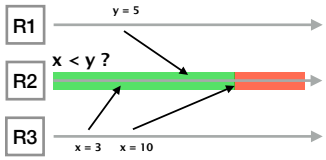
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

Network monitoring with Linear Temporal Logic

Master thesis proposal

Linear Temporal Logic (LTL) [2] is often used in model checking or verification tasks. An example is runtime verification of software. We can e.g. use LTL to formulate predicates such as "the value of a variable x is *always* smaller than variable y". Different algorithms can be used to monitor these predicates and notify a monitoring system whenever a violation occurs.



In network monitoring, we would like to use similar approaches but until recently, the closed nature of most network devices made the use of LTL difficult. With the recent advances in reprogrammable hardware [1] and domain-specific programming languages, such as P4 [3], usage of LTL in communication networks is feasible.

This master thesis explores the possibilities of P4-based LTL in network monitoring/verification. Main questions are: What can we achieve with LTL? How can we efficiently implement LTL formulas on network devices? And how can we cope with the distributed nature of communication networks? More precisely, the work can be roughly divided into the following work packages:

- **WP1**: Exploring the possible use cases. Which network properties can be monitored/verified with the help of LTL? Should we work on a per-flow basis or on a higher level, e.g. traffic forwarding between nodes? Given the capabilities of P4, which LTL primitives can we implement efficiently?
- **WP2**: P4-based implementation of LTL formulas on a *single* device. A possible monitoring objective could be: "a router should only receive traffic for prefixes which it has previously announced via BGP."
- **WP3**: Consider the distributed nature of networks. How can we implement LTL formulas requiring state/observations from multiple devices? How can we exchange information between them? How often do we have to exchange state?

The following two papers could be used as inspiration for efficient monitoring [4] in distributed systems [5] using LTL.

Requirements

- Experience with P4 programming is helpful but not required.

Contact

- Tobias Bühler, buehlert@ethz.ch
- Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch

References

[1] Barefoot Tofino P4 switch. `https://www.barefootnetworks.com/products/brief-tofino/`.

[2] Linear Temporal Logic. `https://en.wikipedia.org/wiki/Linear_temporal_logic`.

[3] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker. P4: Programming protocol-independent packet processors. *SIGCOMM Comput. Commun. Rev.*, 2014.

[4] K. Havelund and G. Roşu. Efficient monitoring of safety properties. *International Journal on Software Tools for Technology Transfer*, 6, 2004.

[5] K. Sen, A. Vardhan, G. Agha, and G. Rosu. Efficient Decentralized Monitoring of Safety in Distributed Systems. In *Proceedings of the 26th International Conference on Software Engineering*, 2004.