Intern Position 2025

Title: Setting up an observer (based on federated learning) to detect anomalies.

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: Machine learning, detection of anomalies, federated learning, security, SDN, network control

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. This interface (named East-West) presents at least two threats: 1) First, an attacker can propagate their attack. Inter-domain routing requires global trust among controllers, and a malicious controller can share false topologies, similar to a BGP hijack. 2) Second, how can we guarantee that a controller applies the rules resulting from the consensus locally? An attacker could take control of a controller, appear to conform to the consensus, but locally apply different decisions to degrade the service.

In our previous work, we proposed adding an observer to the architecture to detect anomalies in the control [1]. This observer does not communicate with the controllers, which removes the threat of attack propagation via the East-West interface. However, the observer was restricted to detect the anomalies of only one controller. Given the geographical distribution of the controllers and the volume of data, a single observer is insufficient. To improve performance, a network of observers will be considered, posing two main challenges: implementation (how to place the observers?) and the detection algorithm (how to ensure distributed detection?). The objective is to compare the on-device and collaborative learning approaches in terms of precision/recall/accuracy, reactivity (time to trigger an alarm), and security (evaluating the new vulnerabilities introduced by the network of observers).

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).
- Machine Learning knowledge and network skills (preferably both).
- Good proficiency with at least one programming language, preferably Java or 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.