SDN DAG Report

The SDN DAG has the following properties which distinguish it from the SHARKS DAG:

1. It is at a finer granularity than the SHARKS attack DAG. This means that the attacks in this DAG are specific instances of a broad class of attacks.
2. The average height of the DAG is much smaller.

Due to the above reasons, a lot of new branches are not possible. But the above reasons make it simpler to analyze the DAG manually and devise new possible branches.

I have come up with 8 new branches. Some of these attacks require new basic blocks. They are as follows:

1. **Node 21 —> Node 42**: A request from a malicious switch to the controller with the datapacket ID (DPID) of another legitimate switch causes the legitimate switch to be disconnected from the controller. A novel attack might be spoofing the legitimate switch by this method.
2. **Node 32 —> Node 42**: Using switch spoofing to launch a man in the middle (MiTM) attack
3. **Node 27 —> Node 42**: Issuing a crafted flow rule from a malicious app in the controller to reroute the traffic of the target switch through a malicious switch, thus launching a MiTM attack.
4. **Node 27 —> Node 17**: Issue a crafted flow rule to cause a cycle in traffic routing. Example: packet A is forwarded to switch X when it arrives in switch Y and is forwarded to switch Y when it arrives in switch X.
5. **Node 29 —> Node 34**: Issue controller command to empty flow rule table of switch. This causes every incoming flow to send a packetIn message to the controller. A high volume of such packetIn messages can cause a DoS attack on the control plane.
6. **Node 44 —> Node 25**: Spoof switches and send packetIn messages t overload control plane.
7. **Node 10 —> Node 25:** Malicious switches send lots of packetIn messages to overload control plane.
8. **Node 48, 49**: New nodes to launch a MiTM attack.

I do not think any more attacks are possible from this DAG. But I shall keep on expanding the DAG and report more attacks if I come across some.

As a next step, I would like to implement some of these 8 attacks in a SDN simulation environment like Mininet.