CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

http://www.cit.ie

Detecting Link Fabrication Attacks in Software-Defined Networks

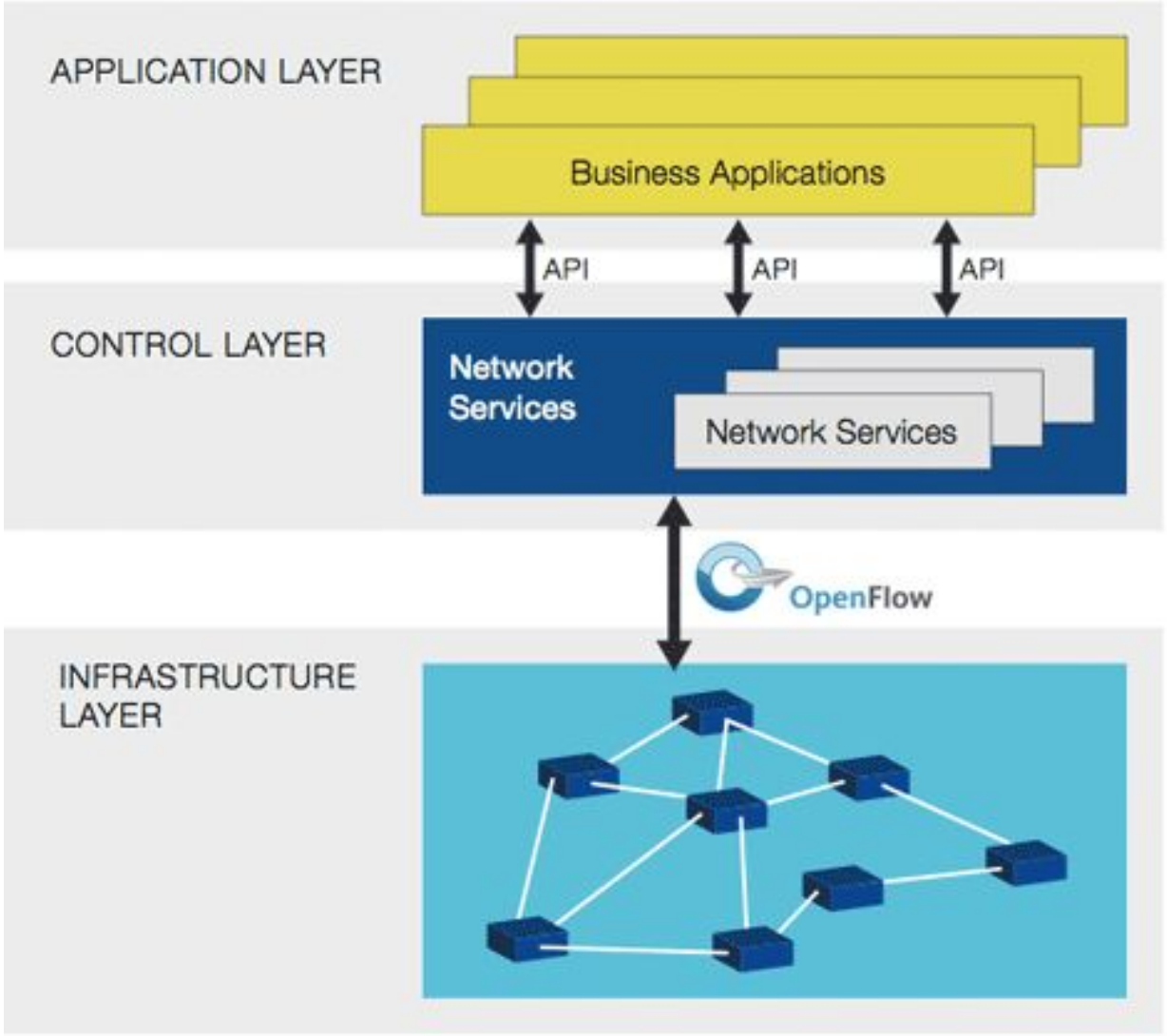
Dylan Smyth
Sean McSweeney
Donna O'Shea
Victor Cionca

August 2nd 2017

Presentation Scope

- SDN Definition
- Link Discovery in SDN
- The Link Fabrication Attack
- Detecting the Attack
- Evaluation
- Conclusion

Software-Defined Networking (SDN)



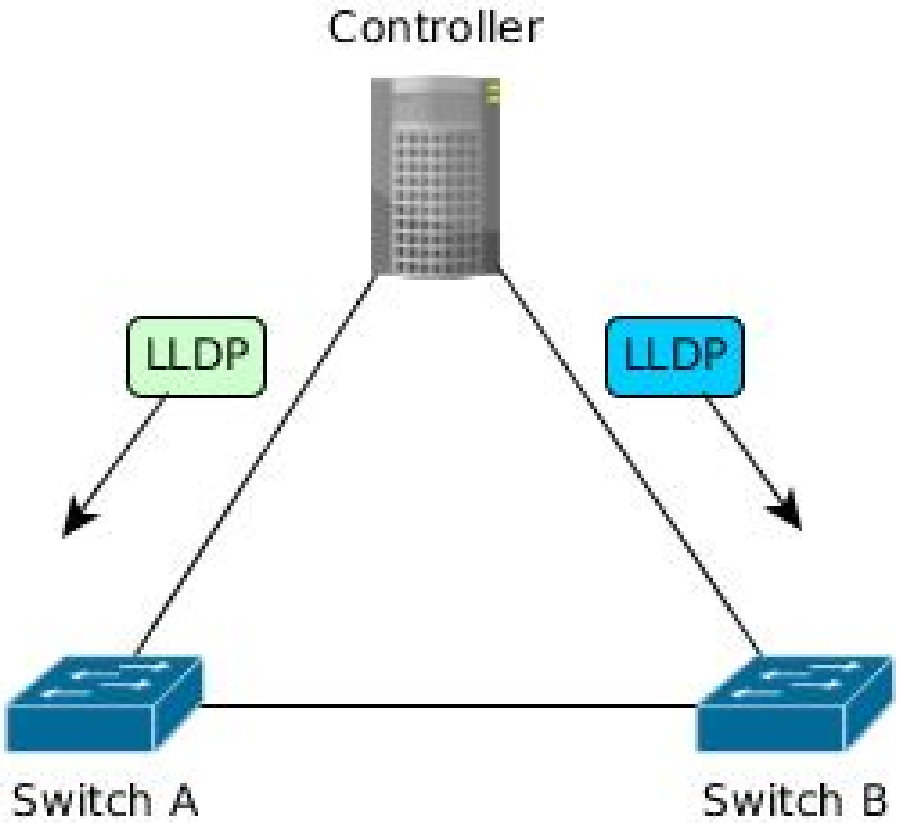
[1] https://www.opennetworking.org/sdn-resources/sdn-definition

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
  - ...

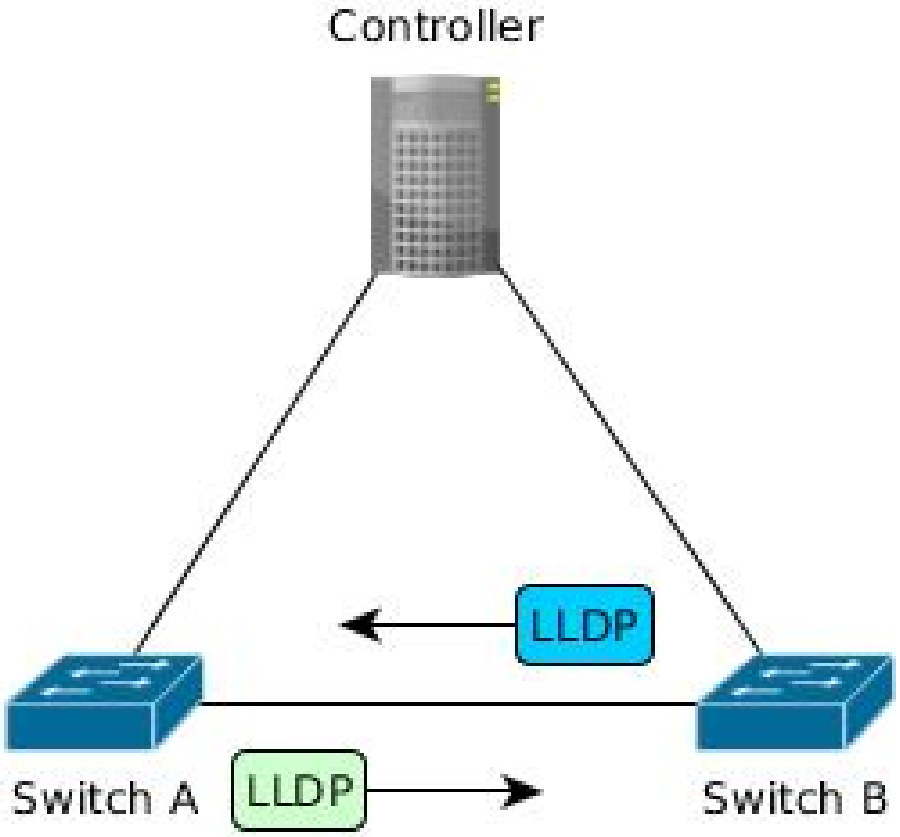
Link Discovery in SDN

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



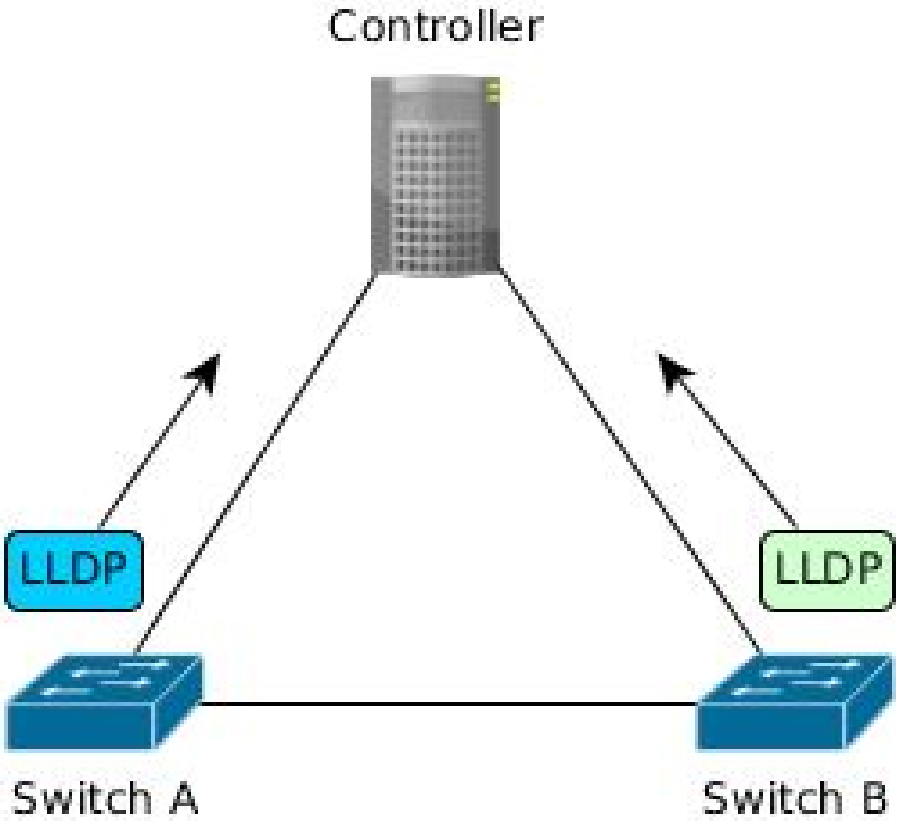
Link Discovery in SDN

- The frame is flooded out all switch ports



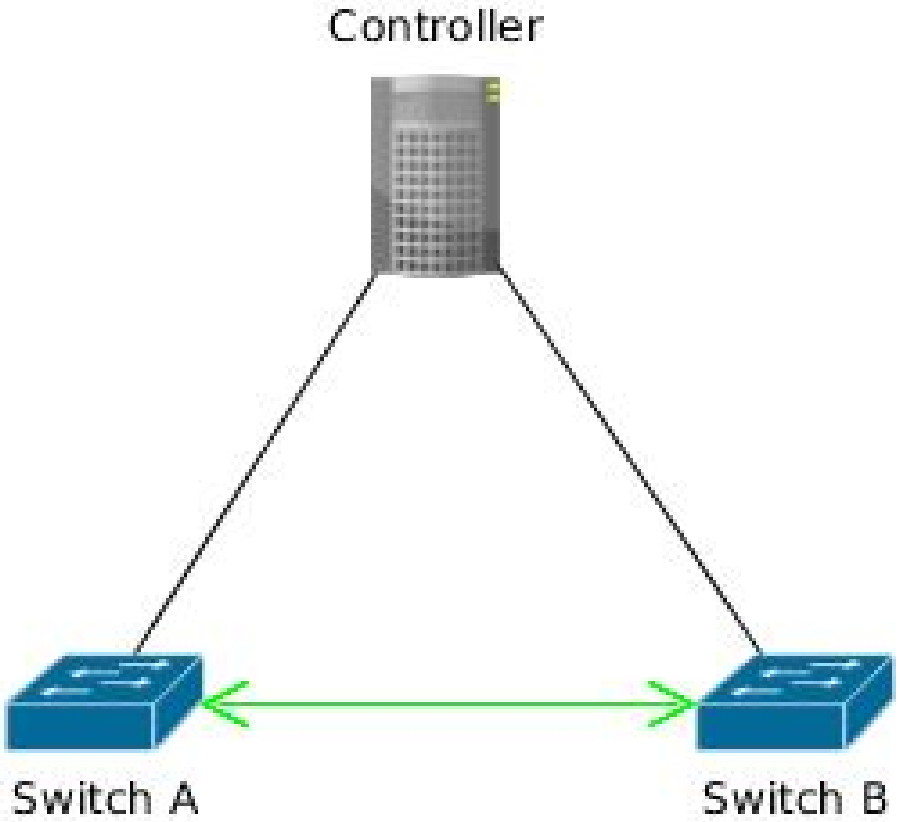
Link Discovery in SDN

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



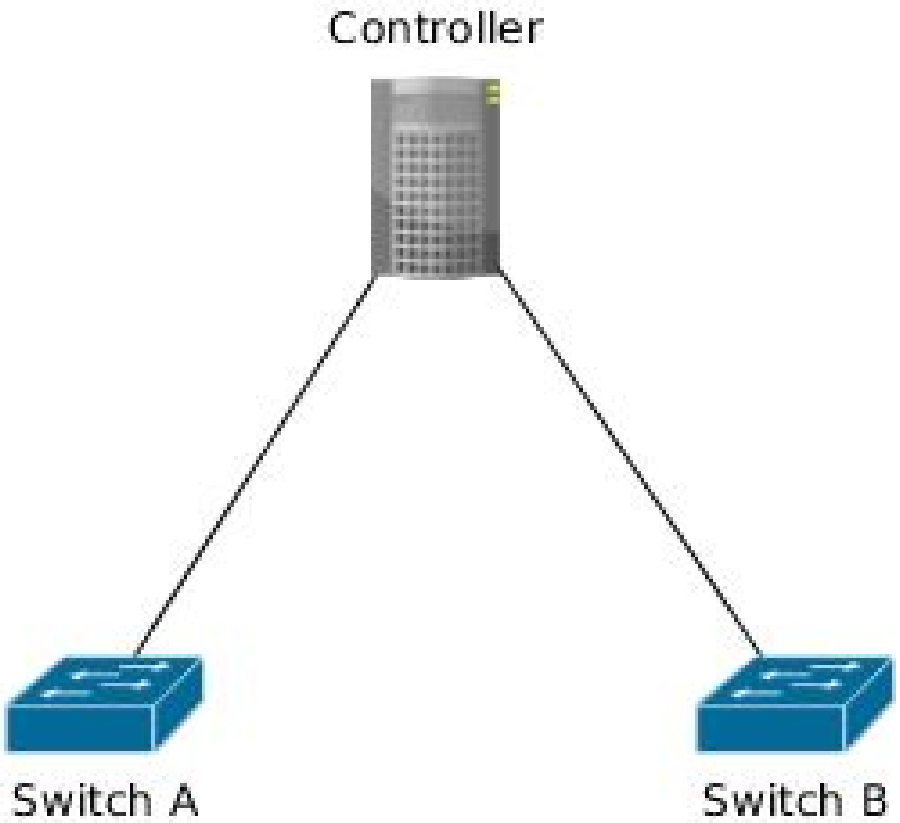
Link Discovery in SDN

- Controller understands links from returned LLDP frames



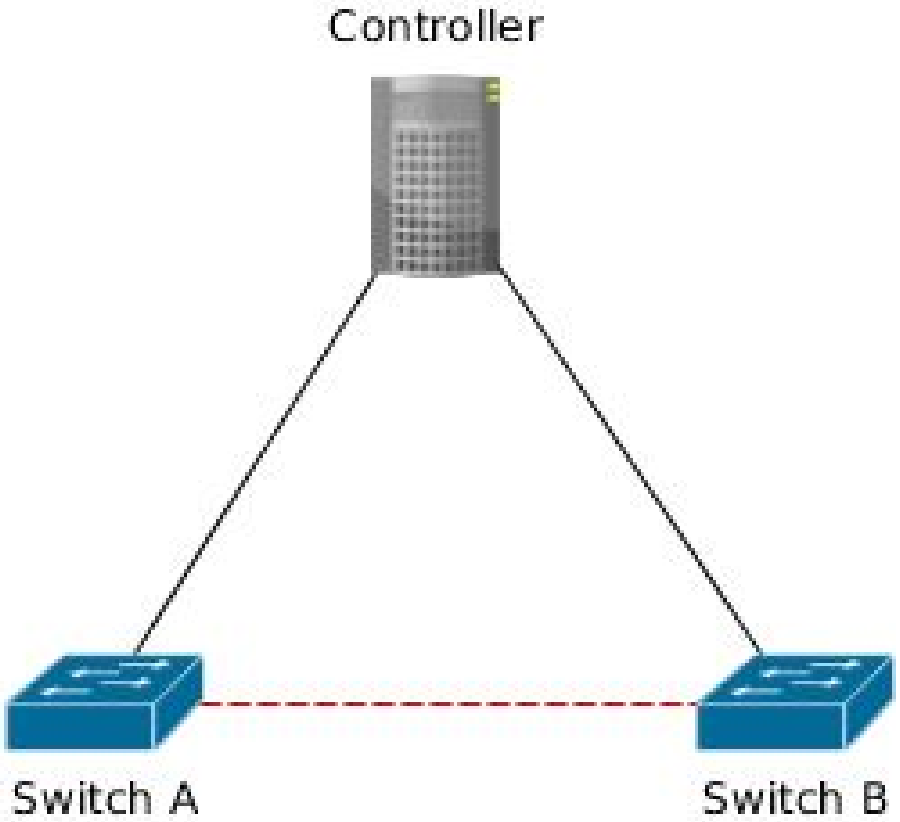
The Link Fabrication Attack

- LLDP frames are trusted to be correct



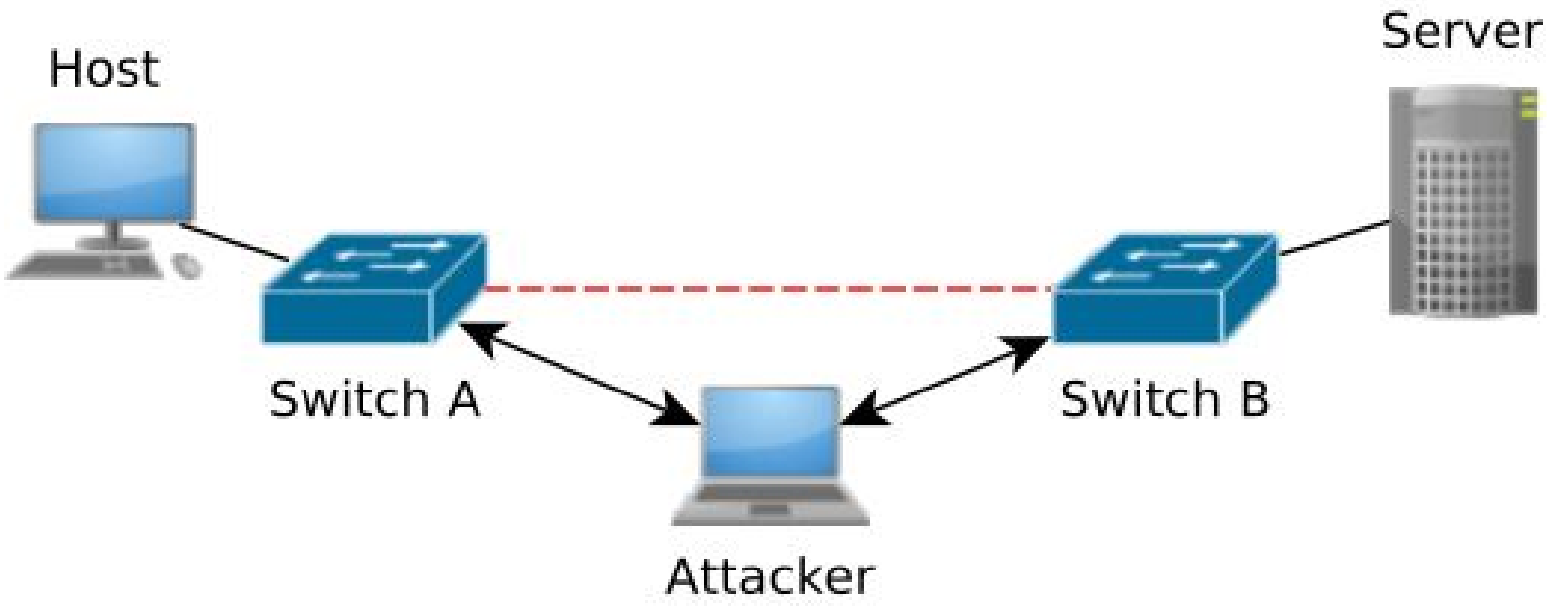
The Link Fabrication Attack

- 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

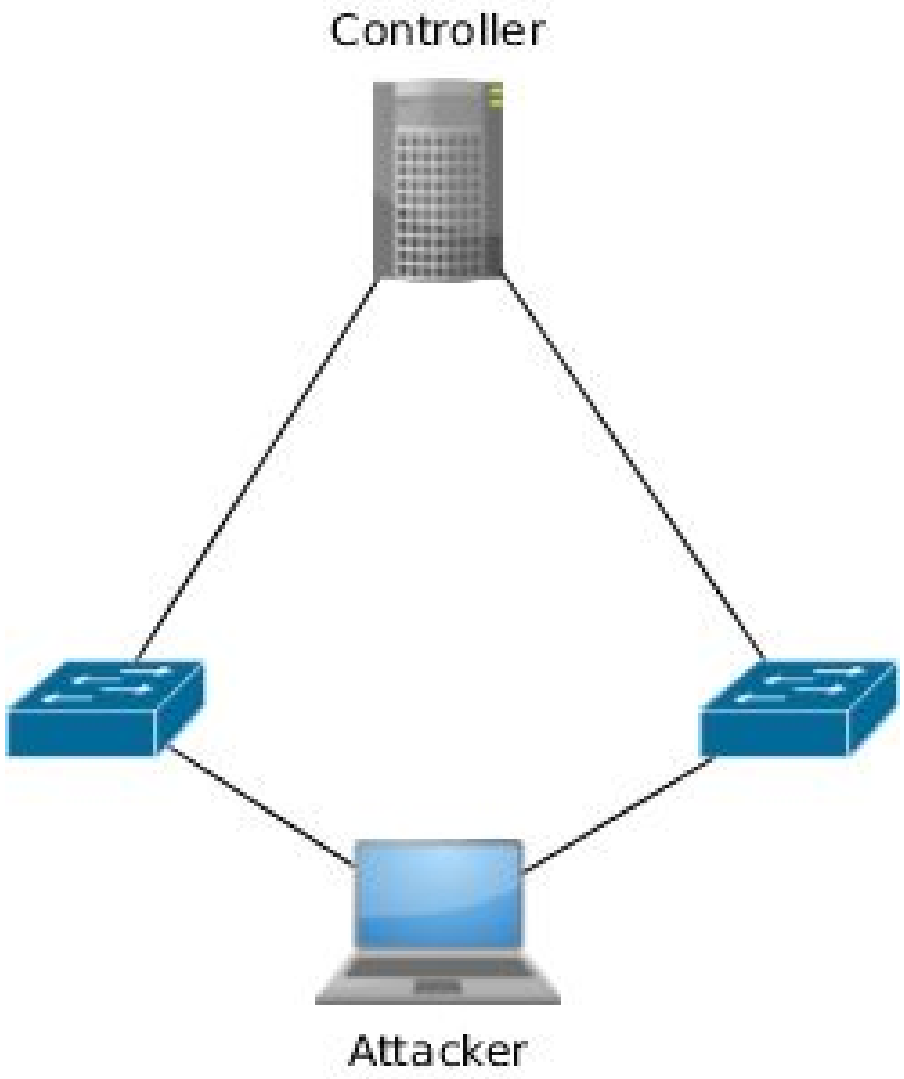
- ~~Generation type~~ Solved: LLDP frame authentication
  - ~~Crafted LLDP frame is sent into the network~~
- ~~Replay type~~ Solved: Unique value for each frame
  - ~~Legitimate frame is captured and replayed (resent) several times~~
- Relay-type
  - Legitimate frame is captured and immediately forwarded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

The Link Fabrication Attack

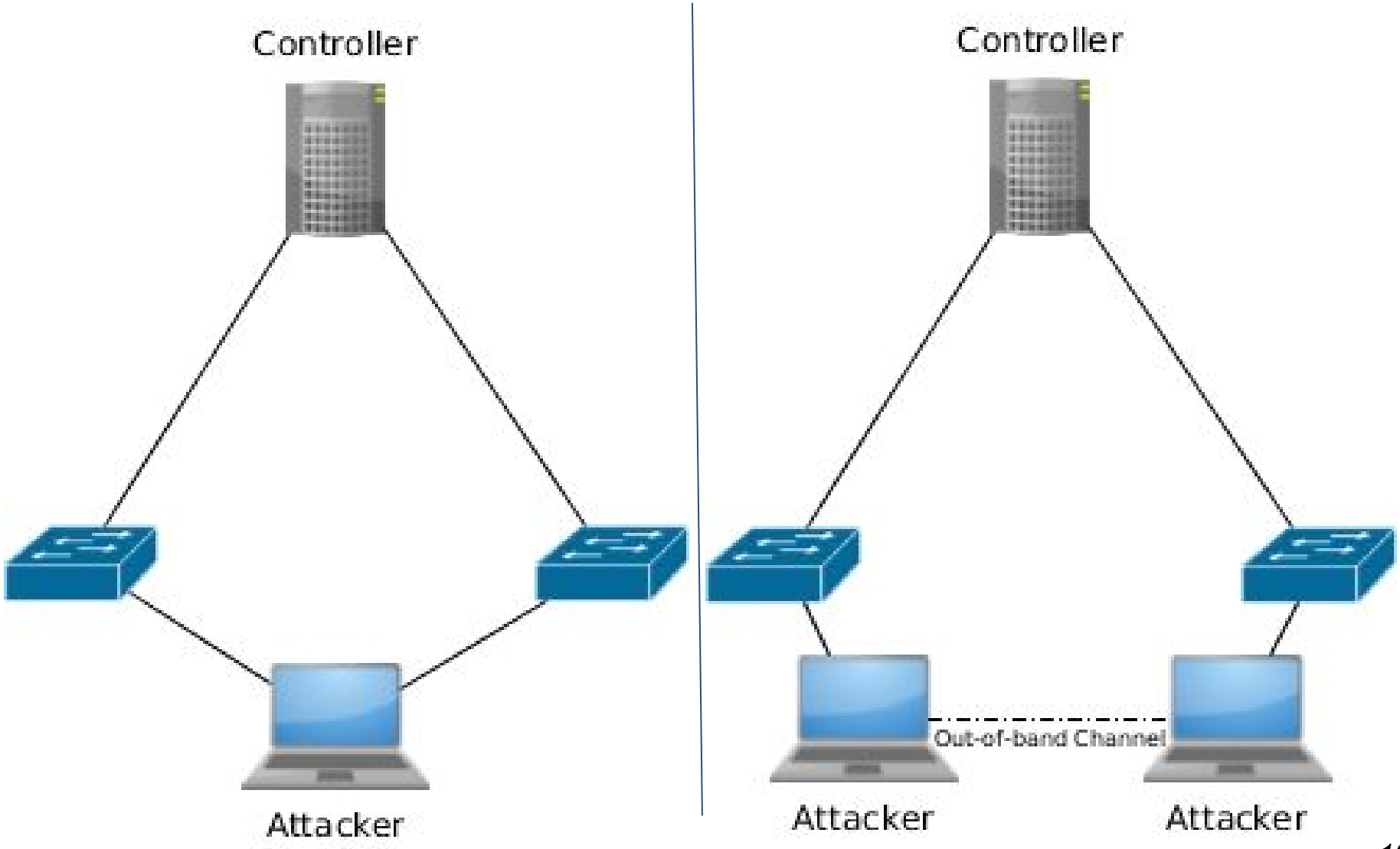
- ~~Generation type~~ Solved: LLDP frame authentication
  - ~~Crafted LLDP frame is sent into the network~~
- ~~Replay type~~ Solved: Unique value for each frame
  - ~~Legitimate frame is captured and replayed (resent) several times~~
- Relay-type Not Solved
  - Legitimate frame is captured and immediately forwarded back into the network

The Link Fabrication Attack

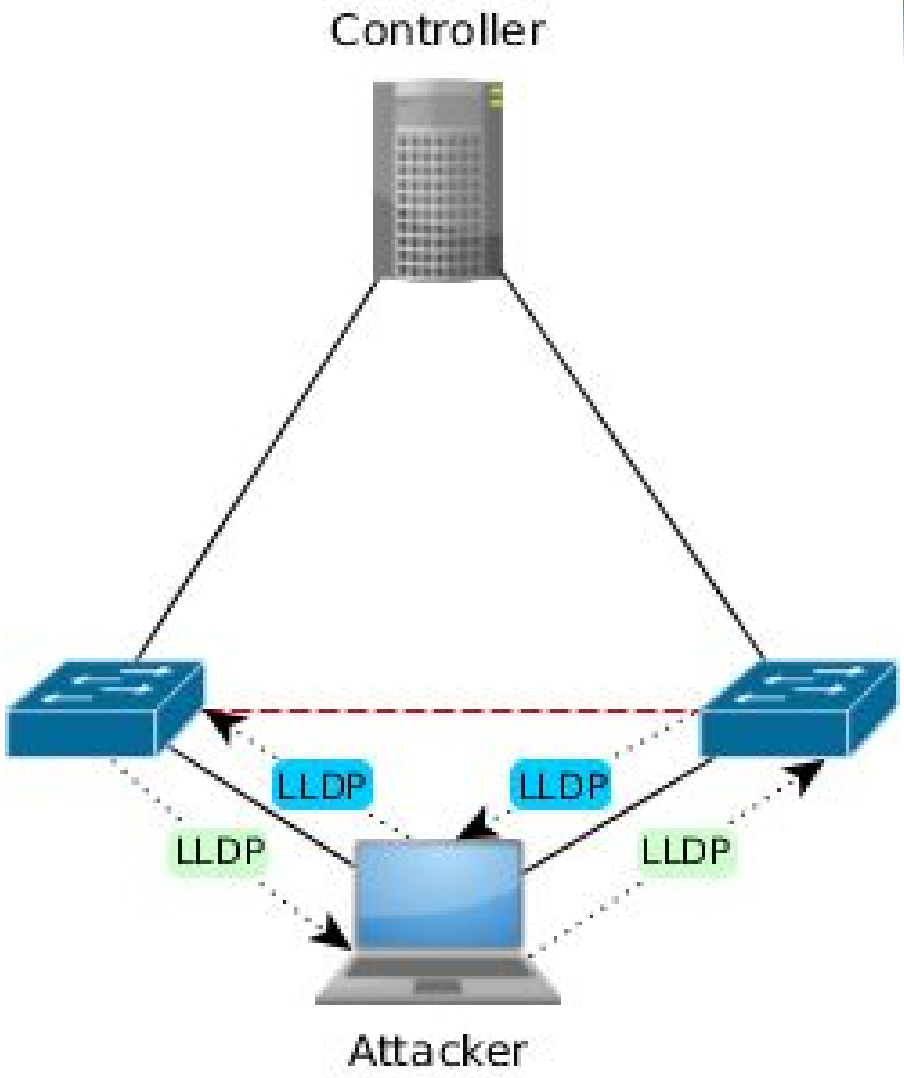
The Link Fabrication Attack

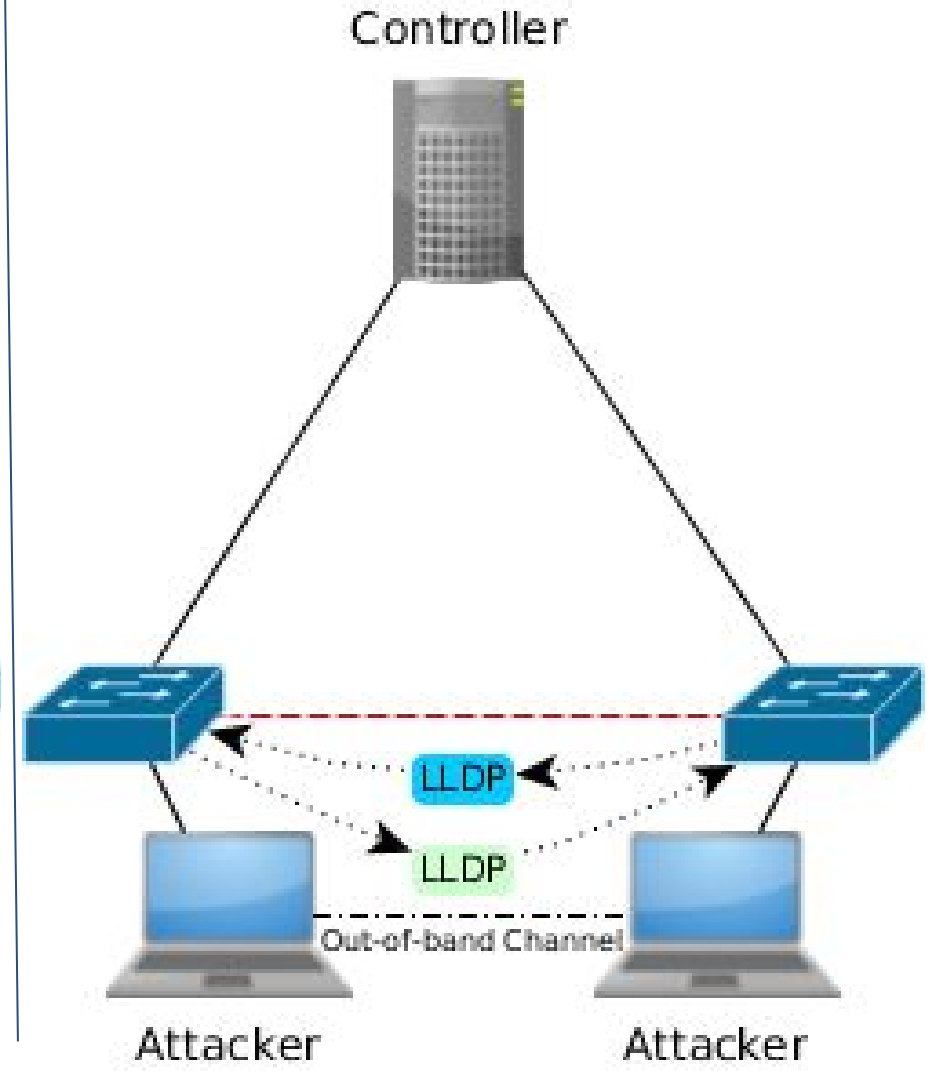


The Link Fabrication Attack



The Link Fabrication Attack





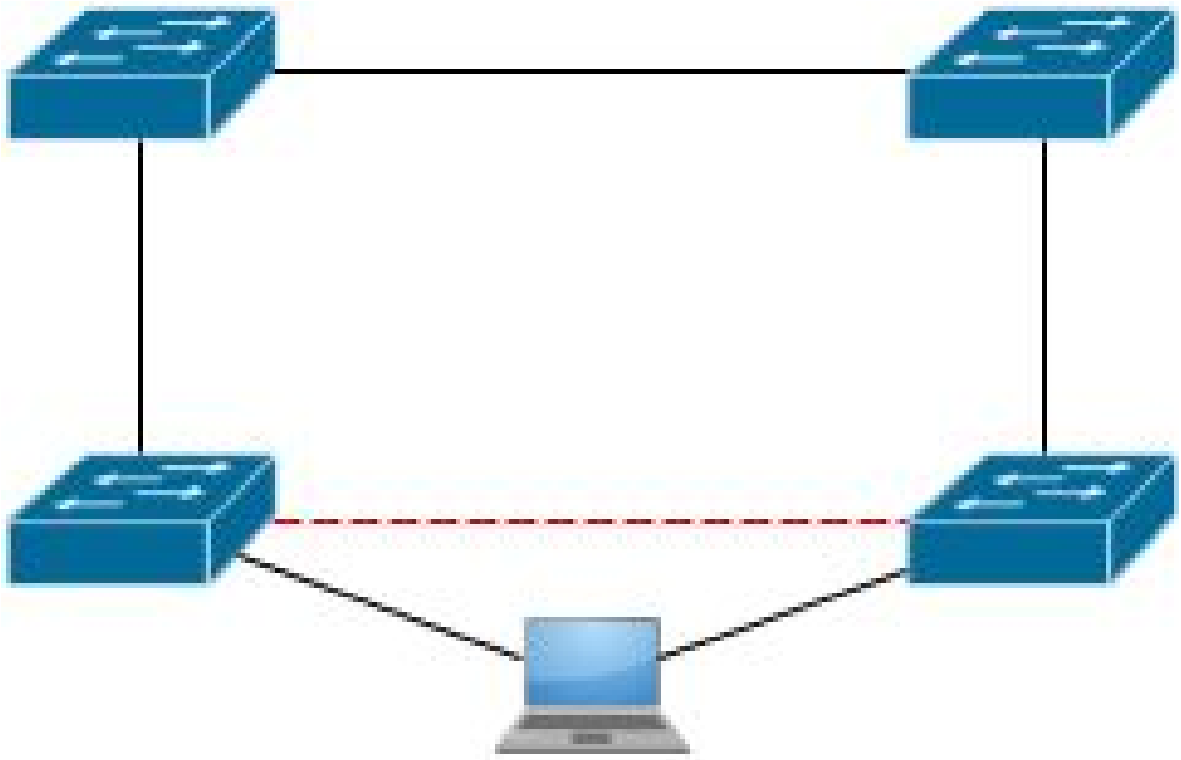
Detecting The Attack

- 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.

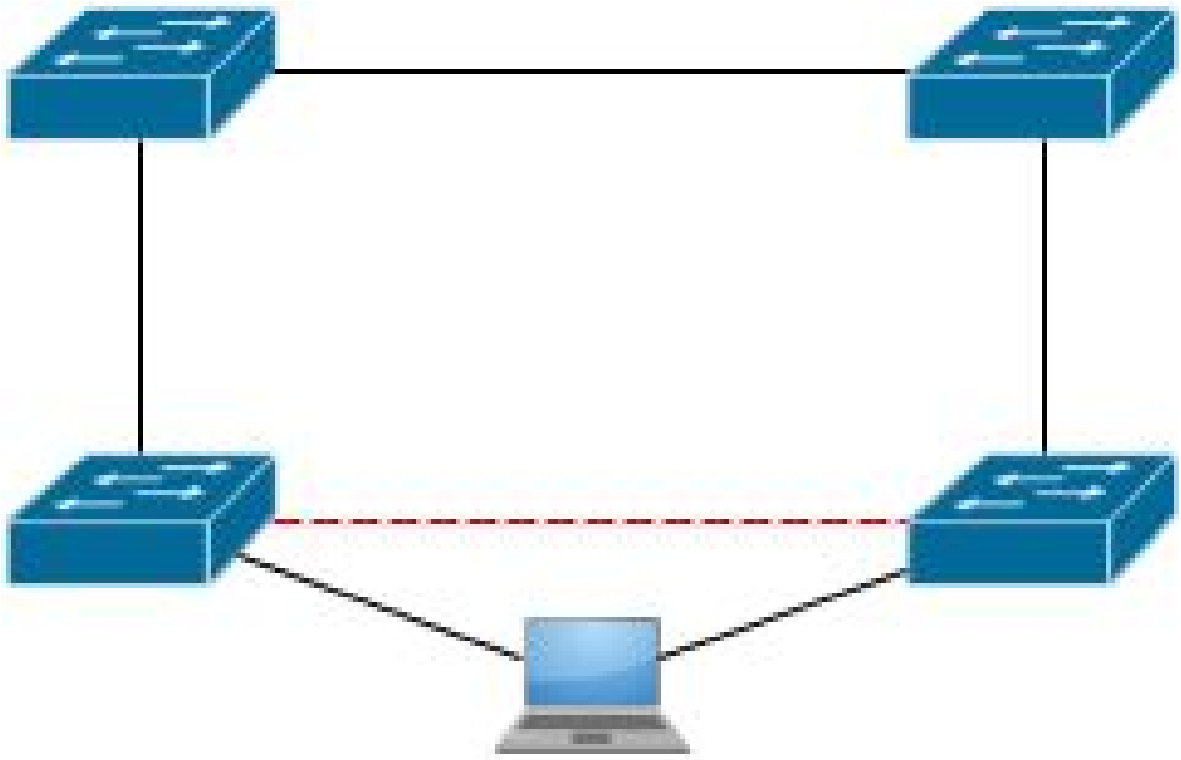
Detecting The Attack

- Fabricated link is not physically the same as normal links



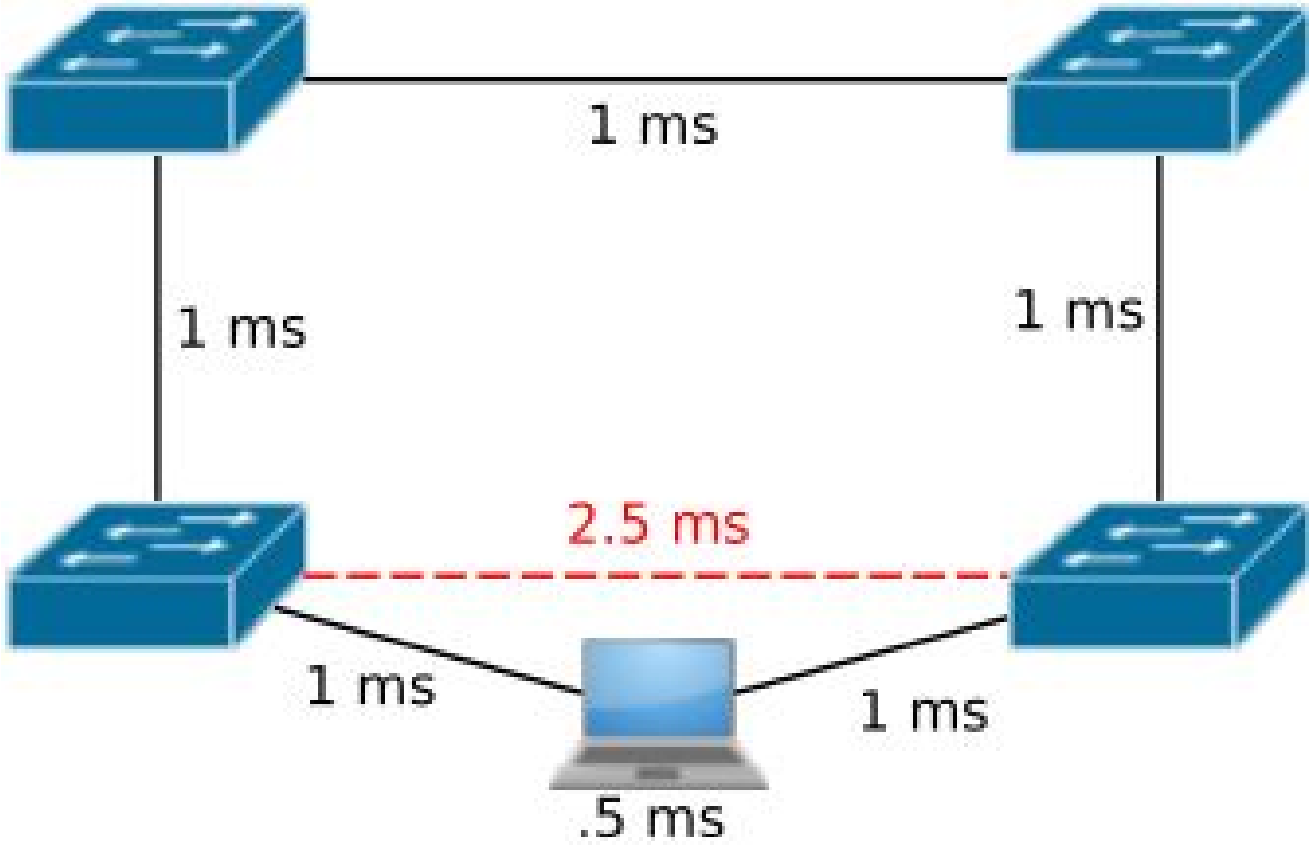
Detecting The Attack

- 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.

Detecting The Attack

- Implemented Statistical Hypothesis Testing
- Steps…
  - Calculate mean latency for new link (*x*)
  - Calculate mean baseline latency (*y*)
  - Calculate *z*-score; Number of standard deviations *x* is from *y*
  - 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

Evaluation

Evaluation

- Determine if proposed detection method is appropriate
- Test the accuracy of detection
  - Measure False Positive Rate (when benign link is tested)
  - Measure False Negative Rate (when fabricated link is tested)
- Examine tradeoff between accuracy and vetting period length

Evaluation

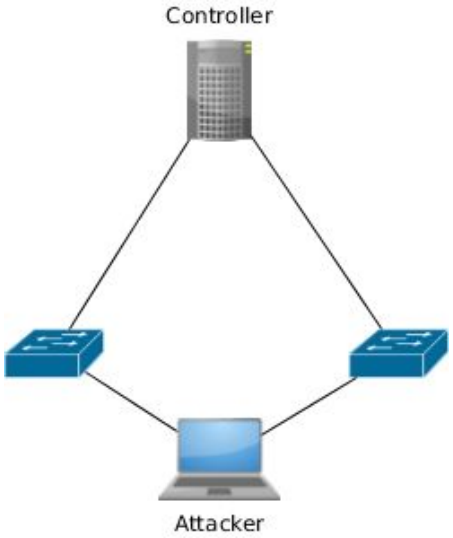
- Tested the proposed detection method using simulations
- Collected latency samples for baseline and attack scenarios
- Smaller sample sets were built from collected latencies
  - Sample sets reflect length of the ‘vetting period’
  - Set sizes ranged from 2 to 500
  - Measured False Positive or Negative 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:
  - Alix boards (x2) running Debian and OpenVSwitch
  - Odroid U3 running Floodlight controller
  - Raspberry Pis at network hosts
- Controller was modified to record latency values
- 2500 samples captured for each attack scenario
- 2500 samples captured for the network baseline

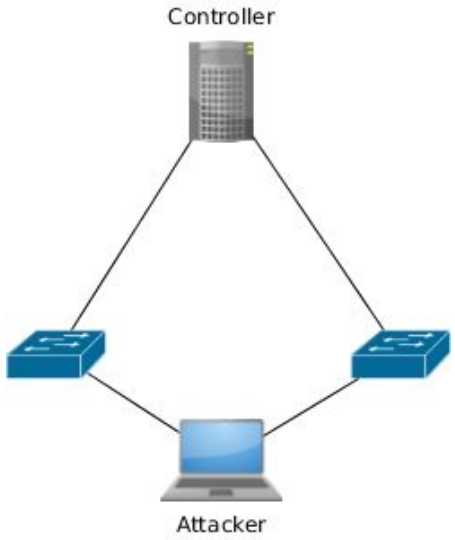
Evaluation

- Dual-homed host
  - Forwarding Using:
    - Bridging (kernel-space)
    - Python (User-space)

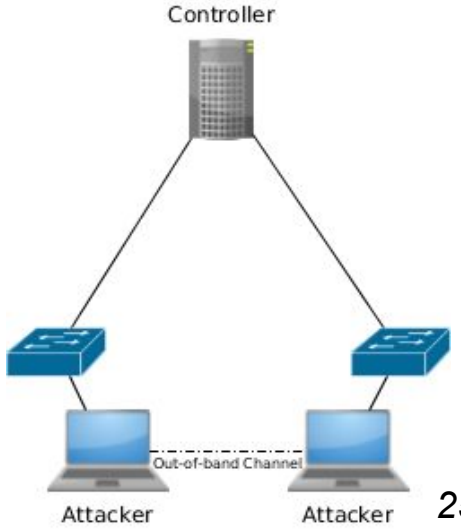


Evaluation

- Dual-homed host
  - Forwarding Using:
    - Bridging (kernel-space)
    - Python (User-space)



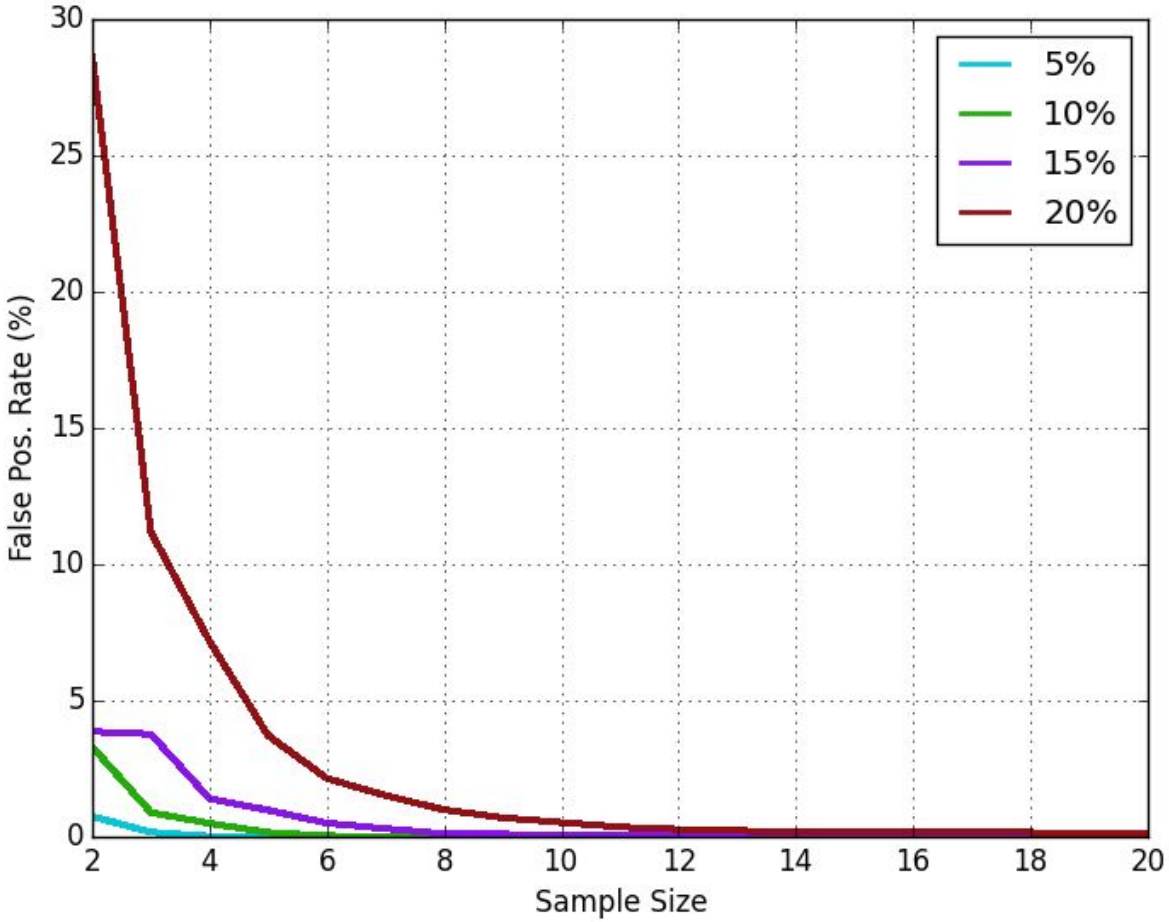
- Out-of-band Connected Hosts
  - Forwarding Using:
    - Bridging via wireless Ad-Hoc (kernel-space)
    - Bridging via wireless infrastructure (kernel-space)
    - Python via wireless Ad-Hoc (User-space)



Results

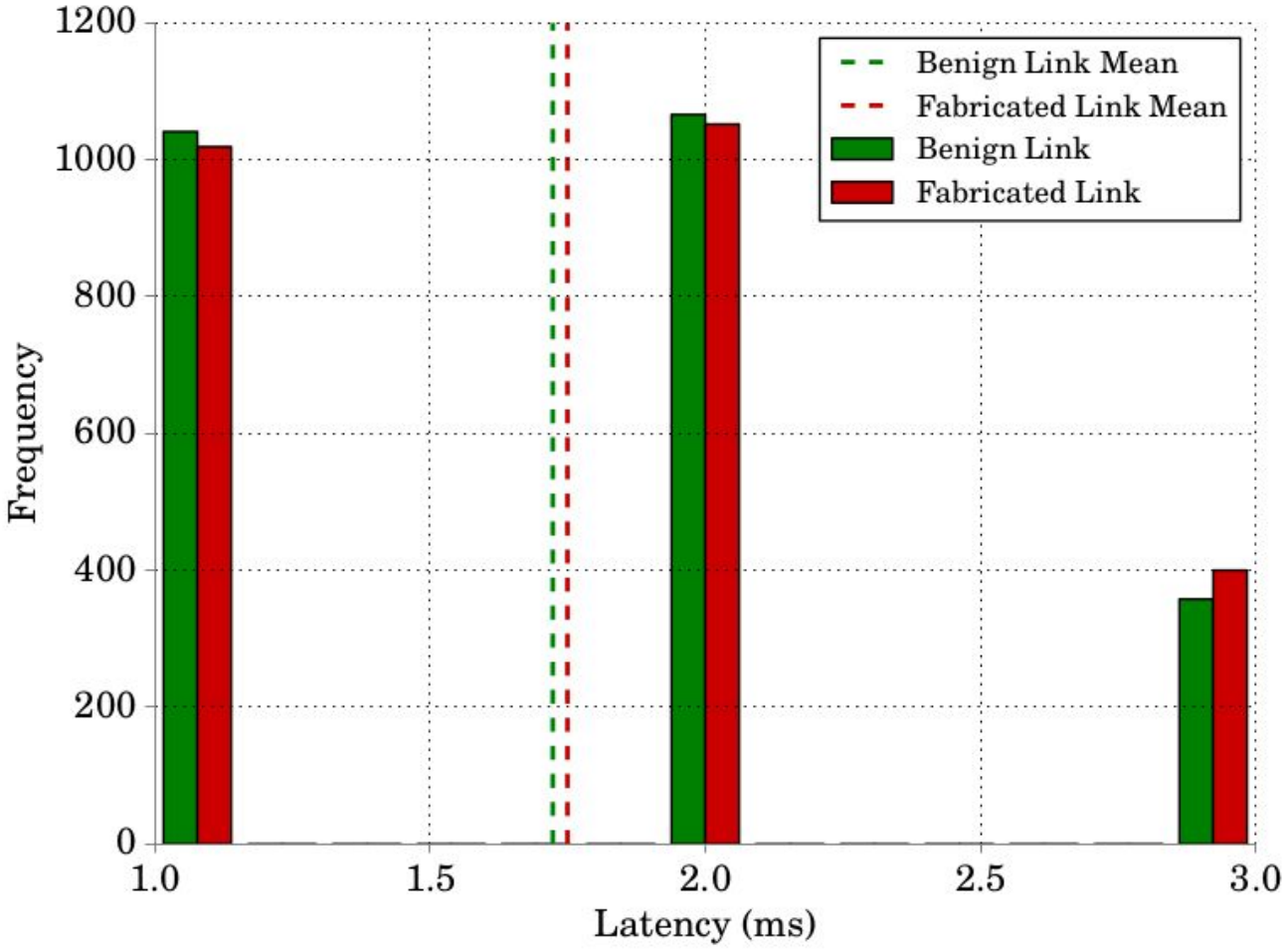
Results

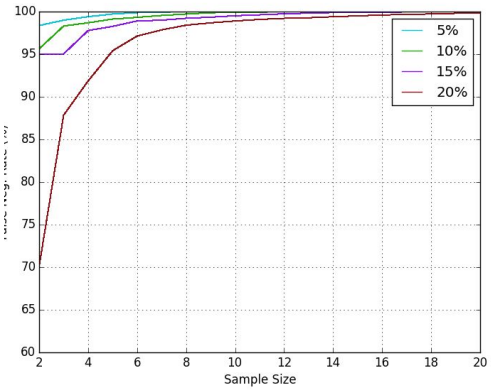
- False Positive Rate for a benign link



Results

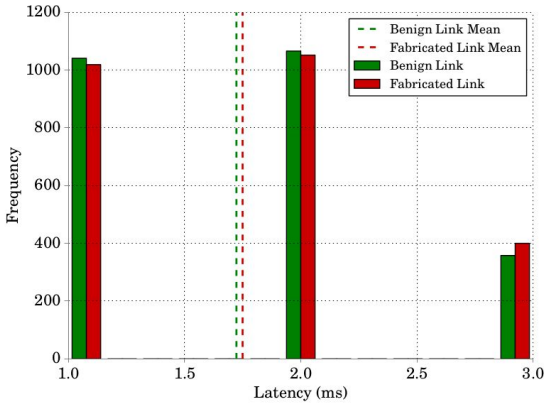
- Distribution for dual-homed bridging

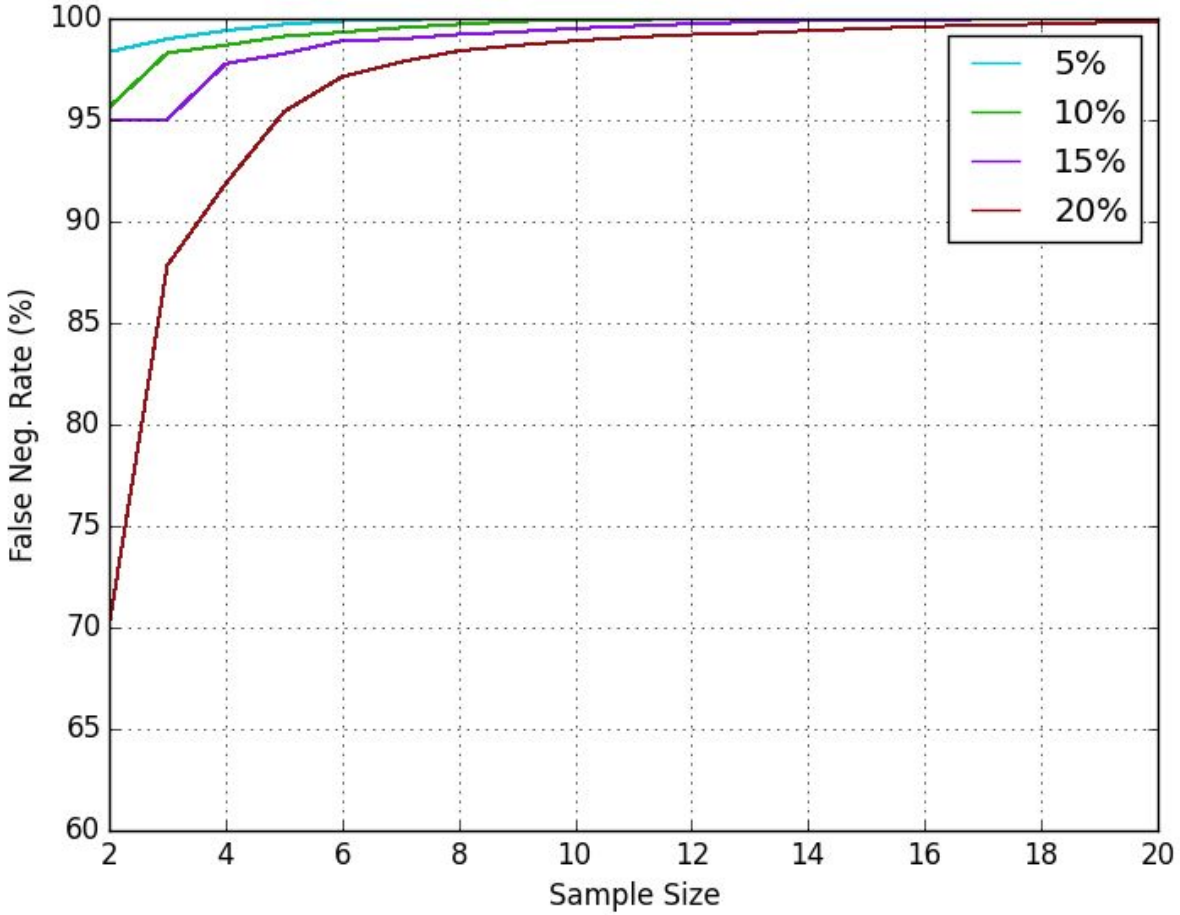




Results

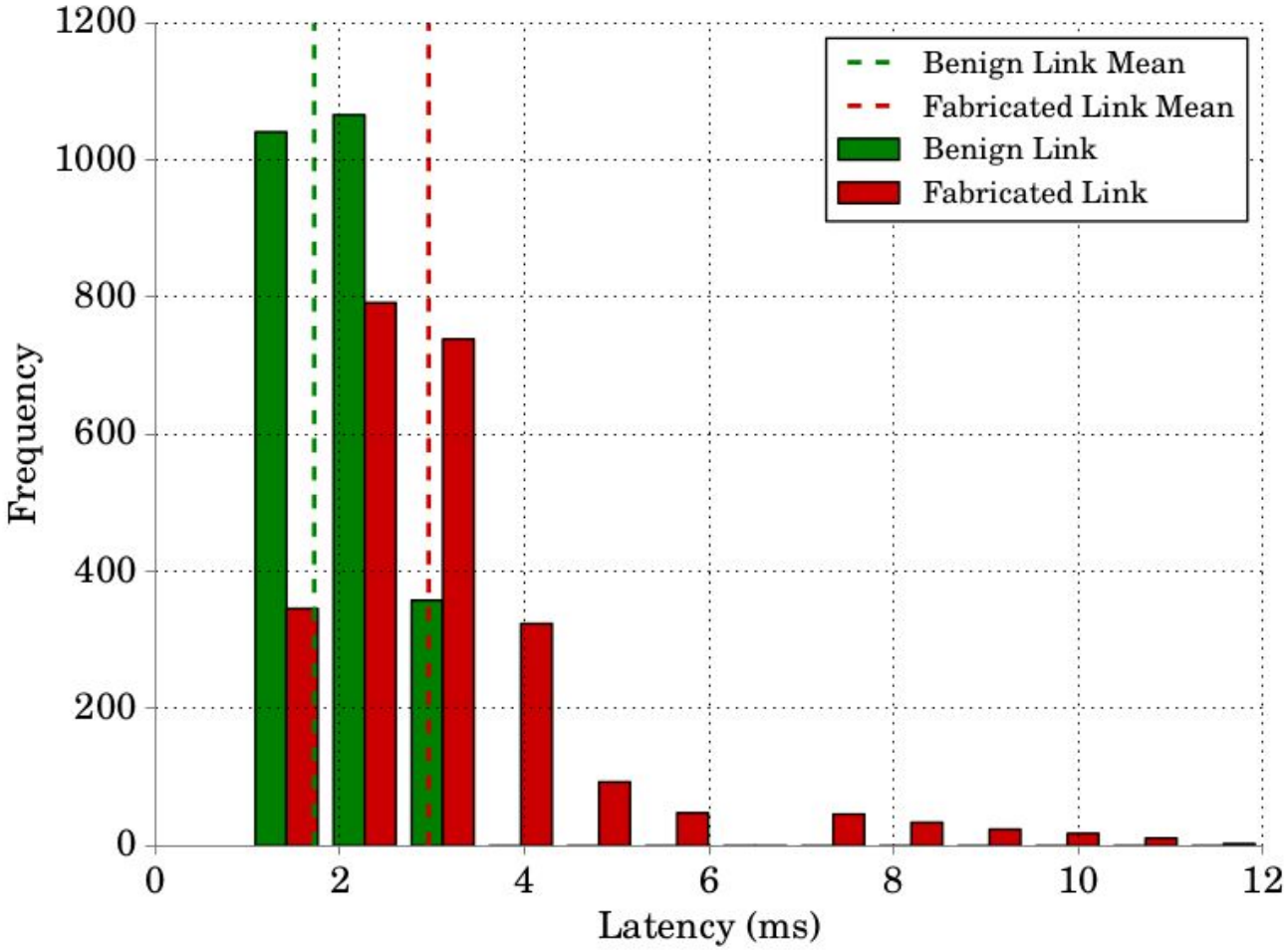
- False Negative Rate for dual-homed bridging

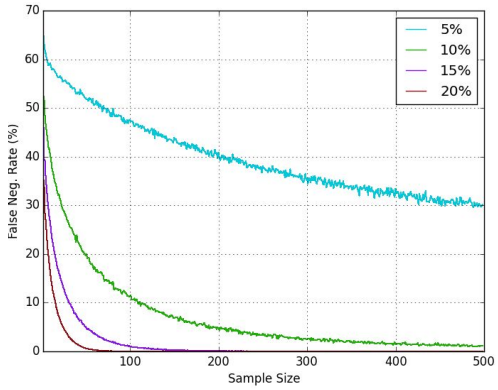




Results

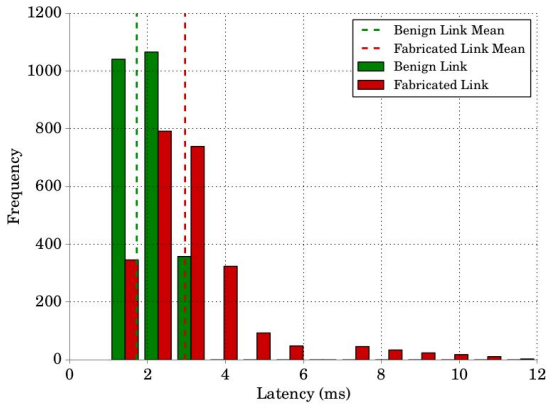
- Distribution for bridging via out-of-band Ad-Hoc

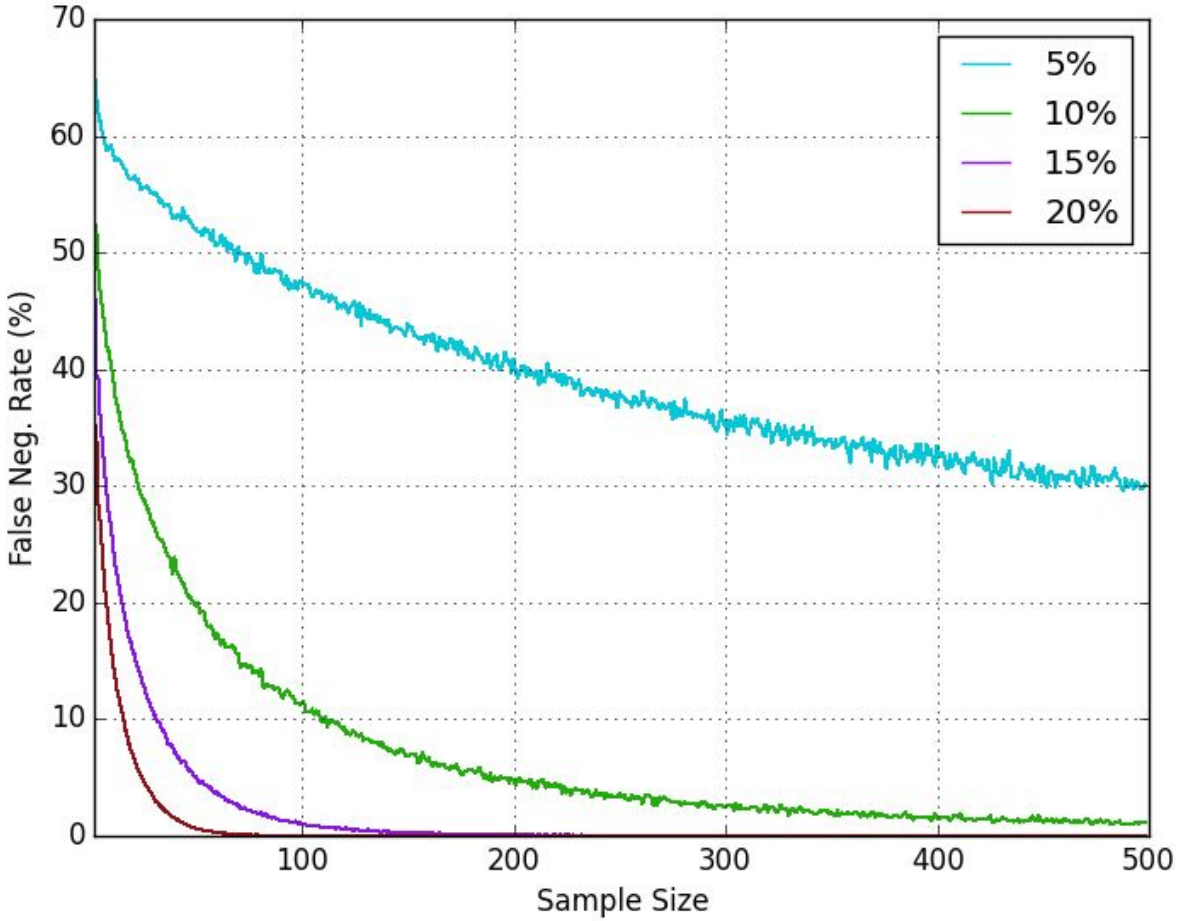




Results

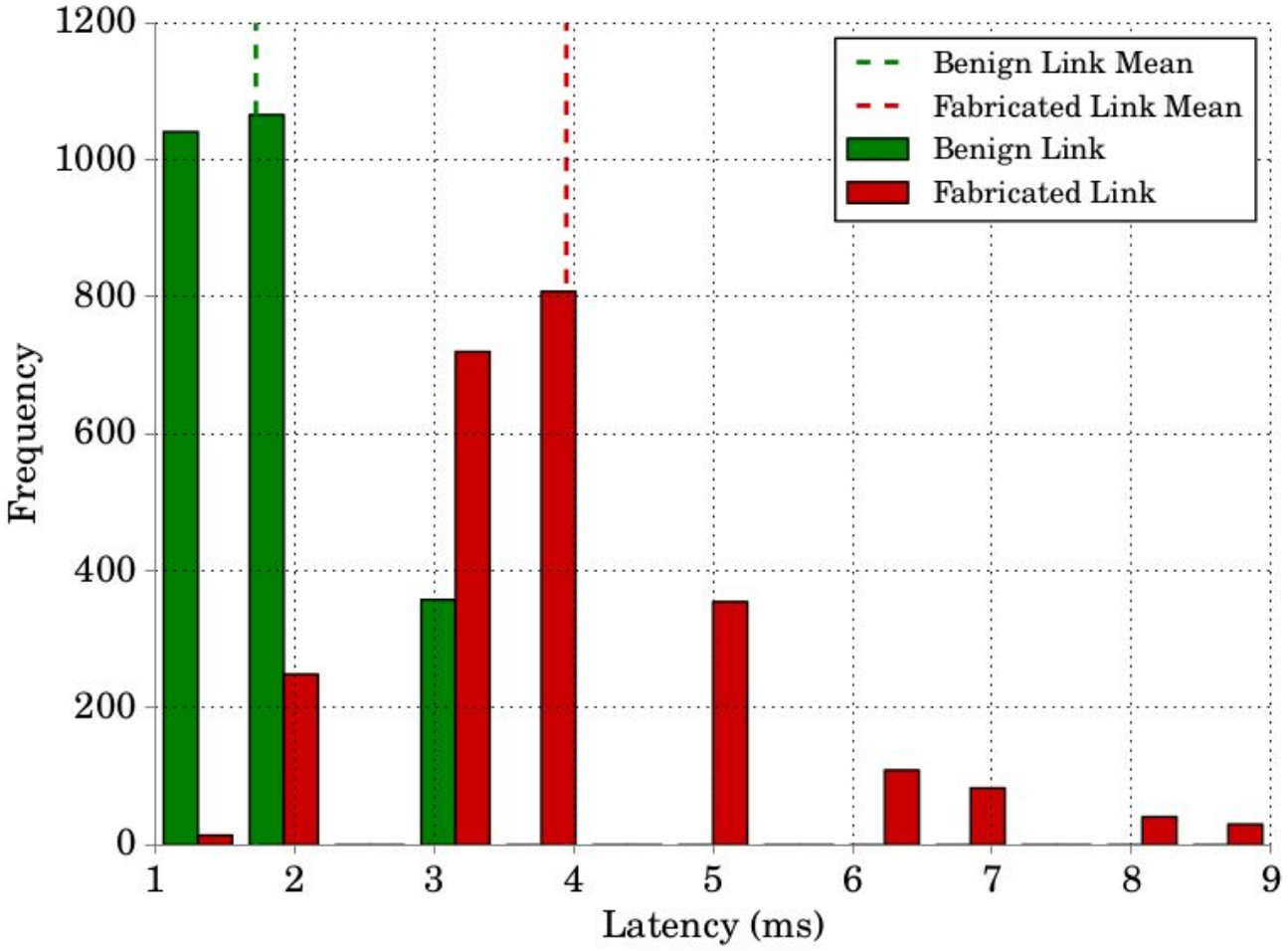
- False Negative Rate for bridging via out-of-band Ad-Hoc

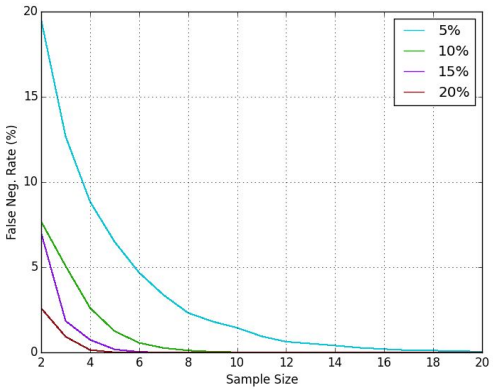




Results

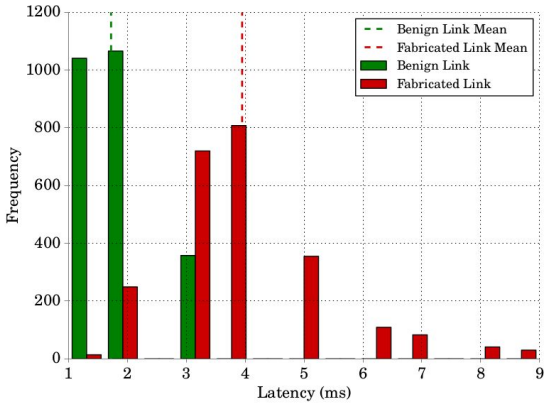
- Distribution for bridging via out-of-band Infra.

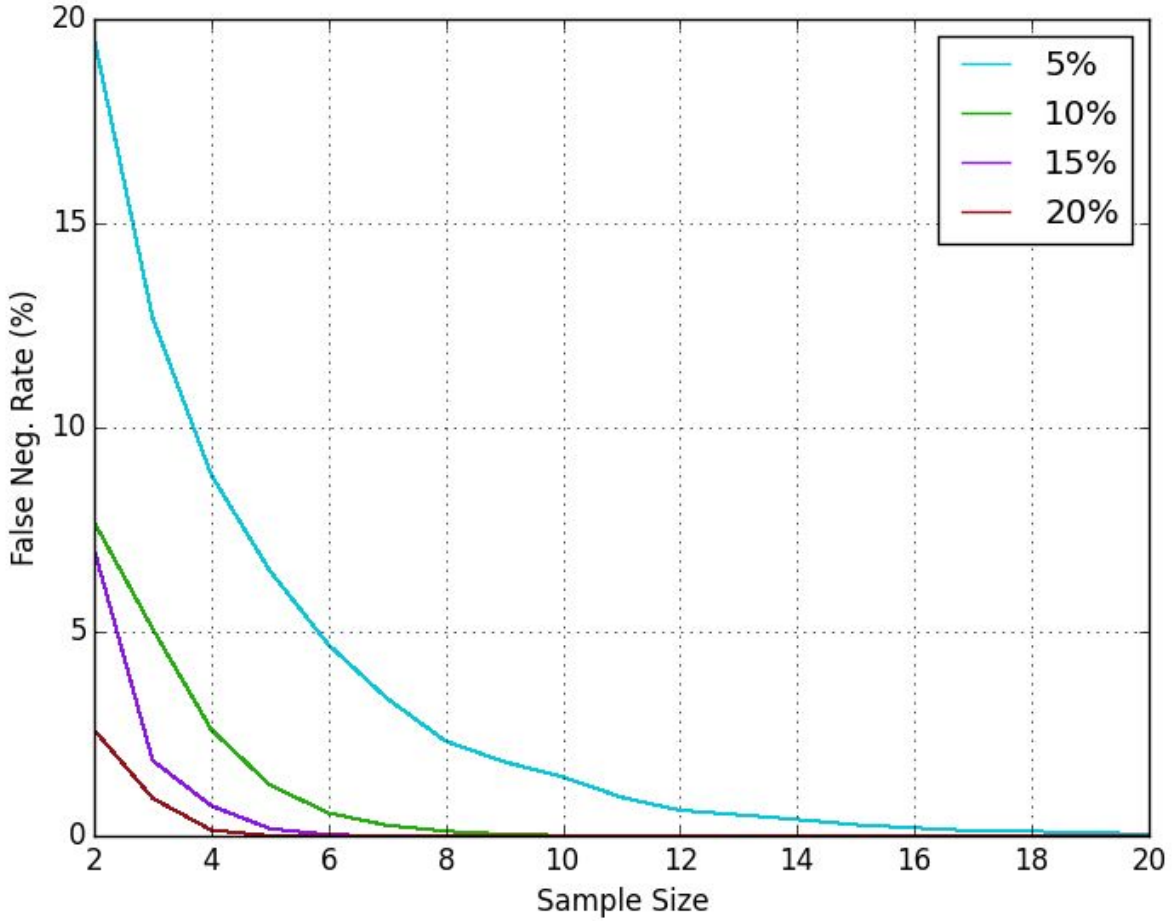




Results

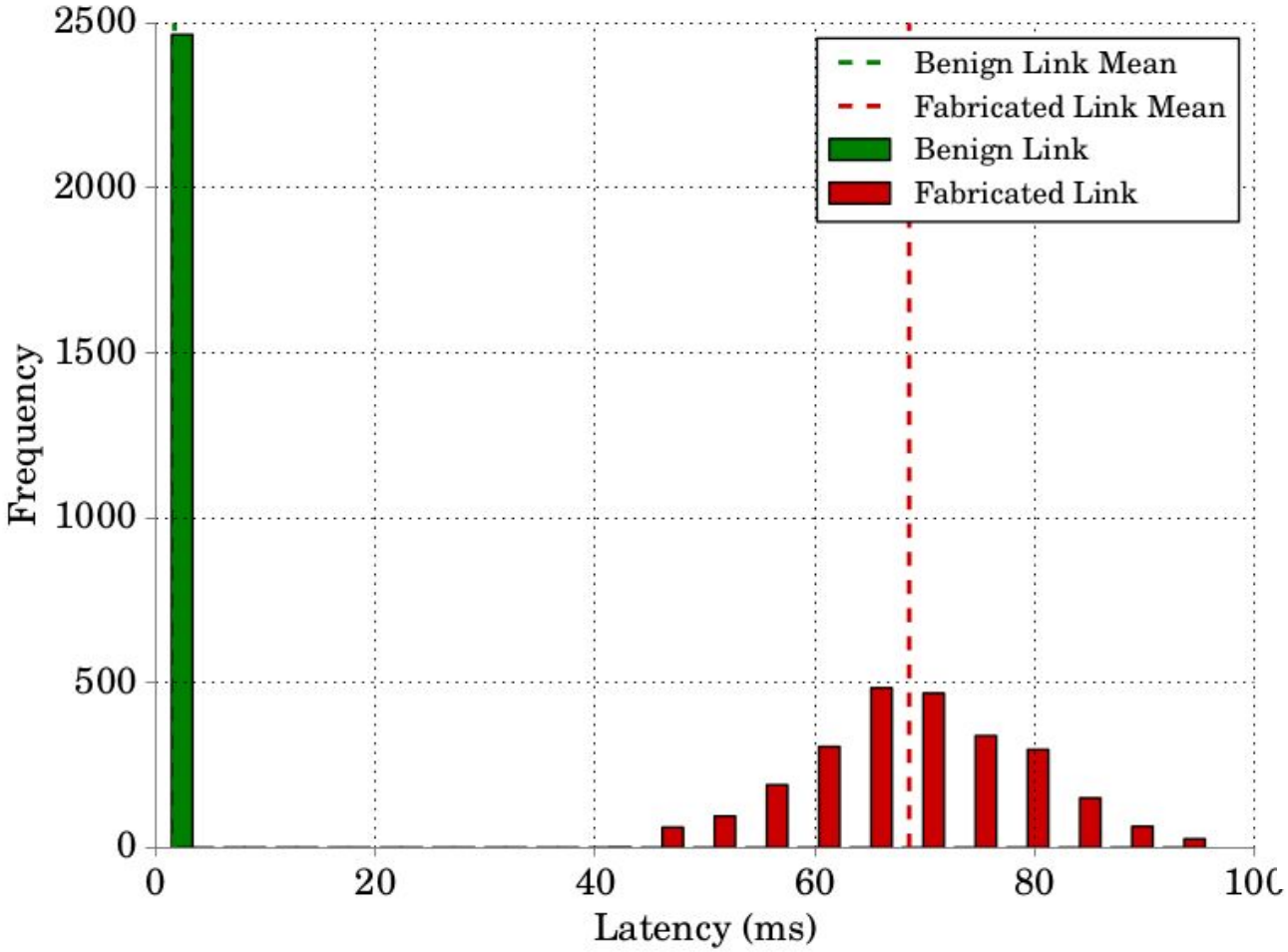
- False Negative Rate for bridging via out-of-band Infra.

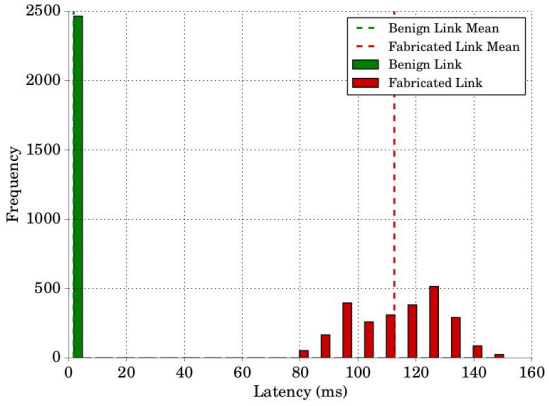




Results

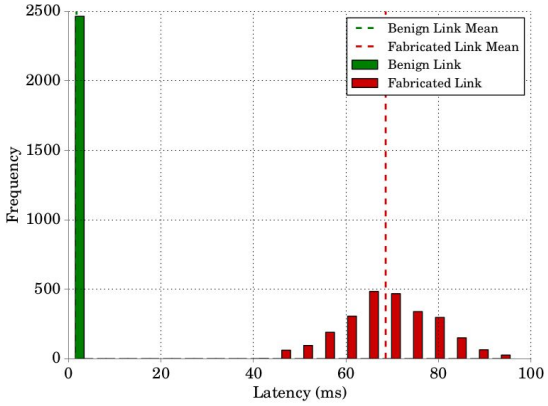
- Distribution for dual-homed Python forwarding

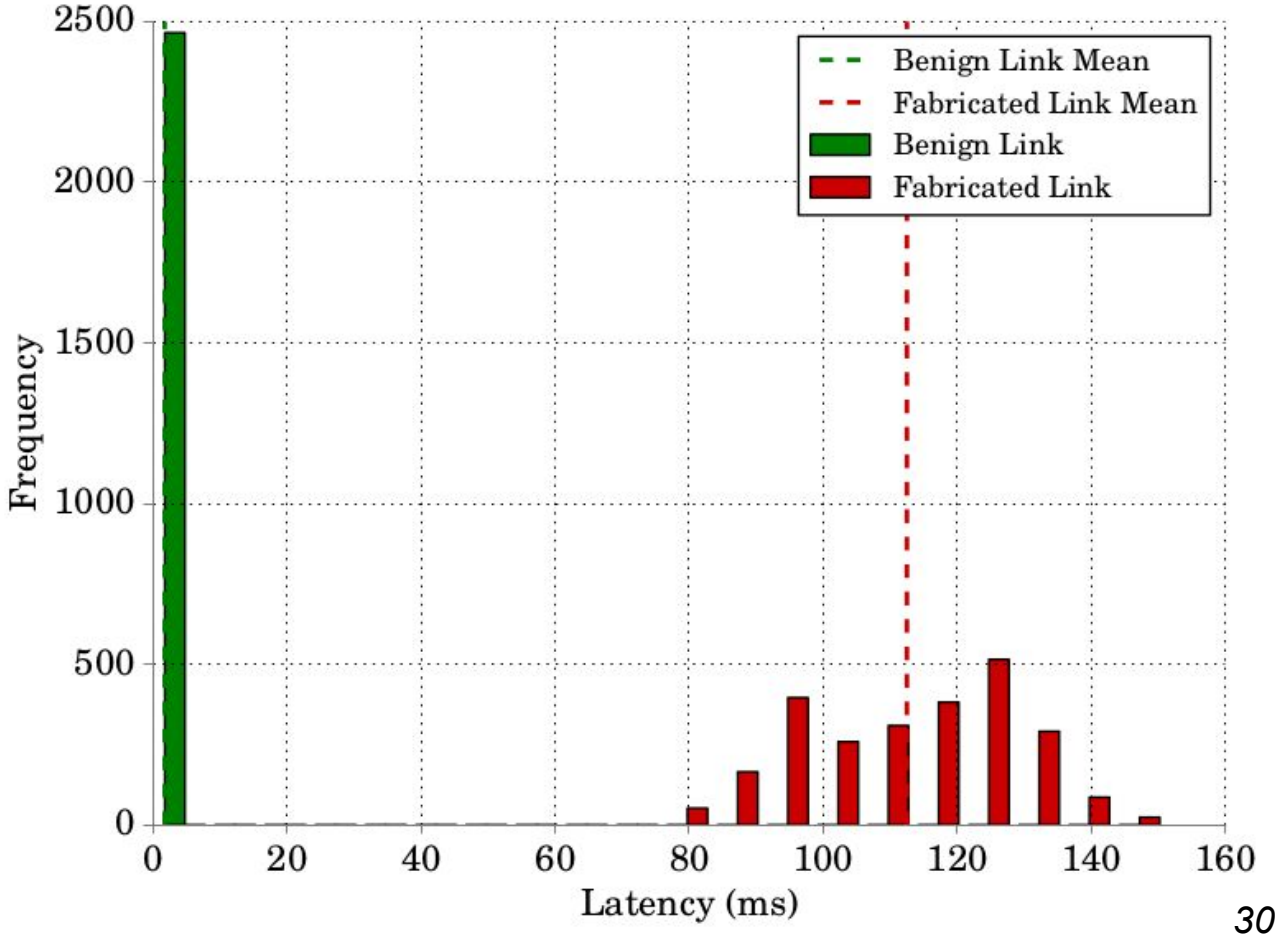




Results

- Distribution for Python forwarding via Ad-Hoc





Results

- Samples needed to reduce False Negative Rate > 5%

Relay Type	Threshold			
	5%	10%	15%	20%
Single Host Bridge	NP	NP	NP	NP
Single Host Python Scapy	2	2	2	2
Wireless Tunnel Ad-Hoc	>500	190	51	25
Wireless Tunnel Infra.	6	4	3	2
Multi-Host Python Scapy	2	2	2	2

- Samples needed to reduce False Positive Rate

FPR achieved	Threshold			
	5%	10%	15%	20%
<1%	2	3	5	8
<5%	2	2	2	5

Conclusion and Future Work

- Link latency can reveal a fabricated link
- Designed a solution to detect a fabricated link
- Evaluated the accuracy of the solution in simulations
- Use alternative statistical tests
- Test effectiveness of technique in other scenarios

CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

http://www.cit.ie

Thank you