CIS 751 Lecture Assignment 13

Chuck Zumbaugh

November 20, 2025

1 Threat Model

The attacker controls a compromised host attached to any switch and can send arbitrary packets to the data plane, can drop and delay discovery packets, and can sniff traffic on its own port. The attacker does not control any switches or controllers, is not privileged in the network, and can only see LLDPs visible on its port.

2 Topology Poisoning Attacks

- **Marionette** - Uses reinforcement learning to compute a poisoned topology target and injects flow entries. This manipulates how link-discovery packets are forwarded in the network.
- **LLDP Spoofing** - Attacker forges LLDP packets to trick the controller into believing false information about the network. This can allow the attacker to create false links, add fake switches to the topology map, or create a link such that the controller routes traffic through an attacker controlled host or switch.
- **Link Fabrication/Removal** - The attacker causes the controller to believe two switches are connected when they are not. The attacker creates a fabricated LLDP packet and injects it near a switch that will forward it to the controller.
- **Control-Plane Saturation** - The attacker generates a very large amount of discovery events (ex. LLDP packets) and sends them to

the controller to overwhelm it. This is a denial-of-service attack that attempts to interrupt the controllers ability to process legitimate tasks.