Effective Topology Tampering Attacks and Defenses in Software-Defined Networks

RICHARD SKOWYRA, LEI XU, GUOFEI GU, VEER DEDHIA, THOMAS HOBSON, HAMED OHKRAVI, JAMES LANDRY

Software Defined Networks

Allows controller to modify network configuration

Control Plane: define network topology, network policies

Data Plane: decisions that are local to a single switch

Controller installs flow tables in switches defines how packets are forwarded

Topology Tampering

Diverge controller’s view of topology from actual physical topology

Introduce new hosts to network topology

Introduce new links to network topology

Delete hosts/links

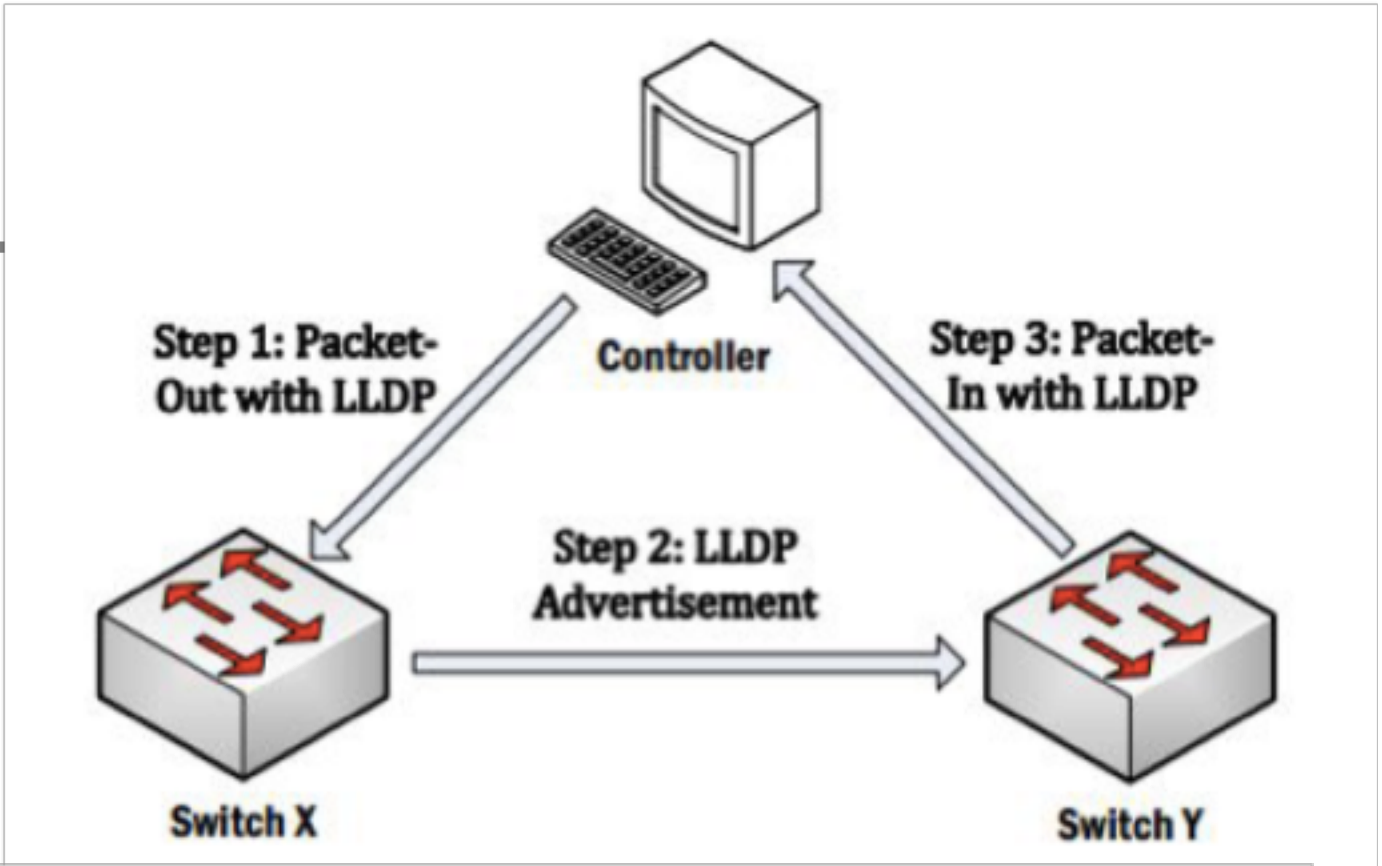
Link Layer Discovery Protocol (LLDP)

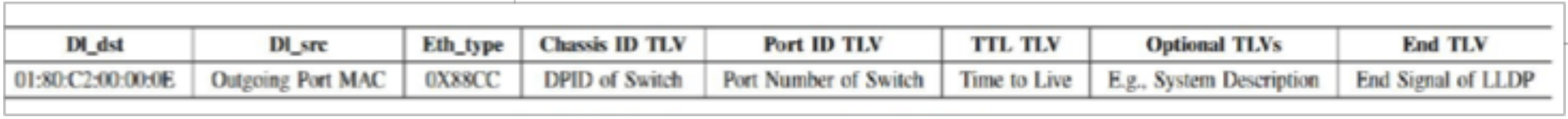
Contains port ID, system name, and system information

Relays information about changing topology, switches added and removed, etc

How the SDN controller gets it’s view of the topology

LLDP


Controller
Step 1: Packet-Out with LLDP
Step 3: Packet-In with LLDP
Step 2: LLDP Advertisement
Switch X
Switch Y



Dl_dst	Dl_src	Eth_type	Chassis ID TLV	Port ID TLV	TTL TLV	Optional TLVs	End TLV
01:80:C2:00:00:0E	Outgoing Port MAC	0X88CC	DPID of Switch	Port Number of Switch	Time to Live	E.g., System Description	End Signal of LLDP

Threat Model

1 or more compromised hosts on network

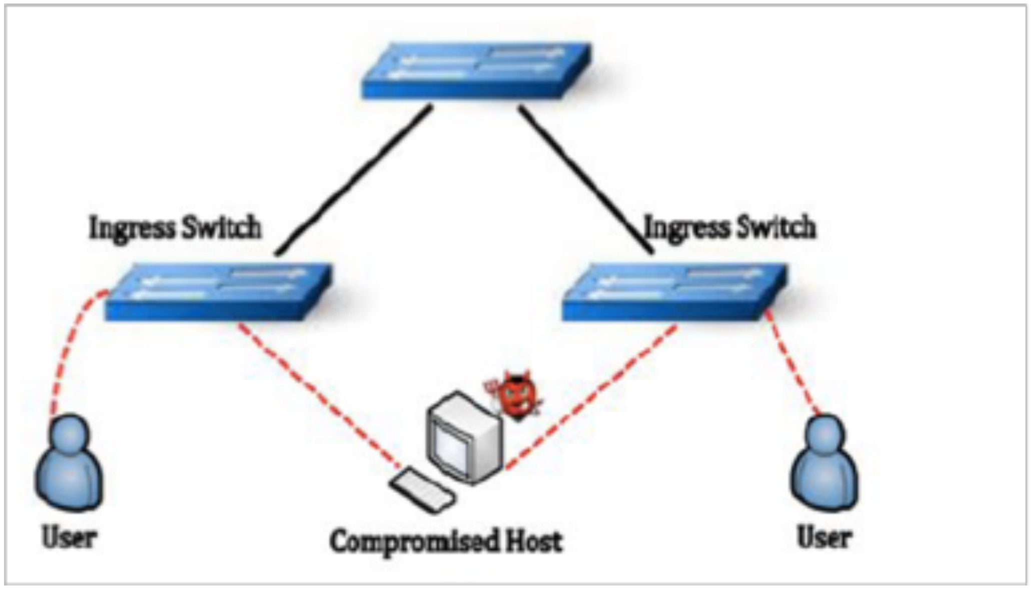
In certain cases, can perform out of band communication with each other

Link Fabrication

Forge or intercept LLDP packet, send to another switch

Attacker attacks as a virtual link

Allows for interception of traffic



Topoguard vs. Link Fabrication

Controller signs LLDP packets

Classify as switch vs host by checking for host generated traffic

Raise alarm when LLDP packet from HOST

Initial Link Fabrication thoughts?

Port Amnesia

Topoguard relies on per port behavioral profiler

Topology of software defined network changes

How can we exploit this?

Port Amnesia

Topoguard relies on per port behavioral profiler

Topology of software defined network changes

Turn it off and on again

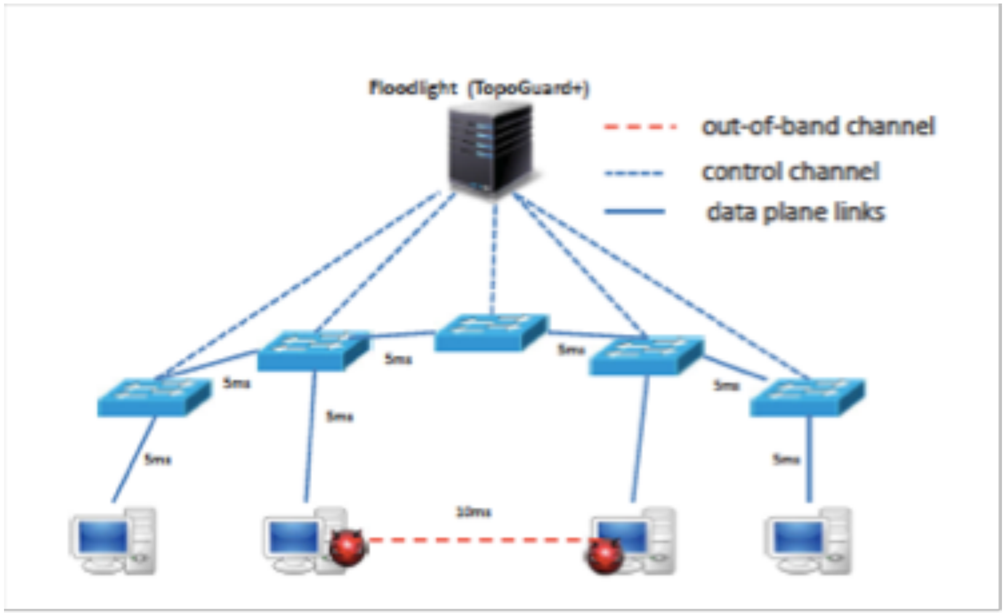
Topoguard+ vs. Port amnesia

Control Message Monitor – During LLDP probe, raise alert if port-up or port-down

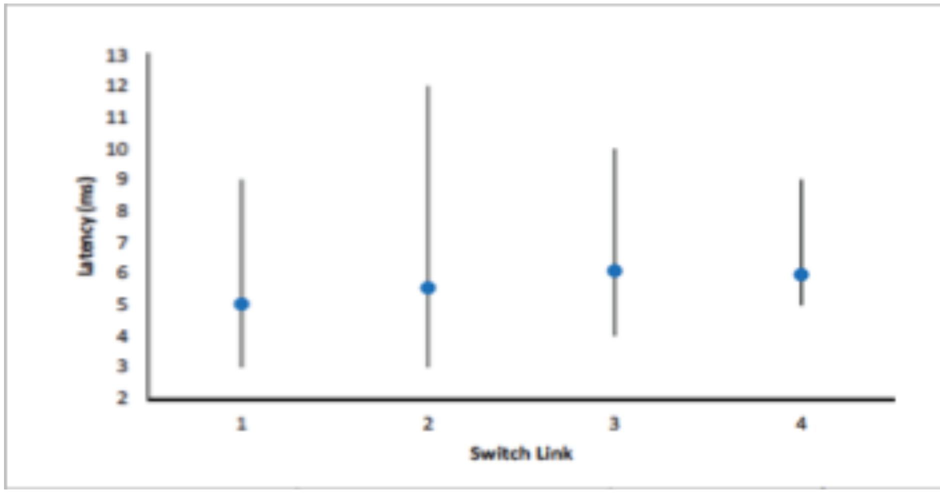
Link Latency Inspector – out of band link fabrication

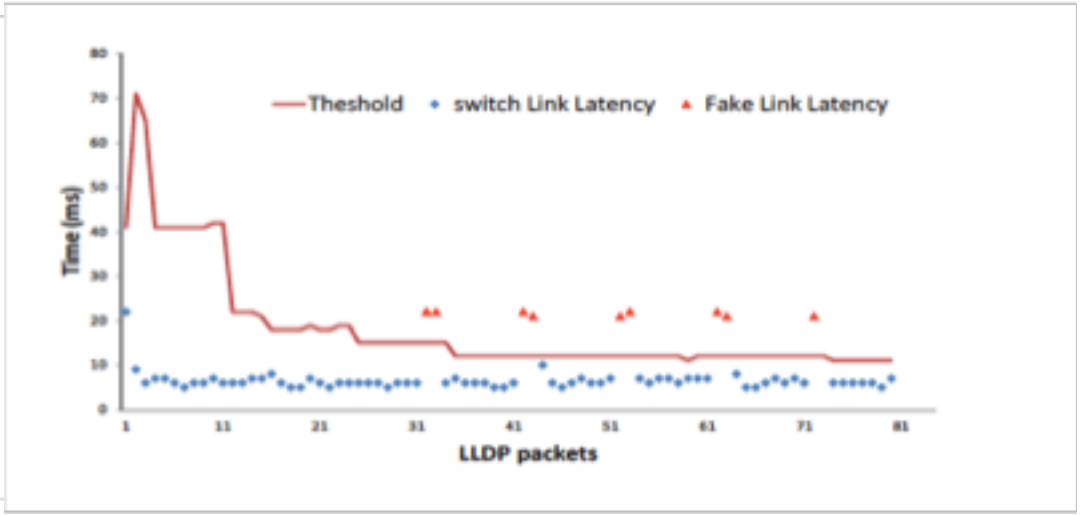
Inspect link latencies, if too high, raise alert

Add encrypted timestamps to LLDP



Link Latency Inspector





Thoughts?

Does Control Message Monitor make sense?

Just defeating their own defenses?

Host Tracking Service

Maintained by SDN controller

Maps IP/MAC to switch port that host is connected to

Host Location Hijacking

Trick HTS into thinking migration from victim location to attacker location has occurred

Spoof victim addressing information

Controller installs flow rules that redirect victim’s traffic to travel to the attacker

Topoguard vs Host Location Hijacking

Host Location Hijacking – migration verification

Check port-down message received from previous location,

Check old location unreachable after migration

Thoughts?

What happens before migration is complete?

Port Probing

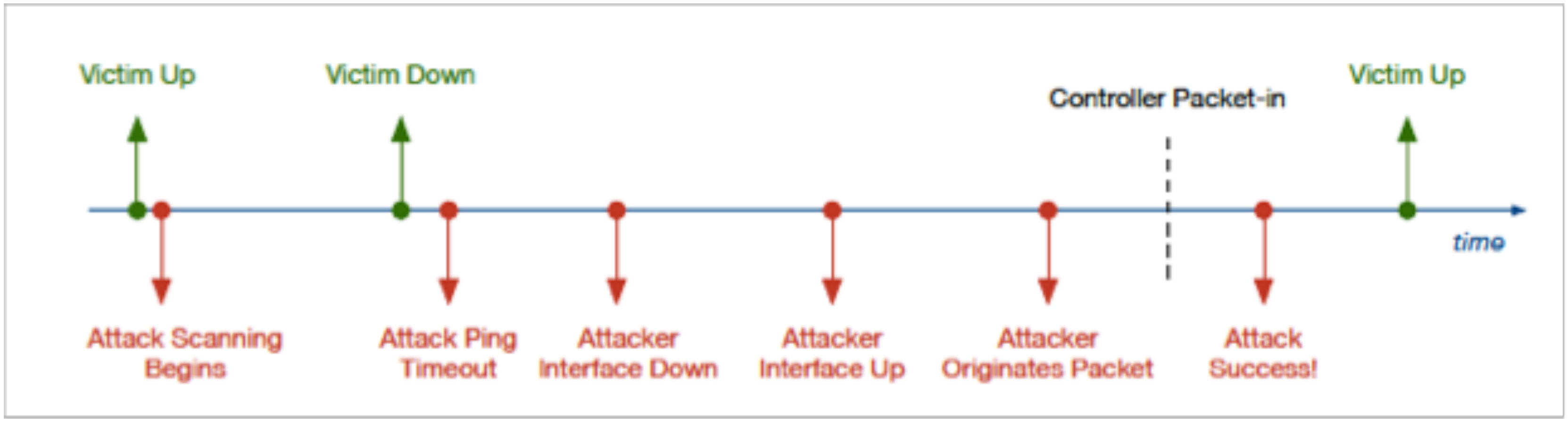
Switches vulnerable between sending port-down and sending LLDP from their new location

Must wait for legitimate movement, or force your own

Goal is to efficiently check when another switch is offline

Port Probing

Observe a vm by pinging it, waiting for migration



Port Probing Mechanisms

ICMP – probably blocked by firewall

TCP SYN scan – can be detected by 0 data flow

Arp ping – slow but stealthy

TCP idle scan – exploits side channel for stealthy scans, lots of preconditions

Port Probing Mechanisms

ICMP – probably blocked by firewall

TCP SYN scan – can be detected by 0 data flow

Arp ping – slow but stealthy

TCP idle scan – exploits side channel for stealthy scans, lots of preconditions

Thoughts on port probing?

Does botched host location hijacking show malicious intent?

Is it reasonable to force vm migration?

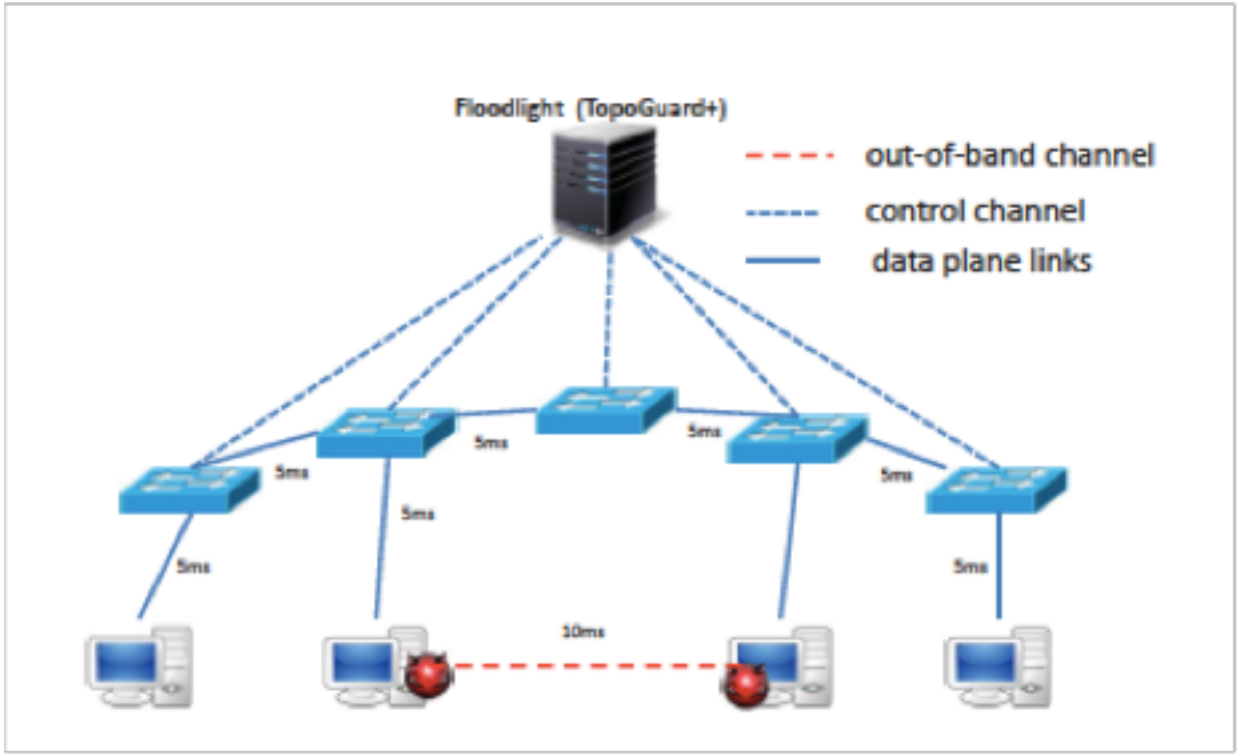
Topoguard+ vs Port Probing

Port Probing – first end host to claim to be target will be treated as such

Bind MAC address to user credentials

Public Key Infrastructure

Evaluation


Floodlight (TopoGuard+)
out-of-band channel
control channel
data plane links
5ms
5ms
5ms
5ms
5ms
5ms
5ms
5ms
10ms

Security Evaluation

Set up testbed in mininet

Every instance of port amnesia was found

Performance Evaluation

Function	Overhead
LLDP Construction	.134ms
LLDP Processing	.299 ms

Thoughts one evaluation?

Takes topoguard one minute to detect, how much damage can you do in that time?

Final Discussion & Questions