RECODIS
Resilient communication services protecting end-user applications from disaster-based failures

Training School on

Design of Disaster-resilient Communication Networks

Venue: Brussels, Belgium (Premises of COST Association)

Date: December 10-11, 2019

The training is addressed primarily to network operators, networking equipment vendors, and regulators.

Scope and Objective

Disaster-induced failures can severely affect any communication network, leading to multiple failures of network elements and making services unavailable. Such scenarios may be triggered by:

a) **natural disasters** such as fires, tornadoes, volcano eruptions, earthquakes, **and disruptions** (heavy rain/fog in the context of high-frequency wireless communications, e.g., in wireless mesh networks),

b) **technology-related** problems following from, e.g., software issues, and other technology-related events such as power blackouts, or inter-dependence of communication networks and power grid networks,

c) **malicious human activities** leading to massive failures of important network elements such as high capacity links, or nodes hosting/switching a large amount of data.

The objective of this training is to familiarize the participants with the essential techniques related to:

- the evaluation of the vulnerability of communication networks to disaster-induced failures,
- methods of design/update of communication network architectures with improved disaster-resilience.

The content of the training is a result of over 3-year cooperation of about 200 leading European researchers in the area of network resilience from over 50 major universities and research centres located in 31 European countries.

Program Overview

DAY 1 (December 10, 2019)		DAY 2 (December 11, 2019)	
9:15-9:40	**Opening Session**	**Session 4** 9:00-11:00	Design of Communication Networks Resilient to Technology-related Disasters
Session 1 9:40-11:00	Evaluation of Vulnerability of Communication Networks to Massive Disruptions and Failures		
COFFEE BREAK		COFFEE BREAK	
Session 2 11:30-13:30	Design of Communication Networks Resilient to Natural Disasters	**Session 5** 11:30-13:30	Design of Communication Networks Resilient to Malicious Activities
LUNCH		LUNCH	
Session 3 14:30-16:30	Design of Communication Networks Resilient to Weather-induced Disruptions	**Session 6** 14:30-15:50	Operation of Communication Networks in a Post-disaster Period
		15:50-16:30	Discussion and **Closing**
16:30-17:00	Discussion		
DINNER			

Knowledge/Skills Learnt

Session 1	Evaluation of Vulnerability of Communication Networks to Massive Disruptions and Failures

Having completed this session of the Training School, participants are expected to get knowledge related to:

- algorithmic approaches for generating lists of SRLGs (and their extensions with failure probabilities) of the communication networks protecting different sets of disasters,
- different models of software failures and their application to SDNs,
- dependability assurance with SRGM and related dependability metrics

Session 2	Design of Communication Networks Resilient to Natural Disasters

Having completed this session of the Training School, participants are expected to understand:

- the type of failures induced in a communications network and caused by natural disasters,
- the concept of path-geodiversity routing and its potential to enhance the resilience of services to natural disasters,
- how routing can be dealt with to provide both high availability and high resilience to natural disasters, as required by critical services,
- how the location of Data Centers impacts the resilience to natural disasters of anycast-based services (like cloud or content delivery services),
- a framework for disaster-resilience, and how it can be used to provide disaster-resilience in critical infrastructures

Session 3	Design of Communication Networks Resilient to Weather-induced Disruptions

Having completed this session of the Training School, participants are expected to know how to:

- capture the correlation between different quality aspects deployed in the context of the resilience of telecommunication networks and systems,
- update wireless networks (or systems) in a pre-disruption stage,
- identify the beginning of the disruption on the wireless transmission and react to it,
- exploit alert time given by an incoming disaster to reconfigure the communication and processing resources of the network and to evacuate data from data centers,
- characterize the impact of weather conditions on wireless links transmission capacity,
- construct an optimization model for designing wireless networks resilient to changing weather conditions

Session 4	Design of Communication Networks Resilient to Technology-related Disasters

Having completed this session of the Training School, participants are expected to understand:

- the concept of network robustness,
- the set of graph metrics and their relevance to the robustness,
- how to model massive attacks to a network,
- how to analyze and visualize the network robustness,
- the concept of volatile cloud resources,
- how to simulate the behavior of volatile cloud resources with the VolatileSim simulation framework,
- how to evaluate and compare different volatile cloud resources case studies,
- how to obtain more reliable networks leveraging on NFV systems

Session 5	Design of Communication Networks Resilient to Malicious Activities

Having completed this session of the Training School, participants are expected to understand:

- the concept of critical nodes and critical links of a communication network topology,
- how to evaluate the resilience of a communications network to the failure of its critical nodes (or links),
- how service networks can be updated to improve the service resilience to multiple failures,
- the trade-off between resilience to multiple failures and routing distance of anycast-based services,
- what are the main physical-layer vulnerabilities in optical networks and how they can be exploited to perform service disruption attacks,
- how to plan the optical network to reduce the attack surface,
- how to detect optical-layer attacks and recover from them

Session 6	Operation of Communication Networks in a Post-Disaster Period

Having completed this session of the Training School, participants are expected to know:

- the main requirements for post-disaster communication systems, and how communication demand volume varies as a function of the characteristics of the post-disaster setup and depending on the set of applications supported,
- how to choose the appropriate communication strategy for a given set of supported applications and a specific disaster scenario,
- how to identify the main weaknesses and vulnerabilities of an emergency communication system, and how to design appropriate measures to minimize their impact on the network performance,
- how to design a situation awareness service based on probabilistic spatial storage paradigms relying on opportunistic communications

Rules Related to Participation in the Training School

The applications related to participation in the RECODIS Training School should be sent to via email to: jrak@pg.edu.pl(with the email title: "**Training School of RECODIS**").

The application should include personal information (**name**, **affiliation**, **country**, **email**), and estimation of travel costs (in the case of air travel, a printout from the Skyscanner or similar service showing an economy fare travel cost is required).

Travel costs will be supported based on the expenses estimated on the day of submitting the application. Accommodation and daily allowance is defined in total as a flat rate reimbursement of 160 EUR per day.

The estimated average total support for the participant from the budget of RECODIS is 700 EUR.

Each approved participant of the RECODIS Training School will be given a fixed grant to provide the financial support related to:

a) travel costs,
b) accommodation and daily meal allowance.

The grant is not guaranteed to cover all expenses of a participant (but it also does not require additional documentation, except for the signing of the attendance list on each day of the Training School).

Approved applicants will be notified of the fact by email and will be required to register for an e-COST profile at https://e-services.cost.eu. The registration of the applicant in e-COST including the bank account details, must be completed by the approved applicant before the start date of the Training School.

A detailed information on participation in COST Training Schools can be found in COST Vademecum (https://www.cost.eu/wp-content/uploads/2019/07/Vademecum_June2019.pdf), section 6.3 (page 30).

The deadline for submitting the application is **November 15, 2019, 23:59:00 CET**

Each participant completing the Training School will receive
the certificate confirming the completion of the training.

DETAILED PROGRAM

Opening Session

Prof. Jacek Rak, Gdansk University of Technology, Poland /

Prof. David Hutchison, Lancaster University, United Kingdom

Date: **Dec. 10, 2019, 9:15 AM – 9:40 AM**

Session 1: Evaluation of Vulnerability of Communication Networks to Massive Disruptions and Failures

Course 1: **How to Model and Enumerate Geographically Correlated Failure Events in Communication Networks**

Trainer: **Balázs Vass, MSc**, Budapest University of Technology and Economics, Hungary

Date: **Dec. 10, 2019, 9:40 AM – 10:20 AM**

Summary:

Several works shed light on the vulnerability of networks against regional failures, which are failures of multiple pieces of equipment in a geographical region as a result of a natural or human-made disaster. The critical difficulty that operation network ignores the geographic information of the physical network. In this course, we overview how this information can be added to existing network protocols through defining Shared Risk Link Groups (SRLGs), and their extensions with failure probabilities. In particular, we are focusing on the state-of-the-art algorithmic approaches for generating lists of SRLGs (and their extensions) of the communication networks protecting different sets of disasters.

Course 2: **Software Reliability**

Trainer: **Prof. Carmen Mas Machuca**, Technical University of Munich, Germany

Date: **Dec. 10, 2019, 10:20 AM – 11:00 AM**

Summary:

Communication networks are evolving towards softwarized networks. Hence, software reliability is becoming a crucial challenge. In this session, software failures will be introduced and classified. Different software prediction models will be presented and applied to SDN. It will be shown how the various SDN failures can be modeled and how different reliability metrics, such as software maturity, can be evaluated.

Session 2: Design of Communication Networks Resilient to Natural Disasters

Course 1: **Routing Schemes Resilient to Natural Disasters**

Trainers: **Prof. Amaro de Sousa**, University of Aveiro, Portugal /
Dorabella Santos, PhD, INESC-Coimbra, Portugal

Date: **Dec. 10, 2019, 11:30 AM – 12:10 AM**

Summary:

Natural disasters affect a set of network nodes and links geographically close between each other. In this course, we discuss how routing can be implemented to minimize the impact of such disasters. The key idea is to take into consideration the geographical information of the network and, for each pair of nodes of interest, to determine a pair of routing paths that are geographically separated by some desired distance. Then, we discuss how such pairs of paths can be computed aiming at different objectives: minimizing the cost, maximizing the service availability or minimizing the number of common regional failures.

Practical part: The trainers will run some examples showing: **(i)** how the geographical information of the network is used to define and solve the optimization problems associated with the different objectives and **(ii)** the trade-off obtained between the geographical separation of the pair of routing paths and the different considered objectives.

Course 2: **Structural Methods to Enhance the Resilience to Natural Disasters**

Trainers: **Prof. Amaro de Sousa**, University of Aveiro, Portugal /
Dorabella Santos, PhD, INESC-Coimbra, Portugal

Date: **Dec. 10, 2019, 12:10 AM – 12:50 AM**

Summary:

In this course, we first discuss how to upgrade the availability of some network links so that both the availability and the resilience to natural disasters are within given desired levels. It is particularly important in the provision of critical services where availability must be high also in the case of natural disasters. Then, we consider the provision of anycast based services, like cloud or content delivery services. When such services are hosted in multiple geographically distributed Data Centers (DCs), we discuss how the DC locations must be selected so that a desired level of resilience to natural disasters is met.

Practical part: The trainers will run some examples addressing the impact on the resilience of anycast based services of different geographical distributions of the DCs on a given network.

Course 3: **A Framework for Disaster Resilience**

Trainer: **Balázs Vass, MSc**, Budapest University of Technology and Economics, Hungary

Date: **Dec. 10, 2019, 12:50 AM – 1:30 PM**

Summary:

In this course, we present a framework for disaster resilience called FRADIR, which incorporates reliable network design, disaster failure modeling and protection routing to improve the availability of mission-critical applications is presented. It is a comprehensive framework which utilizes tools from all these fields in a joint design of disaster-resilient connections. We demonstrate the concept and benefits of FRADIR through experimental results in two real-like network topologies.

Session 3: Design of Communication Networks Resilient to Weather-induced Disruptions

Course 1: **Quality-driven Technique of Alerting to React and Prevent from Service Performance Degradation under Weather-based Disruptions**

Trainers: **Prof. Rasa Bruzgiene**, Kaunas University of Technology, Lithuania /
Lina Narbutaite, PhD, Kaunas University of Technology, Lithuania

Date: **Dec. 10, 2019, 2:30 PM – 3:10 PM**

Summary:

In this course, we discuss how the interrelation among the quality metrics of different layers can be used to design resilient networks/systems, where the aspect of quality is crucial in the case of disruptions. First of all, trainees will be actively involved in the evaluation of the performed service and identification of the beginning of the disruption on the transmission. Secondly, we will give an example of the quality-focused alert technique for an FSO (free-space optical) system. Finally, we will examine the results of subjective/objective evaluation of the perceived quality on the service transmission and discuss how it can be utilized when updating the network/system to prevent from service suspension in the case of weather-induced disruptions.

Course 2: **Alert-based Network Reconfiguration and Data Evacuation**

Trainer: **Prof. Massimo Tornatore**, Politecnico di Milano, Italy

Date: **Dec. 10, 2019, 3:10 PM – 3:50 PM**

Summary:

In this part, we will discuss how to develop data evacuation and network reconfiguration techniques to react to an alert of an incoming disaster. In fact, most, especially weather-based, disasters grant a warning some minutes/hours before the disaster strikes, and this time can be used to reconfigure the network and evacuate data from data centers that might be most likely affected by the disaster. The lecture will show various use cases and network optimization approaches to maximize the amount of data that can be evacuated, and to minimize the impact of the disaster on existing living traffic/services.

Course 3: **Design of Wireless Networks Resilient to Adverse Weather Conditions**

Trainer: **Prof. Dritan Nace**, Université de Technologie de Compiègne, France

Date: **Dec. 10, 2019, 3:50 PM – 4:30 PM**

Summary:

Wireless communications is sensitive to weather conditions that affect the communication channel. Therefore, special network design means must be applied to avoid degradations in transmission capacity available for the users. In this lecture, we will discuss a design approach adequate for an important subclass of wireless networks – FSO (free space optics) wireless metropolitan area networks. We will show how to identify weather states and characterize their impact on the transmission capacity of FSO links. Next, we will present an optimization model that allows for cost-effective dimensioning of the FSO network resilient to representative weather states. Finally, we will illustrate the effectiveness of our approach for a realistic example of the Paris metropolitan area network.

Session 4: Design of Communication Networks Resilient to Technology-related Disasters

Course 1: **Network Robustness Measurement. Massive Failures and Main Metrics. The Network Robustness Simulator: a Tool**

Trainer: **Prof. Jose L. Marzo**, University of Girona, Spain

Date: **Dec. 11, 2019, 9:00 AM – 9:40 AM**

Summary:

Firstly, it will be justified the need to model the networks to be analyzed by graph theory. In massive failures, the dynamics of the attacks is relevant to compute the robustness. Different types of attacks will be described and modelled. Graph metrics will be classified and studied from the robustness relevance point of view. Then by combining the robustness measurements, a Robustness metric R* will be described. Experiments with a different type of challenges to a set of networks will be performed to compute R* in the simulator. Preliminary conclusions will be presented. As visualization is crucial to understand results in networks (graphs), the visualizer of the simulator tool will be used for this purpose.

Course 2: **Resilience, Cost and Performance Trade-off of Volatile Cloud Resources**

Trainer: **Sasko Ristov**, **PhD**, Ss. Cyril and Methodius University, North Macedonia & University of Innsbruck, Austria

Date: **Dec. 11, 2019, 9:40 AM – 10:20 AM**

Summary:

This part addresses how to study the behavior of volatile cloud resources to run services with high resilience, lower cost and higher performance. The trainer will briefly introduce volatile cloud resources, which are much cheaper computing resources (e.g., Amazon Spot Instances, Google Preemptible Instances or Microsoft Low Priority), but some of them (or all) can be reclaimed by the cloud provider at any time during cloud service execution. The trainer will also identify the types of failures that should be considered and the most important parameters to characterize them. A dynamic scheduling algorithm will be presented, which minimizes the makespan by keeping the costs lower than the budget constraint.

Practical part: The trainer will also introduce the VolatileSim simulation framework developed by the University of Innsbruck, Austria, which is able to execute complex workflow applications (with dependencies between tasks) over volatile cloud resources. VolatileSim will be used to simulate and evaluate different scenarios. The participants will be able to create a data center with volatile resources, compare different cases, and evaluate the trade-off in the resilience compared to the overall cost/performance with Volatile and OnDemand resources.

Course 3: **NFV and 5G Orchestration Reliability**

Trainer: **Prof. Stefano Secci**, Cnam, Paris, France

Date: **Dec. 11, 2019, 10:20 AM – 11:00 AM**

Summary:

This part addresses how to study the behavior of volatile cloud resources to run services with high resilience, lower cost and higher performance. Regarding NFV and 5G orchestration, we will show how it is possible to compensate for the potential lower reliability of commodity hardware with new orchestration actions that can be implemented by NFV systems. We will also show at which extent SDN support can be needed in association to reliability-driven NFV orchestration actions.

Practical part: The trainer will also show some demos using `https://ha-nfv.roc.cnam.fr`

Session 5: Design of Communication Networks Resilient to Malicious Activities

Course 1: **Resilience Evaluation and Improvement of Network Topologies to Multiple Targeted Failures**

Trainer: **Prof. Amaro de Sousa**, University of Aveiro, Portugal

Date: **Dec. 11, 2019, 11:30 AM – 12:10 AM**

Summary:

In this part, we discuss how to evaluate and mitigate the impact of multiple failures caused by malicious human activities on the services provided by given network topology. We address the worst case of the simultaneous failure of the critical elements, i.e., the nodes or links with the highest impact on the connectivity of the network. We discuss how the critical nodes (or critical links) of network topology can be identified and how this information can be used to update an optical backbone network with new links.

Course 2: **Structural Methods to Enhance the Resilience of Content Delivery Services to Link Cut Attacks**

Trainers: **Prof. Amaro de Sousa**, University of Aveiro, Portugal /
Prof. Marija Furdek, Chalmers University of Technology, Sweden

Date: **Dec. 11, 2019, 12:10 AM – 12:50 AM**

Summary:

In this part, we discuss how to evaluate and improve the resilience of content delivery networks (CDNs) to malicious link cuts. First, a resilience metric will be described to measure the impact of different possible attacks. Then, three different but related methods will be discussed. The first two methods consider a given CDN using a set of Data Centers (DCs) and address how to add several new network links or new available DCs, aiming to improve the resulting CDN resilience metric. The third method discusses how to replicate the CDN content on different geographically located DCs aiming to provide different trade-offs between the CDN average user-to-content distance and the resilience value.

Practical part: The trainers will run some examples addressing the impact of different content replica locations on the trade-off between the CDN average user-to-content distance and the resilience of the content service provisioning to various malicious link cut attacks.

Course 3: **Physical-layer Security Management in Optical Networks**

Trainer: **Prof. Marija Furdek**, Chalmers University of Technology, Sweden

Date: **Dec. 11, 2019, 12:50 AM – 1:30 PM**

Summary:

In this part, we investigate the physical-layer security of optical backbone networks. We first identify the main security vulnerabilities of optical fibers and switches, as well as attack methods that exploit these vulnerabilities. We then present the preemptive network planning techniques for the *a priori* reducing the attack surface by confining the worst-case attack scope to a limited number of known connections. Next, we present the experiment-based techniques for detection and localization of physical-layer attacks aided by machine learning. Finally, we examine strategies for network reconfiguration to support post-attack recovery.

Session 6: Operation of Communication Networks in a Post-Disaster Period

Course 1: **Emergency Networks: Scenarios and Requirements; State of the art Solutions and Open Issues**

Trainer: **Prof. Gianluca Rizzo**, HES SO Valais, Switzerland

Date: **Dec. 11, 2019, 2:30 PM – 3:50 PM**

Summary:
In the first part of the course, an overview of a set of disaster scenarios of reference, of typical user mobility patterns and spatial distribution will be discussed. The analysis of current and future services and use cases and the analysis of communication requirements will be presented. The second part of the course is to highlight the main approaches to the implementation of emergency networks (with a focus on solutions to integrate the surviving infrastructure and on infrastructure-less, self-organized and collaborative solutions involving user terminals).

Practical part: 10 minutes of demonstration + 20 minutes of an exercise related to the optimization of content routing and replication strategies for a situational awareness service.