SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

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

Action number: ECOST-STSM-Request-CA15127-44254
STSM title: Robustness Analysis of Logically Distributed SDN Networks and application of Machine Learning techniques
STSM start and end date: 23/04/2019 to 30/04/2019
Grantee name: Farhad Rezazadeh, Universitat Politècnica de Catalunya (UPC)

PURPOSE OF THE STSM:

The purpose for taking part in this STSM is twofold. Firstly, I wish to learn from this highly appreciated and prestigious university with skilful research group members. Secondly, I want to improve the work at my home institution and also enrich my future studies and help me in my prospective research. This STSM is to start a collaboration with Dr. Carmen Mas Machuca and her research group in the Communication Networks group at TUM work on finding the number and location of the SDN controllers, which is known as the controller placement problem (CPP). The main objectives during the visit to the host are:

- To work on common paper solve the CPP in Distributed SDN scenarios and then target attacks to find new metrics.
- Work on application of ML and CPP in improving the robustness of SDN-based Networks to mitigate the occurrence failures.
-Plan on setting collaborating for joint publication beyond the date of this STSM

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

The work described herein means an ongoing collaboration between the involved persons. The visit started with the review and compilation of all material and explain activities of both research groups and regular meetings with the scientists from the Communication Networks group at TUM to discuss their achievements in investigations of resilient SDN-based networks over different scenarios and different aspect of controller placement problem as well as recent research issues and results. During the STSM visit, Farhad has given a presentation about their activities in UPC and UdG. Dr. Carmen Mas Machuca has explained previous researche on finding the number and location of the SDN controllers, which is known as the controller placement problem (CPP). For a given maximum switch-controller (SC) delay and a given maximum controller-controller (CC) delay in the regular state, they aim to find a CPP solution that maximizes the network robustness for a given number of malicious node attacks.

Furthermore, we worked on the problem formulation and pseudocode as well as on the definition of an alternative to varience, which considers the optimal cluster size. The proposed variance metric considers the number of components (islands) after the network is attacked and the size of these islands with respect the ideal case. The critical nodes strategy maximizes the damage by selecting the nodes that split the network in more islands with homogeneous size distribution (i.e. less variance). In that case, the number of

switches able to connect to a controller is reduced the the island size.

In addition, we investigated new metrics for current research about "Robust SDN Controller Placement Under Simultaneous Target Attacks". One of the worst scenarios occurs in the case of simultaneous target attacks when these attacks can break the networks in different pieces/islands. In many cases these networks are controlled by one or few nodes that can monitor or manage the network. Moreover, if a failure or attack occur in these controller nodes, the network could become isolated causing a disruption in the service availability. We analyze different simultaneous target attack scenarios and proposed a more robust strategy to locate the controllers preserving the desired service availability level. A new metric based on node criticality aims to find out the best controller locations to maximize the number of nodes connected to a controller in case of an attack. The proposed metric for a node i, N_{ci} is defined as the percentage of nodes connected to node *i* if a controller is placed on it (V_{ci}) with respect the network size (|V|), i.e., $N_{ci}=V_{ci}/|V|$. When generating *N* attacks (e.g., considering different strategies and/or number of failing nodes), $\widehat{N_{ci}}$ is defined for node *i* as the average of N_{ci} with respect all the attacks j, i.e.,

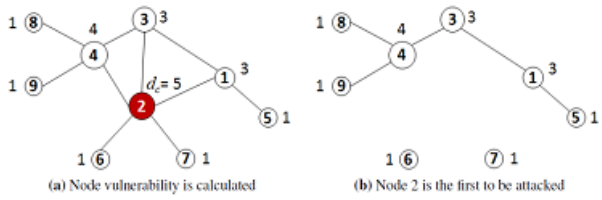
$$\widehat{N_{ci}} = \frac{\sum_{j=1}^{N} N_{ci}}{|V|N} 100$$

The proposed $\widehat{N_{ci}}$ metric gives the importance to nodes which are not usually attacked because when a node is removed the number of nodes of its island is zero (i.e. there is no island), hence it does not sum. The node with the highest $\widehat{N_{ci}}$ percentage should be set as the preferable controller location because it is the node which covers more nodes after a supposed attack is performed.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

The figure below shows a network with nodes labeled with their degree centrality (dc). Based on this metric, the attack is triggered on Node 2 because it has the highest degree centrality (i.e., it is the most harming failure). The failure causes a disconnected graph.

.



(a) Node vulnerability is calculated (b) Node 2 is the first to be attacked

Targeted attacks are not random and the attacker is assumed to know the network topology and able to trigger the attack on the most vulnerable (most important) network elements. Centrality metrics (e.g., degree, betweenness, closeness and eigenvector centrality) are widely used to identify the critical elements (nodes or links) in networks and to discern the probability that an element will be attacked. This probability for a network element *i* with a given property (e.g. centrality metric) value w_i, can be defined as [1]:

$$Pta(w_i) = \frac{w_i}{\sum_{i=1}^{|NE|} w_i}$$

In the simulation results the objective has a double goal. In one hand we compare the effectiveness of simultaneous attacks and on the other hand to analyses what are the requirements, in number of backup controllers, to minimize the consequences of these attacks. According to the first objective we evaluate the effectiveness of different attack strategies (i.e. degree and critical nodes) considering both, the number of components (islands) after the network is attacked.

Results pointed out that classical strategies to locate the controllers (based on delay or centrality characteristics) are not suitable in case of attacks. The proposed methods are based not only the number of resulting island/components to decide what are the number of backup controllers we require to guarantee a specific availability value but also the percentage of attacks to this node and the potential coverage area of this node.

[1] L. K. Gallos et al. "Stability and Topology of Scale-Free Networks under AttackVand Defense Strategies". In: Physical Review Letters 94

FUTURE COLLABORATIONS (if applicable)

During the STSM, it became obvious that the Broadband Communications Systems and Architectures research group (CBA) at Polytechnic University of Catalonia (UPC), The Broadband Communication and Distributed Systems (BCDS) at University of Girona (UdG) and Chair of Communication Networks at TUM share many research interests, and therefore we plan on collaborating well beyond the scope of this STSM. 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