[2] 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. *Proc. of MSWiM*, page 168, 2007.

[3] D.S.J.D. 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.

[4] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. *ACM MobiCom*, pages 255–265, 2000.

[5] S. McCanne, S. Floyd, and K. Fall. Vint project u.c. berkeley, ns-2 network simulator. *Available at URL: http://www.isi.edu/nsnam/ns/*.