# SHORT TERM SCIENTIFIC MISSION (STSM) – SCIENTIFIC REPORT

**The STSM applicant submits this report for approval to the STSM coordinator**

**Action number: 15127**
**STSM title: Robustness Analysis for Logically Centralized vs Logically Distributed SDN Networks**
**STSM start and end date: 15/04/2018 to 21/04/2018**
**Grantee name: Dorabella Martins da Silva Santos**

## PURPOSE OF THE STSM

This STSM contributes to the aims of RECODIS WG4 and will be submitted to Chapter 2.4 Reliable Control and Data Plane for Virtualized Environment of the RECODIS COST Action final book. The aim of this STSM was to continue collaboration with Dr. Carmen Mas Machuca in robust SDN controller placement. The previous STSM (in October) on “Selecting the SDN Controllers Placement to Enhance the Network Robustness to Multiple Node Failures” resulted in a best paper award at DRCN 2018 (D. Santos, A. de Sousa, C. Mas Machuca: “Robust SDN Controller Placement to Malicious Node Attacks”).

In this STSM, we extend our study of robust SDN controller placement to include the worst case disruptive attacks based on optimization and consider a more general robustness metric for solution evaluation. This work will be submitted to a scientific journal.

We also consider a study based on a more realistic clustering case, with a majority controller cluster and compare the results with the ideal case. This work will be submitted as an extended paper to Annals of Telecommunications.

Another aspect discussed in this STSM was the logically distributed SDN control plane. Since the logically centralized SDN control plane is not scalable with network size nor with large amounts of traffic due to latencies in intercontroller synchronization, we have also considered the robust controller placement in a logically distributed SDN control plane. In this case, the network is partitioned into domains, each domain having a primary controller and a given number of backup controllers. The gains in robustness and the delay penalties will be compared with the standard domain model. This work will be submitted as a paper to an international conference.

## DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

In the extended version of the robust controller placement problem (CPP), we have considered another type of attack besides the centrality-based attacks presented in the DRCN 2018 paper cited above. This type of attack is based on the worst case disruptive attack and is solved as an integer linear programming (ILP) problem. However, for the networks that we have considered (one with 50 nodes and another with 75 nodes) the ILP is solved in very short runtimes. Just as for the centrality-based attacks, also in this type of attack we assume that the attacker has full knowledge of the switching plane topology, but does not know where the controllers are placed.

To evaluate the solutions for robustness against the attacks including this more disruptive one, we have considered the same robustness metric as before, but also a more general one (more suitable to assess the robustness against the worst case attack), which features switch-pair connectivity. We then compare the optimal robust solutions and show that in fact, the worst case attack is in general much more disruptive than the centrality-based attacks. We compare the gains in robustness for both metrics and the penalties of the delays against the optimal non-robust solutions minimizing the delays.

For the robust CPP in the logically distributed SDN control plane, we have considered the network partitioned into domains. Each domain is assigned a primary controller collocated in a switching plane node inside the domain. The goal is to propose controller placement strategies against multiple node shutdowns. So for each primary controller, a given number of backup controllers are assigned to it and these are collocated in switching plane nodes that can be in other domains. In this way, we reduce the necessary number of controller nodes minimizing intercontroller communication delays. The purpose of this model is to assess the delay penalties and robustness gains against the traditional SDN domain model, which is having the primary controller and the respective backup controllers collocated in nodes inside the domain.

**DESCRIPTION OF THE MAIN RESULTS OBTAINED**

Considering the work presented in the DRCN 2018 paper cited above, we have considered the robust CPP problem therein. The problem aims to improve network robustness against $\mathrm{p}$ simultaneous node shutdowns, by placing strategically $\mathrm{C} = \mathrm{p} + 1$ controllers in the network (first level of robustness). The controllers are placed in such a way, that if all controllers but one shut down, the switches can still connect to the surviving controller (assuming only controller shutdown and not switching plane node shutdown – second level of robustness). We then evaluate the solutions obtained against centrality-based attacks and use an evaluation metric to select the optimal solutions (third level of robustness).

We extend this study to include the worst case attack based on the maximum connectivity disruptiveness of the switching network. This attack is based on an optimization problem, which has proven to be solved very efficiently for the networks we have considered. To better evaluate the optimal robust solutions against this attack, we use a more generic metric featuring switch node pair connectivity. The computational results show that the worst case attack is, as expected, much more disruptive than the centrality-based attacks. While these latter do not significantly affect the switch node pair connectivity, the worst case attack shows major damage in the connectivity of the switching plane. However, the gains in robustness of the optimal robust solutions compared with the non-robust optimal solutions aiming at minimizing the delays are very significant.

Another analysis being studied is considering the more realistic clustering scenario. In ONOS and ODL which are the two major SDN implementation platforms, due to database consistency issues, the network tolerates $\mathrm{p}$ controller failures if $\mathrm{C} = 2\mathrm{p} + 1$ controllers are placed in the network. In case of network disruption, only the major component having at least $\lfloor \mathrm{C}/2 \rfloor$ controllers will continue to run, while the other components will await reconnection. If the failures causes disruption in network, such that no component has the at least $\lfloor \mathrm{C}/2 \rfloor$ controllers, the network will idle until reconnection is possible. This contrasts with the ideal case described above of placing $\mathrm{C} = \mathrm{p} + 1$ controllers. We intend to compare both the ideal and realistic cases against $\mathrm{p}$ simultaneous node shutdowns and analyse the gains and penalties in terms of robustness and delays.

In the logically distributed SND control plane, we consider a flat architecture with domains. Each domain is assigned a primary controller and a given number $\mathrm{b}$ of backup controllers. The primary controller is collocated in the switching plane node of the corresponding domain. The backup controllers are also collocated in the switching plane nodes but can belong to other domains. This aims at minimizing the number of controllers and, in this way, minimizing intercontroller communication. The goal is to improve robustness against b controller shutdowns in each domain. We compare the gains in robustness and the penalties in the delays with then standard domain model where the primary and backup controllers are collocated inside their respective domains.

**FUTURE COLLABORATIONS (if applicable)**

The work described herein means an ongoing collaboration between the involved persons. While the work on controller placement for the logically centralized control plane has been studied extensively, resulting in a paper to be submitted soon to a scientific journal, many other aspects on robustness of SDN networks can still be considered.

The problem for the logically distributed SDN control plane is ongoing. To our knowledge, very little has been studied in the literature on robustness for this architecture. A more comprehensive study on this problem will be further discussed in the future. In the near future a paper will be submitted to an international conference, and later on a more comprehensive paper will be submitted to a scientific journal.