STSM Report

STSM Applican **: Madhusanka Liyanage**
Host **: Prof. David Hutchison**
Host Institute **: InfoLabs21, Lancaster University, United Kingdom**
Duration **: 2016-12-07 to 2016-12-17**
Title **: "Resilient Cloud Management for Future Cyber-Physical Systems"**

I was invited to visit InfoLabs21, Lancaster University, United Kingdom by Prof. David Hutchison. On arrival, I had a meeting with Prof. David and he explains his research on network and system resilience. Moreover, he explained briefly about ongoing projects in his research group. Where I also explained my research experience and discuss the objectives of STSM. The main topic of STSM is "Resilient Cloud Management for Future Cyber-Physical Systems" which is a research topics which will be addressed under WG4: Malicious human activities in Cost Action CA15127. Then, I met the research group of Prof. David.

I worked mainly with Mr. Syed Noor Shirazi who is a researcher at Infolab21. He explained the current and past resilience projects which are relevant to my STSM. We have discussed mainly on three projects.

1. "A Situation-Aware Information Infrastructure"

   In this project, they design and develop a generic, resilient and adaptive situation-aware information infrastructure that would predict and confront the broad range of challenges faced by the network. Their mechanisms will be incorporated as a protocol suite within a Software-Defined architecture, integrated as a native component in (future) computer networks design.

2. SECCRIT (SEcure Cloud computing for CRitical infrastructure IT) https://www.seccrit.eu/

   The project was focused to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments, and to develop methodologies, technologies, and best practices for creating a secure, trustworthy, and high assurance cloud computing environment for critical infrastructure IT.

3. ResumeNet (Resilience and Survivability for Future Networking: Framework, Mechanisms, and Experimental Evaluation) http://resumenet.eu/

   The ResumeNet project investigated a framework for network resilience. The framework consists of a number of components, including approaches to evaluate network resilience based on metrics, and architectures that can be used to detect challenges and mitigate them in real-time.

I have studied several public deliverables and publications related to each topics.

I discuss with Dr. Antonios Gouglidis who is a Senior Research Associate at Infolab21. He is currently working on HyRiM (Hybrid Risk Management for Utility Providers) project. https://hyrim.net/.

- HyRiM (Hybrid Risk Management for Utility Providers) project. https://hyrim.net/.

  The project is focused on Risk management in critical infrastructures as operated by utility providers. The main objective of this project is to identify and evaluate 'Hybrid Risk Metrics' for assessing and categorizing security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms.

Dr. Antonios discussed his work on HyRiM project and shared the relevant publications. We exchanged our research papers an identified the possible research cooperation.

We planned a joint publication with Mr. Noor and Prof. David (See Annex 1 for more details). The publication will focused on A Framework for Resilience Management in 5G Mobile Networks. We created an action plan to writing the paper, agreed on assigning a local student to perform experiments and perhaps a researcher from University of Lancaster will carry out a future STSM to University of Oulu, Finland. Our university (University of Oulu) is building a 5G Test Network[1]. We will plan to use it to run experiments. Moreover, I discussed Prof. David about possibility to submit a joint proposal H2020 proposal for H2020-CIP-2016-2017[2]. He would consider the options to invite partners from current HyRiM project consortium. We decided to start building the consortium by late January 2017.

I had a meeting with Dr. Steven Simpson about his research work. Dr. Steven is work on prevention of DDoS attacks in communication network.

Then, I have a meeting with Dr. Arsham Farshad. He is working on Towards Ultimate Convergence of All Networks (TOUCAN) project.

- Towards Ultimate Convergence of All Networks (TOUCAN) project http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/L020009/1

  TOUCAN aims to achieve ultimate network convergence enabled by a radically new technology agnostic architecture targeting a wide range of applications and end users. This architecture will facilitate optimal interconnection of any network technology domains, networked devices and data sets with high flexibility, resource and energy efficiency, and will aim to satisfy the full range of Quality of Service (QoS) and Quality of Experience (QoE) requirements.

  TOUCAN will drastically evolve SDN to incorporate fundamentally new technology-specific interfacing and resource description followed by infrastructure resource abstraction, virtualisation and programmability. These features will enable any network technology and device to become "TOUCAN-ready" which means that the devices are programmable and interoperable. This is the foundation upon which the

[1] 5G Test Network http://5gtn.fi/

[2] H2020-CIP-2016-2017 https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/cip-01-2016-2017.html

technology-agnostic feature of the TOUCAN architecture will be realized; thereby ultimate seamless end-to-end convergence will be achieved.

The research work of TOUCAN is quite relevant to my recent research work on SDN based WiFi offloading. We had a long discussion on the synergy between our research work and agreed to work closely in future. Mr. Nicholas Hart who is also working on TOUCAN project had shown me the testbed which they use for TOUCAN project.

Madhusanka Liyanage
Oulu, Finland 20.12.2016

Annex 1: Joint Publication

Tentative Title: *Resilience Management Framework for 5G*

Tentative new paper abstract: *Fifth Generation (5G) Software Defined Mobile Network (SDMN) architecture will integrate SDN (Software Defined Networks), NFV (Network Function Virtualization) and Cloud Computing concepts. As a results, 5G mobile networks will more rely of virtualized and cloud resources in future. Such, virtualized environments make resilience more challenging due to the sharing of non-virtualized resources, frequent reconfigurations, and new cyber-attacks on these flexible and dynamic systems. In this paper, we present Resilience Management Framework (RMF) for 5G Networks, which models and then applies an existing resilience strategy in a 5G networks to diagnose anomalies. The framework uses an end-to-end feedback loop that allows remediation to be integrated with the 5G component. We demonstrate the applicability of the framework with a use-case for effective 5Gresilience management.*

Tentative Outline:

1. *Abstract*
2. *Introduction*
3. *Background*
    a. *5G Architecture*
    b. *Resilience Requirement*
    c. *Existing Resilience Approaches*
4. *Related Work*
5. *5G RMF (5G Resilience Management Framework)*
6. *Qualitative Evolution*
7. *Discussion*
8. *Conclusion*