Detecting Third-party Addresses in Traceroute IP Paths

Pietro Marchetta  Walter de Donato  Antonio Pescapé
Dipartimento di Informatica e Sistemistica, University of Napoli “Federico II”
{pietro.marchetta, walter.dedonato, pescape}@unina.it

The Third-party Addresses Phenomenon

A third-party (TP) address is an IP address which does not belong to the actual IP path toward the destination.

Proposed Methodology:

routers processing the prespecified IP timestamp option [2] commonly insert their own timestamp only if the packet passes through the interface associated to the prespecified address [4].

Being IPx an IP address discovered by Traceroute toward the destination D:

- Ping IPx prespecifying IPx
- IPx provides at least one timestamp: No
- Send UDP probe toward D prespecifying IPx
- IPx provides at least one timestamp: No
- Ping IPx prespecifying IPx
- IPx is not Classifiable!

Is IPx a third-party address?

- Send UDP probe toward D prespecifying IPx
- IPx is on the actual IP path! (Incoming Interface)
- IPx is a third-party address!

Measurement Campaign: to evaluate the proposed approach, we randomly selected 50K destinations among the ones showing stable responsiveness according to the PREDICT project [1]. About 13K destinations replied to UDP probes carrying the TS option. A Traceroute campaign toward those destinations collected a final dataset of 32K IPs.

Preliminary Results

- A single TP address affected several traces:
  - 7.8 traces on average.
  - 7.3K traces at most.

AS-level analysis

- Mapping each IP to the owner AS [3], we found 1.9K distinct ASes and about 2K AS-level links.
- 526 links (26% of total links) involved TP addresses — potential false links.

TP addresses have been not considered as a significant source of AS map distortions [6].

This claim was supported by a limited approach.

References