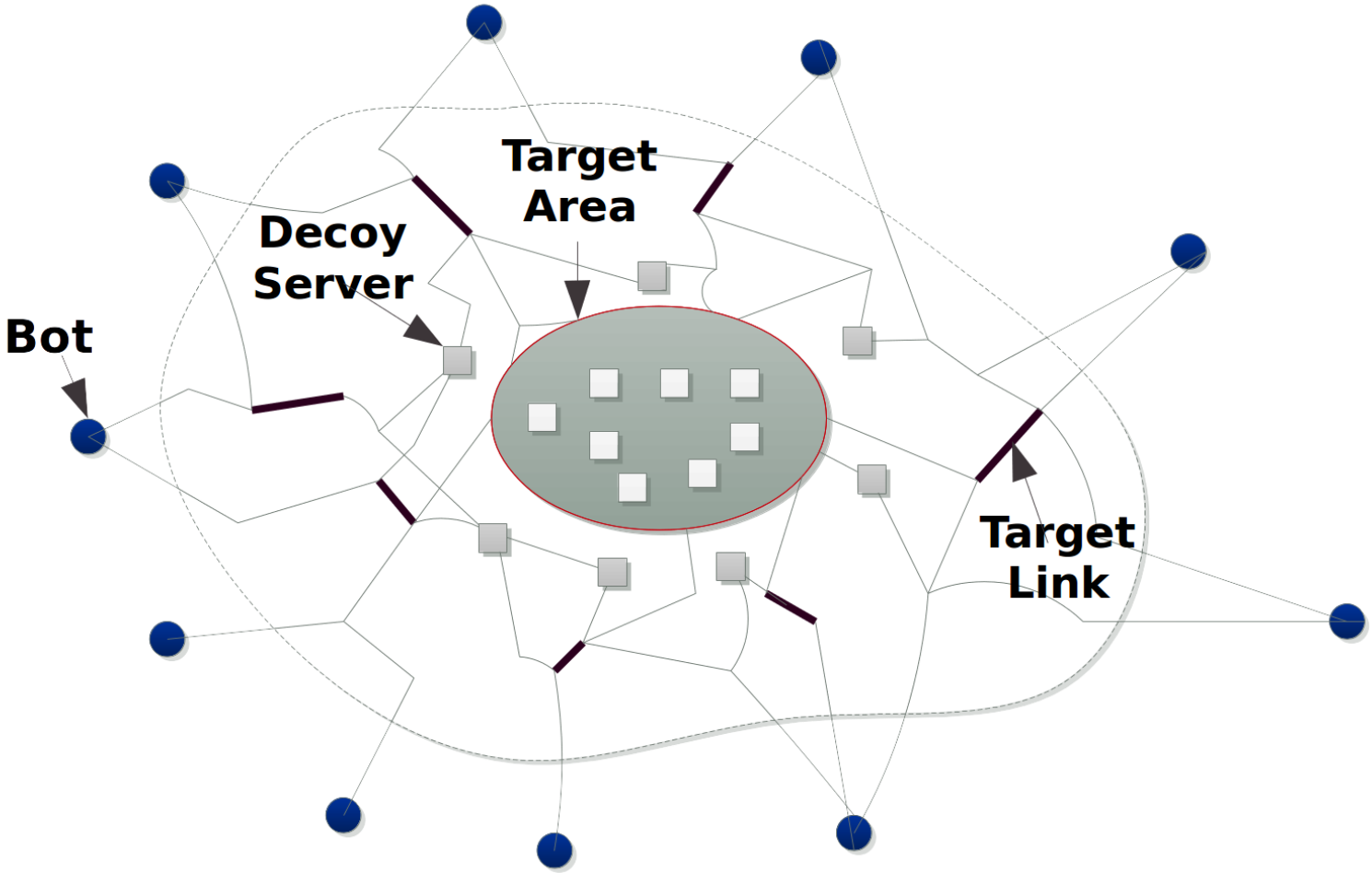
Towards Detecting Target Link Flooding Attack

Lei Xue[+], Xiapu Luo[+↱], Edmond W. W. Chan[+], and Xian Zhan[+]
Department of Computing, The Hong Kong Polytechnic University[+]
The Hong Kong Polytechnic University Shenzhen Research Institute[↱]
{cslxue,csxluo}@comp.polyu.edu.hk, {edmond0chan,chichoxian}@gmail.com

Target Link Flooding Attack



Challenges for Detection

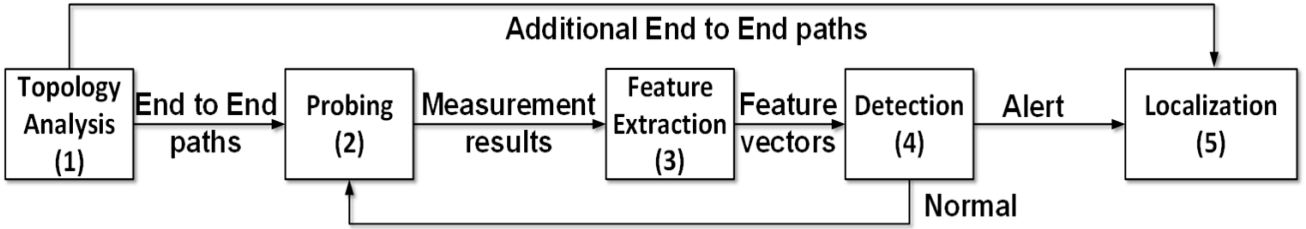
- Attackers use low-rate and legitimate traffic for LFA.
- Target links are not in the target area.
- Attackers can change target links.
- Prevalence of asymmetric routes.

LinkScope

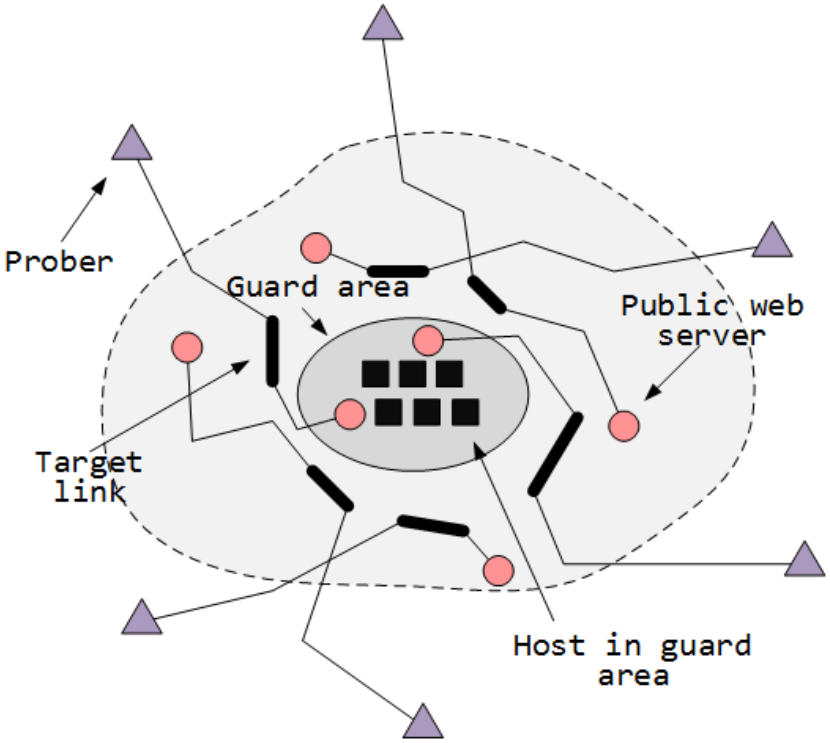
Basic idea

- Congestions caused by LFA will result in anomalies in network path performance.
- Conduct end-to-end active network measurements to capture the anomalies.
- Propose new non-cooperative network measurement approaches to measure a large amount of network paths without the need of controlling the other end of each path.
- Combine both end-to-end and hop-by-hop measurement to locate target links on the forward path.

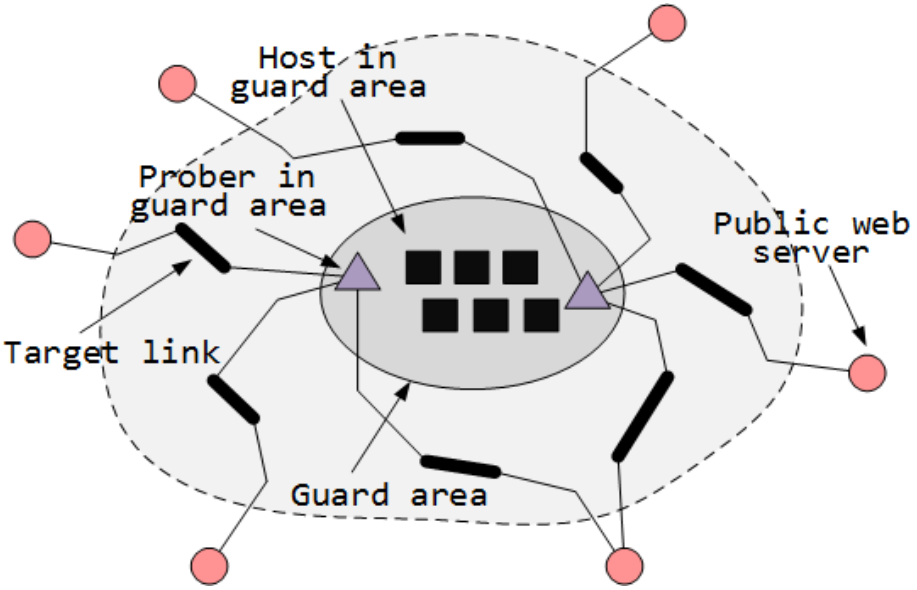
Detection process



Deployment Strategies



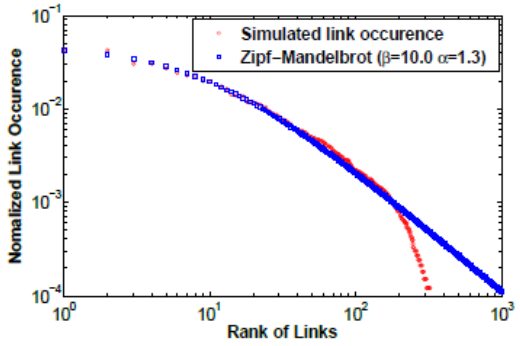
Probe to client



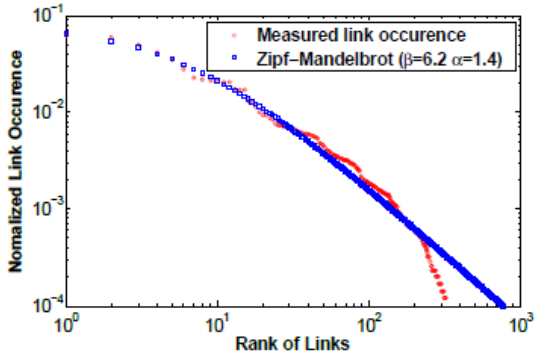
Probe from client

Topology Analysis

- **Persistent links with high Link-occurrence are selected as the conditional monitor links.**



(a) Link-occurrence/rank of routes to Hong Kong



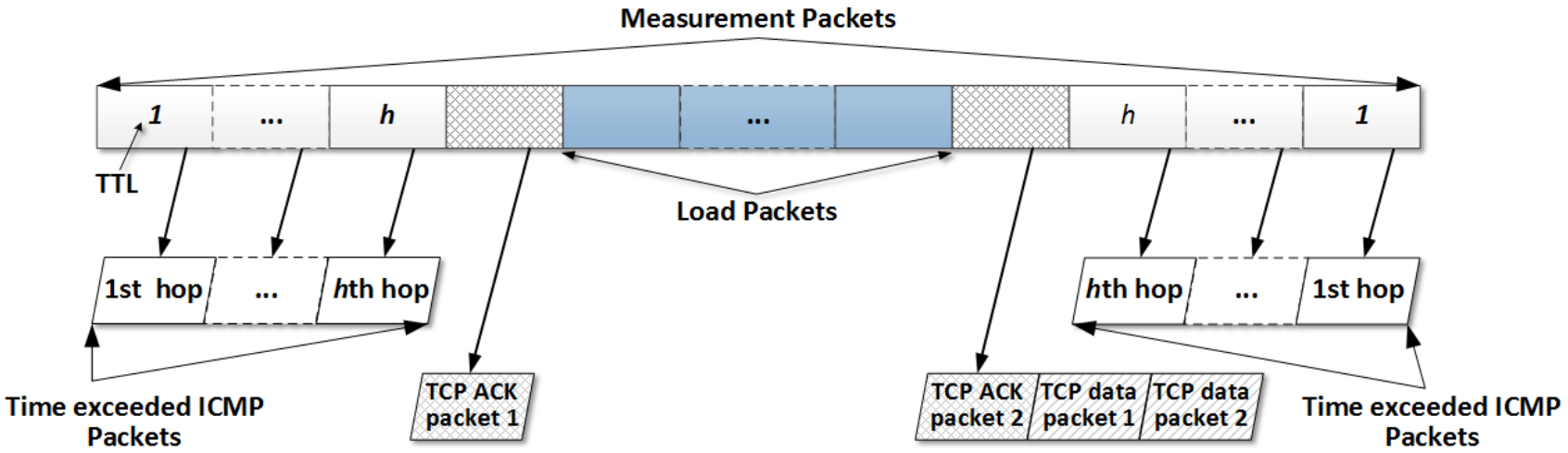
(b) Link-occurrence/rank of routes to Taiwan

- **Monitor path selection.**
  - Paths that contain one target link will be selected.
  - Minimize the number of paths having the same remote host.
  - Minimize the number of paths initialized by one prober.

Probe Approaches

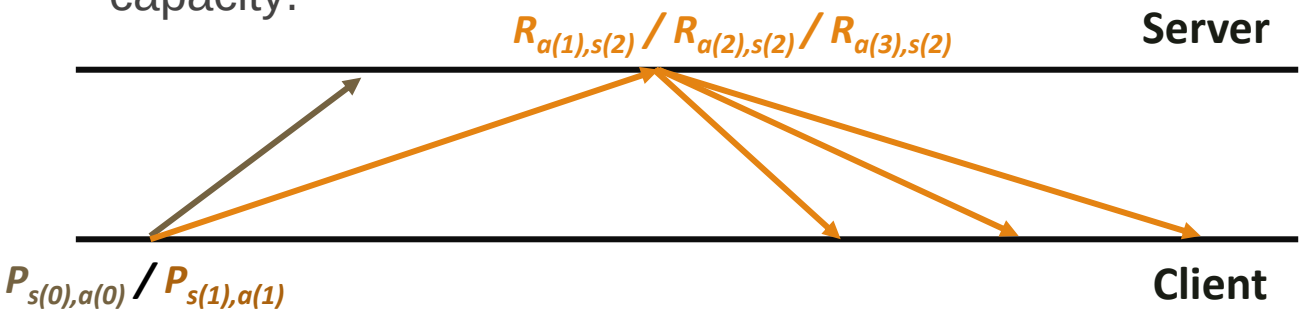
Round Trip Probing (RTP)

- Per-hop RTT, Per-hop θ_e.

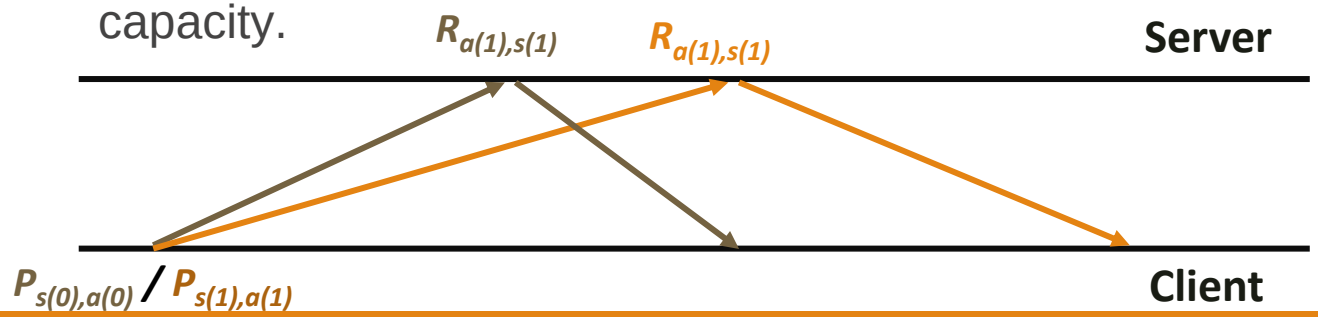


Probe Approaches

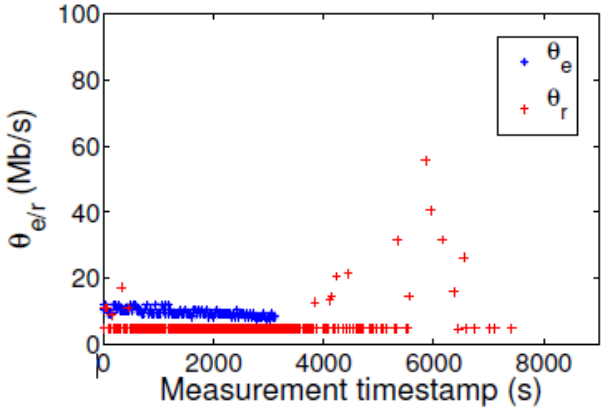
- **Extended Two Way Probing (eTWP)**
  - Packet loss, Packet reordering, RTT, RTT jitter, Backward capacity.



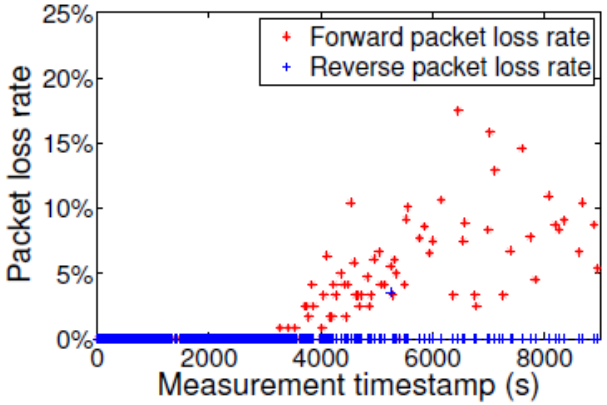
- **Modified Recursive Packet Train (mRPT)**
  - Packet loss, Packet reordering , RTT, RTT jitter, Forward capacity.



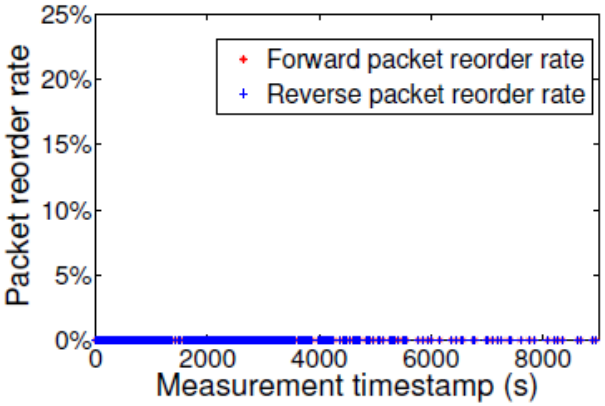
Detection



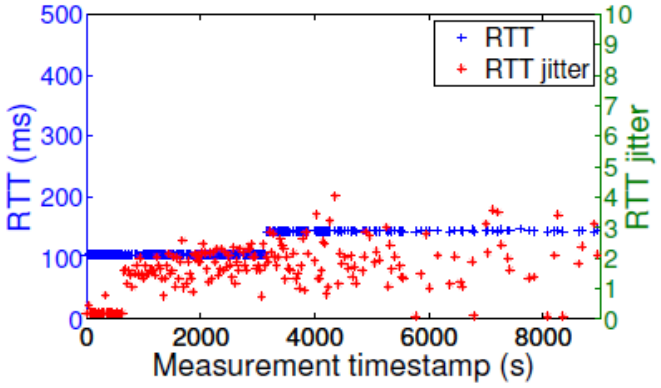
(a) $\theta_{e/r}$



(b) Packet loss.



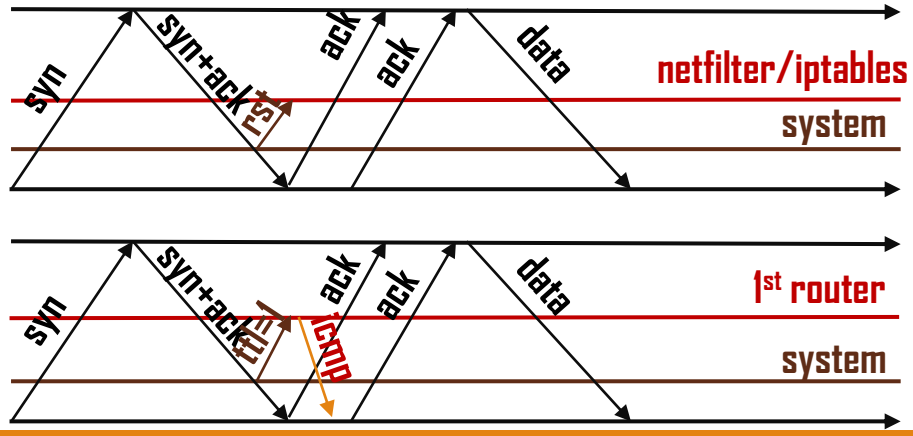
(c) Packet reorder.



(d) RTT and RTT jitter.

Implementation

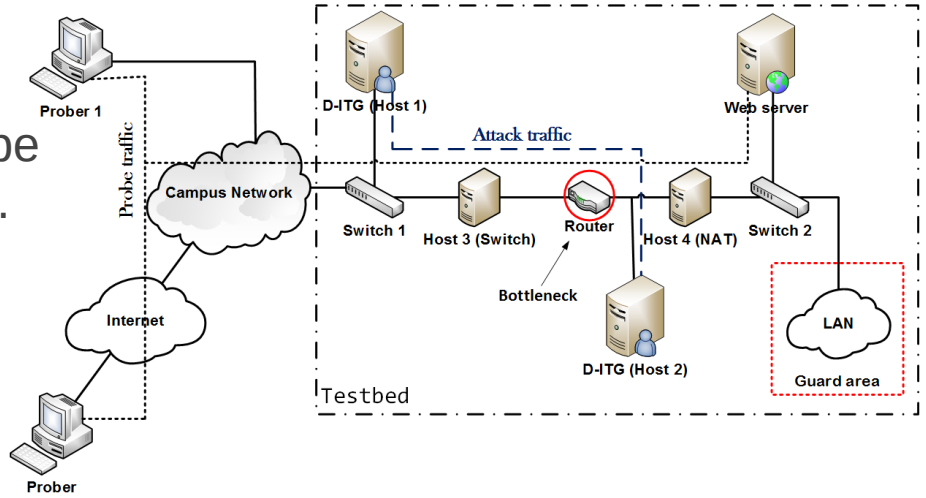
- **Measurement manager**
  - Collect basic information about the path.
  - Enumerate suitable web objects in a web server.
  - Schedule probing processes.
- **Measurement engine**
  - Construct TCP connections.
  - Do probes.
- **RST packet filter**
  - IPTables.
  - Modify TTL.



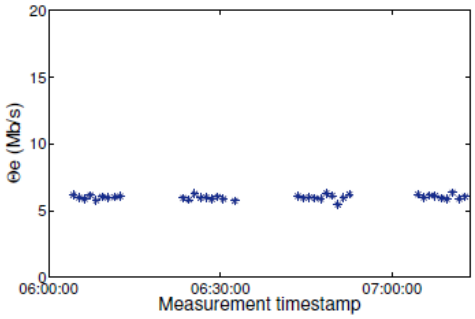
Evaluation in a Test Bed

Goal

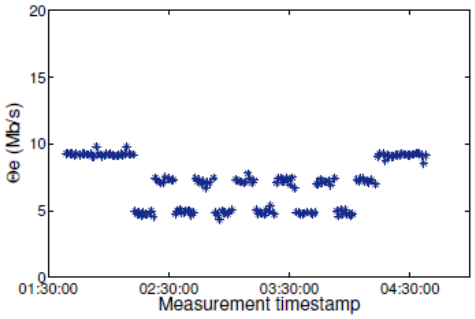
- To validate whether LinkScope can detect different kinds of LFA.



Results



(a) Pulsing LFA.



(b) LFA with variant attack traffic rates.

Detection rate.

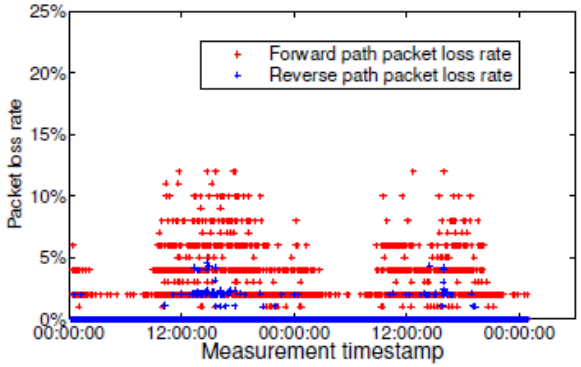
Training data	path	$\alpha = 10$	$\alpha = 20$	$\alpha = 30$
20 probes	path 1	100.0%	100.0%	100.0%
20 probes	path 2	100.0%	100.0%	100.0%
40 probes	path 1	100.0%	100.0%	100.0%
40 probes	path 2	100.0%	100.0%	100.0%

Internet Experiments

Goals

- To evaluate the false positive of LinkScope and characterize network paths' performance.

Result



False positive rate on paths to Hong Kong.

Prober type	Path	$\alpha = 20$	$\alpha = 30$	$\alpha = 40$	$\alpha = 50$	$\alpha = 60$
EC2	Virginia - Hong Kong	6.23%	5.03%	3.84%	3.18%	2.78%
EC2	Sydney - Hong Kong	5.26%	3.42%	3.02%	2.89%	2.76%
EC2	Tokyo - Hong Kong	3.92%	3.01%	1.96%	1.57%	1.57%
EC2	California - Hong Kong	6.07%	4.22%	3.30%	3.17%	3.03%
PL node	Tokyo - Hong Kong	3.53%	2.75%	1.96%	1.57%	1.44%
PL node	Amsterdam - Hong Kong	1.32%	1.19%	0.79%	0.79%	0.66%
PL node	Beijing - Hong Kong	1.95%	1.56%	1.30%	1.04%	0.91%
PL node	South Carolina - Hong Kong	0	0	0	0	0

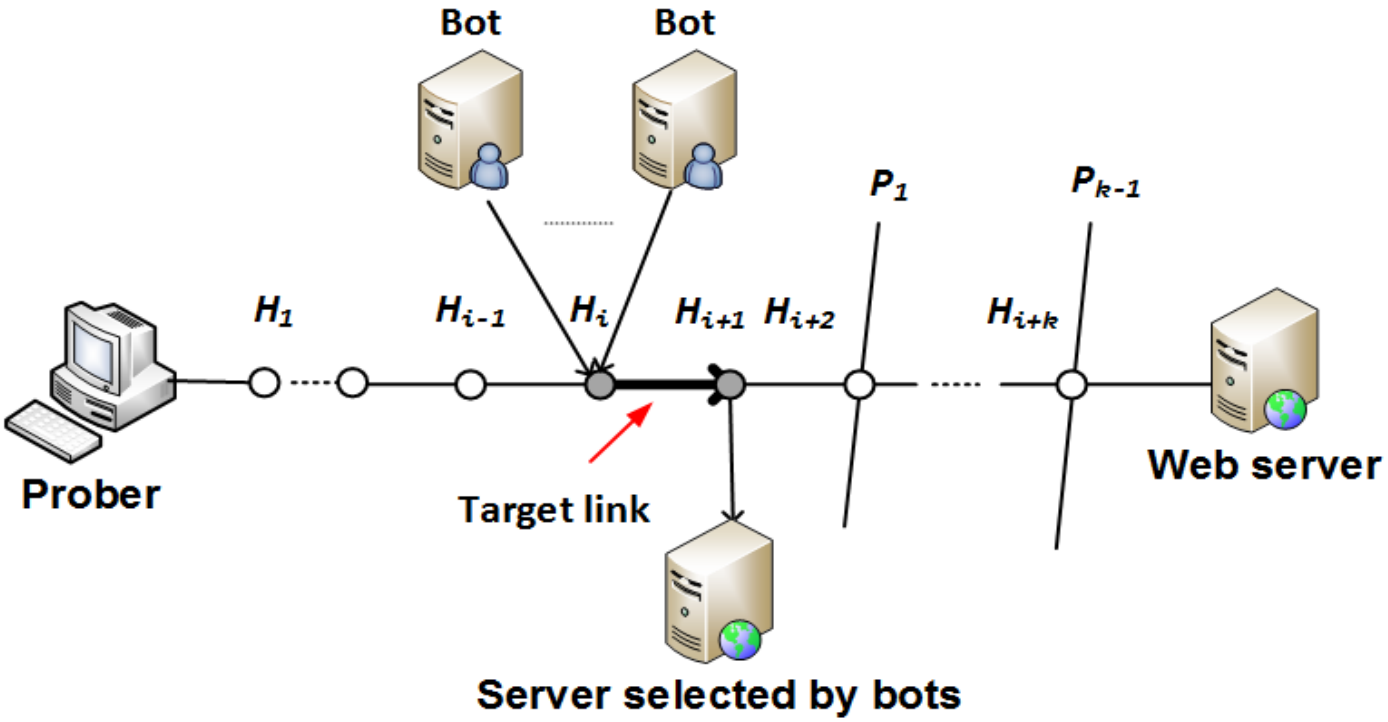
Conclusion

- **Propose LinkScope, a non-cooperative measurement based system to detect LFA.**
- **LinkScope employs both end-to-end and hop-by-hop network measurement to capture anomlies.**
- **Evaluate LinkScope in a test bed and through Internet. experiments.**
- **Future work.**
  - Decide optimal deployment strategy.
  - Conduct large-scale and continuous measurements.

Thanks !

Backup Slides

Locating Target Links



Architecture