CORK INSTITUTE OF TECHNOLOGY

INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

http://www.cit.ie

Detecting Link Fabrication Attacks in Software-Defined Networks

Dylan Smyth

March 15th 2018

Presentation Scope

1. Link Discovery in SDN
2. The Link Fabrication Attack
3. Detecting Link Fabrication in SDNs
4. Implementation and Evaluation on the SoftFIRE Federated Testbed
5. Conclusion

What is the Novelty?

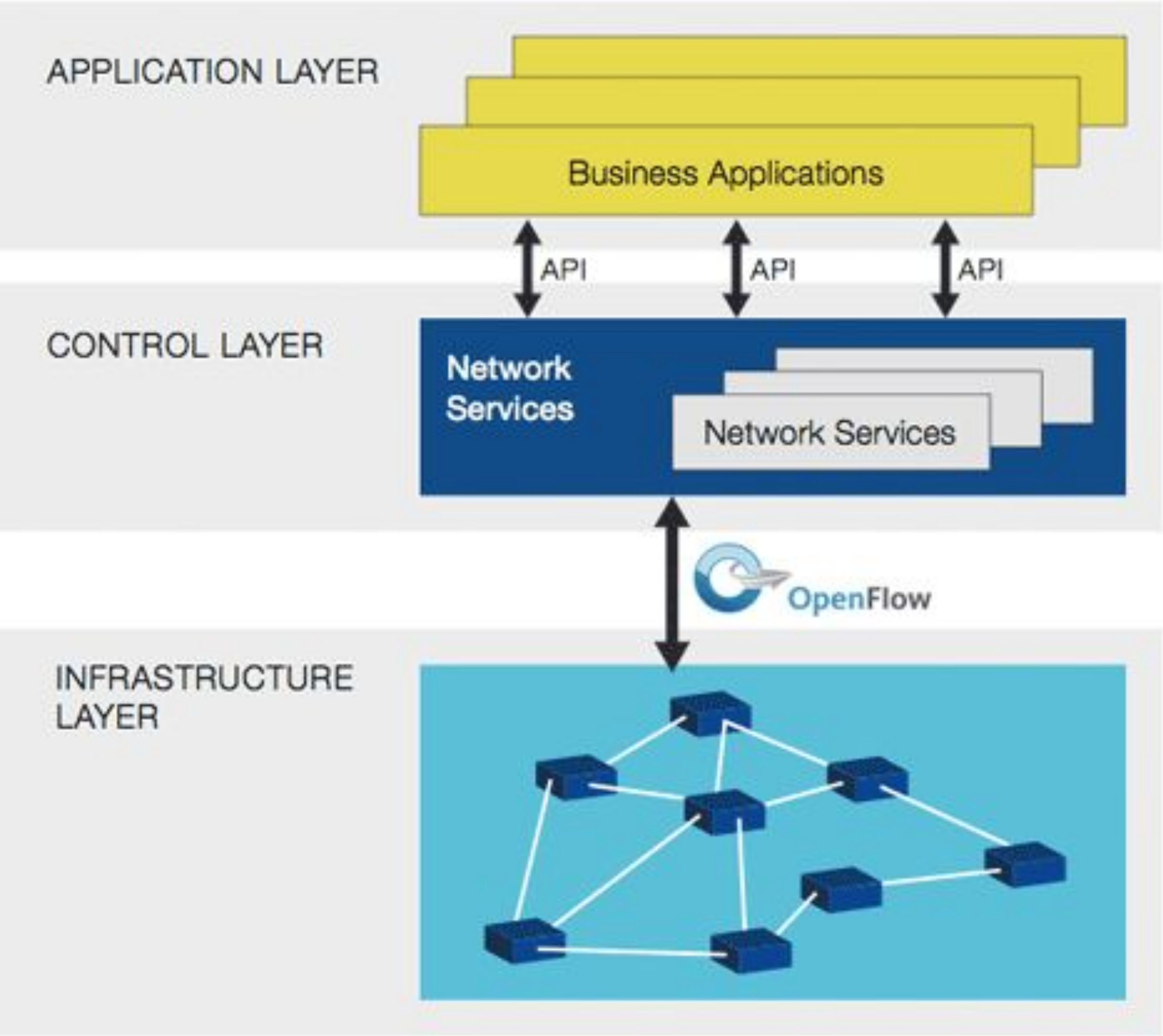
This work will provide two contributions to the current state of the art:

I. An attackers ability to perform the LFA under the conditions of the OpenStack-based architecture will be assessed.

II. The relay-type LFA detection solution proposed in this work which has been verified through simulations will be fully developed and tested on the SoftFire testbed.

Link Discovery in SDN

Software-Defined Networking (SDN)



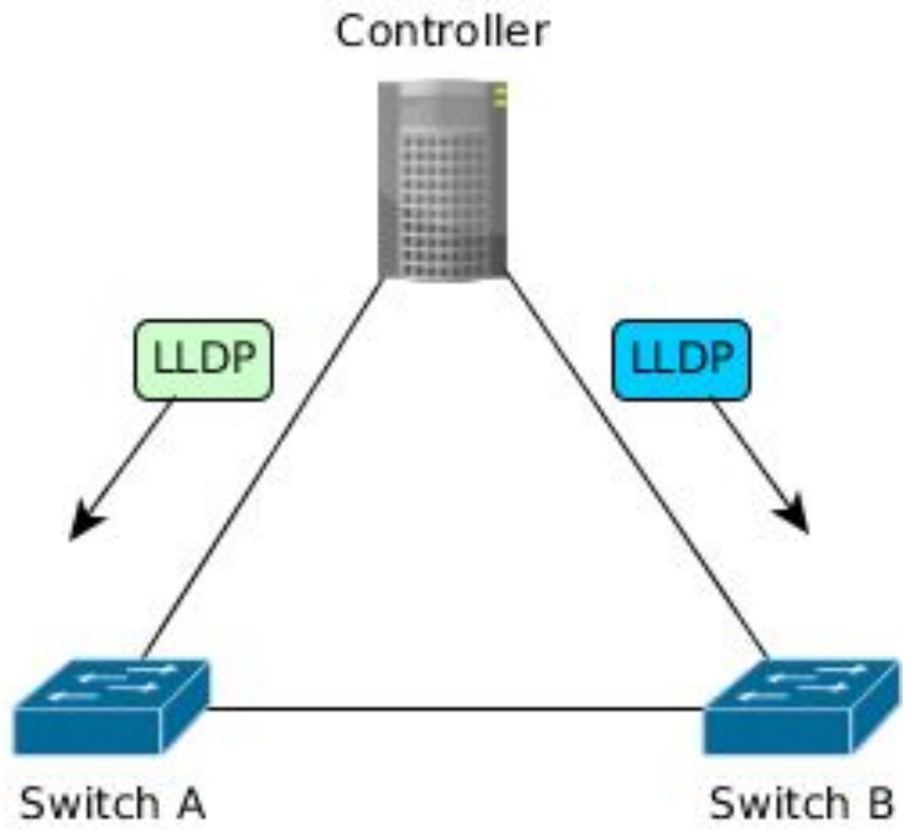
[1] https://www.opennetworking.org/sdn-resources/sdn-definition

Link Discovery in SDN

- Controllers need an idea of the network topology
- Link Layer Discovery Protocol (LLDP)
- LLDP used by
  - OpenDaylight
  - ONOS
  - Floodlight
  - HP VAN
  - ...

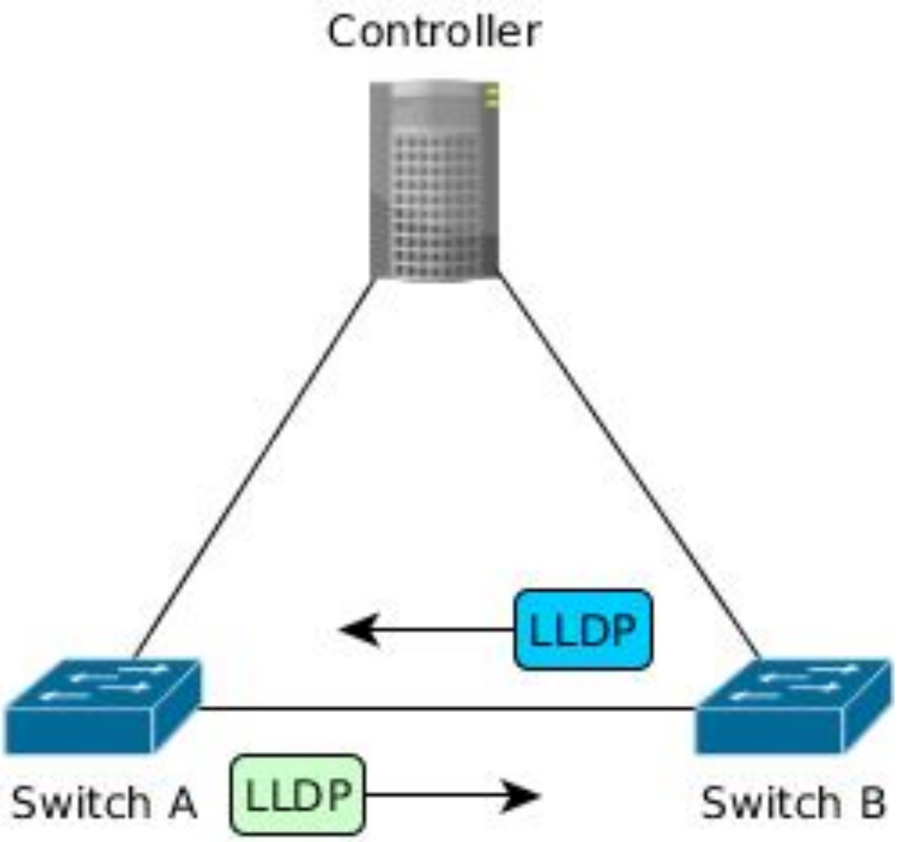
Link Discovery in SDN

- Controller sends an LLDP frame to each network switch as an OF ‘packet-out’ message



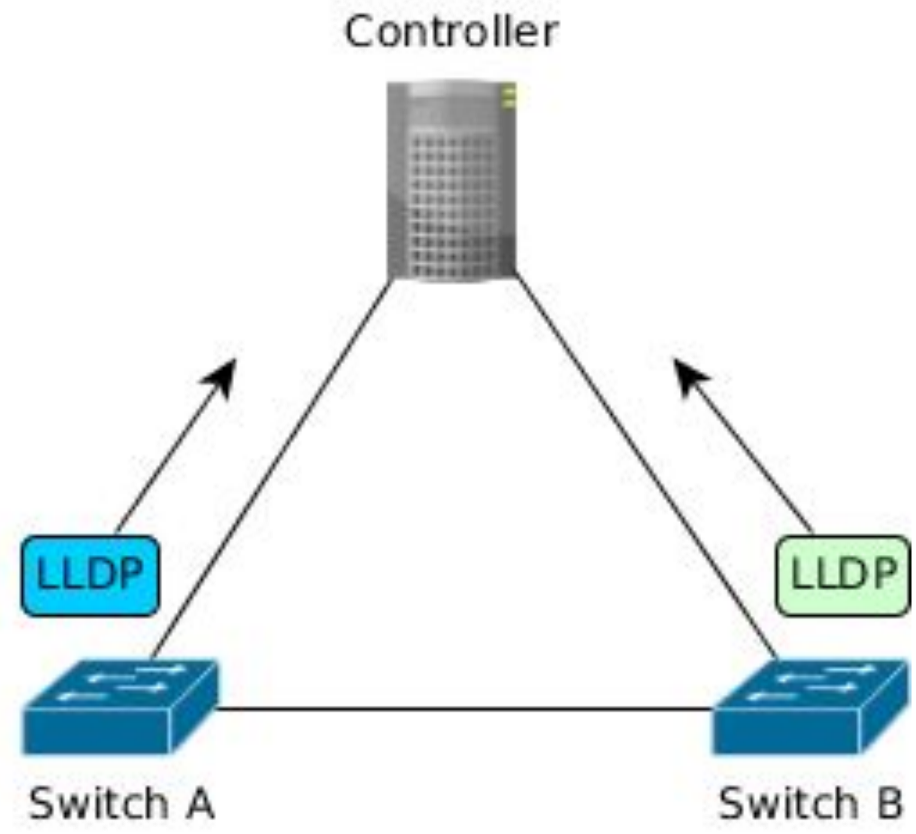
Link Discovery in SDN

- The frame is flooded out all switch ports



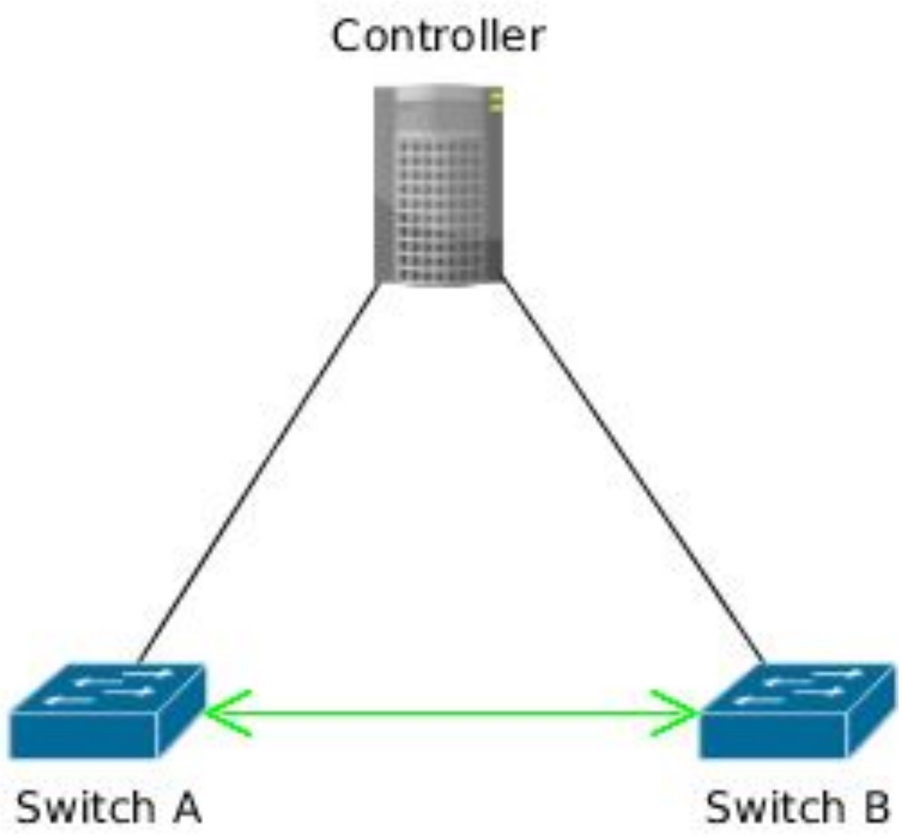
Link Discovery in SDN

- Switches send received LLDP frames to the controller as an OF 'packet-in' message



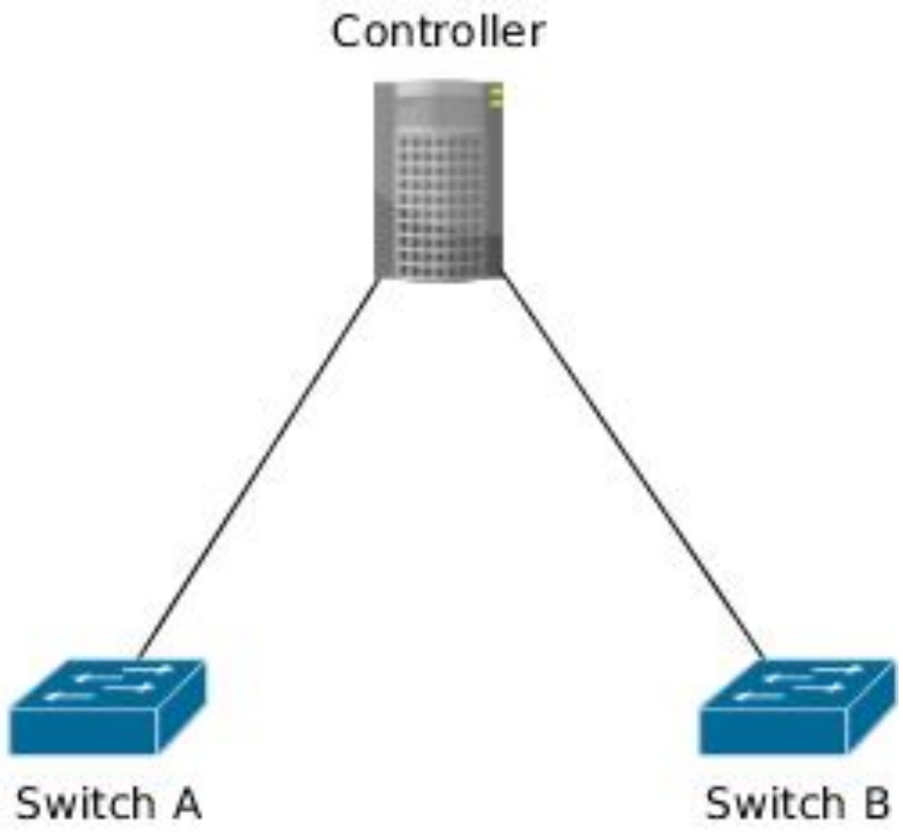
Link Discovery in SDN

- Controller understands links from returned LLDP frames



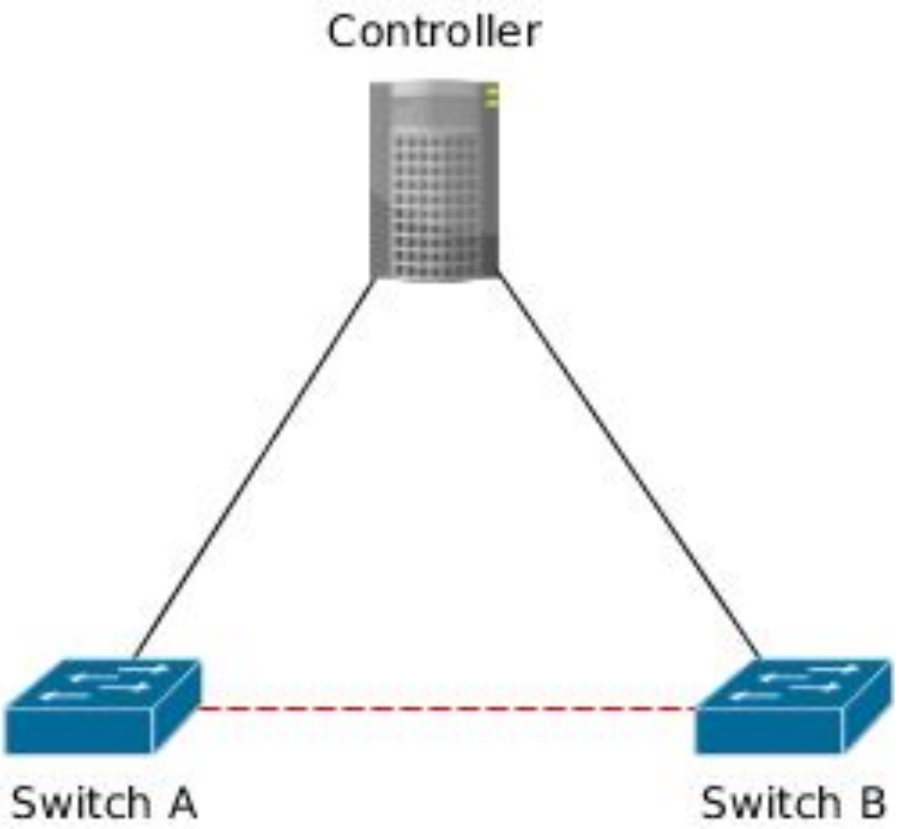
The Link Fabrication Attack

- LLDP frames are trusted to be correct



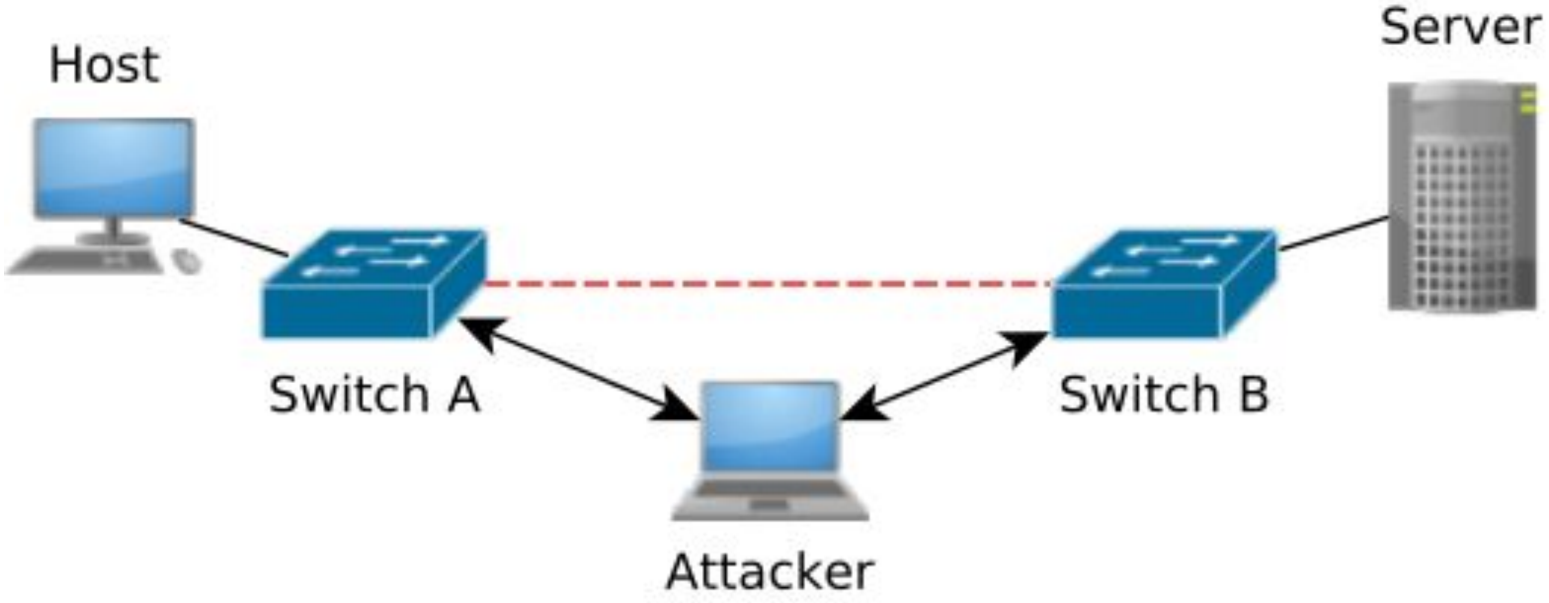
The Link Fabrication Attack

- By taking advantage of this a link can be ‘Fabricated’



The Link Fabrication Attack

- Enables an attacker to perform Man-in-the-Middle attacks



The Link Fabrication Attack

The Link Fabrication Attack

- Generation-type
  - Crafted LLDP frame is sent into the network

The Link Fabrication Attack

- Generation-type
  - Crafted LLDP frame is sent into the network

- Replay-type
  - Legitimate frame is captured and replayed (resent) several times

The Link Fabrication Attack

- Generation-type
  - Crafted LLDP frame is sent into the network
- Replay-type
  - Legitimate frame is captured and replayed (resent) several times
- Relay-type
  - Legitimate frame is captured and immediately forwarded back into the network

The Link Fabrication Attack

- Generation-type
  - Crafted LLDP frame is sent into the network
- Replay-type
  - Legitimate frame is captured and replayed (resent) several times
- Relay-type
  - Legitimate frame is captured and immediately forwarded back into the network

The Link Fabrication Attack

- ~~Generation-type~~ Solved: LLDP frame authentication
  - ~~Crafted LLDP frame is sent into the network~~

- Replay-type
  - Legitimate frame is captured and replayed (resent) several times

- Relay-type
  - Legitimate frame is captured and immediately forwarded back into the network

The Link Fabrication Attack

- ~~Generation-type~~ Solved: LLDP frame authentication
  - ~~Crafted LLDP frame is sent into the network~~
- ~~Replay-type~~ Solved: Unique value for each frame
  - ~~Legitimate frame is captured and replayed (resent) several times~~
- Relay-type
  - Legitimate frame is captured and immediately forwarded back into the network

The Link Fabrication Attack

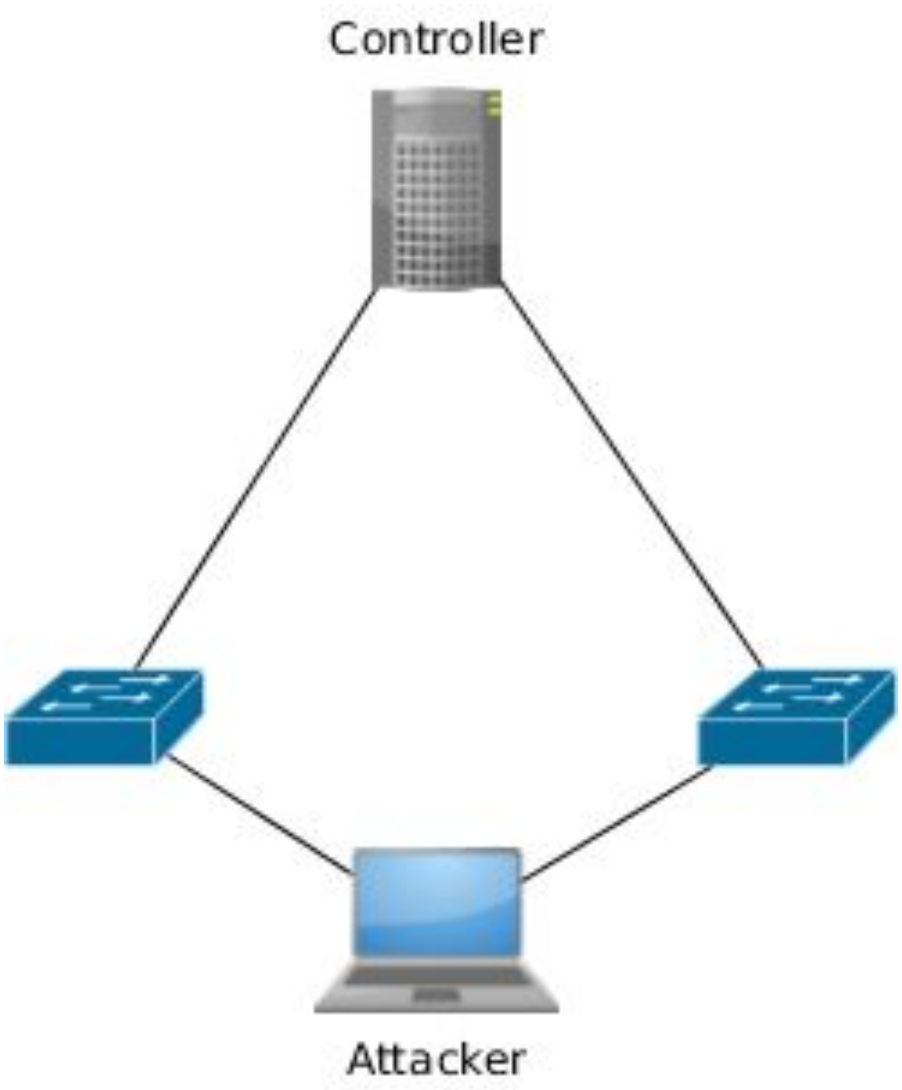
- ~~Generation-type~~ Solved: LLDP frame authentication
  - ~~Crafted LLDP frame is sent into the network~~

- ~~Replay-type~~ Solved: Unique value for each frame
  - ~~Legitimate frame is captured and replayed (resent) several times~~

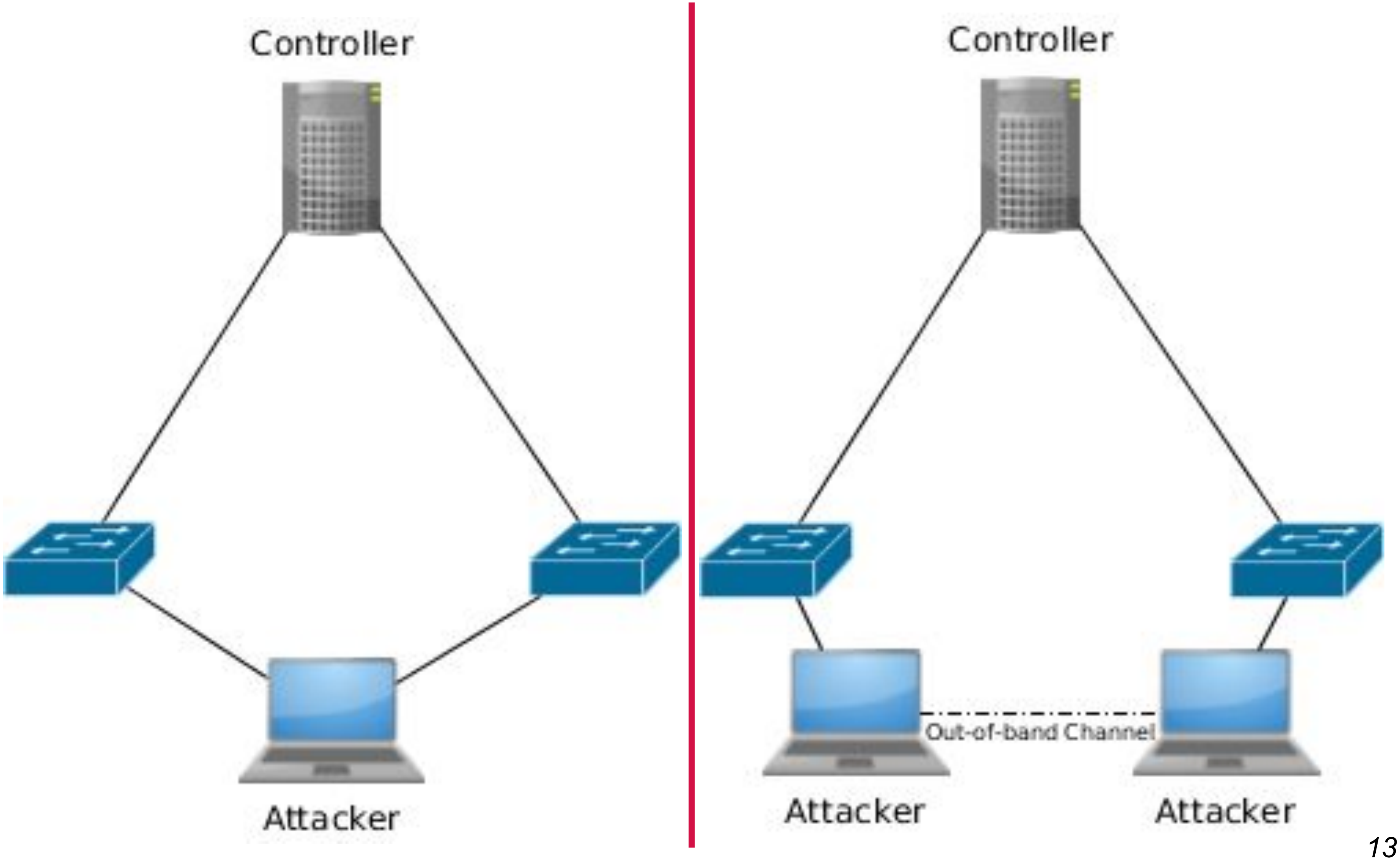
- Relay-type Not Solved
  - Legitimate frame is captured and immediately forwarded back into the network

The Link Fabrication Attack

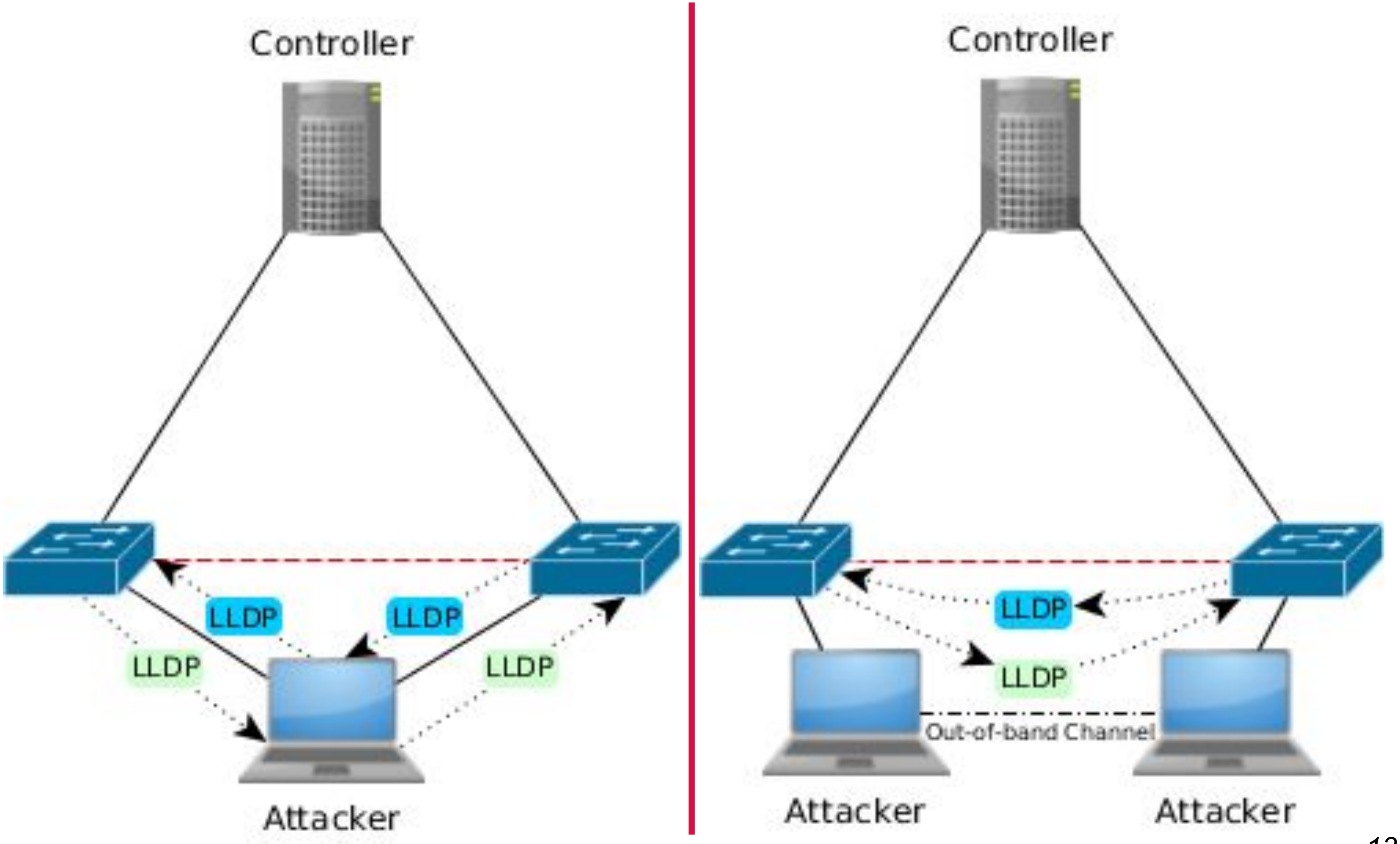
The Link Fabrication Attack



The Link Fabrication Attack

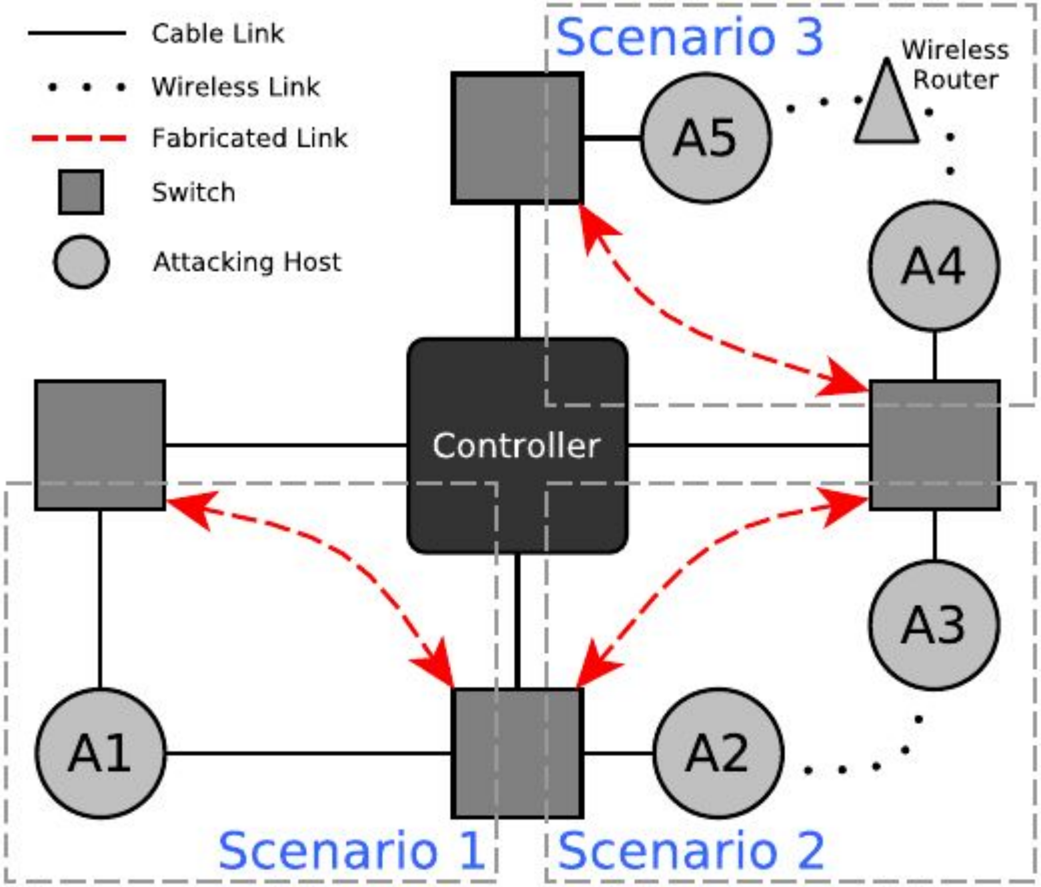


The Link Fabrication Attack



Attack Scenarios

1. Traffic can be forwarded by bridging two interfaces.
2. Out of band wireless channel. Direct ad hoc link. GRE tunnel required.
3. Out of band wireless channel. Wireless access points or routers. GRE tunnel required.



Detecting Link Fabrication in SDNs

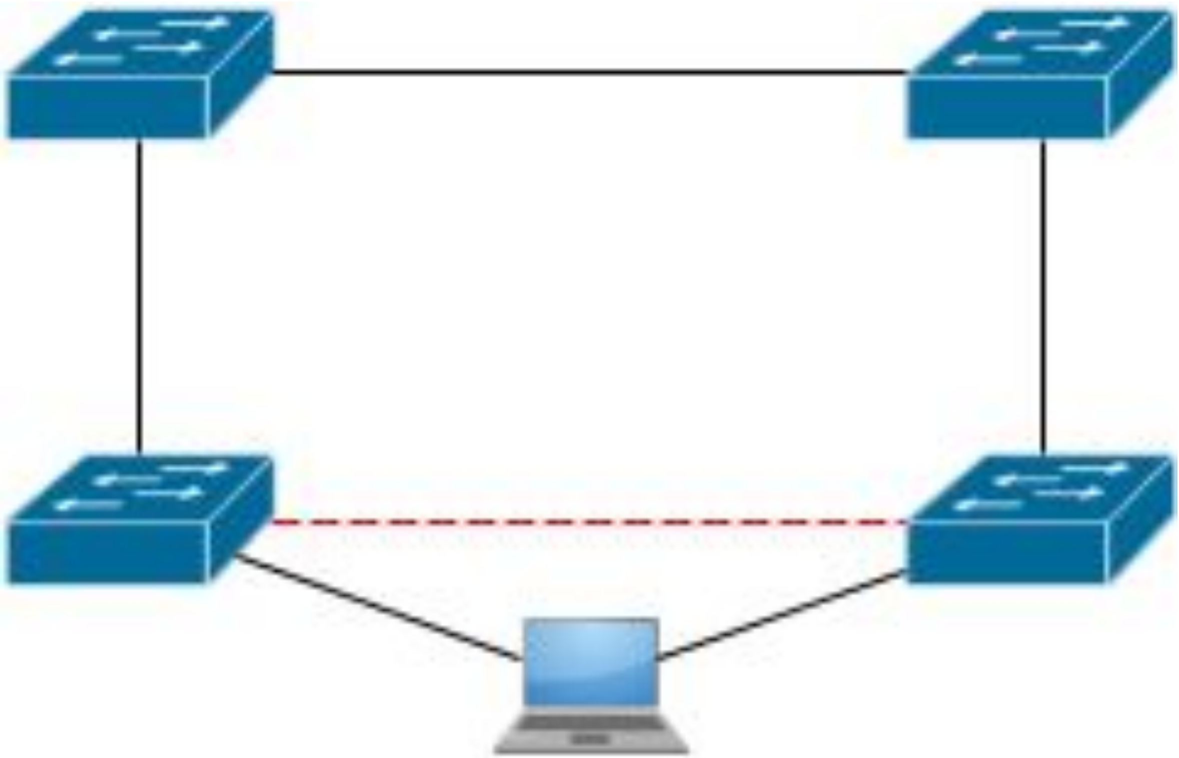
Detecting The Attack

- Detect fabricated link using link latency
- Shown to be possible by previous work [2]
- Our work explores this further

[2] X. Wang, N. Gao, L. Zhang, Z. Liu, and L. Wang, “Novel mitm attacks on security protocols in sdn: A feasibility study,” in Information and Communications Security, Springer, 2016.

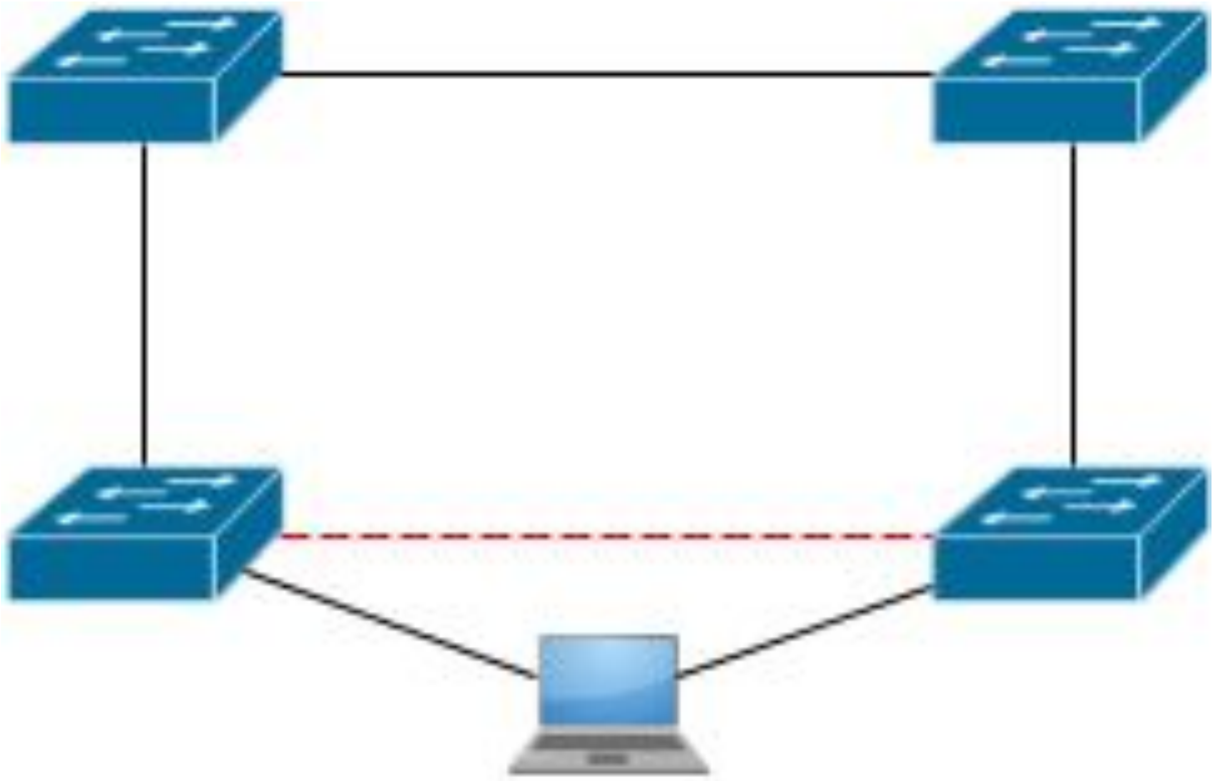
Detecting The Attack

- Fabricated link is not physically the same as normal links



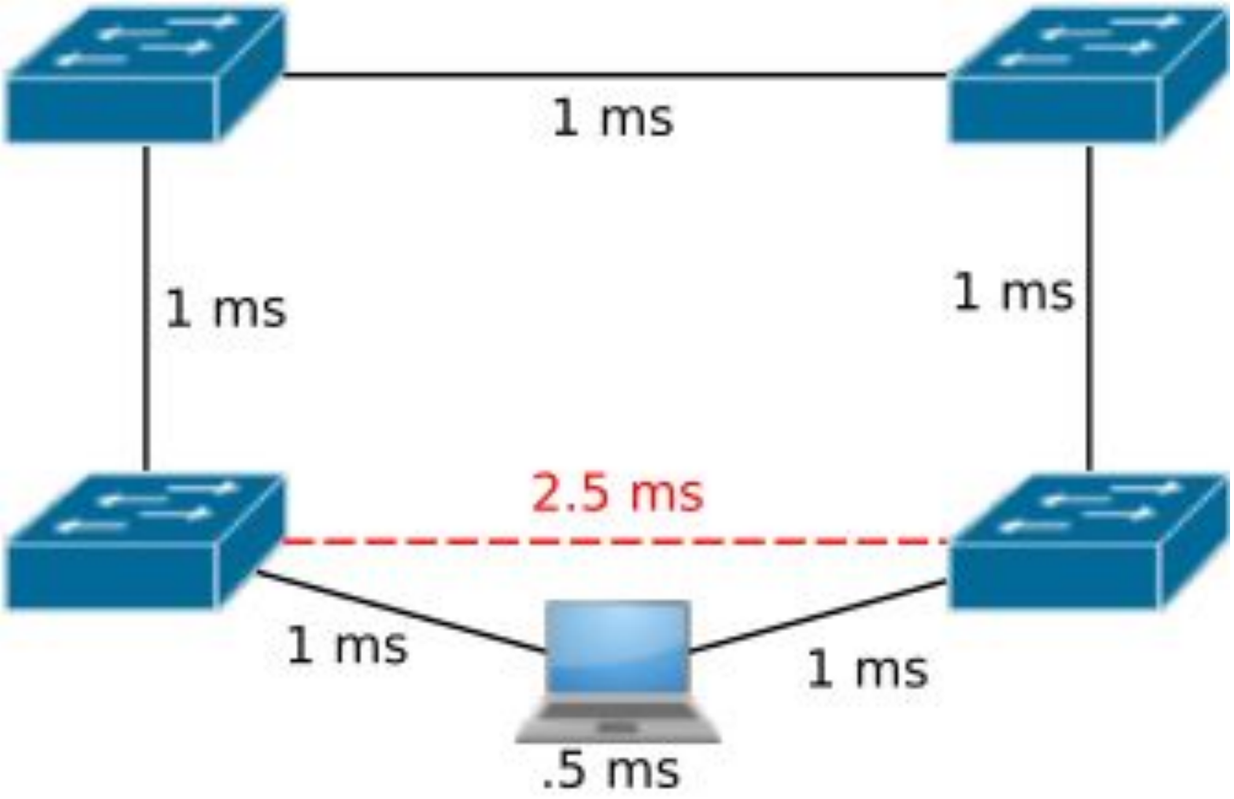
Detecting The Attack

- More links and more hops



Detecting The Attack

- Theoretically, the latency *should* be different



Detecting The Attack

- LLDP mechanism is used to collect link latency
- Monitor link latency at the controller
- Compare latency of new links with a baseline latency for benign links

Detecting The Attack

- LLDP mechanism is used to collect link latency
- Monitor link latency at the controller
- Compare latency of new links with a baseline latency for benign links
- Problem with this...

Detecting The Attack

- Latency can vary depending on network traffic

Detecting The Attack

- Latency can vary depending on network traffic

- Solution:
  - Maintain a static baseline latency
  - Isolate new links and collect a ‘clean’ latency (vetting period)
  - Use statistical tests to check if the new link fits the profile of a benign link
  - If the link is ok allow the controller to use it as a path, Otherwise reject it.

Implementation Solution

- Implemented Statistical Hypothesis Testing

- Steps…
  1. Calculate mean latency for new link (*x*)
  2. Calculate mean baseline latency (*y*)
  3. Calculate *z*-score; Number of standard deviations *x* is from *y*
  4. Calculate *p*-value using a *z*-score table

- *p*-value indicates probability a new link is a normal link

- If *p*-value < a threshold (e.g. 5%) the link is a fabricated link

Implementation and Evaluation on the SoftFire Testbed

Evaluation

- Determine if proposed detection method is appropriate in the SoftFIRE federated testbed infrastructure

- Test the accuracy of detection:
  - Gather latency for all links in the network to determine how latency settles after initial network deployment.
  - Fabricate multiple malicious links using user space and kernel forwarding and determine whether the fabricated link is detected

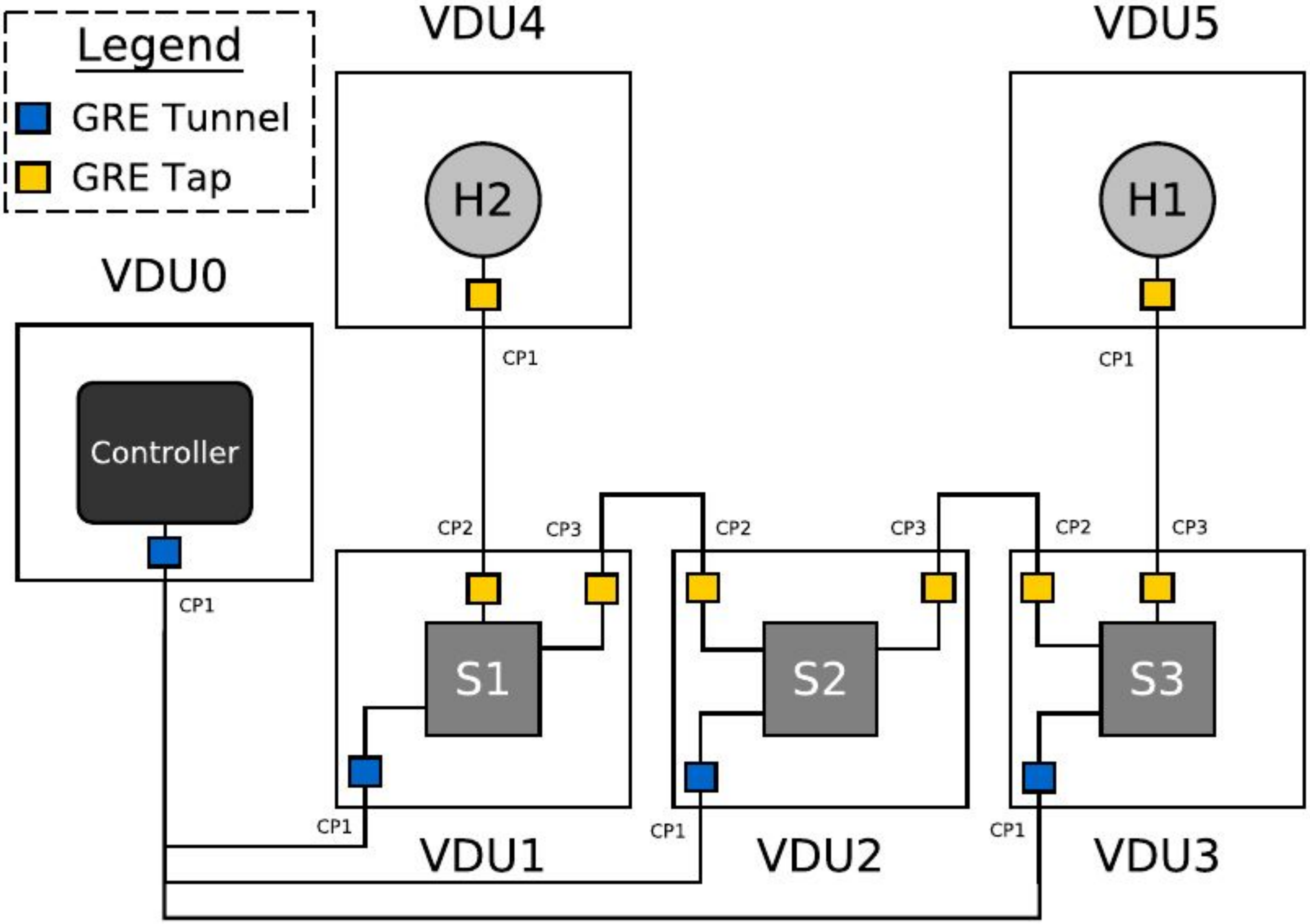
Evaluation

- Collected latency samples for baseline and attack scenarios
- Smaller sample sets were built from collected latencies
  - Sample sets reflect length of the ‘vetting period’
  - Set sizes ranged from 2 to 500
  - Measured False Positive or Negative Rate for each set size
- Sample sets were tested against the full baseline set
- *p*-value tested against 4 thresholds; 5%, 10%, 15%, and 20%

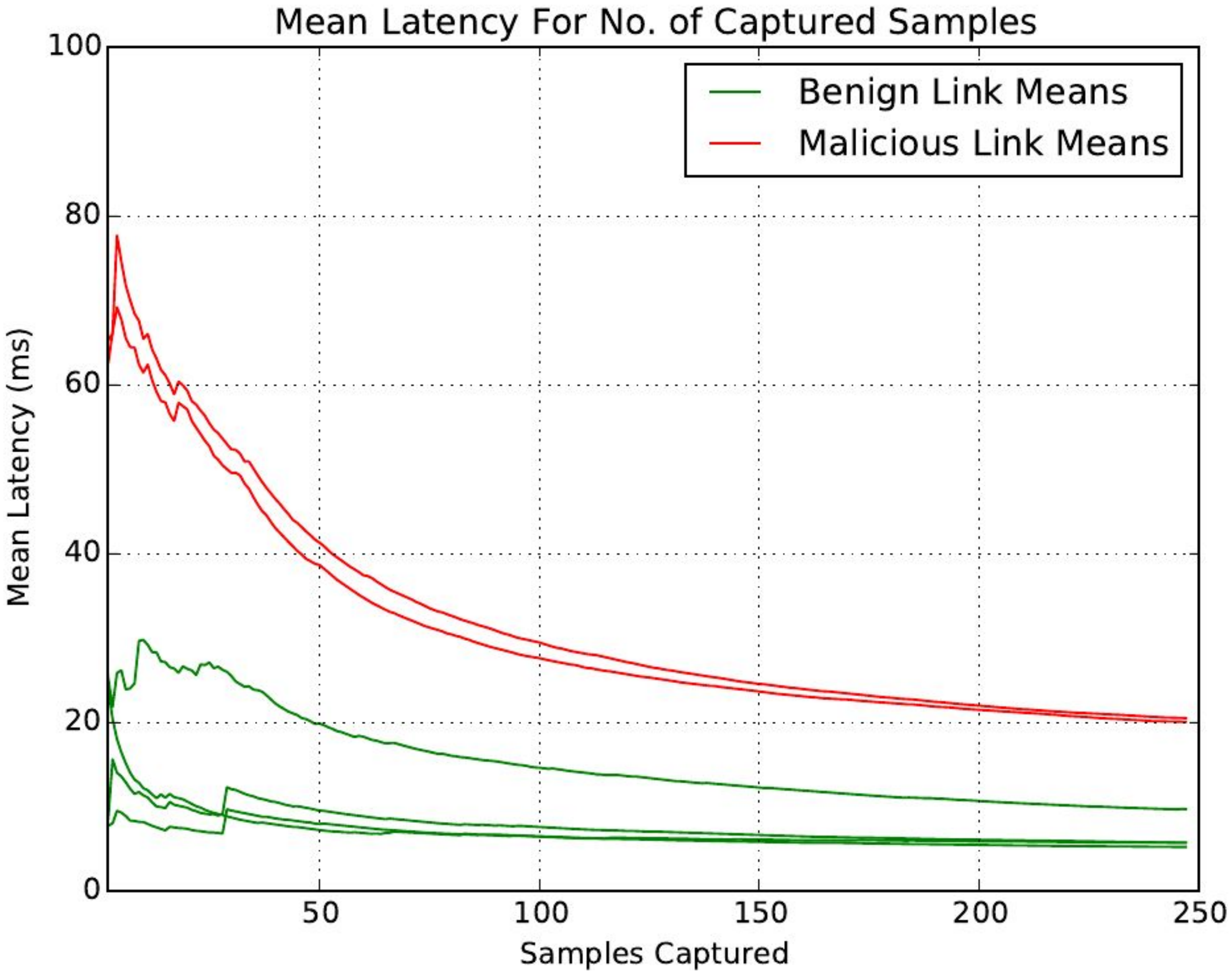
Evaluation

- Testbed:
  - Something about technologies used for each element...
- Controller was modified to record latency values
- 2500 samples captured for each attack scenario
- 2500 samples captured for the network baseline

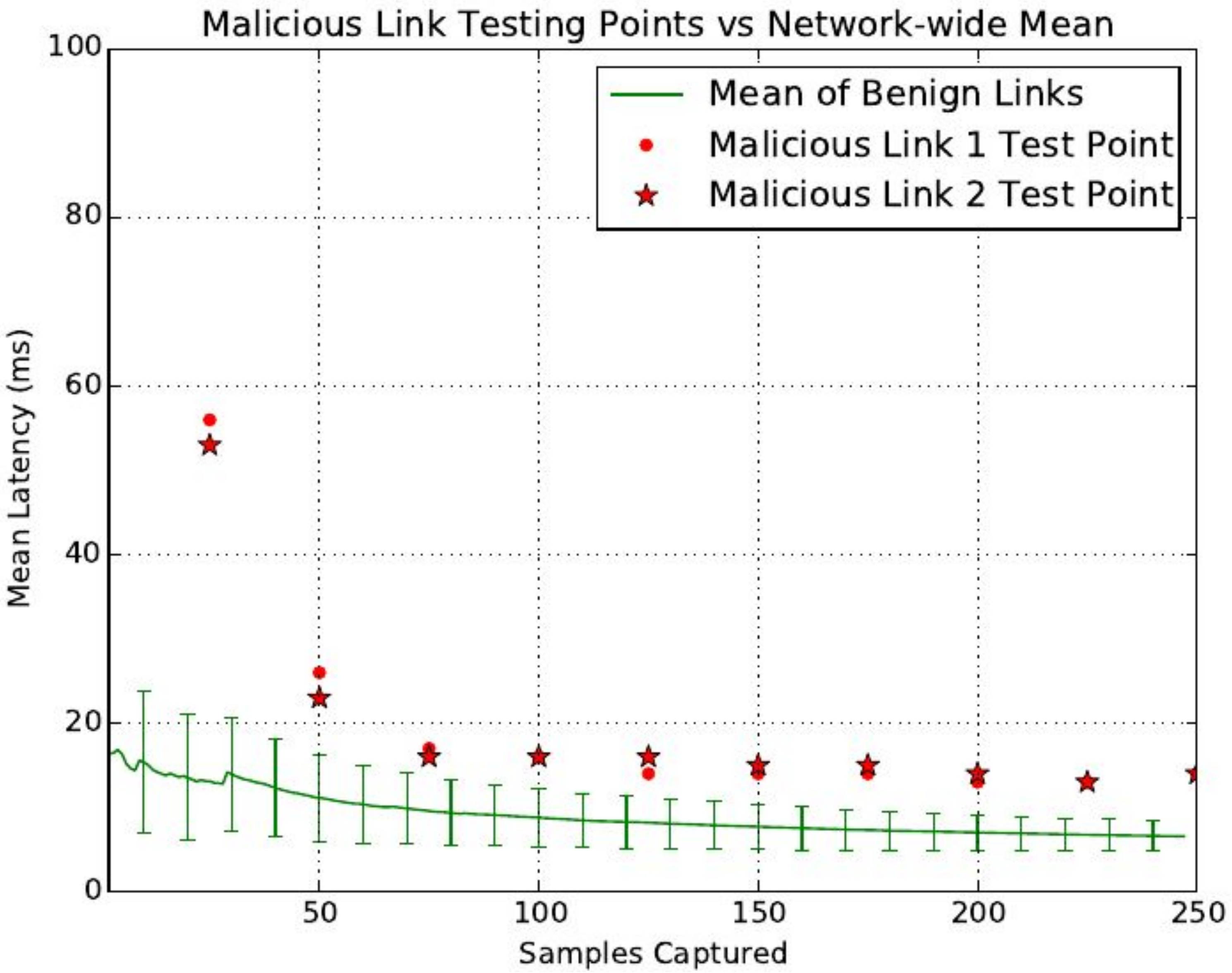
Evaluation


Legend
🟦 GRE Tunnel
🟨 GRE Tap
VDU4
VDU5
H2
H1
VDU0
Controller
CP1
CP1
CP1
CP2
CP3
CP2
CP3
CP2
CP3
S1
S2
S3
CP1
CP1
CP1
VDU1
VDU2
VDU3

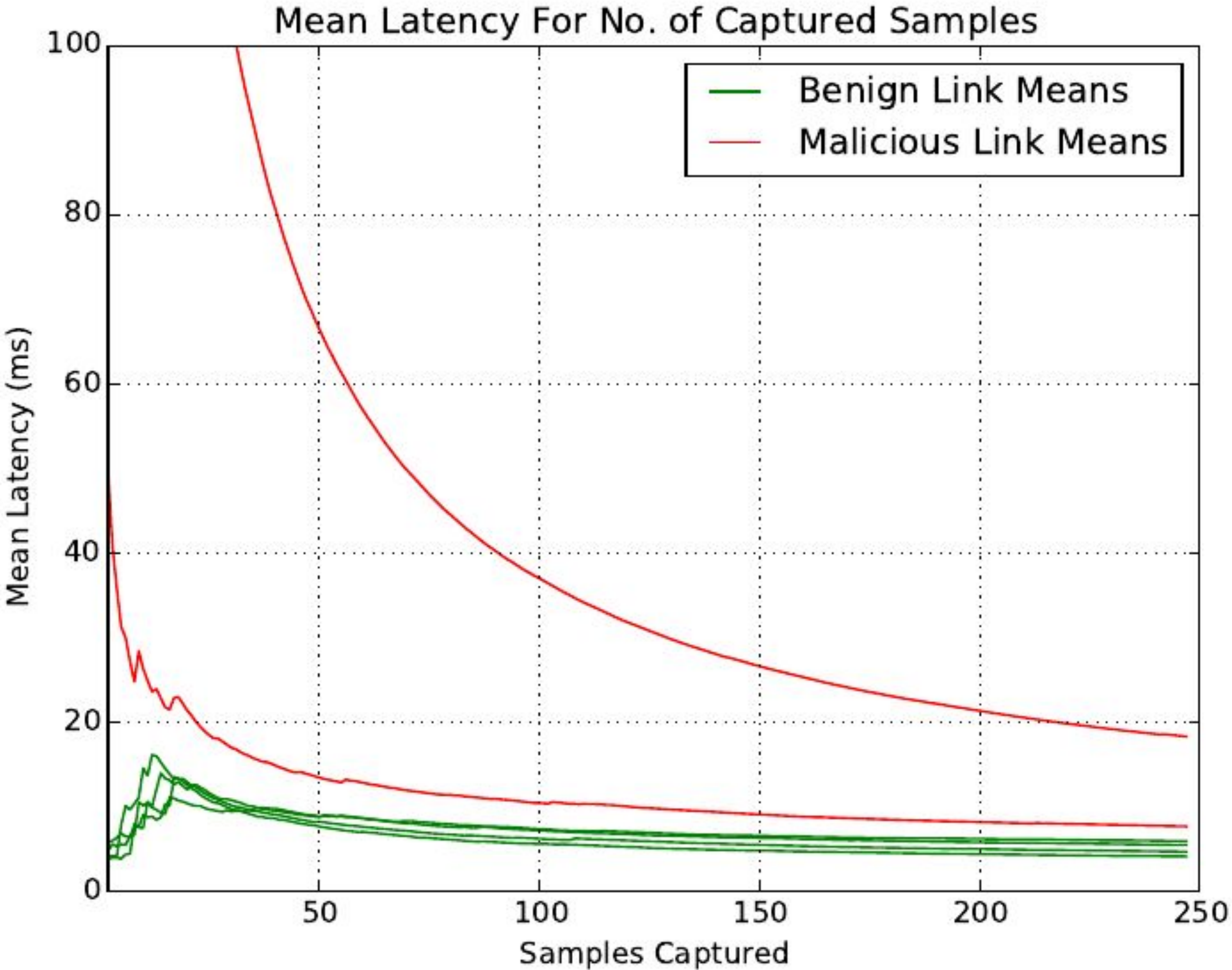
User Space Forwarding Mean Link Latencies



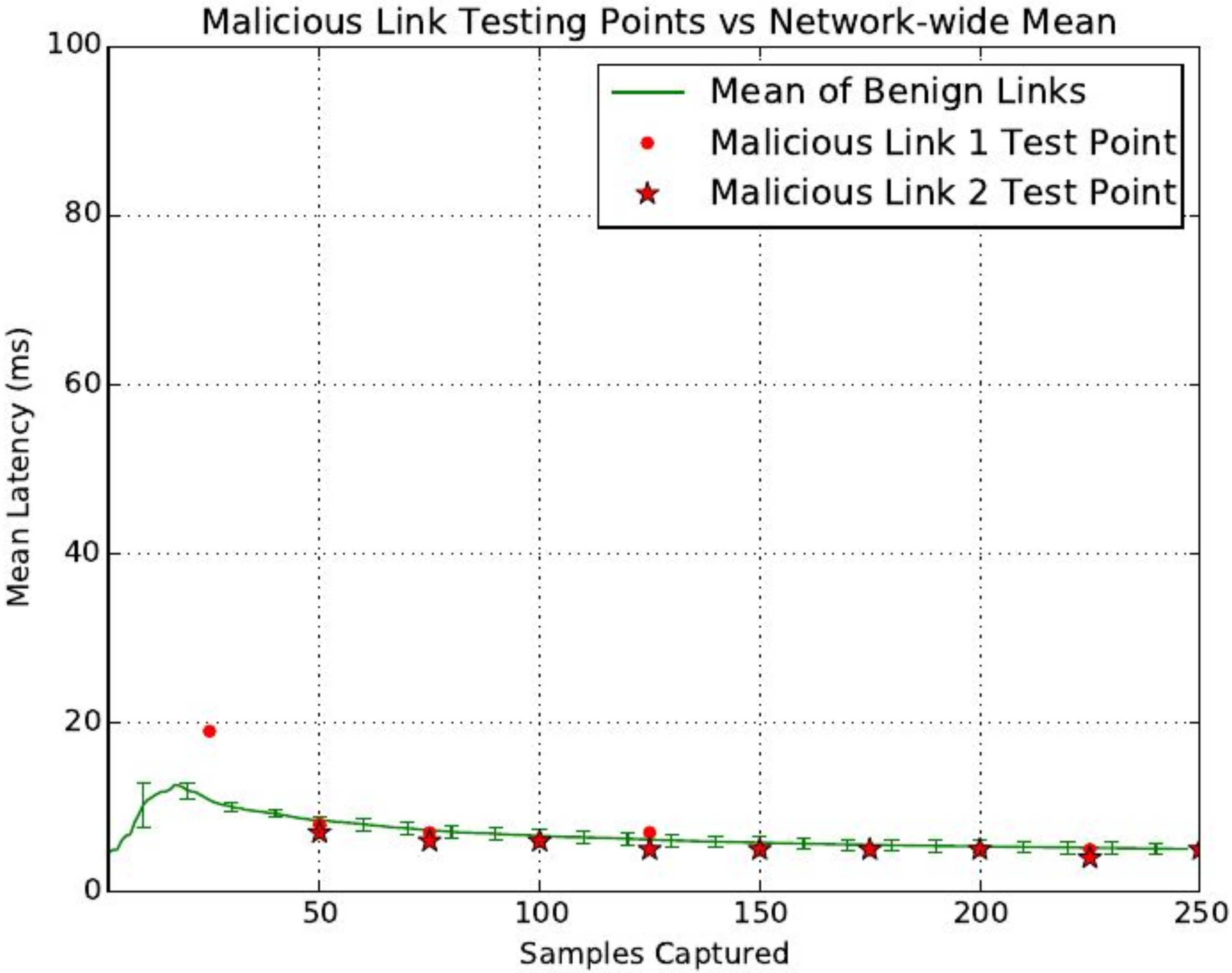
User Space Forwarding Malicious Link Tests



Kernel Forwarding Mean Link Latencies



Kernel Forwarding Malicious Link Tests



Conclusion and Future Work

- It has been demonstrated that a fabricated link can be detected through the statistical testing of link latencies.

- Experiments conducted on the Fokus testbed show that 25 latency samples and an acceptance threshold probability of 20% is enough to detect fabricated links using either kernel-space or user-space forwarding.

CORK INSTITUTE OF TECHNOLOGY

INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

http://www.cit.ie

Thank you