Efficient Processing of Large Network Captures

The uncountable numbers of devices in networks pose a new challenge for monitoring tools: they generate large amounts of network data. This data needs to be processed to generate meaningful insights into a monitored network. Standard methods for processing large amounts of network data take long and are therefore not sufficient. This fosters the need for highly efficient network data (pre-) processing mechanisms.

The goal of this thesis is to develop and implement a pipeline for efficiently parsing and processing network-data at large scale. Therefore, an analysis about existing parsing methods needs to be conducted with respect to their efficiency. Further, a common denominator in network data needs to be found such that data from different sources can be processed and stored in a standardized way. Finally, after processing data, it needs to be stored in an accessible way such that different applications can benefit from the preprocessing and further process the data.

- Analysis of network data processing methods
- Comparison of existing approaches
- Implementation of an own data-parsing pipeline
- Comparison of the developed approach to naive methods.

- Basic network knowledge
- Ability to write efficient and maintainable code
- Experience in Go is a plus

Sources

Lars Wüstrich       wuestrich@net.in.tum.de
Johannes Zirngibl    zirngibl@net.in.tum.de
Christian Lübben    luebben@net.in.tum.de
http://go.tum.de/080755