SHORT TERM SCIENTIFIC MISSION (STSM) – SCIENTIFIC REPORT

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

Action number: CA15127
STSM title: Post-Disaster Resilient and Secure Routing
STSM start and end date: 30/8/2018 to 12/09/2018
Grantee name: Dr Christiancarmine Esposito

PURPOSE OF THE STSM/

(max.500 words)

The topic of this STSM is related to the routing protocols to provide resilient communications in post-disaster scenarios where the network has been severely compromised and the experienced quality of service are extremely exacerbated. Specifically, due to the increased traffic and/or the physical damages to the network infrastructure caused by the occurrence of a natural disaster or severe weather conditions, the exchanged packets can be lost with an higher probability, so that the experienced loss pattern can be higher than the one normally exhibited by the network before the disaster. Resilience is a strongly demanding non-functional requirement and proper recovery schemes must be put in place in order to provide loss tolerance and move a step forward realizing disaster-resilient networks. The scope of this STSM was twofold. On the one hand, the literature on the routing protocols to be used after a disaster to cope with the severe loss patterns had been investigated. On the other hand, after a disaster the network is particularly vulnerable to attacks, and the recovery schemes are not designed to deal with possible malicious activities and attacks. Such an aspect had been investigated and a solution proposed.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

(max.500 words)

Such STSM started on 30st August (with the arrival of the hosted researcher) and ended on 12th September (when the hosted researcher departed), for a total of 14 days, and was structured in two different activities:

1. Finalization of the chapter for the RECODIS book (specifically the RECODIS_Chapter3.9 Routing in Post-Disaster scenarios).

2. Investigation of routing strategies providing disaster resiliency with security guarantees – The security and privacy vulnerabilities of the routing protocols used after the occurrence of a disaster was analysed and a solution proposed.

The scheduling of those activities over the time was planned as follows. As scheduled by the RECODIS management board by the mid-June each contributor to the chapter sent a draft of their section. Specifically, all the contributors were identified and a structure of the chapter was proposed. In the first week of the STSM, the hosted and the hosting researchers discussed about the content of the chapter, and how to strengthen the presentation and technical correctness of their section. They worked together in order to review the sections. Unfortunately, not all the identified contributors were able to provide material for the chapter, however, the available material was enough to fill the chapter. The only remaining part to complete is the introduction, which will be done by 15th November.

Apart from the finalization of the chapter, the STSM has been a fruitful possibility to establish a collaboration between the hosted and hosting researcher. Specifically, the issue of jointly providing resiliency and security for the routing protocols used after the occurrence of a disaster was studied. Such a work started with a presentation of the hosted researcher and a discussion, where the gossip protocol has been selected as the focus of the work. In fact, such a scheme can be used to implement denial of service attacks by maliciously having the scheme sending an excessive number of un-necessary messages towards some nodes of the network. Therefore, the related literature has been investigated and an application of the game theory to protect gossiping from fake requested and forged identifies has been studied. Specifically, in the second week of the STSM, the proposed solution has been implemented in the OMNET++ simulator and a preliminary set of experiments has been conducted. In the days after the STSM a paper describing such a work has been written to be submitted at the 15th International Conference on the Design of Reliable Communication Networks (DRCN 2019), which will be help in 2019 in Coimbra, Portugal.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

(max. 500 words)

The main obtained results were the following ones:

- The Chapter 3.9 has been completed at 70%, the missing part is the introduction and a general restructuring and proof reading in order to check its language and presentation correctness. The chapter has been written with overleaf and it is accessible at https://it.overleaf.com/read/gncpxbcbrkqw
- A paper to DRCN has been written and submitted. Overleaf has been used to write this paper, which can be read at https://it.overleaf.com/read/nnsysbzvfbjg

FUTURE COLLABORATIONS (if applicable)

(max.500 words)

The two researchers have identified topics for future collaborations on the issues of IoT traffic monitoring by means of advanced artificial intelligence solutions, and also the future possibility to write joint project proposals to EU or national funding calls.