Jamming-resistant Distributed Path Selection on Wireless Mesh Networks

Yu Seung Kim and Patrick Tague
Carnegie Mellon University
Email: {yuseungk, tague}@cmu.edu

Abstract—**Wireless mesh network is an emerging network architecture which have been actively standardized for the last few years. Because of its flexible network architecture, wireless mesh network can provide alternative paths even when some of wireless links are broken by node failures or intended attacks. Among various types of mesh network, we focus on the most recent mesh standard, IEEE 802.11s and its resiliency to jamming attack. In the demo, we show jamming effects on wireless mesh network and the performance of the hybrid wireless mesh protocol (HWMP) defined in IEEE 802.11s and our proposed distributed path selection protocol.**

I. Introduction

Owing to its flexibility, wireless mesh network is becoming an essential part in the next-generation network (NGN). Even when a wireless node does not have a direct connection to another wireless node, it enables the communication via the intermediate wireless nodes. This mesh topology not only extends the wireless communication coverage but also provides high service availability based on multiple routes without depending on single point of failure. In various types of network architecture, standardization communities have actively constituted wireless standards such as IEEE 802.16j [1], IEEE 802.15.5 [2], and IEEE 802.11s [3].

On the other hand, an adversary can cut off some network flows in the network by jamming, which is an attack emitting intentional noise to interrupt the legitimate communication. Although jamming is traditionally perceived as a physical-layer attack, an attacker can use the cross-layer information to more effectively interfere with the communication over the entire network. Tague *et al.* define this cross-layer attack as *flow-jamming* and optimize the jamming transmission power and the workload allocation [4]. Therefore, this new type of jamming should be considered as a network-layer threat which severely degrades the routing performance in wireless mesh network. Fig. 1 exemplifies the effect of two jammers on the wireless mesh network which consists of 50 wireless nodes in our simulation model.

Unless it is partitioned by jamming, wireless mesh network still can provide redundant paths detouring the jammed region. In this demo, we show the jamming effect on wireless mesh network and the network resiliency by multi-path selection protocols. We focus on the *hybrid wireless mesh protocol* (HWMP) in the IEEE 802.11s standard which is most recently proposed. Furthermore, we propose a distributed path selection protocol and show its superior performance to the existing mechanism under jamming.

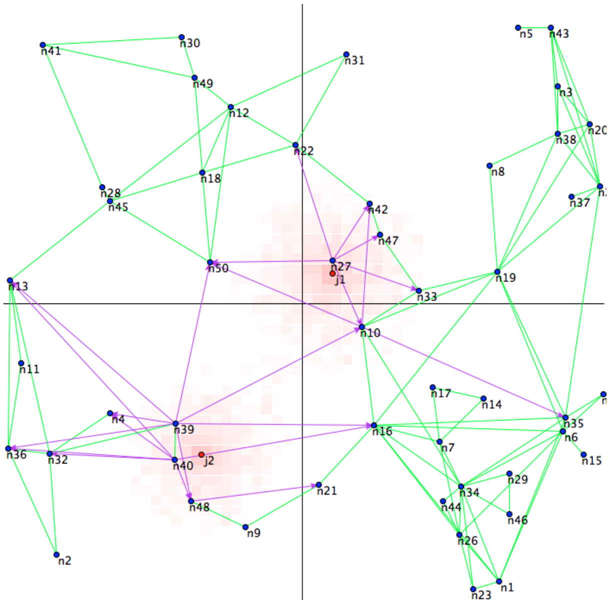

Fig. 1: Jamming effect on wireless mesh network: The two jammers $j1$ and $j2$ are attacking the wireless mesh network. The jammed links are represented with different color.

II. Distributed Path Selection

We summarize the path selection protocols which can be used in wireless mesh network and the problems in existing mechanisms. And we briefly describe our proposed protocol.

A. Existing Approach

We review the two multi-path selection protocols which can be used in the IEEE 802.11s-based wireless mesh network.

- *HWMP* - HWMP is a mesh path selection protocol which is adopted in the IEEE 802.11s mesh network standard. It consists of the on-demand mode, which is similar to Ad Hoc On-Demand Distance Vector (AODV) protocol (IETF RFC 3561 [5]), and the proactive mode, which builds a tree structure by a root mesh station. Both modes are used concurrently. In HWMP, a node selects a path based on the airtime link metric which includes the link speed and the frame error rate (FER).
- *AHV-based path selection* - Mustafa *et al.* propose a multi-path selection based on Availability History Vectors (AHVs) of paths in [6]. To select a best path, each

node collects the link quality information based on the packet delivery ratio (PDR) from each link in the paths. Since selecting path among all the possible paths is computationally prohibitive, the authors divide the selection algorithm into two stages, (1) the path pre-selection stage and (2) the greedy multi-path selection stage.

HWMP itself does not support a multi-path selection mechanism. When the jamming attack is launched in wireless mesh network, HWMP updates forwarding path after a source node detects the link failure by jamming and builds a new path by broadcasting path request message into the network. Moreover, the airtime link metric is based on the link speed affected by link adaptation algorithm and the FER, and they are generally lagging indicators to reflect the attacked link status.

AHV-based path selection also uses the PDR which requires a certain period and enough number of packet transmission attempts to obtain the exact statistics. From the perspective of a source node which intends to select a path, AHV-based path selection is a centralized algorithm since it should collect all the link information from the source node and the target node and calculate the optimal path. Consequently, AHV-based path selection consumes the high communication cost for message delivery and the high computation cost for path optimization. To make matters worse, it might not possible to collect all the link information due to the broken link under jamming.

B. Distributed Path Selection Protocol

Considering the problems arisen in the existing multi-path selection protocols under jamming attack, we develop a distributed path selection protocol which does not depend on the information of entire wireless mesh network, but instead needs only local knowledge. It should be also light weight, so that it does not consume much resources.

We pay our attention to the *non-reciprocal* link status when a link is jammed. Regardless of surrounding environments, we derive that it is possible to decide which node is more affected by jamming attack between two communicating nodes. The decision is accomplished by simply exchanging their transmitting powers and measuring the signal to interference-noise ratio in each node. Ideally, it requires only two frame transmissions to compare the jamming effects on each node. In a real practice, we can add a few more transmissions and average the observed values for high accuracy.

This non-reciprocal link information is integrated with the standard HWMP. Thus, whenever a node forwards a frame, it also considers the jamming effects on the next-hop node and avoids delivering frames towards jamming region.

III. Demo Specification

We detail the demo environment and the evaluation methods to show the result.

A. Demo Set-up

The wireless mesh network simulator is fully coded with a Python script. It requires Python 3.2 [7] or more recent version. The script also uses the Tkinter Python interface to Tcl/Tk which is usually included in Python 3.2. It is a standalone application for which no network connection is required. The screen resolution should be at least 1280x900. It is recommended to have an extra screen which shows the statistics separately.

The simulator can randomly generate a mesh network and store it into a text file. But, for the ease of demo, we will use the pre-configured text files for the mesh network and the jamming model. The simulator includes simple GUI which any audience can easily execute the path selection simulation. The simulator simply animates the frame propagation with the text information. And the results are written into separate files and they are shown with graphs off-line.

B. Evaluation

From this demo, we show the following metrics for comparing results.

- **communication cost** - This is the metric that represents the number of exchanged frames to find an alternative path and make a frame successfully delivered to the destination under jamming.
- **destination reachability** - This means if a path selection protocol can successfully provide an alternative path.
- **path calculation overhead** - This metric shows how fast a path is built in the unit of simulation time.
- **scalability** - This represents how much a path selection protocol is stable in terms of performance while varying the size of network.

IV. Conclusion

We show the jamming effects on wireless mesh network and how the standard HWMP defined in IEEE 802.11s and the proposed distributed path selection protocol achieve the network resiliency against jamming attack in this demo. Our wireless network simulator will help understanding how each path selection mechanism works and how good the performance of the proposed mechanism is. We expect that this tool will also be useful for related studies.

References

[1] *IEEE Std 802.16j-2009, Amendment 1: Multihop Relay Specification*, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society Std.

[2] *IEEE Std 802.15.5-2009, Part 15.5: Mesh Topology Capability in Wireless Personal Area Networks (WPANs)*, IEEE Computer Society Std.

[3] *IEEE Std 802.11s-2011, Amendment 10: Mesh Networking*, IEEE Computer Society Std.

[4] P. Tague, D. Slater, G. Noubir, and R. Poovendran, "Quantifying the impact of efficient cross-layer jamming attacks via network traffic flows," Network Security Lab (NSL), University of Washington, Tech. Rep., 2009. [Online]. Available: http://www.ee.washington.edu/research/nsl/papers/TR005.pdf

[5] C. Perkins, E. Belding-Royer, and S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*, IETF Std., July 2003. [Online]. Available: http://tools.ietf.org/html/rfc3561

[6] H. A. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, "Short paper: Jamming-resilient multipath routing leveraging availability-based correlation," in *Proceedings of the fourth ACM conference on Wireless network security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 41–46. [Online]. Available: http://doi.acm.org/10.1145/1998412.1998421

[7] Python official website. [Online]. Available: http://python.org/