SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA15127
STSM title: Comparison of SDN Controller Placements Robust to Disasters and Failures
STSM start and end date: 14/01/2020 to 21/01/2020
Grantee name: Dorabella Santos

PURPOSE OF THE STSM:

This STSM contributes to the aims of RECODIS WG4 and is the extension of the work submitted to the Chapter 10 (previously numbered 2.4): Reliable Control and Data Planes for Softwarized Networks of the RECODIS COST Action final book. The main aim of this STSM was to discuss some open issues in robust SDN controller placement, especially to evaluate the robust solutions obtained against the more common, but less disruptive types of node and/or link failures: random, targeted and epidemic.

Several network robustness metrics are to be used in the evaluation of the solutions, and more specific metrics related to SDN networks such as control path availability and control plane availability. Also the very specific robustness metrics employed in our previous work will be considered. However, instead of combining the metrics into lexicographic optimization objectives, as done previously, since now we intend to consider more metrics, novel ways of combining them were also dicussed, being the R-value one of the methods to investigate.

This work is planned to be submitted to a conference during 2020, and a more comprenhesive and extended version of this work to be submitted to a journal by the end of 2020.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

In the robust controller placement problem (CPP) addressed in the previous two STSMs, we considered malicious attacks shutting down up to p nodes. We started by computing that the set of CPP solutions satisfying the robustness property: if all controllers shut down, except one, thean all the surviving switches can still connect to the surviving controller. Moreover, (i) a maximum delay is guaranteed between each switch and its primary controller, called the maximum SC delay; (ii) and a maximum delay is guaranteed between any two controllers, called the maximum CC delay. This set of solutions is named robust CPP solutions. Among the robust CPP solutions, we then selected the optimal ones against the considered attacks.

The attacks considered were for the wost-case scenarios: centrality-based attacks for node degree, closeness and betweenness; and the most disruptive in terms of data plane topology, which is the critical node detection (CND) based attack. Each robust CPP solution was evaluated against these four attacks, by the robustness metrics: (a) number of switch-pairs able to connect to each other and to a controller, nsp; (b) number of switches able to connect to a controller satisfying the maximum delay, nsc; (c) number of switches still able to connect to its primary controller, npc. These metrics were then used as a

lexicographical optimization objective, to select the optimal solutions against the worst-case attack (generally the CND-based attack, but not always).

In this STSM, our objective was to evaluate the optimal robust CPP solutions against the more common and less disruptive node and/or link failures: random, targeted and epidemic. We began by considering a 'benchmark' solution, which was chosen to be the protected path CPP solution, minimizing the total delays of the primary and backup paths [1]. For a fair comparison, we have also constrained the solution to satisfy the maximum CC delay between the controllers, and the maximum SC delay only for the primary path between each switch and its controller (the backup does not have any constrained delay).

Furthermore, we consider the robust CPP solution that minimizes the average SC delay, and call it minSC robust CPP solution. We intend to see what is gained in terms of robustness and in terms of SC delay penalties, when going from a protected path solution, to a robust CPP solution and furthermore, to the optimal robust CPP solution.

Beside the robustness metrics mentioned above (nsp, nsc, npc), other more general metrics were discussed as those used in [2]. Since we are considering different types of failures, instead of using lexicographic objective used in our previous works (which was tailored for the considered attacks), we have considered combining the metrics into different weighted sums. Moreover, we have also considered combining them to obtain the network robustness R-value [2].

[1] P. Vizarreta, C. Mas Machuca and W. Kellerer, "Controller placement strategies for a resilient SDN control plane", RNDM 2016, pp. 253-259

[2] M. Manzano, F. Sahneh, C. Scoglio, E. Calle and J. L. Marzo, "Robustness surfaces of complex networks", Scientific Reports 4:6133, 2015

DESCRIPTION OF THE MAIN RESULTS OBTAINED

We have run preliminary tests for the instances of the problems considered in our work against malicious attacks (for Germay50 and Coronet CONUS networks). We have implemented the 'benchmark' solution and considered random and targeted failures affecting up ot 20% of the nodes of the network.

For the random attacks, 100 iterations were performed where up to 20% of the nodes were randomly selected. Each iteration was simulated in the following way: (1) randomly choose the next node to fail; (2) evaluating each of the three solutions ('benchmark', minSC robust CPP, optimal robust CPP) for each instance, against the failed nodes; (3) repeat (1)-(2) until 20% of the nodes have failed.

For the targeted failures, we considered the centrality-based and CND-based failures. For the centrality-based failures, each node was chosen with highest centrality and the centralities were recomputed for the surviving network. In each selection, the solutions were evaluated against the current failure. For the CND-based attack, each configuration of 1 node up to 20% of the nodes was computed and the solutions evaluated accordingly.

We analysed the robustness metrics given by nsp, nsc and npc, individually. We also considered the number of switches that can connect to a controller, irrespective of the delay to it after the attack – ns. We combined these metrics to find the R-value and also combined them into weighted sums that reflected the lexicographical objective used in our previous work.

Instead of considering the worst-case scenario, where the smallest value of each metric is considered among all failures up to p failed nodes, we averaged the values of each metric among all failures, since we are considering up to 20% (more than $p - 1$) failed nodes. Moreover, using the weighted sums and R-value we plotted the surface of the obtained values for each failure configuraton.

It is possible to see that in average, considering the nsp and nsc metrics, the minSC robust CPP and the optimal robust CPP solutions are better than the 'benchmark' solution. Up to p failed nodes, the optimal robust solution is the best on average. When considering more than p failed nodes, the minSC robust CPP solution is sometimes the best.

A more comprehensive study considering the weighted sums and R-value has still to be conducted. The

epidemic failures will be implemented too. Moreover, we will consider failures up to 70% of the nodes for the three types of failures.

FUTURE COLLABORATIONS (if applicable)

The work described herein means an ongoing collaboration between the involved persons. A comprehensive study will be performed for evaluating the robust CPP solutions against the different types of failures. Also regarding natural disasters, geographically correlated failures have also been discussed to be considered later on. Robustness metrics involving control plane availability are also to be included.

Furthermore, work on the logically distributed SDN control plane is still ongoing. The outcome will be submitted to a IEEE Transactions journal in the near future.