Setting up an observer of an encrypted communication to detect anomalies

I. Context

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) can be insecure, requires active maintenance of the connection, and does not benefit from recognized standardized protocols. Thus, an attack can be spread though this interface by the transmission of bad information in the same way as a BGP hijack. One solution is to introduce a network observe which detect anomalies in the control based on the network traffic.

II. Objective

This objective of the internship aims to extend the detection algorithm. Communication between controllers and switches may require **confidentiality and therefore encryption**. In this case, the observer has no access to the full content of the packets, and in particular to the information exchanged between controllers and switches (i.e., requests or commands). However, the observer does have access to some information, for example in the extreme case where the observer observes no communication at all, then it detects an anomaly probably due to a controller failure. This problem is similar to that of **encrypted traffic classification**, solved using machine learning techniques. Indeed, the observer has access to information such as packet size (to, at least, distinguish between commands, requests and other packets), packet destination and message dates (to assess processing times and determine whether they are abnormal).

It will therefore be necessary to model the controller's behavior on the basis of these observations alone and **infer** whether an anomaly is present or not. This model will make it possible to calculate and infer the plausibility of the commands implemented by the controller.

Place of the internship: LIP, ENS de Lyon

Supervisors: Loïc Desgeorges; loic.desgeorges@univ-lyon1.fr

Skills required: network skills (TCP/IP stack, network performance, notion of QoS). Cryptography knowledge is a plus. Fluency in English.

Starting date: between the beginning of February and the end of March 2024