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

Diagram showing the process:
1. Topology Analysis
2. End to End paths
3. Probing Measurement results
4. Feature Extraction Feature vectors
5. Detection Alert Localization

Additional End to End paths
Deployment Strategies

Probe to client

Probe from client
Topology Analysis

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

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 $\theta_e$. 

![Diagram of Round Trip Probing (RTP)]
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.

![TCP connection diagram](image-url)
Evaluation in a Test Bed

➢ Goal
  ▪ To validate whether LinkScope can detect different kinds of LFA.

➢ Results
Internet Experiments

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

- Result
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 anomalies.
- 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

Diagram showing the relationship between the Prober, Bots, Target link, and Web server.
Architecture