Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

TUM

Thesis B.Sc.

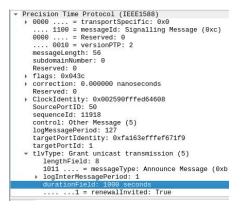**Thesis M.Sc.**

IDP

Uncovering
PTP Master Clocks in the Wild

Motivation

The Precision Time Protocol (PTP) is a clock synchronisation protocol designed for local networks. Compared to the Network Time Protocl (NTP) it promises better accuracy with a sub-microsecond range.

Even though it is specifically designed for local networks, so called master clocks are publicly available in the Internet. Triggered with the correct PTP message, these master clocks start sending PTP messages. As shown in the image, some clocks even initiate a connection that sends 1000 packets with a frequency of 1 pps.

Because PTP promises a high accuracy, most of these clocks are attached to a precise time source, e.g. GPS. Knowledge about responsive clocks in the Internet, their location and their behavior provides a promising pool of precise time sources for future measurements.

The goal of this thesis is to find a possibility to identify PTP master clocks in the Internet and extend ZMAP to be used for active scans. After supervised scans in close collaboration with your advisors, the behavior of found master clocks should be analyzed and categorized.

```
▼ Precision Time Protocol (IEEE1588)
  ▶ 0000 .... = transportSpecific: 0x0
    .... 1100 = messageId: Signalling Message (0xc)
    0000 .... = Reserved: 0
    .... 0010 = versionPTP: 2
    messageLength: 56
    subdomainNumber: 0
    Reserved: 0
  ▶ flags: 0x043c
  ▶ correction: 0.000000 nanoseconds
    Reserved: 0
  ▶ ClockIdentity: 0x002590fffed64608
    SourcePortID: 50
    sequenceId: 11918
    control: Other Message (5)
    logMessagePeriod: 127
    targetPortIdentity: 0xfa163efffef671f9
    targetPortId: 1
  ▼ tlvType: Grant unicast transmission (5)
      lengthField: 8
      1011 .... = messageType: Announce Message (0xb
    ▶ logInterMessagePeriod: 1
      durationField: 1000 seconds
      .... ...1 = renewalInvited: True
```

Your Task

- Develop an approach to effectively detect PTP capable device in the Internet
- Set up supervised scans based on ZMAP
- Extend a pcap library to parse PTP
- Analyze reachable PTP hosts

Requirements

- Basic programming knowledge in Python or Go
- Familiarity with GIYF-Based work approaches

Contact

Johannes Zirngibl   zirngibl@net.in.tum.de
Max Helm   helm@net.in.tum.de
Henning Stubbe   stubbe@net.in.tum.de

https://net.in.tum.de/members/zirngibl/