Intern Position 2025

Title: Formalizing the Optimization Problem for a Secure Multicontroller SDN Network.

Host laboratory: LIP, ENS de Lyon, 46 allée d'Italie, Lyon, France

Advisors:

Loïc Desgeorges MCF UCBL `loic.desgeorges@ens-lyon.fr`

Starting Date: As soon as possible, after January 2025.

Keywords: Optimisation, SDN, control plane, security and consensus

Description.

Today's networks are managed by administrators based on metrological and monitoring information to react to changes in traffic and communication infrastructure failures. A possible architecture consists in automating this network management by deploying network controllers, dynamically capable of detecting and even anticipating the occurrence of changes in network system states and programming its reconfiguration as in the Software-Defined Networking (SDN) architecture. This centralized approach is increasingly used by companies such as Google, the world's number 1 network, which has part of its infrastructure under SDN. SDN controllers are solely responsible for controlling the network. As a result, service on the network is degraded (even blocked) in the event of controller failure or attack. From a security point of view, it seems necessary to consider architectures with multiple controllers, thus avoiding the single point of failure/invasion and ensuring redundancy. Since even if a controller is only in charge of a subnetwork, it must have access to all network information to make decisions. Hence it is necessary to introduce a communication interface between controllers which introduces latency in the communication. This interface (named East-West) can be insecure, requires active maintenance of the connection, and does not benefit from recognized standardized protocols. Thus, an attack can be spread though it by the transmission of bad information [1].

The objective is to propose a reliable control architecture to guarantee a certain level of quality of service on the network, while maintaining a high level of security. Indeed, the introduction of a security mechanism has a cost in terms of performance. Here, we propose to secure the controller decision-making to limit the impact of an attacker by setting up a consensus between the various controllers. The problem of implementing consensus in a multi-controller control architecture is to strike a balance between reactivity and security. Indeed, a consensus may take time to reach (a complexity in $\mathrm{O(n^2)}$ where n is the number of consensus participants). This time is a latency for setting up the data plane and has a direct impact on network quality of service (QoS). Thus, increasing the number n of consensus participants complicates the task of attackers, but increases latency between controllers and thus on the network. The originality of the intership lies in the search for a compromise on the number of controllers participating in the consensus, which is essential for scaling up, to guarantee both a correct level of security and a correct level of quality of service. This compromise can be formalized though an optimisation problem as in [2] and the first objectif is to formalise it.

Candidate Requirements.

- The candidate should have completed a qualifying program by the starting date of the intership.
- Comfortable speaking English or French (French is not required).
- Optimization knowledge and network skills (preferably both)

- Good proficiency with at least one programming language, preferably Python.

What to submit. An up to date CV, university transcripts, and a letter of motivation clearly stating what the motivations to work on the described subject.

References

[1] L. Desgeorges, J.-P. Georges, and T. Divoux. Detection of anomalies of a non-deterministic software-defined networking control. *Computers & Security*, 129:103228, 2023.

[2] A. Naseri, M. Ahmadi, and L. PourKarimi. Placement of sdn controllers based on network setup cost and latency of control packets. *Computer Communications*, 208:15–28, 2023.