Network survivability quantification
Autonomous Control for a Reliable Internet of Services (ACROSS)

Currently, we are witnessing a paradigm shift from the traditional information-oriented Internet into an Internet of Services (IoS). This transition opens up virtually unbounded possibilities for creating and deploying new services. Eventually, the ICT landscape will migrate into a global system where new services are essentially large-scale service chains, combining and integrating the functionality of (possibly huge) numbers of other services offered by third parties, including cloud services. At the same time, as our modern society is becoming more and more dependent on ICT, these developments raise the need for effective means to ensure quality and reliability of the services running in such a complex environment. Motivated by this, the aim of this Action is to create a European network of experts, from both academia and industry, aiming at the development of autonomous control methods and algorithms for a reliable and quality-aware IoS. Keywords: Service oriented internet, cloud services, autonomous control, reliability, pricing.
Threats to Dependability, Security and Survivability

Adequately trustworthy services

Equipment failures
Transmission failures
Environment
Design faults
Operational failures
Eavesdropping
Intrusions
Sabotage

large-scale service chains, combining and integrating the functionality

(trustworthy)
autonomous control

ensure quality and reliability of the services running in such a complex environment
**Dependability** is the trustworthiness of a system such that reliance can justifiably be placed on the service it delivers.

**Resilience** - ability to recover back to normal operation

**Robustness** - ability to tolerate misbehaviour and failures

**Survivability** is the system’s ability to continuously deliver services in compliance with the given requirements in the *presence of failures and other undesired events.*
Disaster/Fault Propagation Weather related / not [ example ]

Earthquake, tsunami, forest fire, hurricane, ...

When something goes wrong

1. Needs ICT

2. Common cause failure?

3. The fault (the cause of the problem)?

Power outage

ICT failure
Modeling and quantification of network survivability

Prof. Poul E. Heegaard, poul.heegaard@ntnu.no
Department of Information Security and Communication Technology (IIK)
Norwegian University of Science and Technology (NTNU)

Prof. Kishor S. Trivedi
kst@ee.duke.edu
Elect. & Comp. Eng. Dept.,
Pratt School of Engineering
Duke University

http://dx.doi.org/10.1016/j.comnet.2009.02.014
Network survivability quantification

The diagram illustrates the quantification of network survivability over time. It shows the service unavailability, maximum metric, and steady state metric after failure. The metric in fault-free operation is also depicted. The diagram includes time (t) and metric (M) axes, with key points marked as failure (t_f), repair (t_r), and t_0. The upper metric acceptance level is indicated as well.
Stages in the recovery process
(detection->localization->isolation->repair/replacement)

Fig. 3: Recovery stages of the phased recovery from a power grid incident (phases are based on ITU-T E.800 (1994) [16]).
II. Network survivability modeling and quantification
Phased recovery model

start from here

normal
undesired event
event detected

failure propagation

new undesired events
events detected
reconfigure/reroute
repair/restore

Undesired event

IV

III

I

II

α_u

α_d

τ
Performance model

Phased recovery model

Composite performability model

Survivability model
Network survivability quantification

![Graph showing network survivability metrics]

- $m_u$: Service unavailability
- $m_T$: Maximum metric
- $t_d$: Time after failure
- $t_T$: Time to achieve upper metric acceptance level
- $m_r$: Steady state metric after failure
- $t_o$: Metric in fault-free operation
- $t_r$: Repair time

Failure → Repair
A General Quantification Procedure

Step 1+2
- Availability model
- Performance model

Step 3
- Composite model

Step 4
- Force failure/attack/disaster
- Survivability measures

Step 5
- Transient analysis
- Truncate model

Combine
Objectives and target system

Transient performance in networks with virtual connections
From occurrence of an undesired event until steady state operation is restored

**Goal:** Survivability model of performance after network failure(s)

\[ a/b \]
\[ q_{ij}(I) = q_{ij}(IV) = a \]
\[ q_{ij}(II) = q_{ij}(III) = b \]

Exponential service time

Source: Poisson process

N=50
Survivability Research at Duke University and Norwegian University of Science and Technology (NTNU)

- **Publications**
  - Lang Xie, Poul E. Heegaard, Yuming Jiang. “Survivability Analysis of a Two-Tier Infrastructure-Based Wireless Network”. Accepted for publication in Elsevier Computer Networks.
  - Poul E. Heegaard and Kishor Trivedi. “Survivability Quantification of Communication Services”. In proceedings from The 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008). June 2008, Anchorage, AK.
  - Liu, Mendiratta & Trivedi, ‘Survivability analysis of telephone access network Proc. of 15th IEEE International Symposium on Software Engineering (ISSRE’04)
References

• Federal standard 1037C, Telecommunications: Glossary of telecommunication terms, 1996
• L. Garber, Denial-of-Service Attacks Rip the Internet, Computer, Vol 33, Issue 4, April 2000, pp. 12-17.
• Poul E. Heegaard and Kishor Trivedi. “Survivability Quantification of Communication Services”. In proceedings from The 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008). June 2008, Anchorage, AK.
References

• J. Knight and K. Sullivan, On the definition of survivability, TR-CS-00-33, University of Virginia, Dec., 2000.
• Y. Liu, V. B. Mendiratta and K. S. Trivedi, Survivability analysis of telephone access network Proc. of 15th IEEE International Symposium on Software Engineering (ISSRE’04)
• Menasché, DS; Avritzer, A; Suresh, S; Leão, RM; de Souza e Silva, E; Diniz, M; Trivedi, K; Happe, L; Koziolek, A, Assessing survivability of smart grid distribution network designs accounting for multiple failures, Concurrency and Computation: Practice and Experience, vol. 26 no. 12 (2014), pp. 1949-1974
• V. B. Mendiratta and C. A. Witschorik. Telephone service survivability. In IEEE workshop on the design of reliable communication networks (DRCN2003), October 2003
References