

MORPHOS

A Method Of Recognizing Prefix Hijacks Of
Stealthiness

Author: Christian McArthur

Prefix Hijacking

- Border Gateway Protocol (BGP) vulnerable due to its trusting nature.
- Attacker falsely announces either it originates a prefix (or subprefix) or that it has a route to the prefix.
- Existing research almost entirely focuses on large scale attacks.

Stealthy Prefix Hijacks

- Attacker announces a path to the victim short enough to attract some traffic, but long enough its effects are not wide scale.
- “Stealthy IP Prefix Hijacking: Don't Bite Off More Than You Can Chew”, SIGCOMM 2008 Poster, Christian McArthur and Mina Guirguis

Detecting Stealthy Prefix Hijacks

- No one detection mechanism seems to be able to detect stealthy hijacks.
- Proposal: Combine two ineffective detection methods to become effective.
 - 1) Comparison between AS Traceroute & BGP routing announcements.
 - 2) Comparison of traceroutes between the target/victim and a reference point.

Term Project Goals

- Implement MORPHOS.
- Tests on the Internet:
 - Determine how the aspects of MORPHOS work with the actual Internet
 - Determine what thresholds prevent false positives.
- Simulate stealthy prefix hijacking.

MORPHOS Implementation

- 1) Perform IP traceroute to the target.
- 2) For each router in the traceroute, convert IP address to AS number.
- 3) Compare AS traceroute to BGP route.
- 4) Perform AS traceroute to reference point.
- 5) Compare AS traceroutes of target & reference point.

IP Traceroute

- Raw socket
- ICMP ECHO requests
- Incrementing TTL value starting from 1 until:
 - Target responds (ICMP type 0)
 - No response for 5 seconds.
 - TTL exceeds 30
- IP address of responding routers stored.

IP Address to AS Number Mapping

- IP-AS mapping file obtained from CAIDA.
 - Derived from Routeviews data from Oct. 15.
- Longest matching prefix from mapping file for each IP address found.
- IP Address & AS number stored.

AS Traceroute to BGP Route Comparison

- BGP Routing data can be obtained from a network's border router.
 - For this project, data from Routeviews (Oct. 28) was used.
- Find the longest common subsequence between the AS Traceroute & BGP Route.
 - Multiple routes for a single prefix may exist. Use the longest LCS.

Target & Reference Point Comparison

- AS Traceroute to reference point performed & compared to traceroute already performed for target.

- Determine similarity:

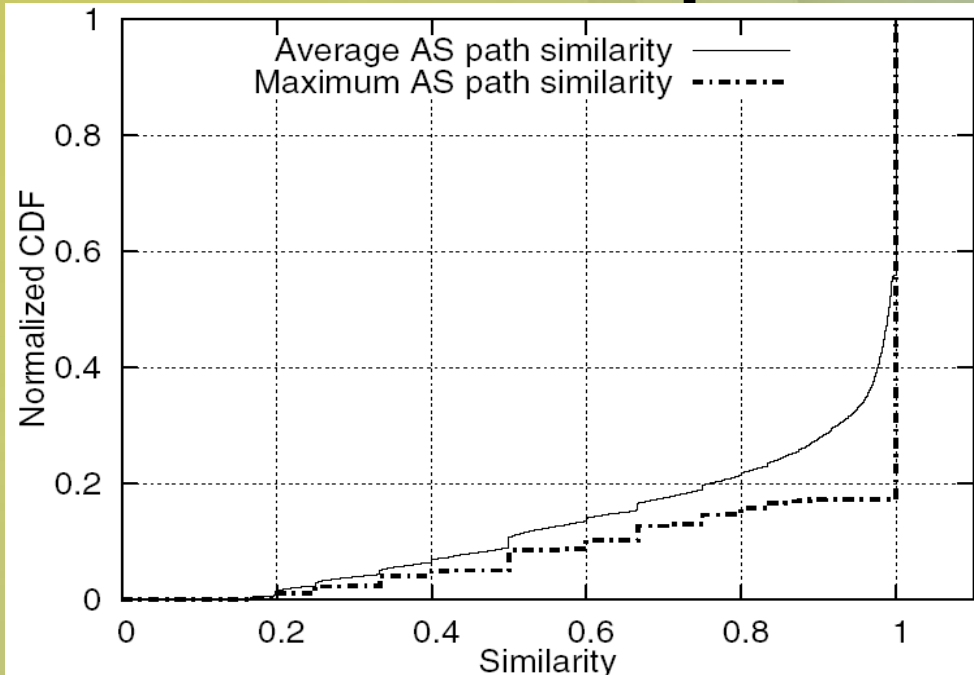
$$\text{similarity} = 1 - d(t,r) / l(r)$$

$d(t,r)$ = hamming distance between target & ref. pt.

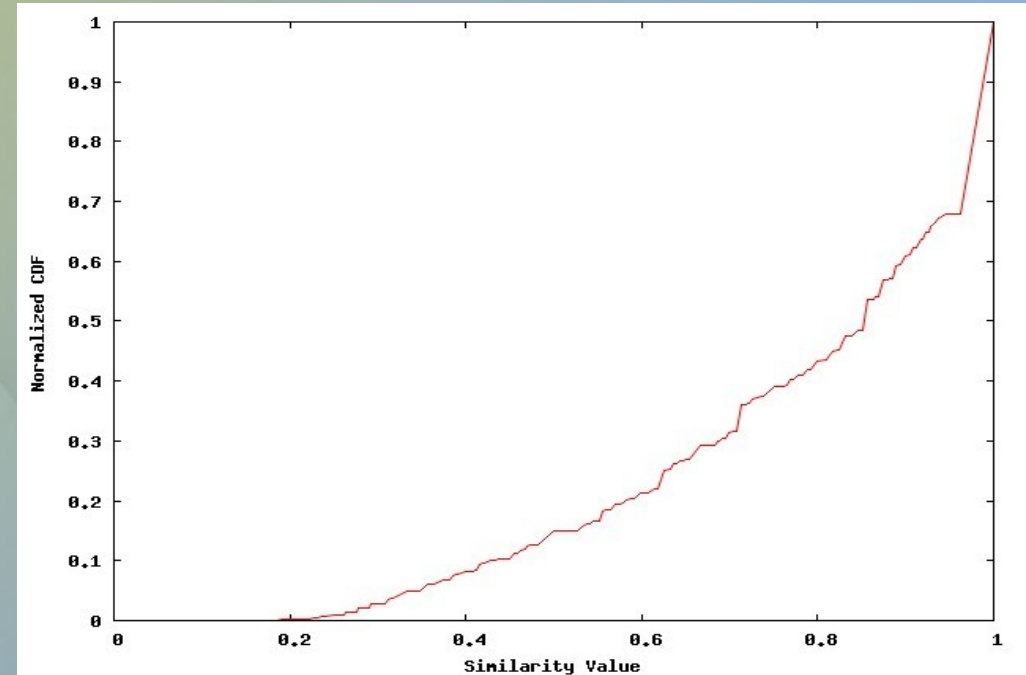
$l(r)$ = length of route to ref. pt.

“A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-Time”, C. Zheng, L. Ji, D. Pei, J. Wang, P. Francis

Target & Reference Point Comparison Results



80% of routes have similarity of 0.8 or better.

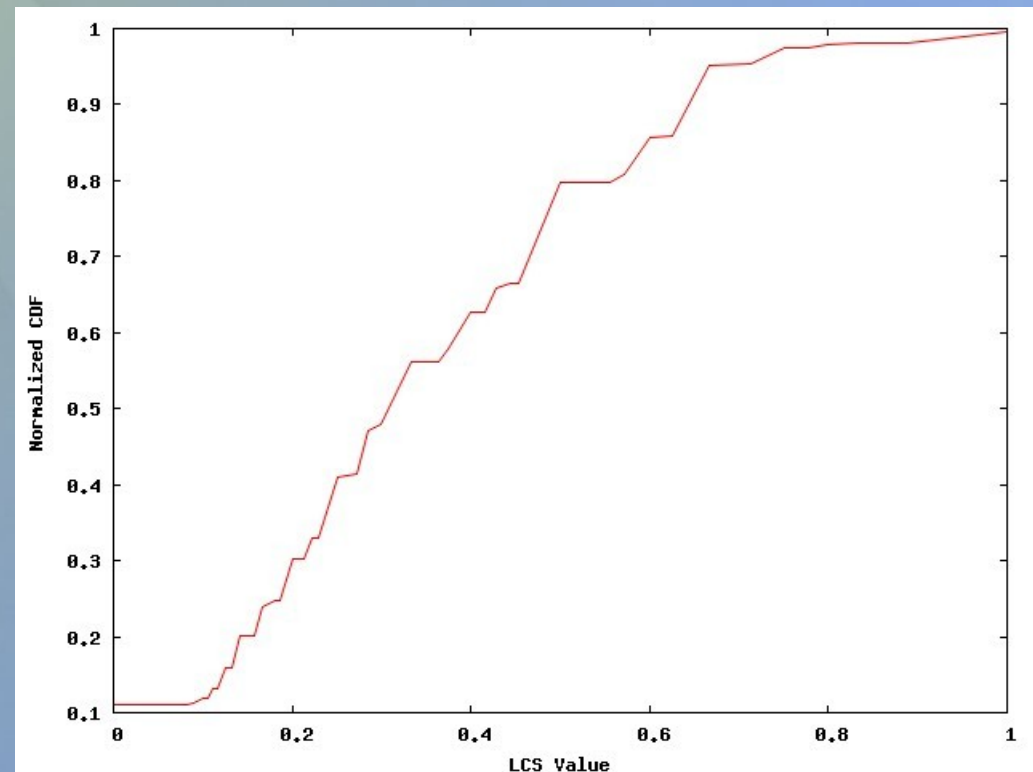


80% of routes have similarity of only 0.6 or better.

60% of routes with similarity of 0.8 or better.

AS TraceRoute & BGP Route Comparison Results

- 50% of routes match only 30% of the available BGP announcements.
- Average number of unique ASes in a route: 5.9
- Average LCS of route & BGP announcement: 1.9



Prefix Hijack Simulator

- Build AS Trees for target & reference point.
- Perform MORPHOS algorithm on these two trees.
- Build AS Tree for target under hijacking conditions.
- Perform MORPHOS on hijacked tree & reference point.

To-Do List & Future Work

- Data reported thus far covers only half of the prefixes on the Internet. Continue scanning prefixes and collect data.
- Data is from a single viewpoint on the Internet. Data collection from multiple viewpoints would provide better information.
- How does data differ in a prefix hijacking (stealthy or otherwise)? Collect expansive data from simulator.