Wireless Mesh Network Simulator for Studying Cross-Layer Jamming Effects

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

***Abstract*—Various wireless mesh network standards have been actively constituted for the last several 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 IEEE 802.11s based on the widely used Wi-Fi networks and its resiliency to jamming attack. In this 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 jamming defense.**

I. Introduction

Wireless mesh network enables a flexible network structure by providing multi-hop connectivity between the communicating ends which are distant away from each other. In addition to this extended wireless coverage, wireless mesh network also provides high service availability through the multiple routes, thus making the network more reliable against the single point of failure. Over the past decade, many mesh standards constituted to support various types of wireless networks show high demand on this flexible network architecture [1] [2] [3].

The path redundancy supported by multiple routes manages to mitigate the small scale link or node failure. However, wireless mesh network can suffer from large scale network failure by intentional attacks such as jamming. Specifically, an adversary can cut off some network flows in the network by 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. Therefore, this type of attack should be considered as a serious network layer threat which significantly degrades the routing performance in wireless mesh network.

Among many mesh protocols, we focus on the *hybrid wireless mesh protocol* (HWMP) in the IEEE 802.11s standard [3] which is based on the popular Wi-Fi networks. After reviewing widely used network simulators such as *ns2* and *Opnet*, we realize that no network simulator can suffice our requirements to study the jamming effects on wireless mesh network. Most network simulators emulate either physical layer or link/network layer, but not both of them sufficiently. Thus, we decide to build an easily configurable network simulator to observe the cross-layer jamming effects on the IEEE 802.11s mesh network.

In this demo, we provide a simulator to study the jamming effect on wireless mesh network and the network resiliency by mesh protocols. Furthermore, we propose a jamming defense mechanism and show its performance under jamming on our simulator.

II. Simulation Assumptions

We describe the path selection protocols used in wireless mesh network and our simulation setup. We then briefly describe our jamming defense mechanism.

A. IEEE 802.11s Mesh Protocol

We assume a wireless mesh network consists of widely deployed Wi-Fi nodes. The network follows the IEEE 802.11s WLAN mesh network standard. The network purely consists of mesh clients without any root node, which is similar to the non-hierarchical ad hoc network configuration.

The IEEE 802.11s mesh network standard adopts a mesh path selection protocol HWMP. It consists of the on-demand mode, which is similar to Ad Hoc On-Demand Distance Vector (AODV) protocol (IETF RFC 3561 [4]), 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).

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.

B. Simulation Setup

Fig. 1 shows the working example of our wireless mesh network simulator. In this example, two jammers are interfering with the mesh network which consists of 50 wireless nodes.

We implement the on-demand path selection of HWMP in IEEE 802.11s. The simulation follows the line-of-sight (LOS) signal propagation model to calculate received signal strength in each node. We set all the antenna gains to 1, and set the path-loss exponent to 2.4. On the center frequency of 2.4 GHz ISM band, the wavelength is set to $\lambda = 0.1249m$. We also set the clear channel assessment threshold to -82 dBm, the noise floor to -95 dBm. In accordance with the standard IEEE 802.11g parameters, each node also changes its rate from BPSK 1/2 to 64-QAM 3/4 depending on the signal to interference noise ratio observed from previous frame transmission.

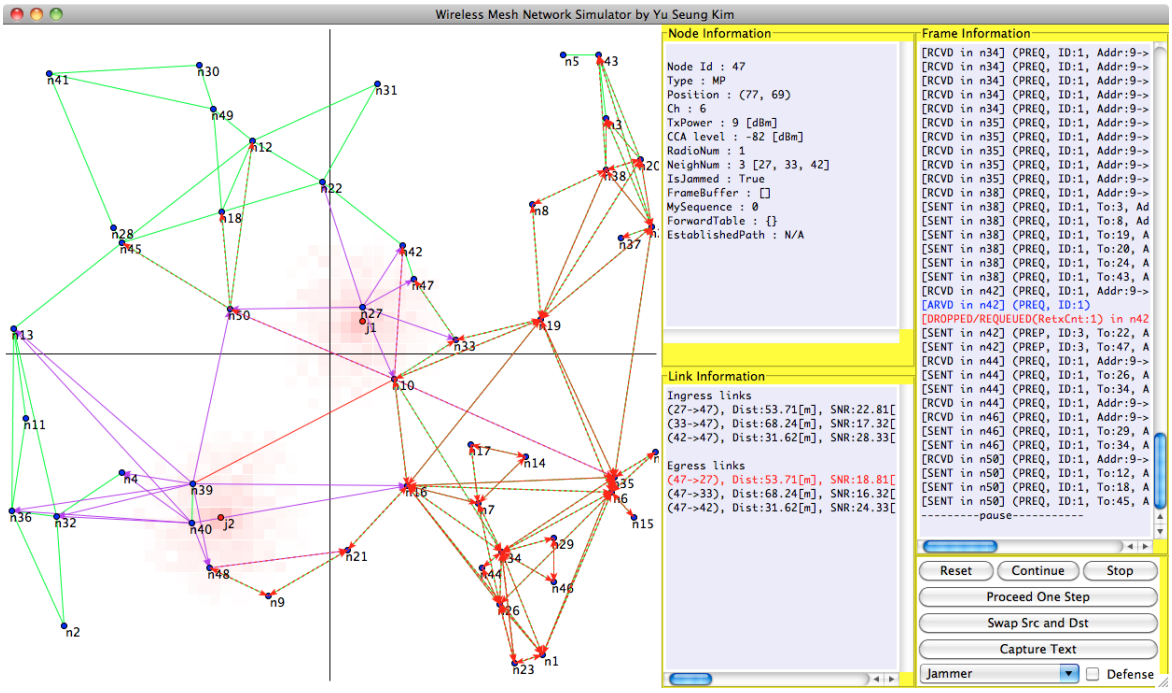

Fig. 1: Jamming effect on wireless mesh network: The two jammers $j1$ and $j2$ are attacking the wireless mesh network. The jammed links are represented with different color.

Each node is allowed to transmit with power ranging from 0 dBm to 20 dBm, and we randomly assign transmission power to each node to simply emulate the irregular signal attenuation by surrounding obstruction. Based on the given configuration, the maximum reachable distance of transmitting frames from each node is calculated as 35 meters at 0 dBm and 244 meters at 20 dBm. A pair of nodes establish a wireless link between them only if both of their frames are reachable to each other.

We assume that jammers transmit within the power range as same as the nodes, in order to not be detected. The jammers also selectively jam the specific mesh frames to save their energy expenditure and to increase their covertness. We denote this type of jammer as *mesh jammer*. To additionally reflect the non-deterministic characteristics of wireless channel such as shadowing, we randomized the amount of jamming signal received at each point of the target area according to the Gaussian distribution.

C. Jamming Defense Using Bi-Directional Path Discovery

From the simulation study, we found that the on-demand path selection can sometimes provide much better path than the original one by only switching the source node and the destination node of a path. This is because the mesh jammers have the directivity for attacking paths. Inspired by this observation, we can think of the bi-directional path discovery, which tries to discover the path both from source to destination and vice versa, and then selects the better path between the found ones depending on the metric of interest.

III. Demo Specification

The wireless mesh network simulator is fully coded with a Python script (Python 3.2 or higher). The script also uses the Tkinter Python interface to Tcl/Tk which is 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. 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 animates the frame propagation with the text information.

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] 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