ISBN 978-82-326-1470-7 (printed version)
ISBN 978-82-326-1471-4 (electronic version)
ISSN 1503-8181

Doctoral theses at NTNU, 2016:66

Eirik Larsen Følstad

Managed access dependability for critical services in wireless inter domain environment

NTNU
Norwegian University of
Science and Technology

Doctoral theses at NTNU, 2016:66

NTNU

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology,
Mathematics and Electrical Engineering
Department of Telematics

NTNU
Norwegian University of
Science and Technology

Eirik Larsen Følstad

Managed access dependability for critical services in wireless inter domain environment

Thesis for the degree of Philosophiae Doctor

Trondheim, March 2016

Norwegian University of Science and Technology
Faculty of Information Technology,
Mathematics and Electrical Engineering
Department of Telematics

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology,
Mathematics and Electrical Engineering
Department of Telematics

ISBN 978-82-326-1470-7 (printed version)
ISBN 978-82-326-1471-4 (electronic version)
ISSN 1503-8181

Doctoral theses at NTNU, 2016:66

Printed by Skipnes Kommunikasjon as

Abstract

The Information and Communications Technology (ICT) industry has through the last decades changed and still continues to affect the way people interact with each other and how they access and share information, services and applications in a global market characterized by constant change and evolution. For a networked and highly dynamic society, with consumers and market actors providing infrastructure, networks, services and applications, the mutual dependencies of failure free operations are getting more and more complex. Service Level Agreements (SLAs) between the various actors and users may be used to describe the offerings along with price schemes and promises regarding the delivered quality. However, there is no guarantee for failure free operations whatever efforts and means deployed. A system fails for a number of reasons, but automatic fault handling mechanisms and operational procedures may be used to decrease the probability for service interruptions.

The global number of mobile broadband Internet subscriptions surpassed the number of broadband subscriptions over fixed technologies in 2010. The User Equipment (UE) has become a powerful device supporting a number of wireless access technologies and the always best connected opportunities have become a reality. Some services, e.g. health care, smart power grid control, surveillance/monitoring etc. called critical services in this thesis, put high requirements on service dependability. A definition of dependability is the ability to deliver services that can justifiably be trusted. For critical services, the access networks become crucial factors for achieving high dependability. A major challenge in a multi operator, multi technology wireless environment is the mobility of the user that necessitates handovers according to the physical movement.

In this thesis it is proposed an approach for how to optimize the dependability for critical services in multi operator, multi technology wireless environment. This approach allows predicting the service availability and continuity at real-time. Predictions of the optimal service availability and continuity are considered crucial for critical services. To increase the dependability for critical services dual homing is proposed where the use of combinations of access points, possibly owned by different operators and using different technologies, are optimized for the specific location and movement of the user.

A central part of the thesis is how to ensure the disjointedness of physical and logical resources so important for utilizing the dependability increase potential with dual homing. To address the interdependency issues between physical and logical resources, a study of Operations, Administrations, and Maintenance (OA&M) processes related to the access network of a commercial Global System for Mobile Communications (GSM)/Universal Mobile Telecommunications System (UMTS) operator was performed. The insight obtained by the study provided valuable information of the inter woven dependencies between different actors in the delivery chain of services.

Based on the insight gained from the study of OA&M processes a technological neutral information model of physical and logical resources in the access networks is proposed. The model is used for service availability and continuity prediction and to unveil interdependencies between resources for the infrastructure. The model is proposed as an extension of the Media Independent Handover (MIH) framework. A field trial in a commercial network was conducted to verify the feasibility in retrieving the model related information from the operators' Operational Support Systems (OSSs) and to emulate the extension and usage of the MIH framework.

In the thesis it is proposed how measurement reports from UE and signalling in networks are used to define virtual cells as part of the proposed extension of the MIH framework. Virtual cells are limited geographical areas where the radio conditions are homogeneous. Virtual cells have radio coverage from a number of access points. A Markovian model is proposed for prediction of the service continuity of a dual homed critical service, where both the infrastructure and radio links are considered. A dependability gain is obtained by choosing a global optimal sequence of access points. Great emphasizes have been on developing computational efficient techniques and near-optimal solutions considered important for being able to predict service continuity at real-time for critical services.

The proposed techniques to obtain the global optimal sequence of access points may be used by handover and multi homing mechanisms/protocols for timely handover decisions and access point selections. With the proposed extension of the MIH framework a global optimal sequence of access points providing the highest reliability may be predicted at real-time.

Preface

This thesis is submitted in partial fulfillment of the requirements for the degree of Philosophiae Doctor (PhD) at the Norwegian University of Science and Technology (NTNU). The PhD study was formally conducted at Department of Telematics (ITEM).

The work was performed at the Centre for Quantifiable Quality of Service in Communication Systems (Q2S), Centre of Excellence (CoE), during 2008-2012 and ITEM during 2012-2015, and has been supervised by Professor Bjarne E. Helvik. Q2S was appointed by the Research Council of Norway January 1st 2003 and fully funded by the research council, NTNU and UNINETT. Q2S was closed December 31st 2012.

In addition to the research work, it included mandatory courses corresponding to one full-time semester study, and a half year teaching assistance, funded by ITEM.

This thesis has been formatted in LaTeX using a modified version of the document class *kapproc.cls* prepared by Amy Hendrickson, TeXnology Inc.

Acknowledgements

First and foremost, I would like to express my gratitude to my supervisor and mentor Professor Bjarne E. Helvik for his thoroughness in discussions, feedback and advices that certainly challenged, motivated and educated me during the period at Q2S/ITEM and through all the phases of the work with the thesis. I would like to thank all the members and co-authors within the EuroNF [1] RISKASIP [2] project for valuable discussions and collaboration with the published paper summing up our findings.

I would also like to acknowledge the valuable help from the Incident Manager, the OSS Manager and the OSS System Administrator at a commercial GSM/UMTS network operator that provided information of OA&M processes and access to data for incident and change management. This data and access allowed early testing of the proposed approach.

I thank all the former people at Q2S and current people working at ITEM for creating an inspiring and enjoyable working and learning atmosphere. I have really enjoyed the lunch and coffee breaks with the colleagues. I appreciate all the efforts of the faculty staff in organizing inspiring colloquiums and meetings for educational and knowledge/information sharing purposes. I also want to thank PhD candidate Laurent Paquereau for his help and support for any LaTeX related questions and the administrative staff for always being positive and helpful making a pleasant working environment.

Finally, I'm thankful to my wonderful fiancée Siw Iren, for her unconditional support and everlasting encouragement always with a great smile, and to our three children, Didrik, Brage and Tilja, for making my life meaningful and the confidence of happiness.

[1] Euro-NF Network of Excellence (Grant Agreement N 216366). Objective: ICT-2007.1.1: The Network of the Future. Funded under the Seventh Framework Programme (2007-2013) of the European Community for research, technological development and demonstration activities.

[2] A specific joint research project within the Euro-NF funded through the second call.

Contents

Abbreviations

3GPP	3^{rd} Generation Partnership Project
ANN	Artificial Neural Network
AP	Access Point
ARPU	Average Revenue Per User
AS	Autonomous system
ASN-GW	Access Service Network Gateway
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
CAPEX	capital expenditure
CINR	Carrier to Interference plus Noise Ratio
CMT	Concurrent Multipath Transfer
CoE	Centre of Excellence
CPU	Central Processing Unit
CRNA	Center for Resilient Networks and Applications
CVaR	*Conditional Value-at-Risk*
DAR	Dynamic Address Reconfiguration
DFT	Discrete Fourier Transform
EDGE	Enhanced Data rates for GSM Evolution

eNB	Evolved Node B
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GA	Genetic Algorithm
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSMA	GSM Association
HPP	homogeneous Poisson process
HSPA	High Speed Data Access
HW	Hardware
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
ILP	Integer Linear Programming
IoT	Internet of Things
IP	Internet Protocol
IQR	Inter Quartiles Range
IS-IS	Intermediate System to Intermediate System
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
ITEM	Department of Telematics
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
JAIPA	Japan Internet Providers Association
KPI	Key Performance Indicator
LTE	Long Term Evolution
M2M	Machine to Machine

MDP	Markov Decision Process
MDT	Mean Down Time
MIB	Management Information Base
MICS	Media Independent Command Services
MIES	Media Independent Event Services
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIIS	Media Independent Information Service
MIPv6	Mobile IPv6
MME	Mobility Management Entity
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failures
MUT	Mean Up Time
n.e.d.	negatively exponentially distributed
NHPP	non-homogeneous Poisson process
NIST	National Institute of Standards and Technology
NTNU	Norwegian University of Science and Technology
OA&M	Operations, Administrations, and Maintenance
OPEX	operational expenditure
OSS	Operational Support System
PC	Personal Computer
PhD	Philosophiae Doctor
PLMN	Public Land Mobile Network
PoA	Point of Attachment
PWE	Pseudo-Wire Emulation
Q2S	Centre for Quantifiable Quality of Service in Communication Systems
QoE	Quality of Experience

QoS	Quality of Service
RNC	Radio Network Controller
RSSI	Received Signal Strength Indicator
S-GW	Serving Gateway
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SHIM6	Site Multihoming by IPv6 Intermediation
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SLO	Service Level Objective
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSID	Service Set Identifier
SW	Software
T-MPLS	Transport MPLS
TCO	Total Cost of Ownership
TDM	Time-Division Multiplexing
TMN	Telecommunications Management Network
TVaR	*Tail Value-at-Risk*
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPS	Uninterruptible Power Supply
VaR	*Value-at-Risk*
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWW	World Wide Web

List of Papers

Publications Included in the Thesis

The papers listed below are included as Part II of this thesis. The numbering sequence of the papers follows the order various topics are adressed and not necessarily the date of publishing.

All papers have been subject to international peer-reviewing before being published in workshop/conference proceedings or journals. Note that some of the papers have been subject to minor editorial changes since their publication.

- **PAPER A**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *Managing availability in wireless inter domain access.* Ultra Modern Telecommunications Workshops, pp. 1-6, St. Petersburg, Russia, October 2009.

- **PAPER B**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *Determining dependencies in multi technology inter domain wireless access; A case study.* GLOBECOM - conference record / IEEE Global Telecommunications Conference, pp. 1146-1150, Miami, USA, October 2010.

- **PAPER C**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *Failures and changes in cellular access networks; A study of field data.* Proceedings of the 9$^{\text{th}}$ International Workshop on Design of Reliable Communication Networks (DRCN), pp. 132-139, Kraków, Poland, October 2011.

- **PAPER D**:
  Piotr Cholda, Eirik Larsen Følstad, Bjarne E. Helvik, Pirkko Kuusela, Maurizio Naldi and Ilkka Norros. *Towards Risk-aware Communications Networking.* Reliability Engineering & System Safety, vol. 109, pp. 160-174. January 2013.

- **PAPER E**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *Reliability modelling of access point selection and handovers in heterogeneous wireless environments.* Proceedings of the 9$^{\text{th}}$ International Workshop on Design of Reliable

Communication Networks (DRCN), pp. 103-110, Budapest, Hungary, March 2013.

- **PAPER F**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *The cost for meeting SLA requirement; implications for customers and providers.* Reliability Engineering & System Safety, vol. 145, pp. 136-146, January 2016.

- **PAPER G**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *Optimizing service continuity in a multi operator multi technology wireless environment.* Proceedings of the 9th International Workshop on Design of Reliable Communication Networks (DRCN), pp. 111-118, Budapest, Hungary, March 2013.

- **PAPER H**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *Using genetic algorithms for optimizing the reliability of dual homed critical services.* Proceedings of the 6th International Workshop on Reliable Networks Design and Modeling (RNDM), pp. 158-164, Barcelona, Spain, November 2014.

- **PAPER I**:
  Eirik Larsen Følstad, Bjarne E. Helvik. *Maximizing the reliability of dual homed, critical services in wireless/cellular networks.* Optical Switching and Networking, vol. 19, part 2, pp. 110-121, January 2016.

Part I

THESIS INTRODUCTION

Introduction

In the modern society the usage of services and applications accessible over any communications network has become an important and integrated part of the everyday life. The number of services, applications and content accessible over the Internet is uncountable. The uptake of new services offered on the global market is very difficult to predict, and some of them such as YouTube, Skype, Facebook, Twitter and Instagram have an exceptional growth. These services were originally meant for social communities, but have been widely used also for business and media firms because of the huge number of individuals using these services and their impacts for reputation and sales [KHMS11]. For business users the access to private networks and remotely hosted services, possible cloud based, are crucial. Machine to Machine (M2M) markets are fast growing [Emm10, FFK+11, WTJ+11], widely used for alarm/monitoring systems, health care, transportation etc. With the Internet of Things (IoT) the M2M markets are expected to accelerate even faster [AIM10, BZ14]. The business and M2M services may be more tailor made, e.g. providing end-to-end integrated solutions, than the more general available services.

To provide the users with services there are several market actors. Network operators want to provide access for the users to their own services/content and to the Internet and other service providers in a cost and quality efficient manner. Network operators often use services from other actors to fulfil the requirements and demands from their own users and for being competitive and cost effective. National and international regulators use regulations to ensure public affordable services with reasonable quality.

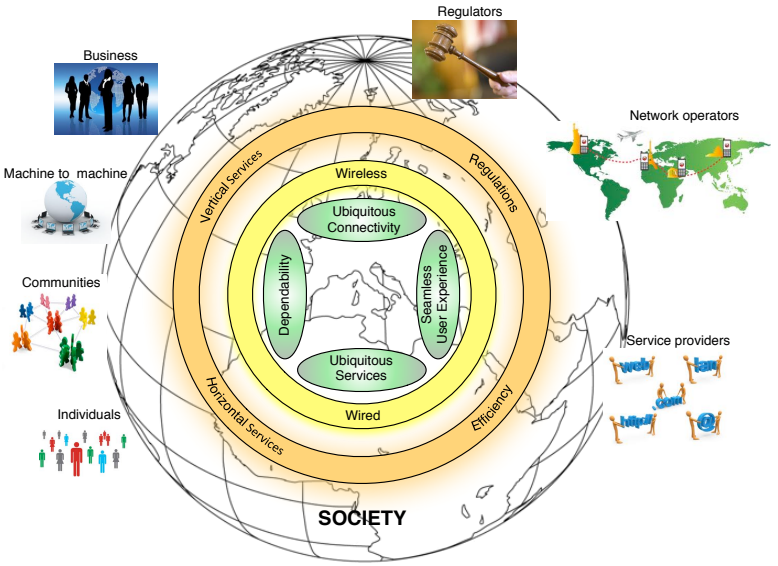

Figure 1. Actors - users perspective the communication eco-system (adapted from [TCv10]).

Fig.1 (adapted from [TCv10]) is a sketch of the communication eco-system of users and market actors. The users require access to the desired services through any connection, wired or wireless, with seamless experience. Similarly, the service and content providers want to make their services and content available to the users through any network. The usage of cellular access has boosted with the increased available throughput, reduced delay/jitter with commonly available High Speed Data Access (HSPA) and Long Term Evolution (LTE) networks [BD12] and widespread of affordable and powerful User Equipment (UE) world wide. The growth of the global number of mobile broadband Internet subscriptions has been so high that it surpassed the number of broadband subscriptions over fixed technologies already in 2010 [BD12]. Further more, it is predicted that the volume of traffic in Wireless Fidelity (WiFi) networks, that already exceed that of cellular networks, can be expected to grow even faster [Sco13]. Cisco [Cis15] estimates that the WiFi will increase to offload the cellular networks in the period 2014 to 2019.

Trust of the system, consisting of the technology, services, operators and service/content providers, is required for the users to use services and applications. To quantify the trust, dependability of a system is defined as *"Trustworthiness of a system such that reliance can justifiably be placed on the service it delivers"* [ALRL04]. Different services require different dependability requirements depending on their usage. For instance, emergency calls require higher dependability requirements than ordinary voice calls. Other critical services may be

used for health care [PKV+02, NSTW06, Var07], smart power grid control [CP10, GSK+11], surveillance/monitoring etc. where the role of wireless access is expected to become more prominent. For critical services using the wireless access the user mobility and radio coverage are challenging. Opportunities for improving the dependability of critical services are the potential diversity in the wireless access through different operators/domains and technologies to increase the dependability of the access. This is also one of the key findings reported [KAB+14] by the Center for Resilient Networks and Applications (CRNA) based on their measurement performed in Norway during July to December 2013. The topic of the PhD thesis is how to manage the access dependability for critical services in wireless inter domain environment.

1. Dependability in wireless/cellular context

In this section a description of wireless/cellular context and the definitions used in the thesis for the wireless access network is given followed by an introduction to service dependability.

1.1 Network and service domains

Since the end of the monopolies of telecom industry, the number of network operators and service providers has increased significantly and changed the industry in terms of new business models and strategies [LW02]. In contrast to the age of monopoly, the users may now select from a wide range of different network operators that offer wireless or wired access to Internet. And of course, once reached the Internet, the user may select from uncountable services and applications. In spite of this diversity of network operators, the corresponding networks are not necessarily independent entities. Without proper information it is difficult to distinguish between miscellaneous network operators and operator/service brands. Subscriptions, correlated to a Subscriber Identity Module (SIM) or another identification for service activation and payment, or network access identity, such as Service Set Identifier (SSID) or Public Land Mobile Network (PLMN) codes, are typically to market brands and do not provide information about the actual access network operator(s).

A network is often composed of a web of autonomous subnetworks, aka. domains, each with its own business model, strategy and operational processes. In such an inter domain environment, the end user services are delivered through a structure of interconnected domains. Even though Internet Protocol (IP) is used between the UE and the server(s) hosting the service/application, the connection may traverse a wide range of different technology layers through a number of domains. For example, in wireless operations it is not uncommon that competitors are leasing backhaul transmission from the same network operator. The distribution of power/electricity may be seen as a domain, but unlike the telecom industry the power/electricity distribution actors still have a de facto monopoly in regional areas.

When analyzing the dependability of services the *system* needs to be understood and modelled. The *system* consists of physical and logical entities from the UE through the web of interconnected domains to the service/application server(s) that are planned, operated and maintained by the owners of the domains.

A sketch of the *system* for users accessing services in wireless environment focused on the network and service domains is depicted in Fig.2. Each domain owner has a number of activities/processes like business, Operations, Administrations, and Maintenance (OA&M) and planning for changing the physical and logical entities in their network and services for fulfilling the customers' needs and for restoration after failures. Important aspects shown in the figure are the different provider-customer relations and the dynamics between the domain owners governed by their activities/processes. An end-user may use one wireless access network, where the operator of this domain again use services from several other domains. In such an environment, a failure in one domain has possible consequences for several other domains and end-users of all affected domains.

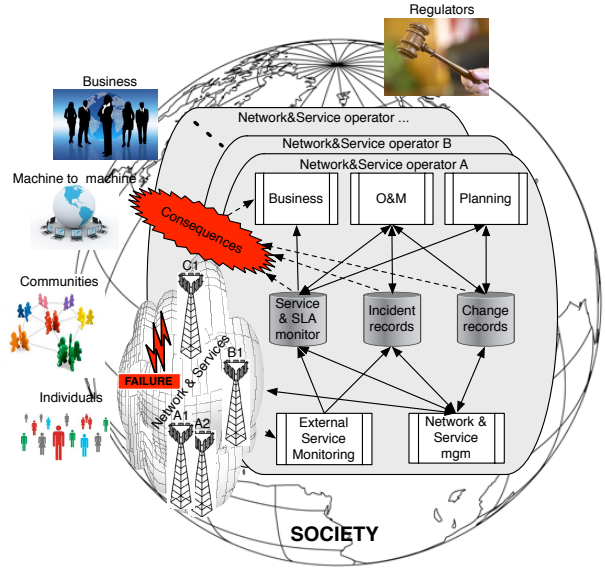

Figure 2. The wireless environment and dependability context.

It is very hard to evaluate the consequences of a failure in one of the domains, because the failure may cause a cascade of service interruptions for other domains and users. In addition, the consequences cannot necessarily be

monetarily measured since the actual used services affected by the failure may be unknown.

The OA&M procedures related to physical and logical modifications and changes in the various domains effectively contribute to a highly dynamic environment for service provisioning through the various parts of the *system*. Appropriate failure measurement data combined with actual *system* topology information at the time of failure are rarely publicly available. Even though failure measurement data was available, a dependability analysis with this data only may easily become invalid since the underlying *system* topology affecting the service may already have changed considerably.

1.2 Access networks

The on-going technology trends and the emerging networks are converging towards diverse sets of access networks, wired or wireless, connected and integrated into IP networks. In this thesis the focus is on the wireless access networks. The wireless networks provide a flavour of different technologies such as WiFi, Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), LTE and Worldwide Interoperability for Microwave Access (WiMAX). Different wireless technologies are expected to co-exist because of business models, deployed infrastructure, widespread of supported UEs, regional competition, regulatory issues etc.

In this thesis the term wireless access network is used to describe the infrastructure and the radio link between the UE and the core network as exemplified in Fig.3. The infrastructure is not limited to only active elements such as access points and routers, but includes also passive elements like fibres, power and cooling equipment. The interfaces between the wireless access networks and the core network are constituted by the radio controllers, called Wireless Local Area Network (WLAN) Controller, Access Service Network Gateway (ASN-GW), Base Station Controller (BSC) and Radio Network Controller (RNC) for WLAN, WiMAX, GSM and UMTS respectively. The radio controllers manage often several wireless access points and perform functions such as SW/configuration management, radio resources management, admission control, mobility, handover control, security and Quality of Service (QoS).

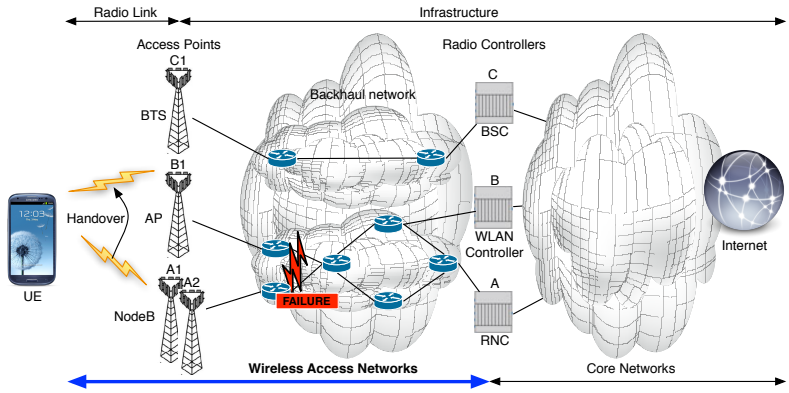

Figure 3. Overview of relations between a UE and some example wireless access networks and core networks.

Similar as described in Section 1.1 the wireless access networks consist of different interconnected domains. In Fig.3 three access network operators are indicated, named A, B and C. In this simple example the network operators A and B share parts of the backhaul network between the particular access points and the radio controllers. The failure illustrated in one router in the figure affects though only access points A1 and A2 of access network operator A. In a situation where a UE used A1 or A2 a handover had to be initiated to either B1 or C1 assuming these were the only other access points in the area.

Handover from one access point to another without service interruption is challenging in an inter domain environment. Adding mobility of the user makes this challenge even harder, caused by the need for access point discovery, decision for handover and the actual handover execution. Without timely handover execution the user may easily move outside the radio coverage of the access point used with the consequence of a service interruption. In Fig.3 only four access points are indicated with the backhaul network and radio controllers. With user mobility different sets of access points may be accessible according to the movement of the user. This movement contributes effectively to structure dynamics of the access points as well as the backhaul network and interdependencies between the domains.

1.3 Service dependability

Many people have experienced themselves or been informed, through e.g. online newspapers or social media, about failures in a wireless access system that have affected some services in a negative way. Typical in a wireless access system is the loss of coverage from an access point that will lead to a service interruption if a handover to another access point is not possible or not executed in due time. The cause of loss of coverage may be due to

e.g. the distance, geographical or building constraints that degrade the signal level or quality from the access point. However, the loss of coverage from an access point fails for a number of other reasons such as e.g. power loss, interference/noise, antenna misalignment and HW failures in the access point. Further, in addition come the effect of failures in the backhaul network and consequences of capacity constraints, SW bugs, OA&M activities and malicious actions. In the thesis failures are limited to unintentionally events whereas malicious actions are not taken into account.

A failure may affect services in different ways depending on the requirements or expectations the service in concern puts on the *system* as well as the service differentiation and related mechanisms deployed in the *system*. A service specification in terms of packet loss, throughput and packet delay/jitter may describe the minimum to be delivered from the *system* for providing a satisfactory service otherwise it will become a service interruption. Often more parties are involved in a compound service delivery chain where the delivery of the services between them and the related economic transactions are regulated through Service Level Agreements (SLAs), see for instance [E-806, Har05, WB10, TBvdZ04]. SLAs may also include dependability aspects of the delivered services, but an SLA cannot in general guarantee the dependability promises.

Aviziensis et al. [ALRL04] define the dependability as the ability to deliver services that can justifiably be trusted. Dependability is an aggregated concept which consists of the attributes as defined in [ALRL04] and [E.808];

1.) *Availability*: readiness for correct service.
2.) *Reliability*: continuity of correct service.
3.) *Safety*: absence of catastrophic consequences for the user(s) and the environment.
4.) *Integrity*: absence of improper system alterations.
5.) *Maintainability*: ability to undergo modifications and repairs.

This thesis mainly addresses the dependability attributes availability and reliability for the service delivery session in the wireless access networks as described in Section 1.2. The service delivery session is from the start of using the actual service/application to a defined end of service mission. In wireless environment, it may have a great impact on the service dependability whether the user is moving or not. This is mainly due to the need of change of access point when the user is on the move. For a user on the move the service reliability may be of utmost importance and therefore it is advantageous if the reliability throughout the service mission may be optimized and predicted before the service is started.

The availability and reliability of a *system* may be found by a number of different approaches, usually separated into two categories: combinatorial model methods and state-based stochastic model methods. In the thesis the main models used are structure functions and Markov models. The predicted

interval availability for an observation interval may be found as

$$A(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} I(t)dt \tag{1}$$

where $I(t)$ is the a function describing whether the *system* provides a satisfactory service, $I(t) = 1$ or service interruption, $I(t) = 0$. The predicted continuity of correct service from a given time instant for a service mission time t_m, i.e., with no service interruptions, is given by the reliability function

$$R(t_m) = P(T_{FF} > t_m) = P\big(I(t) = 1, 0 \leq t < t_m\big) \tag{2}$$

where T_{FF} is the time to the first failure event, i.e., service interruption, since the start of the session. For a critical service delivery session the probability for a service interruption during the mission time t_m should be minimized.

The prediction of the dependability attributes availability and reliability of a service in wireless environment is challenging. Firstly, the wireless access may be composed of a number of subsystems and domains in a structure that interwork together to deliver the service. Secondly, as the user moves these structures of subsystems and domains change dependent on the access point used. Thirdly, as the user moves in the wireless environment a number of access point may be selected. These characteristics indicate the need to have suitable information and models of the wireless access networks to predict and optimize the service dependability.

2. Initial motivation

New services are launched in a tremendous speed in a global market where the services are accessible over any access network irrespective of the location of the user. For instance, after just 16 months Instagram had more than 25 million users with only 13 employees [BGC12]. Similar, the smart power grid and health care services are fast growing markets where wireless communication technologies are important [NSTW06, AE10, FMXY12, SAU12, ABC13].

The various services are fulfilling different needs and demands from the users, network operators, service providers and the society in general. The context and actual usage play a significant role for expectations and requirements for the service. For example, the emergency voice calls have different requirements than ordinary voice calls. Both emergency voice calls and ordinary voice calls use the same basic voice service, but the called numbers differ and are recognized and handled accordingly in the UE and networks/domains.

With the increasing usage of the wireless access as the primary means in emerging regions [BD12], and maybe the only possible in certain geographical locations, the dependability requirements are essential. Unlike the wired access the wireless access causes a continuously change of the *system* structure and radio link conditions with the mobility of the user.

The definition of critical services will not be explicit given nor described in the thesis, though examples of such could be health care services, alarm

monitoring, surveillance and similar. Common for critical services are the availability and reliability requirement, i.e., probability of finding the service in the satisfactoriness state when needed and with no service interruption during the service session. For instance, the availability of a needed wireless access may be critical and a service interruption is not acceptable once the service is started. This illustrates fundamental challenges, how to predict the optimal service reliability and how this may be achieved.

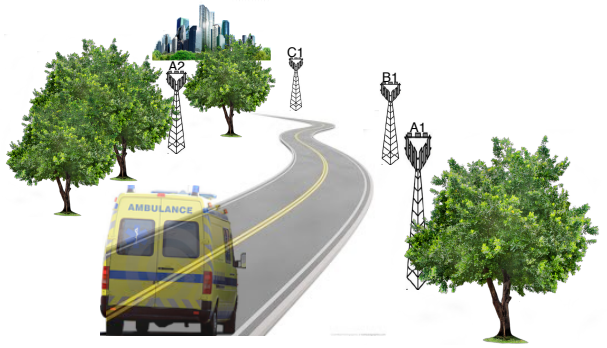

Figure 4. Critical services exemplified where communication between hospital and ambulance is needed for an extensive medical care of the patient.

A scenario is illustrated in Fig.4 where an ambulance with a patient is driving towards the hospital. For extensive medical care of the patient the paramedics need to communicate with the emergency physicians at the hospital. This communication exemplifies a critical service. As may be found in the figure only part of the road towards the hospital is shown and just few of the access points are indicated.

The initial motivation is how to *predict the optimal service continuity, i.e., the reliability, of critical services and be warned if the requirements are not met or likely to be violated if she/he proceeds in wireless environment.*

The optimal service reliability may be achieved by using a given series of access points S along the selected road satisfying

$$\arg\max_{S} R(t_m) = \arg\max_{S} P(T_{FF} > t_m) \tag{3}$$

How to find this series of access points S that optimizes the service reliability leads to the initial main questions as basis for the thesis:

i.) **How to manage the optimal service continuity?**
The main challenges are to establish a prediction model of the service continuity and then find the optimal sequence of access points and handovers from the start to the end of the service session. This model must take into account the multi domain, multi technology wireless access

environment and the mobility of the user. To increase the probability for service continuity the model should accomplish to build a fault tolerant *system* from the available subsystems of independent multi domain, multi technology wireless access networks.

ii.) **Is a technical solution feasible?**
Even with a model for managing and keeping control of the optimal service continuity there exists a number of issues for having a feasible technical solution. The model itself needs to be designed and populated with information of the behaviour of each of the subsystems. This information needs to be updated and maintained to reflect the actual subsystems behaviours that undergo continuously modifications and changes. The subsystems may correspond to different actors, with their own organizational structure, business model, OA&M procedures/processes etc. When an optimal sequence of access points is identified with the model the UE needs to connect to specific access points at appropriate geographical locations.

3. Dependability challenges and opportunities

In this section a background and discussion of how the dependability aspects of critical services relate to the different actors, in a compound delivery chain of various domains and technologies. The challenges and opportunities are lead towards the initial motivation given in Section 2.

To give an overview of the discussion Fig.5 illustrates the scope of the work and is used as a reference figure in the thesis. On the right hand side of the figure the backhaul network and the radio controllers are exemplified. The left hand side shows the access points with their indicated radio coverage. Note that the power and cooling infrastructure are not explicitly shown in the figure. Three access network domains are indicated in the figure, but e.g. the backhaul network and power distribution add more domains. In the figure, two failures are indicated, one failure affecting one of the radio links for a dual homed service and one failure affecting a router in the backhaul network. The figure and it's context will be explained in more details in the following.

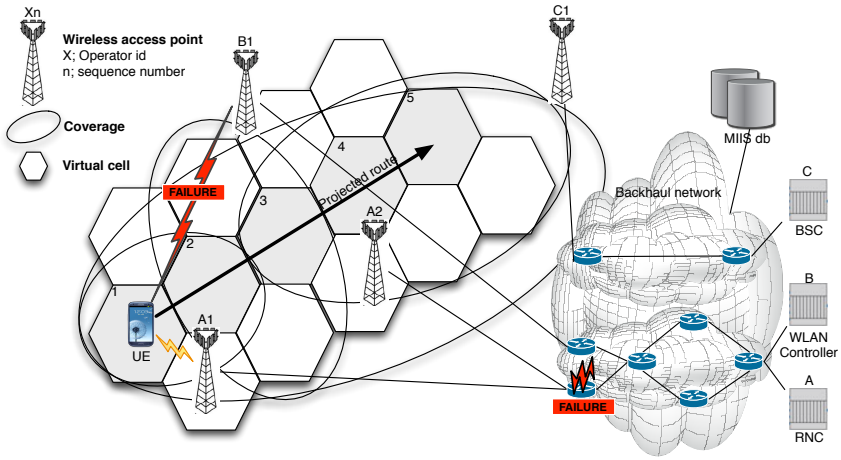

Figure 5. A reference figure as basis for the thesis. Two failures are indicated, one failure affecting one of the radio links for a dual homed service and one failure affecting a router in the backhaul network.

3.1 Users

Users' behaviours have changed with the evolution of wireless technology and services. Services and applications are accessed using UEs, like PC's, dongles, tablets and smartphones, supporting a variety of wireless technologies. Users select the UE and the network according to their preferences and the expected needs. The concept *always best connected* was defined in [GJ03] as a user that is connected through the best available access network and device at all times. This concept includes several aspects such as personal preferences, QoS requirements, cost, available network resources and network coverage. An SLA may be used to describe the services and the related QoS requirements as Service Level Objectives (SLOs). In the thesis it is assumed that the suitable UE is supporting the critical services with appropriate Central Processing Unit (CPU), memory, external interfaces and position means like Global Positioning System (GPS).

Personal preferences for wireless network access selection criteria have, with few exceptions, been dominated by the cost of usage and throughput, while the dependability attributes have been more or less neglected. Though, the radio coverage itself of an access network operator may be seen as a availability requirement. Some users therefore tend to actively select the access network that provides radio coverage in the desired geographical areas. Radio coverage is a competitive asset for the wireless network operators and subscriptions or payments are needed for being granted access.

For critical services the dependability is crucial and for emergency calls, particular in cellular environment, it has been a requirement from the regulators that these services shall be offered for free, independent of subscriptions. This means that a user that makes an emergency call may use any available network supported by the UE covering the particular geographical area.

The emergency call scenario is in general not sufficient for critical services, where the service continuity independent of mobility is essential. Handovers to different networks/domains must be possible. Subscription or free access in all networks/domains is an advantage, but it does not solve the service continuity and handover alone. Before any handover might take place, the target networks must be discovered. This is a cumbersome and time-consuming process, since there are a number of frequencies and technologies to search through for identifying suitable access points. Not only does this take long time, but it also consumes the UE battery. Even if the target access points could be discovered, the handover decision and execution are not straightforward and might take too much time to perform successfully [DDF+07, CIRG09, NFS+09].

With reference to Fig.5 the projected route is the physical movement of the user. The projected route may be determined by physical constraints, like roads and traffic, or by other means such as navigation tools. Even though the projected route of the user is known, the possible access points along the route, network domains and radio conditions are not known in advance. In the figure radio coverage from the access points are indicated with ellipses that demonstrate the need for handovers along the projected route. For optimal service continuity, handovers should also be considered if another more dependable access exists within the radio coverage of the access point already used. With prediction of the service continuity of several possible projected routes, the user may select the projected route that provides the lowest probability for service interruption.

Referring to the initial main question i.) in Section 2 a partitioning of the geographical area into virtual cells, exemplified with hexagons in Fig.5, allows a UE to select the most dependable access point in each virtual cell. However, a handover from an access point in one virtual cell to another may cause a probability for service interruption. How to identify the virtual cells, represented by hexagons in Fig.5, will be described in the papers presented in the second part of the thesis.

3.2 Network operators and service providers

Running business and the return of investments for the stakeholders are main targets for network operators and service providers. To position themselves these actors need to be competitive for the service offerings and to attract customers to use their networks and services. One of the major challenges is to balance the cost vs. the revenue both in short and long term.

The widespread of wireless access and powerful UE combined with their capabilities have changed the service delivery. For traditional cellular operators

this is a mixed blessing, since the traditional profitable services like e.g. voice and messaging (SMS/MMS) are becoming threatened by new similar services that other service providers may provide over the data bearers. The revenue per bit/s for traditional voice services and messaging has been considerable higher than the revenue per bit/s for data for the network operators. For this reason it is a trend that network operators offers access for a fixed fee per unit of time (e.g. day or month) independent of the actual services used. Such price models are means to avoid price competition with the new services and to avoid reduction in Average Revenue Per User (ARPU).

With the ambitions to continuously increase or stabilize the ARPU combined with mature markets, high competition and very fast growing demand for data services, the pressure on cost efficiency has become more evident. The traditional cooperations between network operators based on site sharing and hiring leased line transmission are becoming by far more developed [BS05, KKKY11, LY15]. Such cooperations also include network sharing and outsourcing of development and maintenance.

The enhanced cooperations between domains introduce more dependencies between the access networks. For critical services the dependencies between domains may reduce the possible network access diversity. The cooperations between operators are governed by SLAs, but this do not prevent a single failure to affect several access network operators simultaneously.

For operational efficiency and to achieve the necessary control and management of the network and work force Operational Support Systems (OSSs) are important for the network operators and market actors in general. The OSSs may be used for a number of network related activities such as change management and incident management [Off07a, Off07b]. Change management includes information of all activities related to network planning, planned changes, ongoing network implementations and current network configuration. Incident management provides information and status of all undesired events in the network and is used for governance of the work force performing the repair.

Referring to the initial main question i.) in Section 2 the network operators' OSSs contain viable information of the network structure and possible interdependencies between the different domains. Information from the change management may be used to extract the network structure from the access points to the radio controllers exemplified in Fig.5. Further, the information from the incident management provides empirical behaviour of the network as well as the current failure status. How utilize the network operators' OSS will be described in the papers presented in the second part of the thesis.

3.3 Regulators

In a simple way the role the regulators may be described as to stimulate and regulate for competition and to promote innovation among network operators and service providers vs. affordable and worthy services for users and society.

In this context, the innovation does not only cover the services per se, but also other aspects such as the operational issues to find cost optimal solutions. As highlighted by the International Telecommunication Union (ITU) [Int13], the regulators need to consider carefully whether their existing legal and regulatory frameworks effectively address the non-discriminatory practices and transparency of information from network and service providers for transnational service offerings. This relates also to the complexity of service provisioning and delivery across interdependent domains.

The role of the regulator may be seen as a double-edged intention, since the operators/providers and users are influenced by the regulation schemes. For instance, on one hand it is desirable to have several network operators for competition, but since the frequency bands are natural limited resources these bands have to be divided between the network operators. The subdivision of the total frequency bands reduces the theoretical throughput available for the users under a varying stochastic workload. On the other hand, too few network operators may introduce duopolies or oligopolies where market shares and market price are stabilized. In addition, the regulator must address the dependability issues of the networks that may affect how networks, and in some extent also the services, are deployed and provisioned.

In the modern society the communication networks have become part of the critical infrastructure for delivering particular services, such as e.g. emergency calls. However, other services beyond the traditional emergency calls are also becoming critical for the society. In recognition the criticality of wireless access networks for the society the regulator needs information of the access network interdependencies, their topologies, insights into OA&M processes etc. for evaluating the dependability of each of the access networks. The evaluations and insights may be used to instruct the access network operators to take actions to remedy against the undesired vulnerableness. For instance, in 2012 the Finnish Communications Regulatory Authority [Fic12] issued regulation applying to the priority rating of the elements in communications networks and services, redundancy, reserve routes, power supply and physical protection.

For the regulators the initial main question i.) in Section 2 is also relevant for being able to evaluate the dependability and interdependencies in the access networks.

3.4 Technical

3.4.1 Media Independent Handover (MIH)

The MIH [IEE09] is an IEEE standard allowing the UE or network to perform the handover decision by utilizing information about the possible access points in the area. Various access points are providing services over a number of different access technologies, such as e.g. WiMAX, WLAN and UMTS. The basic architecture of MIH, adapted from [IEE09], is shown in Fig.6. The Media Independent Handover Function (MIHF) is an immediate

layer between the link layers and the upper layers providing media independent services and commands. The MIHF has basically the same structure both in the UE and in the access point.

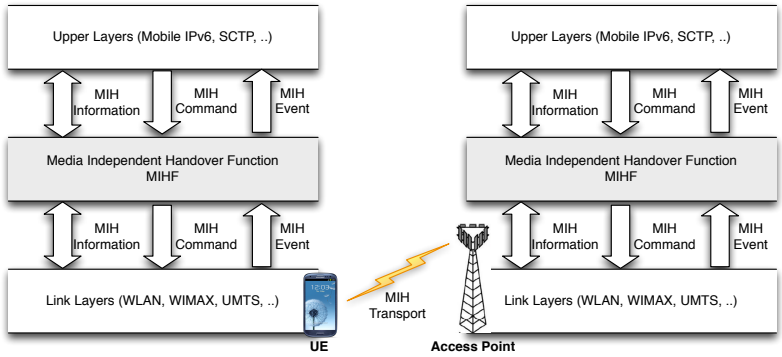

Figure 6. Basic architecture of *Media Independent Handover Function* (MIHF), adapted from [IEE09].

The MIHF provides Media Independent Event Services (MIES), Media Independent Command Services (MICS) and Media Independent Information Service (MIIS) to the upper layer to both local and remote MIHF entities. An upper layer may subscribe to event services from the MIHF, such as e.g. LINK_DOWN and LINK_UP. The MIIS provides information to discover and receive advertisements from other networks, and to request additional information. For discovering/querying of network information of the serving and neighbour networks the MIIS database may be used. MICS provides the MIH users to send commands to the lower layers. With this the MIH users can utilize command services to determine status of wireless links and/or control the multi-mode device for optimal service continuity.

MIH is an attractive framework because it facilitates how a MIH user may request information services independent on the actual access point used. The MIH framework defines a transport service that allows a MIH user in the network to send and receive commands, events and information from other MIHF entities in the network.

Referring to the initial main question ii.) in Section 2 the MIH framework provides a generic solution for updating, storing and retrieving structure and topology of the access networks. For instance, in Fig.5 the upper layers in UE may use any access points, e.g. C1, and utilize its local MIHF to get information about the other access points in the neighbour area. Though, the MIH framework does neighter describe the actual implementation of the MIIS database nor how it is populated. How to extend the MIH framework and populate the MIIS database with access network structure and dependability

attributes will be described in the papers presented in the second part of the thesis.

3.4.2 Handover

Fundamental challenges for handover algorithms are the decision and the actual execution phases. The decision phase has to evaluate the performance of the serving access point versus the performance of target access points. To identify potential target access points a search have to be accomplished. After performance evaluation selecting the desired access point a handover execution is needed in due time to the new best fitted target access point.

A lot of research has been performed to analyze efficient, reliable and seamless handovers. Overviews and surveys of handovers in multi domain, multi technology environment may be found in [KKP08, YSN10, MBCCM11, ZJZ12, WK13]. There exists some promising handover algorithms for certain user requirements and preferences for some network scenarios and conditions, but a general conclusion is that devising an algorithm optimal for all situations is difficult. Even though an optimal mixture of metrics could be defined for optimizing the handover, potential target access points have to be efficiently found. This identification has to be combined with an optimal timing when the current access point is predicted to no longer being the best access point to use. The MIH framework has some properties that may be used for initiating a handover decision.

The MIH framework provides the LINK_GOING_DOWN event to the upper layers such that the upper layers can initiate the handover procedure. The trigger for this event is not part of the MIH framework. A proposal for the trigger was proposed in [LMK08] based on the Received Signal Strength Indicator (RSSI) in WLAN and Carrier to Interference plus Noise Ratio (CINR) for WiMAX and it was showed that a LINK_GOING_DOWN could be predicted more than one second ahead of time. With the information proposed in MIIS, a LINK_GOING_DOWN event is initiated [YCG07] according to the estimated time needed to perform the actual handover. The actual time need for handover is depending on a variety of factors, such as e.g. mobility issues [DDF+07] , authentication [CIRG09] and resource allocation [NFS+09].

For critical services the service continuity must be predicted in advance before the actual service session is started. Referring to the initial main questions i.) and ii.) in Section 2 the MIH framework may be used as a basis to predict the service continuity and by the handover decision algorithms for finding optimal series of access points along a projected route. Needed handovers may be executed at the boundaries of the virtual cells. Details will be described in the papers presented in the second part of the thesis.

3.4.3 Multi homing

For seamless handover execution it is necessary to facilitate a mobility management mechanism that ensures addressing schemes for no service interruption. For instance, in a cellular network there are inherent network functionalities that provide the UE with the same IP address irrespective of the mobility. Such addresses mechanisms are in general not available in inter domains.

Multi homing capabilities may be used to achieve higher dependability for the critical services, but this depends on the disjointedness of the used resources in the access networks and how multi homing protocols utilizes the different connections. Common for all multi homing protocols is the challenge related to connection management, i.e., which access points to use. On top of connection management, the multi homing protocols have to ensure seamless switchover between the connections in case of a failure event of either of the connections.

An overview and discussions of multi homing management and protocols may be found in [SPC11, ZJZ12]. Examples of multi homing protocols are Mobile Stream Control Transmission Protocol (SCTP) and Site Multihoming by IPv6 Intermediation (SHIM6) allowing having multiple IP addresses, one active and the other as candidates when the primary breaks.

In the thesis dual homed critical services are assumed to be used to increase the dependability using one appropriate multi homing protocols such as SCTP or SHIM6. Similar as for a single homed service, the MIH framework may be used to predict the service continuity and by the handover decision algorithms for finding optimal series of access points along a projected route. Within each virtual cell, two disjointed access points are used for the dual homing. The multi homing protocols combined with the extended MIH framework are opportunities to partly answer the main questions i.) and ii.) in Section 2. Details will be described in the papers presented in the second part of the thesis.

4. Related work

The context of the thesis has been described in the previous sections along with some challenges and opportunities for dependable critical services in wireless environment. In this section a description of how the thesis is related to other work is given.

Recall that the context of the thesis is a highly dynamic wireless environment where critical services are delivered through a wide range of different technology layers through a number of interdependent domains, each with its own business model, strategy and operational processes. As consequences of increasing pressure on capital expenditure (CAPEX) and operational expenditure (OPEX) different wireless network sharing principles are deployed to reduce the Total Cost of Ownership (TCO) as discussed in [BS05, KKKY11]. Beckman and Smith [BS05] believe that network sharing allows the value chain to be

disaggregated into a number of new domains which facilitates development of innovative new business models and advanced services.

4.1 Network topology discovery

The information of the network topology has been used in the research community for different needs. Various means have been proposed to achieve the needed granularity of the network topology. Donnet et. al. [DF07] provide a survey for Internet topology discovery mechanisms at the network layer and explained that the most common techniques used are based upon traceroute, Border Gateway Protocol (BGP) routing information and registry information. These techniques do not capture the link level granularity which is one of several pitfalls using traceroute described by Willinger et.al. [WAD09]. Breitbart et. al. [BGM+00] use the Simple Network Management Protocol (SNMP) Management Information Base (MIB) in the network elements (bridges and switches) to obtain the address forwarding tables. Markopoulou et. al. [MIB+08] analyze Intermediate System to Intermediate System (IS-IS) routing updates from the Sprint IP backbone network to characterize failures that affect IP connectivity. They also found it necessary to include failure information from underlying Synchronous Digital Hierarchy (SDH) network to further confirm their failure classification methodology. In wireless access networks where the end users are given an IP address the underlying network structure cannot easily be identified with IP analyze alone since encapsulation and tunneling mechanisms are used in the different domains.

Surveys of applications utilizing and extending the MIH framework may be found in [SSY12, GM13]. Little attention has been put into the network topology, more specifically the backhaul network, and the potential use of the MIH framework for dependability analysis. The dependability parameters related to the physical resources may either be estimated from the domains' failure handling mechanisms and OA&M procedures or using values as provided by e.g. [VCD+05] and [MIB+08]. Note that the values of the dependability attributes in [VCD+05] and [MIB+08] are for certain equipment in certain environment and operational procedures and are not necessarily applicable in other cases.

In a wireless inter domain environment, where the enhanced co-operations and network sharing principles among the domains may be prominent, it is a need for new approaches for obtaining the dynamic network topology of inter woven technologies and to unveil the inter dependencies between the domains. This thesis propose how to utilize the network operator's OSSs for network topology and how this information may be populated into the MIIS database suitable for dependability analysis.

4.2 Radio coverage discovery

Planning and deployment of wireless access points for the access network operators are needed to achieve the desired radio coverage and quality. Typically the access network operators use some prediction/simulation tools to optimize the deployment for the access points. Various propagation models may be used as basis for these algorithms, see e.g. [IY02] for a review of the propagation prediction models for wireless communication systems. Prediction/simulation tools cannot derive actual radio coverage and quality due to a number of model inaccuracies such as e.g. buildings and their materials, geometry of buildings and terrains.

Within 3^{rd} Generation Partnership Project (3GPP) the standardization of measurement reports from UEs [TS313c, TS313b, TS313a, HUI+12] is conducted to minimize the need for network operators' excessive drive tests to verify and monitor radio coverage and to detect problems in the network. Measurement reports are basis for proposals in e.g. [FL09, KAK11, TRDA11, SRM+12] for radio coverage estimation and anomaly detections.

Pahlavan et.al [PKH+00] propose how Artificial Neural Networks (ANNs) may be trained with e.g. RSSI inputs for geographical locations and where some RSSI measurements performed by the UEs are used to select the most appropriate access point in the area. Similar, Nasser et. al. [NGAM07] propose how an ANN algorithm may be fed with network, device and user features/attributes. The network features are collected by the UEs and sent to the ANN for generating a local hop-by-hop handover decision.

For critical services in a wireless multi domain, multi technology environment there is need for new approaches for service continuity predictions. Since the planned radio coverage does not necessarily provide the actual experienced radio coverage and quality, collected measurement reports for UEs may be used as input to a knowledge/experienced base. Several proposals for extensions of the MIH framework have been described in [SSY12, GM13] to allow an UE to retrieve static and dynamic information of access points in the neighbourhood. Similar as Mateus and Marinheiro [MM10] describe an overall architecture where UEs report information about networks currently visited.

This thesis propose how to utilize UE measurement reports as basis for defining the virtual cells, as briefly described in Section 3.1, suitable for dependability analysis. The derived dependability attributes from numerous UE measurement reports are used and not the instantaneous load/quality attributes of the access points as used by most of the approaches found in [SSY12, GM13].

4.3 Dual homing

Multi homing mechanisms have been used to increase dependability and performance. Sousa et. al. [SPC11] provide a survey of multi homing support

from the network to the application layers. For instance, among these surveyed protocols the SCTP protocol has a natively support for multi homing.

Budzisz et. al. [BGBF12] have provided a taxonomy and survey of SCTP research and specific on the multi homing as this has attached the most attention from the research on SCTP. With the Dynamic Address Reconfiguration (DAR), often referenced as mobile SCTP (mSCTP) [RT07], and the Concurrent Multipath Transfer (CMT) extensions [ASS03, IAS06, LWZ08, HLC10] of SCTP the IP mobility handling and the reliability of SCTP is addressed in heterogeneous wireless networks. In [IAS06, LWZ08, HLC10] buffer management approaches are proposed to increase the throughput sending data on several of the available interface. To reduce the packet loss during a handover Aydi et.al. [ASS03] propose to send the same data to two interfaces. In a similar way Kashihara et. al. [KIK+04] describe an approach where both interfaces may be used during periods of unstable transmissions. When the transmission is stable, only one interface is used to reduce the used bandwidth.

Even though dual homing mechanisms have been proposed and are already deployed in various contexts, new techniques are needed for reliability prediction for a dual homed service in a multi domain, multi technology wireless environment. In this thesis it is proposed how such a prediction may be used by dual homing mechanisms to achieve increased reliability for the service.

4.4 Network selection and handover

The network selection and handover decision surveys [KKP08, YSN10, ZJZ12, WK13] describe how context, user preferences and network conditions are used as criteria for handover decisions and the describe the complexity for a handover decision to take all these constraints into account. The algorithms presented in the surveys do maximize the benefits with regards to the desired criteria on a local hop-by-hop basis, except the the Markov Decision Processes (MDPs) that may be used to maximize benefits for the total session.

The MDP approaches [SNLW08, SSNW08, TFC11] describe the handover decisions at certain time epochs where the UE selects the access point to use based upon the current state for a single homed service. A state is described by a number of variables, such as e.g. current access point, indicated instantaneous capacity and delay for all access points in the area. At each time epoch the handover decision is governed by an action with reward and cost. A probability transition function defines the evolution to the next state(s) for the given action. This probability transition function is Markovian since it depends only on the current state and the selected action and not on the previous states and actions. In [SNLW08, SSNW08, TFC11] an optimal stationary deterministic policy matrix is derived that indicates the optimal next state for the current state. By using the stationary deterministic policy matrix the set of access points to use for during each time epochs is found that optimizes the difference between reward and cost. The time epochs are used to discretize the handover decision points for a single homed service. The transition probabilities for next

state at each time epoch may found by simulations [SNLW08, SSNW08] or by some algorithms [TFC11] with given parameters of arrival and departure of users.

For dual homed critical services there is a need for new approaches to predict the highest service continuity where a global projected route is taken into consideration to avoid local radio coverage problems that may threaded the service continuity.

5. Research objectives

The research objectives are based upon the initial main questions i.) and ii.) in Section 2, the challenges and opportunities, and related work as briefly discussed in Section 3 and Section 4.

The initial main questions are partitioned into four research objectives. The first objective is the design and verification of an information model of the access networks suitable for dependability predictions. Then, the second objective is to better understand the operational context of the network operators and the implications on the dependability for the services. With the information model, a prediction method for reliability of critical services is pursued as the third research objective. The fourth research objective is the optimization schemes for critical service continuity. In the following each research objective is described.

5.1 New information models suited for dependability analsysis

The understanding of the *system* is needed for performing dependability analysis. For dual homed critical services in multi domain, multi technology access network environment where co-operations between operators are very likely, the *system* structure is important for unveiling dependencies. The target is to propose an information model of the access networks suitable for dependability analysis. Further, the objective is to propose how this information may be obtained. This method must ensure that the information model is updated and reflecting the actual network conditions. A verification of the concept solution should be conducted.

5.2 Provide insigth into operational context

Prediction of dependability attributes, e.g. service continuity, relates to the likelihood of some future failure events. To better understand such predictions, the networks operator's OA&M strategies in a broad sense are important. In the research community, there are very limited information of failure and repair statistics, *system* dynamics and operational processes in commercial networks. However, recognizing the importance of structure and dynamics network the empirical statistics must be accomplished with insight into the operational processes and strategies. The operational processes and strategies are changing

over time along with the usage, competition and regulations. The target is to provide better insight into the networks operator's OA&M strategies and thereby the also the implications and inter dependencies between domains.

5.3 New prediction methods for dependability

For critical services the service continuity must be predicted in advance before the actual service session is started. The target is to propose new methods for dependability prediction for dual homed critical services based upon an information model identified by the research objective described in subsection 5.1. The prediction method shall include both the radio link and the infrastructure of the access networks for the given set of access points used along a projected route for a dual homed critical service. An efficient access point discovery scheme in a multi domain, multi technology access network environment is needed to ensure an always best connected scenario where service reliability is the desired metric.

5.4 New optimizing schemes for dependability

The research objective described in Section 5.3 provides a prediction method for a given series of access points for a dual homed critical service. For a projected route there exists numerous of possible series of access points with different service reliability. Now, based on the prediction methods pursued by the third research objective described in Section 5.3 the target is to find the series of access points that provides the optimal reliability for a dual homed critical service. Important aspects of this research objective is to find efficient methods that may match the real-time response constraints for the optimal series of access points by the users of the dual homed critical service.

6. Research methodology and approach

Considering the challenges of the research objectives defined in Section 5 for dual homed critical services in multi domain, multi technology wireless environment, the methodology and approach in this thesis, as depicted in Fig.7, are described in the following.

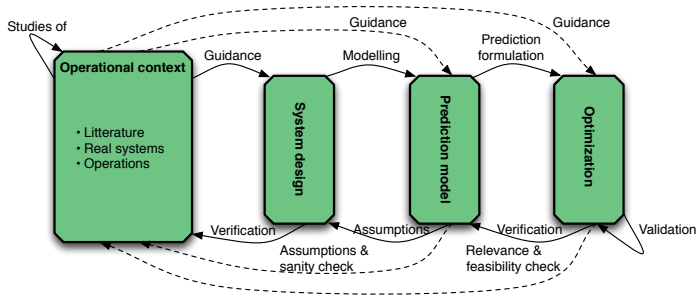

Figure 7. Illustration of the research methodology and approach.

6.1 Operational context

With the capabilities and convenience of extensively use of wireless access to any services and where the trend/vision of using wireless access also for critical purposes, such as e.g. smart power grid and health care services, the service availability and continuity may easily become the prime concerns. In this thesis it is proposed to use dual homing to increase the service availability and continuity for critical services.

A literature study was conducted for better understanding of the challenges, problem identification and analyze, and for pinpointing possible research directions. The literature study covered not only the research community but also industrial communities and standardization bodies, such as GSM Association (GSMA), 3GPP and Internet Engineering Task Force (IETF).

For critical services the prediction of the service continuity prior to actual usage of the service is required due to the risk associated with a service interrupt during the mission time of the service. The consequences of failures are not directly considered in the thesis, but the prediction of the optimal dual homed service continuity is a mean to lower the probability for a service interruption with a possible fatal consequence for the usage. The challenge is to find the optimal access points to use for the dual homing in a highly dynamic environment where each domain rapidly may change its network structure and OA&M processes, and where co-operations between the different domain operators may be prominent.

The dynamics of the domains, governed by their business models and OA&M processes are often considered to be (semi-)static in the research community. In context of critical services, the dynamics of interdependencies of physical and logical entities across domains are important to unveil, to ensure the diversity of the dual homed connections. The thesis author was granted access to OSSs of one commercial GSM/UMTS operator to better understand the operations of real wireless networks and domains. Even tough only one commercial access network operator is basis for the insights, this turned out to provide valuable

information regarding OA&M processes. Such information is rarely publicly available.

6.2 System design

For dual homed critical services the capability at real-time to obtain and predict the optimal service availability and continuity are needed. Time used to derive these predictions are vital as these delay the actual start of the service. With the operational context as a guidance a system design were proposed around extensions of the MIH framework. The basic idea is that with extensions of the MIH framework the optimal service availability or continuity may be derived by identifying the optimal access points to use for a dual homed critical service.

At an early stage with the thesis work it was decided to spilt the wireless access networks into two parts; the radio link and the infrastructure. The background for this separation was due to the different characteristics and how information could be gathered, systematized and modelled. In addition, this allows research to be conducted for each part separately and thereafter combined together. For the radio link, the virtual cells are proposed defined from measurement reports from UE and signaling in the networks. Infrastructure, network topology and interdependencies between domains, are proposed derived from the domains OSSs. A naming convention of resources, for instance the access points, is proposed to keep the various domain specific naming schemes unique also across different domains. A technology neutral model was proposed for logical and physical resources of the infrastructure. The proposed model is able to unveil correlation between entities.

Important prerequisites of the system design were a feasible solution and the ability to perform verification. Based upon the granted access to OSSs of one commercial GSM/UMTS operator, experiments were performed for the infrastructure. A trial implementation and experimental validation of the radio link part remains.

6.3 Prediction model

Service availability and continuity are probabilistic predictions of future events that require a prediction model of the system in concern. Likewise as for the system design, prediction models for radio link and the infrastructure were developed separately and combined. The prediction model is tightly coupled with the overall system design and iterations between system design and prediction model were needed.

As a starting point for the service continuity prediction of a dual homed service, a model for a specific set of access points used along a projected route was developed. This was used as basis for an extended model, where a number of access points were available in every virtual cell. The model was completed by also including the infrastructure. A phased mission Markovian model is

proposed containing phases according to the number of virtual cells along the projected route.

From the given abstractions and assumptions a prediction formulation for selecting the set of access points that optimize the service continuity were developed. In addition, an approximated prediction formulation is proposed with the intension to reduce the computation effort to derive the optimal selection of access points. Once the optimal solution is found with the approximation it may be easily compared with the non-approximated model.

6.4 Optimization

Even with an approximated prediction formulation suitable for optimization, there are different means and techniques to efficient find the optimal sequence of access points with the corresponding predicted service continuity. As a starting point for the optimization, the Integer Linear Programming (ILP) was chosen. The reason for this decision was two fold; ILP optimization was expected to find the (near-)optimal solution, and the solution found may be used as reference for other heuristic optimization techniques. Since the object function of ILP was an approximate formulation of the predicted service continuity, the solution found was not necessarily the optimal.

To avoid the computation effort required to solve the ILP optimization, several heuristic techniques are proposed. The heuristic techniques were not able to use the complete approximated prediction formulation as the ILP. The heuristic techniques were based upon Dijkstra [Dij59] and Bhandari [Bha94]. Even though these heuristics where less computing demanding than ILP, they suffered in finding the near-optimal solutions.

The ILP and heuristic techniques are considered global route optimization techniques. A local hop-by-hop optimization technique was developed to compare the benefit of global route optimization techniques both for service continuity and the number of handovers needed.

A number of synthetic network scenarios were investigated with virtual cells and infrastructure representing access points and domains. The network scenarios are used to benchmark the optimization techniques for the solutions found and the computation effort. To manage the high number of dependability attributes for the virtual cells and infrastructure Mathematica [Wol11] was used. Mathematica is strong in symbolic calculations and has a feature-rich in-build functionality. For the ILP implementation the commercial AMPL and the solver gurobi were selected as this is "state of the art" reference tool in the research community. To efficiently manage an incremental and repetitive research with fairly large data sets, MySQL [MyS10] was used as storage of input data and configurations, immediately results and the final results.

For larger synthetic network scenarios, the computation effort of ILP optimization was consistently far more demanding than all heuristic techniques together, but it always found the (near-)optimal solution. To try to close the gap between the solution found by ILP optimization and the heuristic

techniques, a Genetic Algorithm (GA) was developed. By using the solutions found by the heuristic techniques as seeds for the initial population of the GA better near-optimal solutions than the heuristics were found. The computation effort of GA was still lower than needed by ILP optimization. Even though a fairly large number of replications and control parameter sets were tested the GA did not find better solutions than the ILP optimization which also verified the approximated prediction formulation used.

In the final optimization where also the infrastructure were considered, a problem reformulation was developed that could use Dijkstra's shortest path algorithm [Dij59] directly. But unlike the other developed heuristic techniques using Dijkstra, this new technique was able to always find the same solution as the ILP. In addition, the Dijkstra algorithm is the asymptotic fastest known algorithm for shortest path problems between two points. The computation effort used by Dijkstra outperformed significantly the ILP optimization.

7. Contributions

The main contributions and summaries of the **Papers A** through **I** in Part II are given in this section. A discussion of the papers' assumptions and results are given in the last part of this section.

For all papers, except **Paper D**, **Paper F** and **Paper H**, the thesis author had the original idea and performed the work and wrote the papers under supervision of and in cooperation with the co-author Professor Bjarne E. Helvik.

Paper D is a joint work between AGH University of Science and Technology Kraków, entre for Quantifiable Quality of Service in Communication Systems Norwegian University of Science and Technology, Trondheim, VTT, Technical Research Centre of Finland, Helsinki and Dipartimento di Informatica Sistemi Produzione (DISP) Università di Roma "Tor Vergata", Roma. For this paper the thesis author has been participating in meetings and discussions with the main contributions related to the dependencies between market actors and operational practices at network operators.

For **Paper F** the co-author professor Bjarne E. Helvik had the original idea. We jointly developed the detailed models and performed the analysis. I put the model into and did the discussion on the operational context, developed the necessary analytical, simulation and optimization software and produced the quantitative results.

For **Paper H** the co-author professor Bjarne E. Helvik had the original idea to use genetic algorithms as an optimization method. I put the model into and did the discussion on the optimization context, developed the necessary analytical and optimization software and produced the quantitative results for the defined network scenarios.

7.1 Contributions of the papers

Each paper included in Part II pursue one or several of the research objectives in Section 5. Fig.8 depicts an illustration of contributions of each of the papers to the research objectives. The illustration shows how the research objectives are address by several papers and the how objectives are inter related by development through other objectives.

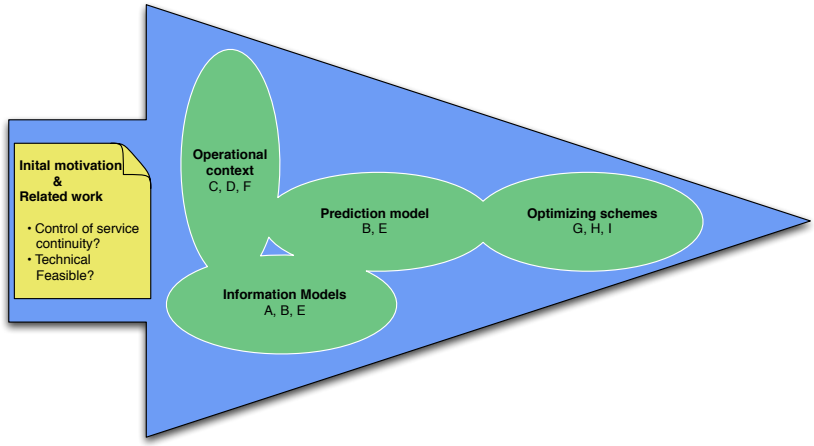

Figure 8. Illustration of the contributions of the papers related to initial motivation, related work and the research objectives.

PAPER A

Managing availability in wireless inter domain access

With the diverse set of emerged wireless networks integrated into IP-based networks, the interdependencies between the domains are important to understand for dependability analysis. **Paper A** deals with how wireless access networks depend on cooperation between the network operators as well as with backhaul network operators and professional land lords.

The main contributions of **Paper A** are the proposed extension of the MIH framework with an information model and the ability to perform real-time availability and reliability predictions for the *system's* infrastructure as one of the criteria for handover decision. The proposed MIH extension allows updating and storing *system* structure with dependability attributes for subsystems of a diverse set of domains. More specific, the information from domains' OSSs is proposed to populate the MIIS database.

PAPER B

Determining dependencies in multi technology inter domain wireless access; A case study

In **Paper A** an extension of the MIH framework was proposed, but how the *system* structure and information model was retrieved from the domains' OSSs was not described in detail. This paper extends the work described in **Paper A**.

The main contributions of **Paper B** are the feasibility to actual populate the MIIS database from the operators' OSSs and how to identify the physical resources that are used between the access points and the radio controllers. A method and algorithm are presented for how to generate a structure function for the domains using unambiguous naming conventions for resources in a technology neutral manner. The naming conventions of the resources may be used to unveil dependencies between the domains.

The second main contribution of **Paper B** is a feasibility demonstration where the emulation of the proposed framework combined with a case study in a commercial GSM/UMTS network. This case study involved population of an emulated MIIS database from the operator's OSSs and the generation of the structure function from the used access points to the radio controllers for a UE moving along a trajectory. Measurement reports for GSM/UMTS, as sent from the UE along the trajectory, were used to identify the serving access points as well as the other access points in the neighbourhood.

The structure functions generated may be used to predict the availability or reliability of the resources needed for each access point or a combination of a number of access points. For the operator in concern the structure functions can be used to identify the root cause(s) affecting several access points and regulators may use the information for dependability evaluations. In addition, the case study gives insight into the operational dependencies between different access technologies and that multi homing cannot take for granted independent connections when using different access points.

PAPER C

Failures and changes in cellular access networks; A study of field data

In **Paper A** and **Paper B** the MIH framework was proposed extended with information to unveil the dependencies between the domains. The dependencies were in general described, but no quantification or insight was given to describe such dependencies. Analyses of dependencies between domains have been difficult to perform due to limited access to operational data

The main contribution of **Paper C** is the insight into the OA&M activities in a commercial GSM/UMTS network operator related to incident and change

management. Operator staff logged incidents records and changes records were studied from a data set covering more than 1000 days.

In **Paper C** the categorizing and quantifications of failures related network operator, power and leased services give valuable insight into how failures are related between actors and network operators in the market place. **Paper C** and **Paper B** show the importance to unveil the actual dependencies between the domains. The failure intensity was not found to be constant, but where found to follow an overall time periodicity with dominant frequencies of 12 hours, 24 hours and 7 days. Rural areas showed higher failure intensity than in urban areas. Failures identified as having same common root cause were analyzed and the restoration time for each affected Base Transceiver Station (BTS)/NodeB was found to be quite different, in contrary to assumptions used in research.

The significance of having updated information in the MIIS database may be described by the actual changes performed in the domains. One change operation, as logged by a change record by the operator staff, may impact several resources in the network and includes any modification in the network, such as e.g., HW, SW or configuration modification. In the study of field data, the number of changes in the network is significantly compared with the number of failures. This shows that the commonly research assumption of static networks during a long period of time do not necessarily hold.

PAPER D

Towards Risk-aware Communications

Paper D promotes the necessity to take into account risk-awareness during design and operation of communication networks and services. With the importance of the Internet, constituting a web of interdependent and continuously changing networks and domains, the consequences of failures that affect individuals, companies and a society in general have to be acknowledged and understood. Even though **Paper D** is related to the Internet as a whole, the same challenges in a smaller scale are valid for the wireless access networks related to this thesis.

The main contributions of **Paper D** are the review of state of the art and suggestions forward for a risk management cycle with the ambition of having explicit and systematic considerations of the consequences of failures in underlaying networks/domains. Consequences are beyond the network/domain operational view, to also consider the total economical risk associated with the predicted probability and impacts of failures. Parts of the risk management cycle are the continuously monitoring of risks and corrective actions to reduce the risks.

Paper D may be seen as suggestion for a framework for risk-awareness in communication networks. The paper addresses the importance of insights into OA&M processes of networks/domains and the interdependencies between

networks/domains for proper predictions of failure probabilities. In this context, **Paper A**, **Paper B** and **Paper C** are some of the means to achieve such insights for access networks. In this thesis we have not pursued the momentary cost related to the risks for critical services, but have focused on obtaining the minimal risk in terms of reliability. The objective has been to reduce the risk by using dual homing as corrective actions where interdependencies between networks/domains have been controlled.

PAPER E

Reliability modelling of access point selection and handovers in heterogeneous wireless environments

In **Paper B** an information model for the infrastructure was proposed. From this model dependability analysis may be performed for the *system* composed of the physical resources from the access point to the radio controllers. In **Paper E** a modelling approach for prediction of the reliability is developed for a dual homed critical service where radio coverage and handover are taken into account.

The main contribution of **Paper E** is the proposed model that may be used to predict the reliability for a dual homed critical service along a projected route, i.e., the physical movement. Similar as for **Paper B**, the MIH is proposed extended. The extension of MIH is proposed supporting collection of measurement reports from UE and signalling in the networks. Measurement reports contain experienced radio conditions for given geographical areas. By combining measurement reports and signalling from networks limited geographical areas are identified having homogenous radio conditions. These limited geographical areas are defined as virtual cells.

A trajectory is defined as the series of access points used in the virtual cells by the dual homed service from the UE to the network for a projected route. For a projected route there exist numerous of possible trajectories. where the reliabilities of the critical service are different. In **Paper E** an approximation of the reliability of a trajectory is proposed that is suitable for optimization. Based upon the approximation, optimization methods may be used to find the optimal trajectory for a dual homed critical service.

PAPER F

The cost for meeting SLA requirements; implications for customers and providers

Paper D describes a framework for risk-awareness during design and operation of communication networks and services. The risk may be beyond momentary cost. With a two-state semi-Markov model **Paper F** provides insights into the trade-off for the provider between the cost for increasing

the service dependability and the potential risk associated with the expected compensation to be paid to the customer. These insights are estimated from SLAs where dependability related SLO parameters have been extended to cover maximum allowed number of failures and maximum allowed number of long down times longer than a threshold in addition to commonly used parameter (un)availability for a given observation interval.

The result of **Paper F** indicates that the provider should deploy services with asymptotic dependability attributes with better values than given by the related SLOs. This safety-margin is dependent on the observation interval and the compensation. Secondly, the insights provide valuable information of the impacts by the failure and the repair processes for both the customer and the provider, and an SLA should therefore also include the maximum number of failures and maximum number of long down times longer than a threshold. For the customer this is valuable for better estimation of the behaviour of the system and how the service may fulfills the actual needs. In addition, this may be used by the customer to benchmark different providers. For the provider this may be used as a way to estimate the deployment cost trying to meet demands from the customers.

A major contribution **Paper F** is the relationships between the dependability SLOs, observation interval and the compensation and the corresponding optimal failure and repair processes to be deployed the by provider for the particular service. For the provider it is a trade-off whether investments should be used for improving the fault tolerance, i.e., failure process, or get better control on the repair process. As indicated in **Paper F** the observation interval has a significant impact on the optimal deployment. The shorter the interval gets, the more investment should be used to improve the fault tolerance. At a certain lower limit of the observation interval, only the failure process gets are crucial for meeting the SLOs since the repair process is expected to breach the SLOs.

PAPER G

Optimizing service continuity in a multi operator multi technology wireless environment

In **Paper E** a model is proposed for prediction of service continuity of a dual homed critical service. The model proposed is based upon the concept of virtual cells. Virtual cells are defined as limited geographical areas where the radio conditions are homogenous. In **Paper G** optimization methods are proposed for finding the trajectory that maximizes the service continuity. The optimization methods are using the approximation for the reliability of a trajectory as proposed in **Paper E**.

The main contribution of **Paper G** is the ILP formulation for finding the optimal trajectory. The ILP is formulated with an objective function for the reliability to be maximized given a set of constraints to be fulfilled. In addition, heuristic optimizations are derived as means to solve large systems since finding

the optimal solution with ILP optimization may need considerable computation effort. The heuristic optimizations are based upon shortest path algorithms [Dij59, Bel56] and Bhandari [Bha99] where different dependability attributes are used as weights for graph models representing the combinations of access points in the virtual cells.

Multi homing protocols may use the proposed methods in **Paper G** for finding the optimal trajectory for a critical service. The proposed methods supports a global projected route based handover mechanism where all handovers throughout the session time are taken into account and not only as local hop-by-hop based decisions. Comparisons of the proposed methods for several larger synthetic network scenarios show that global projected route based handover mechanism provides significantly improved reliability than local hop-by-hop based decisions. Even though ILP optimization always finds the trajectory with the highest reliability, the computational effort of ILP optimization is much higher than all the heuristic methods together. The computation effort of the ILP optimization is seen as a challenge for critical services as the trajectory with the predicted optimal service continuity is required at real-time.

PAPER H

Using genetic algorithms for improving the reliability of dual homed wireless services

The trajectory with the highest reliability for a dual homed critical service where found by ILP optimization in **Paper G**. In the same paper heuristic methods were proposed for computation efficiency on behalf on the optimality of the trajectory. In **Paper H** GA is used to improve the (near-)optimal solution and still be computational efficient compared with an ILP optimization.

The main contribution of **Paper H** is how the GA may be used to find the (near-)optimal trajectory. A chromosome structure is defined from the model and reliability approximation proposed in **Paper G**. This chromosome structure allows efficient GA crossover and mutation procedures with no complex repair of non-feasible trajectories represented by chromosomes.

With the proposed chromosome structure and GA procedures **Paper H** shows that a seeding of the initial population with chromosomes identified by the heuristic methods proposed in **Paper G** provides overall more reliable trajectories than with no seeding when also the computation effort is taken into account. Comparisons between GA and ILP optimization for several synthetic network scenarios show that GA may be used to find a (near-)optimal trajectory with less computation effort than using ILP optimization. However, it is shown that the GA does not necessarily find the optimal trajectory not even for a large number of replications.

PAPER I

Maximizing the reliability of dual homed, critical services in wireless/cellular networks

In **Paper B** a model for dependability prediction of the infrastructure was proposed, whereas the corresponding model for the radio part was proposed in **Paper E**. In **Paper I** a combined model is proposed for prediction and efficient optimization of the reliability of a dual homed critical service where both the infrastructure and the radio part are taken into account.

The main contribution of **Paper I** is how to find the optimal trajectory by establishing a global route handover decision schema where the MIH framework is used for the selection of handovers. The optimization task is efficiently solved with the Dijkstra's algorithm [Dij59]. Unlike the problem formulation in **Paper G**, also solved with Dijkstra's algorithm, where the reliability of the trajectory found did not match the reliability of the trajectory found by ILP optimization, **Paper I** does find the same trajectory as the ILP. In **Paper I** the Dijkstra's algorithm use the same object function as the ILP in **Paper G**, but solves the optimization task significantly more computation efficient. With the use of the method proposed in **Paper I**, the (near-)optimal trajectory for large networks may be found.

In **Paper I** it is illustrated how the backhaul network connection and dependencies influence the (near-)optimal trajectory, both with respect to the reliability and the access points selected. Comparisons of the reliability of the trajectory obtained by global route optimization and trajectory obtained by a local hop-by-hop optimization are provided. These comparisons show significant gains with the use of a global route optimization.

7.2 Summary of contributions

To achieve the topic of the thesis *managed access dependability for critical services in wireless inter domain* four research objectives where defined in Section 5. An illustration of the main contributions of the papers to the research objectives is depicted in Fig.9.

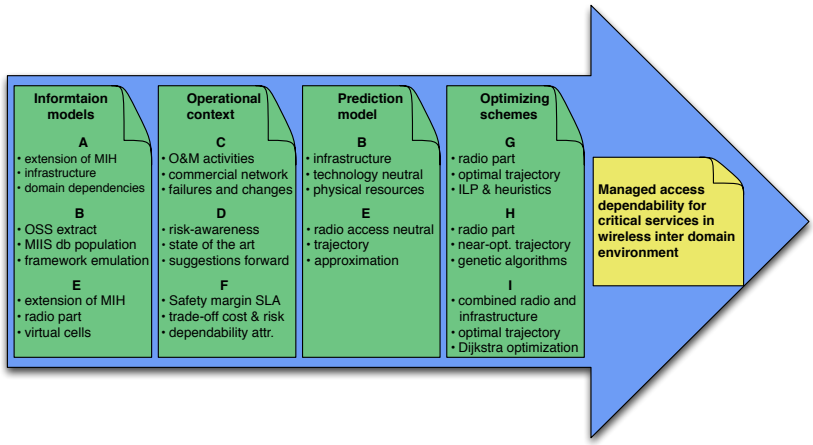

Figure 9. Illustration of the research objectives with summary of the contributions for achieving the topic of the thesis.

The summary of the contributions is described in relation the research goals as follows;

Design and verification: The essence of this thesis contribution is that for dependability analysis for critical services the *system* structure and inter dependencies between the subsystems need to be understood. In this thesis the dual homed critical service is achieved by the *system* designed by combining subsystems from the multi domain, multi technology access network environment.

An extension of the MIH framework is proposed for retrieving information from the different domains' OSSs to reflect the physical resources and structures in a technology neutral manner for the infrastructure. For the radio link, measurement reports from UE and signalling in the network are proposed used to identify virtual cells. Measurement reports are proposed stored in extended MIIS database(s). A field trial in a commercial network gained insight into the feasibility to actually retrieve information from domains' OSSs.

A network operator may use the proposed approach to unveil vulnerableness in the network provisioning and as a means to analyze and finding root cause of network failures. This may also be used by regulatory authorities to assess the diversities in multi operator networks.

Operational context: Insight into operational activities and empirical statistics from operational domains are very limited in the research community. However, assumptions, sometimes simplistic, about these issues are very common. Insight into these issues are very valuable for society in gen-

eral, but also for research, development and operations for improved service dependability.

This thesis has provided new insights into operational activities and empirical statistics related to failures and changes in a commercial network. The high dynamics in service provisioning, network deployment and evolution, combined with cooperations between domain operators may significantly change the service dependability relatively to the assumptions of static conditions. The insights provided are valuable for users and providers of critical services, showing that the service dependability has to be continuously assessed along with the changing environments. Static conditions over time cannot be taken for granted.

Prediction method: To build a dependable *system*, combinations of fault prevention and fault tolerant techniques are typically used. In this thesis the dual homed critical service is achieved by a *system* designed by combining subsystems from the multi domain, multi technology wireless environment. With the concept of virtual cells, where the radio conditions are homogeneous, a prediction method is proposed for the reliability of the changing structure of the *system* along a projected route. Basics for the predictions are information from domains' OSSs and UE measurement reports.

The prediction model for the reliability of a dual homed critical service is suited for optimization of a trajectory. The prediction model may also be suited for a local hop-by-hop handover decision where possible target access points in the next virtual cell are identified in due time before the actual handover execution.

Optimizing schemes: For a dual homed critical service the trajectory with the highest reliability should be predicted prior to the actual start of the service. This allows the user to accept the risk or not start the critical service session. In the thesis several methods for finding trajectory with the highest reliability is proposed. The methods differ in computation effort and closeness to the optimal trajectory. The use of Dijkstra algorithm [Dij59] provided the lowest computation effort and optimality of the trajectory.

The optimized trajectory may be used by dual homed protocols and handover procedures. The predicted optimized trajectory may be used for connection management and to efficiently identify the optimal access points. Even though the thesis has considered a multi domain environment, the same approach for finding the optimal trajectory within a single domain may be used.

7.3 Discussions

This thesis has focused on the dependability for critical services in multi domain, multi technology wireless environment. Main results of the research are the proposed extension of MIH for access network dependability related information and development of a Markov model of radio and backhaul net-

works for efficiently obtaining the most reliable trajectory. Throughout the introduction part of this thesis it has been stressed the importance of the knowledge and understanding of the systems that are the basis for the abstraction and proposed solutions. In the light of this some essential assumptions and discussions are given in this section.

7.3.1 Service description

In the thesis the critical services have not been described in detail nor the performance specification that actually defines the two states; service satisfactoriness or service interruption. Such performance specification is needed along with the dependability requirements. For instance, a performance specification could define the maximum number of dropped consecutive IP packets and if this threshold is crossed, the service is deemed to be interrupted. Such performance specification and related dependability requirements are linked to the service and usage context. These specifications are assumed to exist for the critical services handled in the thesis.

7.3.2 Magnetism effect

Similar as for emergency calls in cellular networks, users of critical services are assumed to have certain privileges compared to other arbitrary services. For instance, the number of users of critical services should be limited and only these users should be granted access to MIIS for obtaining the dependability parameters needed to derive the optimal trajectory. This ensures controlled load on the MIIS and to avoid "magnetism effects" that guide to many users to the most dependable access points. Such magnetism effects may easily result in overload of these access points and influence dependability of the trajectory itself. This has to be carefully considered for commercial aspects of providing differentiated services.

7.3.3 Operational aspects of MIIS database

As discussed in **Paper A**, **Paper B** and **Paper E** the population of dependability information from the domains OSSs to the MIIS databases requires a standardization efforts along with a mutual trust between the domains and the operator of the MIIS db. The information stored in the MIIS databases should only be used for the agreed purpose and the information pushed to the database should be trustworthy. Measurement reports from UE are of privacy concern and should be decoupled from the user and UE identity.

7.3.4 Virtual cell

Although **Paper E** provides indicative description of how measurement reports from UE and signalling in networks may be used to identify virtual cells, details and actual parameter estimations are not described. With the acknowledgement of the challenges and issues related to defining virtual cells

with estimated parameters and its geographical extent related to positioning and speed of the UE, the diversity of UE types and time of day as well as reason for handover, reason for failed handover, service used in terms of capacity needs, delay/jitter constraints etc., it is assumed that such estimations may be done.

The approximation of the Markovian based prediction model that is suitable for optimization, as identified in **Paper E** is valid when the time spent in a virtual cell is at least four times longer than the expected handover time. This implies that if a virtual cell gets too small or the velocity of the UE gets too high, the approximation does not hold. In **Paper E** the robustness of the boundaries of the virtual cells is discussed and how this affects the dependability related attributes of the virtual cells. If the boundaries of virtual cells need to be changed due to changed environment, the dependability related attributes need to be adjusted.

7.3.5 Optimization

Whether the optimization task, described in **Paper B**, **Paper E**, **Paper G**, **Paper H** or **Paper I** should be implement in the servers associated with MIH or in powerful UEs are not thoroughly discussed. Both alternatives are possible, but the amount of information transferred from MIIS to the UE and the danger of misuse has to considered. In same way, execution of handovers and dual homing path management where the optimal trajectory is basis for decisions may be performed by the UE or by the serving and target networks. Challenges associated with either solution are the possible authentication and resource allocation in target networks as addressed in e.g. [CIRG09, NFS+09].

The modelling aspects in [SNLW08, SSNW08], using Markov Decision Process (MDP) algorithms, are related to the proposed approach in this thesis for selecting the optimal series of access points for a trajectory. The time epochs are used to discretize the handover decision points for a single homed service whereas virtual cells in this thesis are the basis for decision points for a dual homed service. The transition probabilities for next state at each time epoch are based upon simulation with given parameters of arrival and departure of users. In the thesis the estimated dependability parameters are based upon measurement reports and the optimal series of access points are derived for dual homed service optimized for service continuity. Given the result obtained in **Paper E** and **Paper I** with an approximation of the service continuity suitable for optimization, the optimal series of access points for a trajectory may be found by using MDP algorithms, but where the Dijkstra shortest path algorithm [Dij59] as used in **Paper I** is the most computational efficient algorithm.

8. Conclusion

In the digital and networked society the dependencies to Information and Communications Technology (ICT) have become part of the everyday life in the emerged part of the world. Behind the scenes services are delivered to the users through a web of interdepended domains each with their own business and operational strategies. Service deliveries are transnational in a global market place where users may select a variety of different services independent of the type of access technology and network access operator. With the powerful UE and wireline comparable features and capabilities the wireless is the primary access. While traditional emergency calls in cellular system have been regulated to provide free access to any cellular network, similar regulations are not introduced for data centric services. It may be questionable if the free market forces will offer the ICT robustness as the future society needs without interventions from regulators that have to act both national, regional and in a global perspective.

In this thesis it is focused on critical services and the wireless/cellular access networks. Wireless access is a critical factor in highly dependable mobile services. The wireless access is foreseen to have prominent importance in health care, smart power grid, and more. Such critical services demonstrate clearly that the loss due to non satisfactory service delivery cannot only be momentarily measured. The risk of service interruption has to be acknowledged and understood by all actors in the service chain. Even though SLAs may be used to describe the service, dependability attributes and possible penalties in case the dependability requirements are not met, the SLAs itself cannot guarantee failure free operations.

The thesis addresses the importance of insights into OA&M processes of networks/domains and the interdependencies between networks/domains for proper predictions of failure probabilities. The centre of interest have been on obtaining the optimal service reliability in the multi domain, multi technology access network. The objective has been to reduce possibility of failures and their consequences by using dual homing as means where interdependencies between networks/domains have been controlled.

The proposed schemes in this thesis seem technical feasible. Central parts of the scheme are how information from operators' OSSs and experienced radio conditions are gathered and populated into the MIH framework suitable for service availability and continuity prediction, important for critical services. From the proposed prediction approach a dependability gain is obtained by choosing the global optimal sequence of access points. Computational efficient techniques have been proposed to predict and deriving the corresponding sequence of access points and handovers. The optimal sequence of access points may be a set from a variety of technologies and operated by different network operators. A trial implementation is a next step in pursuing the proposed ideas and approaches.

Part II

INCLUDED PAPERS

PAPER A

Managing availability in wireless inter domain access

Eirik Larsen Følstad and Bjarne E. Helvik

Ultra Modern Telecommunications Workshops

St. Petersburg, Russia, October 2009

MANAGING AVAILABILITY IN WIRELESS INTER DOMAIN ACCESS

Eirik Larsen Følstad, Bjarne E. Helvik
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@q2s.ntnu.no

Abstract This paper deals with how the availability of wireless/cellular access networks depend on the cooperation between the operators as well as with transmission network operators and professional land lords. The forthcoming 4G network will consist of diverse sets of wireless/cellular networks integrated into IP-based networks. Mobility, QoS and seamless handover between the networks are key features. In [GJ03] the concept of Always Best Connected is defined as means that the user is connected through the best available device and access technology at all times. Availability of the access is fundamental for QoS and critical services (e.g. emergency services, health services) are more and more dependent of wireless/mobile access. Availability can be increased by utilization of several accesses through seamless handover and/or multihoming. Usually, the availability has been calculated assuming independencies between the access network operators, but in this paper we show that the actual cooperation between the market actors has significant impact on the availability. We propose a solution by usage of the MIH 802.21 framework to build and distribute network topology information with availability estimates allowing to predict the overall availability for the access networks accessible as one of the criteria for a handover decision.

1. Introduction

The wireless access (packet based) to Internet was standardized by IEEE with the 802.11b protocol and for cellular environment by ETSI with GPRS in 1999, with start of deployments in 2000/2001. Later both wireless as well as cellular environments have enhanced functionality/QoS with WiMAX and UMTS/LTE respectively. The traditional cellular phone has become a multi purpose equipment capable of multiple access technologies with open operating systems supporting third party applications and the difference between such a terminal and a PC is not obvious any more.

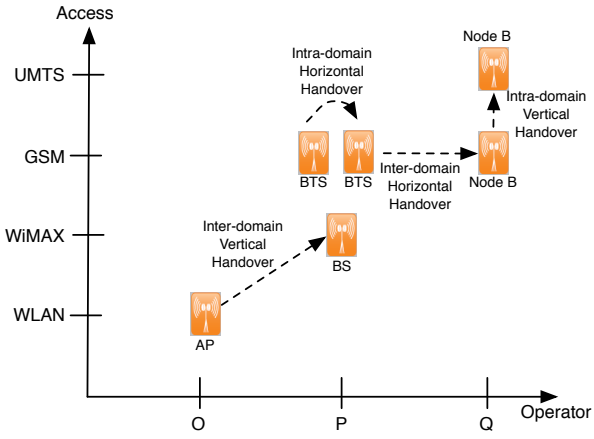

Figure 1. Handover and multihoming for a given location.

In this paper we consider how to manage availability of the network access where the user can use different access technologies from one or several operators. Availability of the access is fundamental for QoS and critical services (e.g. emergency services, health services) are more an more dependent of wireless/mobile access. Each access network provides a certain availability for access at the location in concern. With usage of user equipment capable of utilizing several access technologies, either simultaneously or one access at any given time, the availability of the access will be increased. Both multihoming (simultaneously access) [KMH05] and handover requires mechanisms in the user equipment and network to ensure seamless service continuity. Such mechanisms are outside the scope of this paper. Fig.1 gives an example of possible accesses the user equipment can utilize at a certain location. Vertical handover is the term used to change the point of attachment from one access technology (e.g. GSM) to one another (e.g. UMTS). Horizontal handover is the term for a change of point of attachment within the same access technology (e.g from GSM to GSM). If the point of attachment is within the same operator, it is an intra-domain handover, otherwise it is a inter-domain handover. Multihoming can also be used and in this scheme a handover is more the execution of moving from the primary path to one of the secondary paths. The availability predictions can be used as one of the criteria for handover execution to ensure service continuity.

Analytical and simulation methods for dependability analysis for repairable computer/network systems have been an active area of research for a long time, see e.g [PDGB+03], [PCR+08] and Chu [CPRW06]. Han et al. [HWJ06]

performed an experimental measurement-based analysis (usage of trace route and routing tables) of the Internet path diversity, focusing on the impact of path diversity on multi-homed and overlay networks. A background for this study was that the Internet routing infrastructure is highly fault tolerant and that paths traversing different Internet Service Providers (ISPs) (or overlay nodes) would enjoy a high degree of diversity. The study showed that multi-homing route control or current overlay network did not ensure path diversity. In Yannuzz et al. [YMBB05] the challenge of inter domain routing between ASs is described based on BGP where load sharing and multi-homing are the main reasons for the BGP tables to grow so fast and that this again slows/prevents the actual usage of the redundancy. For critical infrastructure (national electrical grid, oil and gas system, telecommunication networks, transportation networks etc) there is related research, see e.g. [Rin04] and [SW07]. However, these are focused on regional and nation wide concern related to large scale natural disasters and coordinated acts of terrorism.

In this paper we will describe how the availability of wireless/cellular access networks are dependent on the cooperation between the market actors. The novelty of this paper is the real time calculation of availability prediction for a user at a given location by usage of the MIH framework. We consider a given location where the user have coverage from three different access technologies, WLAN, WiMAX and UMTS. The availability for the wireless links are important, and will be treated separately and is not dealt with in this paper.

The rest of the paper is organized as follows. Section two gives information of market trends in deployment and operation of access networks. In section three a possible deployment scenario with three operators each providing WLAN, WiMAX, GSM and UMTS respectively are described. Section four describes the proposes model. In section five we conclude this paper.

2. Market trends in deployment and operation

2.1 Cooperations in general

The usage of wireless/cellular access has become important both for business as well as for the social communities, infotainment and gaming. The expectations for access with any device at any time anywhere to any application/information are now taken for granted. Such expectations put a lot of requirements and generates complexity for the standardization bodies/forums, operators and service/content providers. In [GJ03] the concept of Always Best Connected is defined as means that the user is connected through the best available device and access technology at all times. This definition covers aspect such as e.g. personal preferences, size and capabilities of the device, application requirements, security, operator or corporate policies, available network resources and network coverage. The market actors, such as network

operators, service providers or content providers, ultimate goal are to earn money for the stake holders. For the operators it is a huge challenge to balance the cost vs. benefits both in short and long term. The traditional cooperation between network operators based on site sharing and hiring leased line transmission is becoming by far more developed. Such cooperations include e.g.;

- building multi purpose network independent of actual traffic (e.g. signaling, user data).
- equipment/network sharing through e.g. virtualization.
- outsourcing of development and maintenance.

The complexity of performing a dependability analysis has increased with the increased dependencies between logical resources and networks operated by different operators that are combined in shared physical entities. A physical router might be divided into a number of virtual routers each used/operated by different operators, transmission media (cables/fibres) might be placed in the same ditch, the same power supply might be used to feed several network elements operated by different operators etc.

2.2 Wireless access networks

The interface between access and core network is constituted by the WLAN Controller, Access Service Network Gateway (ASN-GW), Base Station Controller (BSC) and Radio Network Controller (RNC) for WLAN, WiMAX, GSM and UMTS respectively. The WLAN Controller, ASN-GW, BSC and RNC (Access Controllers) are part of the access networks with interfaces to the core network as shown in Fig.2. The different accesses have very similar network architectures, with one or several wireless access points connected to a controller. The Access Controllers for the different access networks perform several similar functions such as e.g. SW/config management, radio resources management, admission control, mobility, handover control, security and Quality of Service (QoS) for the access points (AP/BS/BTS/Node B) connected. The Access Controllers might use the measurements (e.g. signal strength, signal quality) from the user terminals to execute handovers and radio resource management. The Access Controllers can also be seen as a transmission concentrator for connections to the access points.

Consider a location from where the user have coverage from four access technologies as shown in Fig.2. The access technologies are operated by three different access network operators. In the figure the access network operators are denoted O, P and Q. Assume that the user has a terminal that supports these access technologies and that the applications/services that it uses ensure a seamless vertical and horizontal as well as inter- and intra domain handover. In the figure the operator owning the equipment is given by the identifier in the upper left corner of the equipment. For the transmission the named cloud surrounding the equipment is the owning operator. The owner of the sites, is shown with the identifier in upper left corner of the squashed rectangles.The

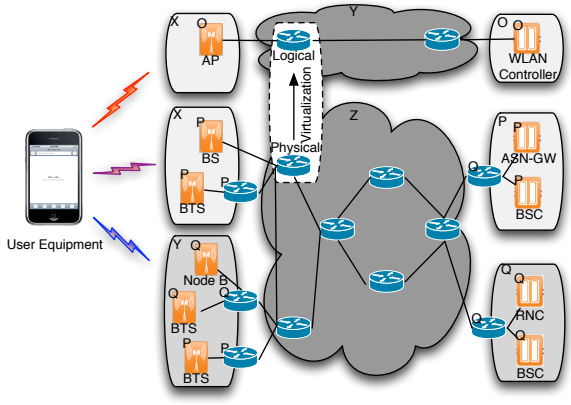

Figure 2. WLAN, WiMAX, GSM and UMTS Network sharing.

black and white genres of the surrounding squashed rectangles or clouds indicates different maintenance and repair organizations.

Furthermore, assume that the network access operators are using leased transmission from a transmission network operator, denoted Y and Z in the figure. It is possible that a transmission network operator, as operator Y, has leased a virtual equipment from transmission operator Z. Usage of leasing may be encouraged by timing and cost. With leasing existing infrastructure, there will be less time needed to establish the connections needed since the acquisition of sites/ditches are already in place. By regulation some operators having a strong marked position are regulated to provide leasing agreements. The usage of leased transmission from a regulated transmission network operators or under normal unregulated market conditions should be attractive, as this may be at lower cost and with better timing than achievable with own infrastructure.

Let say the access network operator lease the site from professional land lords, denoted X and Y in the figure. The land lords may also require that the access network operators lease power and cooling, since a common power infrastructure (AC/DC with possible diesel aggregates) and cooling is most efficient if common room(s) is used for the access network operators.

3. Case scenario

3.1 Overview

Fig.3 gives an overview of the case used for illustration of the availability effected. The transmission network operator has divided the transmission network into two main parts; the metropolitan and the regional part. In this

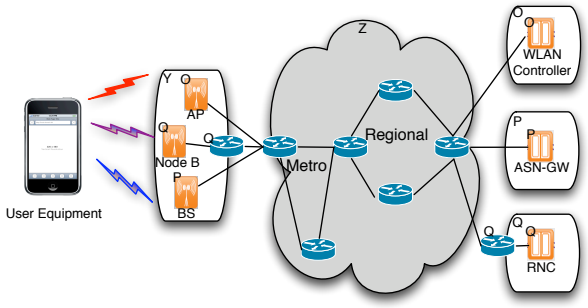

Figure 3. A dependent access scenario.

scenario, the leased transmission is Ethernet. Due to the need for synchronization and pseudo-wire emulation between the RNC and Node B, operator Q has deployed necessary equipment at RNC site and Node B. The transmission network (metro and regional) is expected to have fault tolerant and network recovery mechanisms deployed. The regional part might have a higher fault tolerant solution than the metro part. Similarly, both the power and cooling are expected to be fault tolerant (e.g. using A and B power with battery backup). We assume that the access network operators are buying the same product from the transmission network operator and the land lord, i.e. they have the same SLA (regulated e.g. the availability terms). The operators perform the maintenance and repair on their own equipment.

3.2 Availability calculations

The most common availability measure is the asymptotic availability, denoted A. This assumes that the system in concern have reached its steady state, and A gives the probability of finding the system in a working state at a random time. There is a well known relationship between the Mean Up Time (MUT) and Mean Down Time (MDT) and Mean Time Between Failures ($MTBF$) under stationary conditions. MUT^{-1} is equal to the failure intensity λ for the system in concern.

$$A = \frac{MUT}{MDT + MUT} = \frac{MUT}{MTBF} = \frac{1/\lambda}{MDT + 1/\lambda} \tag{1}$$

Traditionally calculations of the overall availability for the access networks for the critical service would assume independently failures between the access networks. Let A_i be the availability of the equipment specific for technology $i \in \theta$, where $\theta = \{\text{WLAN}, \text{WiMAX}, \text{UMTS}\}$. Taking into account the availability of the other elements, the metro transmission (A_{met}), regional transmission (A_{reg})

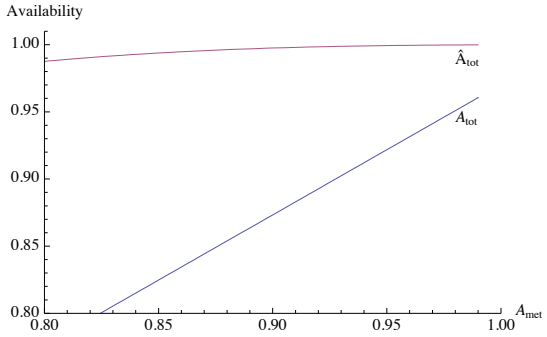

Figure 4. Availability with varying A_{met} and the other estimates set to 0.99.

and power (A_{power}) and cooling ($A_{cooling}$) at the BS/AP/Node B sites, the availability prediction from a multi access technology user assuming independence becomes;

$$\hat{A}_{tot} = 1 - \prod_{i \in \theta} (1 - A_i A_{met} A_{reg} A_{power} A_{cooling}) \tag{2}$$

Since the transmission is leased from the same transmission network operator, the overall availability of the transmission network and common infrastructure at the BS/AP/Node B site are no longer independent between the access networks. The correct availability equation prediction should be;

$$A_{tot} = (1 - \prod_{i \in \theta} (1 - A_i)) A_{met} A_{reg} A_{power} A_{cooling} \tag{3}$$

The common infrastructure and transmission lines have a fundamental effect on the overall availability as seen with (3) compared with (2). The common factor $A_{met} A_{reg} A_{power} A_{cooling}$ is independent of the number of access systems and dominates the availability. This may be illustrated by Fig.4, assuming that all the availability estimates except A_{met} are 0.99 and varies the A_{met} between 0.80 and 0.99. As shown, $\hat{A}_{tot}$ is over estimating the availability.

4. Proposed model

4.1 Network topology

For availability predictions the insight into of the underlaying structure of the system is required. In an inter domain environment the network structure and interaction as well as dependencies between the domain are very complex. Taesombut [TC07] evaluates the network information models on resource efficiency and application performance in lambda-grids in multi domain environment. The key finding is that the domain topology information is crucial for

achieving good resource efficiency. However, there are some concerns regarding the operators willingness to share such information of their internal resources based on;

1 Security

2 Financial benefits

3 Internal network management

4 Inter domain routing policy enforcement

5 Protocol heterogeneity

Taesombut assume that the such collaboration should be possible with a trustworthy third-party agent. We do believe that the same concerns are also valid for an information sharing concerning network topology and availability estimates. However, with increasing demands for QoS and trustworthiness of the system, more information has to be provided to the customers. For network access topology, the most fundamental is the coverage area. Some access network operators already provide coverage maps, accessible through their WWW home page, with the actual sites. The availability predictions for the access are already given for some business customers in the SLA. The availability estimates will most probably be given as aggregates for the network or parts of the network.

4.2 A topology and dependability aware MIIS

We propose a solution to the availability prediction challenge based upon Media Independent Handover (MIH) framework, IEEE 802.21 [IEE08]. This may be used to obtain the network topology information with availability estimates together with coverage information.

The MIH enables a given network to discover and receive advertisements from other networks, and to request additional information. It defines a database, the Media Independent Information Service (MIIS) database, for discovery/querying of network information, mostly static, of the serving and neighbor networks, but has neither defined the actual implementation of this database nor how this is populated. The information is separated into three main categories, each defined with Information Elements;

1 Network Specific Information.

2 Point-of-Attachment Information.

3 Vendor specific information elements.

Moon et al. [MYY07] have addressed the access network discovery for MIH, since access network discovery is undefined in the framework. In this paper it has been observed that the decentralized access network discovery with

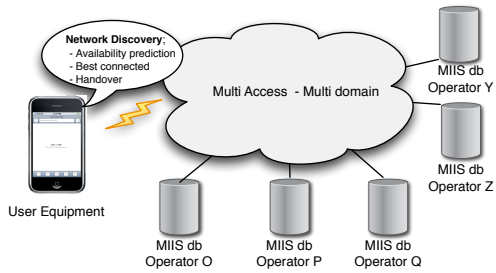

Figure 5. Network Discovery through framework.

dynamic monitoring of access network based on the terminal moving speed may save user equipment consumption. Monitoring of fewer access network has benefit in power consumption but may degrade the QoS. To ensure service continuity we propose to use the availability prediction for the access networks as one criteria for network selection and to perform handover execution.

4.3 Population of MIIS database

To populate the MIIS database we propose a solution where the infrastructure providers (access network operators, transmission network operators etc.) push the network topology data with corresponding availability estimates to their MIIS database. To obtain the complete network topology for a certain location, it might therefore be necessary to use information from several operator MIIS databases. Access network topology, with necessary availability estimates, should be possible to obtain from the Operational Support Systems (OSSs) used by the infrastructure providers. The infrastructure providers use OSS to configure the network/infrastructure, for monitoring and maintenance and for optimization. An infrastructure provider may have several OSSs for different parts of the network/infrastructure. In Fig.5, the operators described in subsection 3.1 have their own MIIS database. The user terminal will access the MIIS database belonging to the access network operator for the point of attachment (i.e. operator A, B or C). The information obtained from the MIIS databases is for network discovery and to select the best point of attachment based on e.g. availability prediction.

4.4 MIIS database Information

Since the infrastructure providers are leasing/sharing infrastructure, the MIIS database must be able to identify such shared resources. To be able to reflect the actual dependencies between the infrastructure providers, we propose to use the identifier of the resource prefixed with the owner of the

Table 1. New Information element IE_POA_STRUCT

Information element	Description	Data type
IE_POA_STRUCT	system function expressed in a minimal product-of-sums form.	STRUCT_INFO

resource. In this way we avoid possible duplications of resource identifiers. For instance, if operator O is leasing a transmission from operator Y from site A to site B, this is identified by a element identifier, which is unique within operator Y. Operator O has the knowledge of the ingress and egress, while the operator Y has the knowledge of the resources used between ingress and egress, though it is possible that operator Y lease resources/lines from operator Z. The same identification mechanism is used for all resources such as network elements, virtualization of routers, ditches/cables, infrastructure (power, cooling), etc.

The actual access network topology of an infrastructure provider might be aggregated as long as the aggregate only consist of its own resources and independent of egress and ingress (e.g must be independent on elements included). For instance, for an UMTS access network operator the RNC site having central synchronization equipment used for Ethernet transmission to Node B is aggregated into one resource with associated availability estimates, see Fig.3. Aggregates can only be used as long as the aggregate represent a building block that is independent of the operator leasing capacity. An example of such independency can be metro transmission rings, where the ring is independent of the actual site connected or leasing operator.

We propose to include the availability estimates for the access network in the Point of Attachment (PoA) specific information, i.e. in the IE_Container_PoA of [IEE08]. This gives the possibility to provide different availability estimates for each PoA, i.e. BS/AP/Node B. The new information element IE_POA_STRUCT, see Table 1, provides information to define a structure function expressed in minimal product-of-sum of the SYS_ID (Table 2) contained. The structure function is a logical function that expresses whether the system is working or not. The product-of-sum structure provides a concise way of expressing the structure function without explicit need for operators. A minimal sum-of-products is a irreducible boolean sum (logical OR, $\vee$) of minterms, where a minterm is a boolean product (logical AND, $\wedge$) that may include a variable only once. Each of the maxterm of the structure function expressed in a minimal sum-of-products corresponds to a minimal cut set.

Each of the SYS_ID has an estimated availability attached, the SYS_AVA (Table 2). The SYS_AVA is used to combine the availability predictions for the PoA from the structure function for the PoA. Since the SYS_ID is unique, a system structure for all accesses seen by the user can be constructed, also in expressed in minimal product-of-sum. From this the availability prediction for all access networks can be derived.

Table 2. New type

Type name	Derived From	Definition
STRUCT_INFO	LIST(CUT_SET)	A type for structure
CUT_SET	LIST(SUB_SYS)	A type for maxterm
SUB_SYS	SEQUENCE(	A type for availability
	SYS_ID	for each sub system
	SYS_AVA	
	CHOICE(SYS_FAIL_INT,	
	NULL))	
SYS_ID	SEQUENCE(	A Type for operator
	OPERATOR_ID	subsystem id
	OP_SUBSYS)	
OP_SUBSYS	OCTET_STRING	Subsystem id
SYS_AVA	OCTET_STRING	Availability
SYS_FAIL_INT	OCTET_STRING	Failure intensity year

Table 3. Example used for SUB_SYS in shared scenario

Definition	Value	Description
SUB_SYS	(O w30, 99, 1.0)	Operator O, AP WLAN #30
SUB_SYS	(O c1, 999, 0.1)	Operator O, WiFi controller #1
SUB_SYS	(P w10, 99, 1.0)	Operator P, WiMAX BS #10
SUB_SYS	(P g2, 999, 0.1)	Operator P, ASN-GW #2
SUB_SYS	(Q u89, 995, 0.5)	Operator Q, Node B (w/router) #89
SUB_SYS	(Q c4, 9999, 0.01)	Operator Q, RNC (w/router) #4
SUB_SYS	(Y p1, 999, 0.1)	Operator Y, Power #1
SUB_SYS	(Y c7, 999, 0.1)	Operator Y, Cooling #7
SUB_SYS	(Z m9, 99, 1.0)	Operator Z, Metro #9
SUB_SYS	(Z r2, 999, 0.1)	Operator Z, Regional #2

4.5 Availability calculation based on MIIS

Consider the same scenario as defined in section 3. Assume that a MIH user, could be an application/service deciding when to execute a handover, request the MIH for information of the available networks, as well as the availability estimates through the IE_POA_STRUCT information element. Fig.6 shows how the MIH framework uses the existing established link to obtain the necessary information from the MIIS databases. From the location information in the request message, the MIIS can derive the available PoA. In this example, there exists several MIIS databases with the necessary information. The obtained information can be used by the MIH user to predict the availability for each access as well for the overall availability. The failure intensity is an optional type, see definition of SUB_SYS (Table 2). Assume that the elements have the identities as given in Table 3. The system structure function for each access, in minimal product-of-sum, is constructed as;

$$\phi(\text{wlan}) = O_{w30} \wedge O_{c1} \wedge Z_{r2} \wedge Z_{m9} \wedge Y_{p1} \wedge Y_{c7} \tag{4}$$

$$\phi(\text{wimax}) = P_{w10} \wedge P_{g2} \wedge Z_{r2} \wedge Z_{m9} \wedge Y_{p1} \wedge Y_{c7} \tag{5}$$

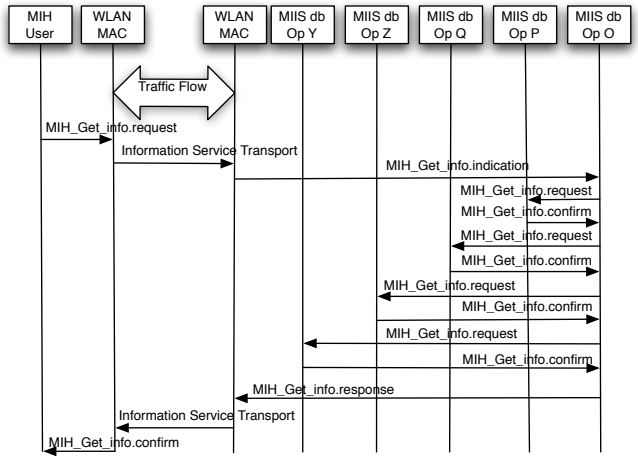

Figure 6. Availability estimates obtained through MIH framework.

$$\phi(\text{umts}) = Q_{u89} \wedge Q_{c4} \wedge Z_{r2} \wedge Z_{m9} \wedge Y_{p1} \wedge Y_{c7} \tag{6}$$

The dependencies between the access networks are identified by the common values of the SYS_ID in the system structure functions. The system structure function all accesses are $\phi(tot) = \phi(\text{wlan}) \vee \phi(\text{wimax}) \vee \phi(\text{umts})$, i.e. this yields;

$$\begin{aligned}\phi(\text{tot}) = (&O_{w30} \wedge O_{c1} \vee P_{w10} \wedge P_{g2} \vee Q_{u89} \wedge Q_{c4}) \\ &\wedge Z_{r2} \wedge Z_{m9} \wedge Y_{p1} \wedge Y_{c7}\end{aligned} \tag{7}$$

Assume that the elements have the availability predictions as given in Table 3. Let A_i be the availability of the equipment specific for technology $i \in \theta$, where $\theta = \{\text{WLAN}, \text{WiMAX}, \text{UMTS}\}$. The availability prediction for A_i is $A_{Ow30}A_{Oc1}$, $A_{Pw10}A_{Pg2}$ and $A_{Qu89}A_{Qc4}$ respectively. Taking into account the availability of the other elements, the availability prediction of all accesses can be derived from (6) and we get;

$$A_{tot} = (1 - \prod_{i \in \theta}(1 - A_i))A_{Zr2}A_{Zm9}A_{Yp1}A_{Yc7} \tag{8}$$

The structure of (8) identical to structure given in (3). A minimal product-of-sum of $\phi(tot)$ given in (6) is;

$$\begin{aligned}\phi(tot) = &(O_{c1} \vee P_{g2} \vee Q_{c4}) \wedge (O_{c1} \vee P_{g2} \vee Q_{u89}) \\ &\wedge (O_{c1} \vee P_{w10} \vee Q_{c4}) \wedge (O_{c1} \vee P_{w10} \vee Q_{u89}) \\ &\wedge (O_{w30} \vee P_{g2} \vee Q_{c4}) \wedge (O_{w30} \vee P_{g2} \vee Q_{u89}) \\ &\wedge (O_{w30} \vee P_{w10} \vee Q_{c4}) \wedge (O_{w30} \vee P_{w10} \vee Q_{u89}) \\ &\wedge Z_{r2} \wedge Z_{m9} \wedge Y_{p1} \wedge Y_{c7} \end{aligned} \tag{9}$$

As shown with (8) the minimal product-of-sum can be significantly reduced with boolean operations and we can get the expression given by (6). To predict the availability from a structure function where one or more elements are represented more than only once in the structure function, the inclusion-exclusion method can be used as described in [BP75] to successive bound the system availability.

5. Conclusion

Based upon the MIH framework we have proposed how to model the inter dependencies between access network operators. The MIIS database is proposed populated with information from the OSSs used by the access network providers. A MIH user can request from information from the MIIS database to gather information of interdependencies between the accesses and the availability estimates for the subsystems. New information element and data types are proposed to describe the dependencies in terms of cut sets. The usage of cut sets has limitation since it assumes independencies in failures as well as restoration of the subsystems. We will further investigate the proposed model for how to include the wireless links, failure intensity and dependencies in failures and restoration. As long as there is limited resources or when the maintenance is outsourced to a third party, there exists dependencies in restoration between subsystems.

References

[BP75] R. Barlow and F. Proschan. *Statistical theory of reliability and life testing: probability models*. Holt, Rinehart and Winston New York, 1975.

[CPRW06] C.-H. K. Chu, H. Pant, S. H. Richman, and P. Wu. Enterprise VoIP reliability. In *Proc. 12th International Telecommunications Network Strategy and Planning Symposium NETWORKS 2006*, pages 1–6, New Delhi, India, November 2006.

[GJ03] E. Gustafsson and A. Jonsson. Always best connected. *IEEE Wireless Communications*, 10(1):49–55, February 2003.

[HWJ06] J. Han, D. Watson, and F. Jahanian. An experimental study of Internet path diversity. *IEEE Transactions on Dependable and Secure Computing*, 3(4):273–288, October/December 2006.

[IEE08] IEEE 802.21,D11; Draft standard for local and metropolitan area networks: Media indepenedent handover services, 2008.

[KMH05] K. Kim, S. Min, and Y. Han. Fast handover method for mSCTP using FMIPv6. *Lecture notes in computer science*, 3794:846–855, December 13–15 2005.

[MYY07] C. Moon, S. Yang, and I. Yeom. Performance analysis of decentralized RAN (radio access network) discovery schemes for IEEE 802.21. In *Proc.66th IEEE Vehicular Technology Conference VTC-2007 Fall*, pages 41–45, Baltimore, MD, September 30 – October 3 2007.

[PCR+08] H. Pant, C. Chu, S. Richman, A. Jrad, and G. O'Reilly. Reliability of next-generation networks with a focus on IMS architecture. *Bell Labs Technical Journal*, 12(4):109–126, 2008.

[PDGB+03] S. Porcarelli, F. Di Giandomenico, A. Bondavalli, M. Barbera, and I. Mura. Service-level availability estimation of GPRS. *IEEE Transactions on Mobile Computing*, 2(3):233–247, July/September 2003.

[Rin04] S. M. Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *Proc. 37th Annual Hawaii International Conference on System Sciences*, page 8pp., Big Island, HI, January 5–8 2004.

[SW07] N. Svendsen and S. Wolthusen. Graph models of critical infrastructure interdependencies. *Lecture Notes in Computer Science*, 4543:208–211, 2007.

[TC07] N. Taesombut and A. A. Chien. Evaluating network information models on resource efficiency and application performance in lambda-grids. In *Proc.ACM/IEEE conference on Supercomputing SC '07*, pages 1–12, New York, NY, USA, 2007. ACM.

[YMBB05] M. Yannuzzi, X. Masip-Bruin, and O. Bonaventure. Open issues in interdomain routing: a survey. *IEEE Network*, 19(6):49–56, 2005.

PAPER B

Determining dependencies in multi technology inter domain wireless access; A case study

Eirik Larsen Følstad and Bjarne E. Helvik

IEEE Global Telecommunications Conference

Miami, USA, October 2010

DETERMINING DEPENDENCIES IN MULTI TECHNOLOGY INTER DOMAIN WIRELESS ACCESS; A CASE STUDY

Eirik Larsen Følstad, Bjarne E. Helvik
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@q2s.ntnu.no

Abstract For critical services the availability of the wireless access is one of the fundamental QoS requirements. Availability can be used as one of the criteria in handover/multihoming decision. Assuming independency between different access networks will over estimate the availability. Dependencies will be retrieved by a detailed structure function including all equipment used. In this paper we address the feasibility to derive the structure function from the Operational Support Systems (OSSs) for the access networks available at a given location, in a multi technology multi operator wireless access environment. A field trial is performed to derive the detailed structure function in a commercial network.

1. Introduction

The forthcoming 4G networks will consist of a variety of cellular and wireless networks integrated into IP-based networks. With lower price and improved QoS deployed, especially throughput and delay/jitter, further incitements are promoting the wireless access instead of the fixed access. The operator has planned for seamless handover between the access points for service continuity. A location has therefore often coverage from several access points, that can have different technologies and be owned by different operators. Gustafsson et. al. [GJ03] defined the Always Best Connected concept as means that the user is connected through the best available device and access technology at all times. Traditionally, the usage of the access technology (operator) has been on basis on coverage, price and throughput. For critical services the availability of the access is fundamental. Availability can be increased by utilization of several accesses through seamless handover and/or multihoming.

In this paper we address how to find the interdependencies between the accesses, based on different technologies and operators, that have effects on

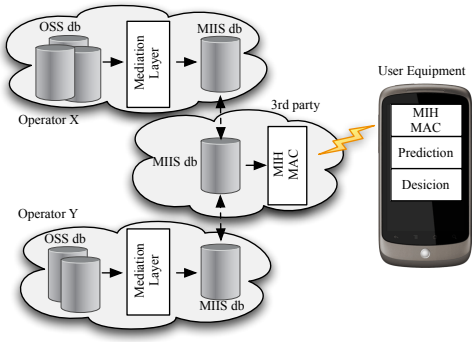

Figure 1. Network Discovery and availability prediction with MIH framework.

the overall availability at a given location. Usage of access points might increase the overall availability. However, tight physical and commercial integration between operators and use of common infrastructure by many access technologies introduce dependencies. Incorrectly assuming independencies will over estimate the availability. In this work we generate and identify the structure function of the accesses at a location from the access point(s) to the access controller(s). We describe an approach for generating the structure function from the operators' Operational Support Systems (OSSs). This work extends [FH09] that presented a solution by usage of the Media Independent Handover (MIH) [IEE08] for availability predictions. The MIH enables to discover and receive advertisements from networks, and to request additional information. The Media Independent Information Service (MIIS) database is central for discovery/querying of network informations, but neither the actual implementation nor how this is populated is defined within the MIH framework. Fig.1 shows an overview of the main components in our solution. The Mediation Layer represents the algorithm to extract the structure function from the operators OSSs. Each operator has its own MIIS database, which is connected to a trustworthy third-party agent. The MIIS database from the third-party provides the information for availability predictions that can be used for e.g. handover decision at the user equipment.

The rest of the paper is organized as follows. In section two a description of the wireless access architecture and topology is given. Section three describes the proposed approach. A feasibility study and a field trial are described in section four and five respectively. In section six we conclude this paper.

2. Wireless Access Architecture and Topology

The wireless access architecture evolves to provide the end user with increased service level. Service level is defined by the quality (e.g. throughput,

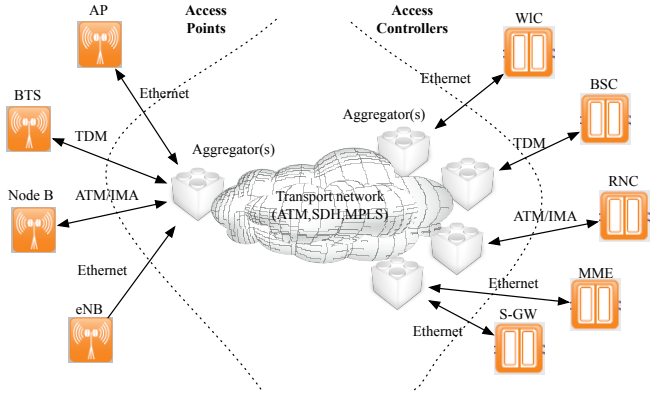

Figure 2. Some wireless access networks.

delay/jitter, reliability) and the cost. The operators have to produce cost-effective solutions to maintain a competitive position. In Fig.2 some wireless access technologies are shown. Basically, they have very similar architectures. The access points (AP/BTS/NodeB/eNB) provide the wireless interface to the user equipment. Access points are connected to access controllers (WLAN Controller, BSC, RNC, MME/S-GW) that ensure mobility control, interface to core etc. The bandwidth requirements on the transport network are rapidly increasing caused by the capabilities of the wireless interface and the customers usage.

Even though new systems such as e.g. LTE is introduced, it is believed that it will co-exist older generations such as GSM/EDGE and UMTS/HSPA for many years. Large challenges for operators are locations/sites for access points and the needed transmission. Existing access point locations are good candidates and it is common that operators hire from each other. The different access technologies have different requirements and interfaces to the transmission network. In Fig.2, it is shown some layer two protocols used. The transmission network has to support both packet data traffic (from LTE, WLAN) and the legacy TDM/ATM based (GSM and UMTS). The transmission network might be dedicated for each access technology or be a multi purpose transmission network. The transmission network may be owned by the access operator itself, or it could be provided by another operator. The underlying protocol could be SDH, ATM, IP or Ethernet. Ethernet can provide Pseudo-Wire Emulation (PWE) [BP05] to emulate ATM/TDM services over Ethernet. The Transport MPLS (T-MPLS) [G8106] is based on the definitions of MPLS to include support for the traditional transport models (e.g SDH).

For dependability analysis the structure of the system is essential. The structure function of a system is one way to describe the system and can

be used to estimate dependability parameters, such as e.g. availability. In [VCD+05] general availability numbers have been collected for several network equipment types. These numbers can be used to calculate the end-to-end availability based on the structure function. Operators own experiences and measurements for failures and availability estimates for network elements can also be used. As far as we are aware of there are no other paper that use the operator OSS to construct structure functions for estimation of availability. There is related research within critical infrastructure (national electrical grid, oil and gas system, telecommunication networks, transportation networks etc) see e.g. [Rin04] and [SW07]. Within that research, large scale natural disasters and coordinated acts of regional and nation wide terrorism are of concern. The infrastructure topology is clearly also essential in this area of research. Efficient mobility management and handoff solutions in wireless networks to ensure service continuity are utmost important [SZ06]. Availability of the access has been central, but the main focus has been on the wireless link, its capacity and throughput, and not on the underlying common resources.

3. Structure function algorithm

A solution where the operators push their network topology data with availability estimates to MIIS databases was proposed in [FH09]. Here we will describe an algorithm for how to retrieve this information from the operators' OSSs. The aim is to construct a structure function for the access networks accessible from a given location by multiple technologies and operators. Define the structure function as;

$$\phi(system) = \begin{cases} False, & \text{if system fails} \\ True, & \text{if system operates} \end{cases} \tag{1}$$

Assume that the *system* in (1) defines the wireless access(es) that can be used by a user at a given location. If the location has coverage for several access points (*signals*) with different technologies (*techns*) operated by different operators (*opers*) the structure function can be given as;

$$\phi(tot) = \bigvee_{i=\forall opers} \bigvee_{j=\forall techns} \bigvee_{k=\forall signals} \phi(ap_{i,j,k}) \tag{2}$$

The structure function for each access point is given by $\phi(ap_{i,j,k})$. For each of the access points possible to use, we want to identify the structure function in a minimum product-of-sum form and to obtain the overall $\phi(tot)$ also in minimum product-of-sum form. The product-of-sum structure provides a concise way of expressing the structure function without explicit need for operators. Each of the maxterm in a minimal product-of-sum corresponds to a minimal cut set, see e.g. [BP75] for introduction. The product-of-sum represents the underlying structure as a series arrangement of i parallel cut set structures (cs), and we may write $\phi(tot) = \wedge_{\forall i} cs_i$. A structure function

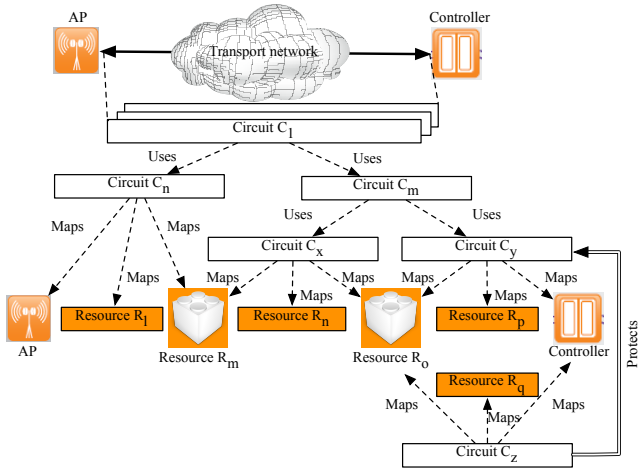

Figure 3. Topological view with relations between circuits and resources.

in minimal product-of-sum form focus on the combinations of failed elements that make the system to fail. Define the following;

Circuit A logical circuit between two end points, e.g. ATM virtual circuit, Ethernet pseudo wire.

Resource A physical resource that realizes the actual logical circuits. e.g a fiber, an ATM node.

The recursive properties of the circuits allow different protocols to be nested in a technology neutral manner where the same protocol can be used at several layers. Different operators can apply to the nested circuits. The number of layers of circuits is dependent of the technology/protocols used, but it is not unusual to find more than six layers. Obviously, unambiguous naming conventions for the circuits and the resources are essential in the structure functions. Prefixing the circuits and resources with the owning operator's unique identifier solves the inter domain naming space. For the intra domain, the operator could use their own method to ensure unique names. Alternatively, the naming could be based upon the TMN principles [X.792] using global name forms. Circuits and resources can be protected by other circuits and resources respectively. Different connection oriented protocols, such as e.g. ATM, SDH, T-MPLS have similar protection schemes, typical 1+1, 1:1 and ring protections.

Fig.3 shows some relations between circuits and resources used between an access point and the controller. The prefixes C and R represent the operator prefix concatenated with a possible operator internal prefix. Between the access point and the controller there are several circuits, one of them is C_1. C_1 could be an ATM virtual circuit. The circuits between access point and controller

could have different quality of service and use different underlying circuits, see e.g [LSGTG08]. In Fig.3 only the underlying circuits of C_1 is shown. C_1 uses C_n and C_m. A circuit can be protected by another circuit as shown in Fig.3. Here circuit C_z protects circuit C_y. Finally, the circuits are mapped to resources. In the figure, the circuits are mapped to nodes (but this could be ports as well) and fibers/coax. Note also that the protecting circuit C_x, use the same nodes as the protected circuit C_y, but use different fiber/coax.

With the Fig.3 as the relations between circuits and resources, we want to construct a structure function, $\phi(ap)$, for each of the access points. The structure functions will be pushed to the MIIS databases. The structure function is built from the information in the operators OSSs. The operators use OSSs to configure the network/infrastructure, for monitoring, maintenance and for optimization. An operator may have several OSSs for different parts of the network/infrastructure. All together the OSSs have the information of the actual configuration of the network end-to-end. Assume the following;

- Operator OSSs mirror the actual deployed network (all layers and different technologies).
- Logical circuit engineered network.
- A Logical circuit between two end points follows the same physical path in both directions.
- For the construction of $\phi(ap)$ the system is considered operating when all end-to-end circuits, the roots, between the access point and controller are operating.
- Protection logical circuits are dedicated for each of protected logical circuits.
- Automatic Protection mechanisms at the different layers are tuned to ensure undisturbed operation, see e.g. [LMB+02].

To predict the availability where one or more elements are represented more than only once in the structure function, the inclusion-exclusion method can be used as described in [BP75] to successive bound the system availability. To convert a general structure function to minimal product-of sums-form is NP-hard. The minimal product-of-sums is used to predict the availability. The technical challenge is to combine parts of the structure function to find conservative bounds of the availability. To limit the computation of the minimal product-of-sums we limited the cardinality of the cut set for the access points included in the structure function. The pseudocode for the algorithm is given in the Appendix.

4. Feasibility Study

To verify the algorithm presented in section 3 a feasibility study was performed to extract the structure function from a commercial network. The structure of operator OSSs used will not be described specific. Fig.4 shows the prototype implementation of the mediation layer shown in Fig.1. The OSS db in the figure represents the operator OSS . The Data Migration is the process of extracting the data from the operator OSS into a desired format. MySQL

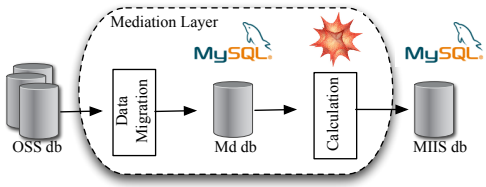

Figure 4. Sketch of the mediation layer.

[MyS10] database was used as a mediation database, called Md db in the figure. The main tables created were the tables for relations between circuits and mapping of circuits to resources. Circuits between the access points and controllers were the roots of the recursive circuit trees. Protection schemes were also included in the circuit tables. Mathematica [Wol10] was used for calculation of the structure functions in product-of-sums form. The structure function of the access points as well as the wanted combinations of access points where stored in a database implemented in MySQL. The information of this database represents as such some of the information in a MIIS database.

We believe that similar extraction of structure functions can be obtained from other operators. Since we have only extracted structure function from one operator, a complete structure function cannot be made if something is leased from or to other operators. But with the naming convention, it is possible to identify if something is rented. For the sake of simplification, we have not included power and cooling resources. Only with automatic protection schemes are included.

5. Field trial

A field trial was conducted, without using the MIH framework. The goal with the field trial was to derive the structure functions for access points at certain locations along a route. With the prototype of the mediation layer implemented as described in section 4 locations in the network were identified through the user equipment. The setup of the scenario consisted of two car mounted user equipment with tracing capabilities. One user equipment had a dedicated GSM/EDGE connection and the other a dedicated UMTS/HSPA connection. The car was moving in an almost straight line from start to the end point. The user equipment performed the needed handover between cells. At each 200 meter interval away from the start point the structure function was calculated. The measurement reports [TS410] [TS210b] issued by the user terminals were used to find the cells covering the same location as the serving cell. The cells were mapped to access points (BTS/NodeB).

In Table 1 the cardinality of the structure function in a product-of-sums is shown for each of the access points in the second column. GSM access points are

identified with $G_i, i \in \{0..9\}$ and UMTS access points with $U_i, i \in \{2, 4, 9..12\}$ in the column named AP in the table. When the indexes of G_i and U_i are identical, this means that the GSM and UMTS access points are co-located at the same site like e.g. G_2 and U_2. The $G_{\forall i}$, $U_{\forall i}$ and *All* shown in AP column represent all GSM, UMTS and GSM/UMTS access points respectively. For $G_{\forall i}$, $U_{\forall i}$ and All cases only the cut-set with cardinality equal or lower than two are shown. The locations where the cut-sets are calculated are numbered from 0 to 16. The coverage from the access points is shown with the symbol $\odot$ in Table 1.

For instance the U_{10} has cut-set cardinality (1,15), (2,8). This means 15 possible single faults and 8 possible combinations of two simultaneous faults may cause the access to fail. As expected the number of cut-set with cardinality one is decreasing when increasing the number of combined access points. For the *All* cases the number of single fault is completely removed, except at locations 3, 4 and 5 Since measurement reports from GSM [TS410] only includes the six strongest neighbor cells, the actual number of neighbor cells could be significantly higher. This implies that the structure function generated, and more especially the number of single faults, could be lower than given in Table 1.

In this scenario we have only included the structure function as extracted from one operator. However, the same algorithm is possible to use with several operators. With the naming conventions the algorithm will be able to generate the complete structure functions across operators and access technologies. With the same naming conventions the structure functions generated from one operator only could give information about the dependencies to third party. For example, if cut-sets with cardinality higher than one contain only resources from third party this could indicate tentative single point of failure.

6. Conclusion

In this paper we have proposed an approach to determine the dependencies in a multi technology multi operator wireless access environment affecting the availabilities provided to the mobile end-user. This may, if the necessary information elements are included in the "handover protocols", enable tightly managed end-user availability. A feasibility study and a field trial have been conducted in a commercial network to derive the structure functions for the access network. With proper naming conventions of the circuits and resources the interdependencies between operators are possible to identify and to build a structure function. Standardization efforts in e.g. IEEE, IETF and 3GPP are needed for our proposed approach. Multihoming/handover between the user equipment and the network might increase the availability, but underlying common resources may have significant effect on the availability. To convert a general structure function to minimal product-of-sums form is NP-hard. The technical challenge is to combine parts of the structure function to find conservative bounds of the estimated availability. This might be a processing

constraint on the user equipment and therefore a solution where most of the computation is performed within the network is preferable.

References

[BP75] R. Barlow and F. Proschan. *Statistical theory of reliability and life testing: probability models*. Holt, Rinehart and Winston New York, 1975.

[BP05] S. Bryant and P. Pate. RFC 3985: Pseudo wire emulation edge-to-edge (PWE3) architecture. IETF, Internet Engineering Task Force, 2005.

[FH09] E. L. Følstad and B. E. Helvik. Managing availability in wireless inter domain access. In *Proc. International Conference on Ultra Modern Telecommunications Workshops ICUMT '09*, pages 1–6, October 12–14 2009.

[G8106] ITU-T G.8110.1; Architecture of transport MPLS (T-MPLS) layer networks, November 2006.

[GJ03] E. Gustafsson and A. Jonsson. Always best connected. *IEEE Wireless Communications*, 10(1):49–55, February 2003.

[IEE08] IEEE 802.21,D11; Draft standard for local and metropolitan area networks: Media indepenedent handover services, 2008.

[LMB+02] W. Lai, D. McDysan, J. Boyle, M. Carlzon, R. Coltun, T. Griffin, E. Kern, and T. Reddington. Network hierarchy and multilayer survivability, November 2002.

[LSGTG08] X. Li, R. Schelb, C. Görg, and A. Timm-Giel. UMTS HSPA and R99 traffic separation. *Wireless and Mobile Networking*, 284:213–224, 2008.

[MyS10] MySQL Team. MySQL reference manuals. `http://dev.mysql.com/doc/`, 2010.

[Rin04] S. M. Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *Proc. 37th Annual Hawaii International Conference on System Sciences*, page 8pp., Big Island, HI, January 5–8 2004.

[SW07] N. Svendsen and S. Wolthusen. Graph models of critical infrastructure interdependencies. *Lecture Notes in Computer Science*, 4543:208–211, 2007.

[SZ06] F. Siddiqui and S. Zeadally. Mobility management across hybrid wireless networks: Trends and challenges. *Computer Communications*, 29(9):1363–1385, 2006.

[TS210b] 3GPP TS 25.331; Mobile radio interface layer 3 specification; radio resource control (rrc) protocol, February 2010.

[TS410] 3GPP TS 44.018; Mobile radio interface layer 3 specification; radio resource control (rrc) protocol, March 2010.

[VCD+05] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M. Jaeger. General availability model for multilayer transport networks. In *Proc. 5th International Workshop on Design of Reliable Communication Networks (DRCN 2005)*, pages 85–92, Lacco Ameno, Island of Ischia, Italy, October 16–19 2005.

[Wol10] Wolfram Research, Inc. Documentation centre. `http://reference.wolfram.com/mathematica/guide/Mathematica.html`, 2010.

[X.792] CCITT X.720; Information technology open systems interconnection structure of management information: Management information model, January 1992.

Appendix

The following assumptions and notations are used;

circuitsT	table in the Md db, see Section 4.
resourcesT	table in the Md db, see Section 4.
POS	product-of-sums.
Cardinality	max cut set cardinality in structure function.

The semantic of the procedures not explicit shown in the algorithm below is a Mathematica [Wol10] like notation.

Algorithm 1 Structure function

```
 1: procedure GetStructureFunction(apList, structfunc)
 2:     for each ap in apList do
 3:         structfunc ← Null
 4:         protectingList ← Null
 5:         GetPrimaryCircuits(ap, structfunc, protectingList)
 6:         GetProtectingCircuits(structfunc, protectingList)
 7:         MapResource(structfunc)
 8:         AppendTo(totfunc, BooleanConvert(!structfunc, "POS")
 9:     end for
10:     if Length(totfunc)==1 then
11:         structfunc ← First(totfunc)
12:         else structfunc ← ReduceCutCardinality(totfunc)
13:     end if
14: end procedure

15: procedure ReduceCutCardinality(totfunc)
16:     reducedfunc ← Null
17:     from totfunc generate potentialcutset with ≤ Cardinality
18:     for each potentialcutset do
19:         if it is a valid cut set then
              reducedfunc ← reducedfunc ∧ potentialcutset
20:     end for
21:     totfunc ← reducedfunc
22: end procedure
```

Algorithm 2 Part 2

```
23: procedure GetPrimaryCircuits(ap, structfunc, pList)
24:     topList ← Select roots from circuitsT where AP = ap
25:     for each top in topList do
26:         structfunc ← structfunc ∧ top
27:         usedList ← Select used from circuitsT where root = top
28:         for each used in usedList do
29:             if used is protected by a pCircuit then
30:                 Union(AppendTo(pList, pCircuit))
31:                 strucfunc ← structfunc ∧ (used ∨ pCircuit)
32:                 else structfunc ← structfunc ∧ used
33:             end if
34:         end for
35:     end for
36: end procedure

37: procedure GetProtectingCircuits(structfunc, pList)
38:     while top ← First(pList) do
39:         pList ← Remove(pList, top)
40:         usedList ← Select used from circuitsT where root = top
41:         for each used in usedList do
42:             if used is protected by a pCircuit then
43:                 Union(AppendTo(pList, pCircuit))
44:                 Replace(structfunc, top → used ∨ pCircuit)
45:             end if
46:         end for
47:     end while
48: end procedure

49: procedure MapResources(structfunc)
50:     for each circuit in structfunc do
51:         mList ← Select equip from resourcesT where circuit=circuit
52:         for each equip in mList do
53:             Replace(structfunc, circuit → circuit ∧ equip)
54:         end for
55:         Replace(structfunc, circuit → True)
56:     end for
57: end procedure
```

Table 1. Cut-set in access network

AP	Cut-set	Location-spot (⊙ represents coverage) 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
G_9	(1,42),(2,11)	⊙	⊙	⊙	⊙	⊙	⊙											
G_8	(1,18)	⊙	⊙	⊙		⊙			⊙						⊙	⊙		
G_7	(1,18)			⊙														
G_6	(1,21)	⊙	⊙		⊙													
G_5	(1,18)					⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
G_4	(1,17)	⊙	⊙	⊙	⊙	⊙	⊙	⊙		⊙								⊙
G_3	(1,18)						⊙	⊙	⊙				⊙	⊙	⊙	⊙	⊙	⊙
G_2	(1,25),(2,11)	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
G_1	(1,17)				⊙	⊙	⊙	⊙		⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
G_0	(1,25),(2,11)							⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
$G_{\forall i}$		(1,4)	(1,4),	(1,4) (2,42),..	(1,4),	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4), (2,14),..	(1,4) (2,14),..
All		(2,8),..	(2,28),..	(2,36),..	(1,1), (2,63),..	(1,1), (2,77),..	(1,1), (2,77),..	(2,4),..	(2,4),..	(2,4),..	(2,4),..	(2,4),..	(2,4),..	(2,4),..	(2,4),..	(2,4),..	(2,28),..	(2,4),..
$U_{\forall i}$		((1,1), (2,84),..	((1,1), (2,504),..	((1,1), (2,504),..	((1,22), (2,9),..	((1,22), (2,9),..	((1,22), (2,9),..	((1,1), (2,46),..	((1,1), (2,8),..	((1,1), (2,8),..	((1,1), (2,56),..	((1,1), (2,56),..	((1,1), (2,56),..	((1,1), (2,56),..	((1,1), (2,56),..	((1,1), (2,56),..	((1,5), (2,382),..	((1,5) (2,322),..
U_2	(1,25),(2,2)	⊙							⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	
U_4	(1,22),(2,9)	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙								
U_9	(1,25),(2,2)	⊙	⊙	⊙														
U_{10}	(1,15), (2,8)							⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙		⊙
U_{11}	(1,11),(2,4)								⊙									
U_{12}	(1,24),(2,2)							⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙

PAPER C

Failures and changes in cellular access networks; A study of field data

Eirik Larsen Følstad and Bjarne E. Helvik

Proceedings of the 8th International Workshop on Design of Reliable Communication Networks (DRCN)

Kraków, Poland, October 2011

FAILURES AND CHANGES IN CELLULAR ACCESS NETWORKS; A STUDY OF FIELD DATA

Eirik Larsen Følstad, Bjarne E. Helvik
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@q2s.ntnu.no

Abstract The operator diversity of different wireless and cellular networks integrated by IP-based networks does not imply independencies in the respective access networks. We have used incident and change records covering more than 1000 days from a GSM/UMTS network operator. Service failures vs. population density and time periodicity of failures have been studied. Our results indicate higher failure intensity in rural areas than in the urban areas and higher failure intensity during working hours. Leased services and power give major contributions to the failure intensity. This indicates dependencies between network operators. The operator staff's logged common root causes for failures show that the restoration times for the affected BTS/NodeB are not identical. The number of changes in the network is significant compared to the number of failures. Our analysis does not indicate correlations between logged network changes and failures.

Keywords: Wireless networks, reliability, availability, measurement, evaluation

1. Introduction

For dependability analysis in a multi operator multi technology access environment the dependencies between the operators are important to understand. Especially in the access networks the dependencies have become common as operators, to lower investments and operational expenses, use common infrastructure/equipment and exchange services. Site sharing, including e.g. power and cooling, as well as equipment sharing and transmission to central locations are elements in commercial deals between competitors other market actors. A proposal based upon the Media Independent Handover [IEE08] framework, for finding dependencies between access networks in real time is proposed in [FH09]. Dependencies in the access networks were described by structure functions. In this paper we analyze the failure effects on services offered by

a GSM/UMTS network and provide new insight into possible dependencies between operators.

Analyses of failures in commercial networks have been difficult to perform due to limited access to operational data. There are a few exceptions, in [SK01], [MIB+08] and [OS07] failures are analyzed based upon automated failure logs, while e.g. in [MVM02] and [SG10] failures are analyzed based on information from manual failure logs. Basically, automated failure logs are created by the system without system administrator's interventions whereas manual failure logs have been created by the system administrators. In [SK01] an availability study of networked Unix machines based upon the reboot messages in the failure logs was performed. In [MIB+08] the Intermediate System to Intermediate System (IS-IS) routing updates from the Sprint IP backbone network was analyzed to characterize failures that affect IP connectivity. A study of the the failure logs from five supercomputers was performed in [OS07] and the authors provided recommendations on how to use failure logs. One of the main recommendations is that failure logs do not contain sufficient information to do automated detection of failures and root causes. In [MVM02] the failure and recovery behavior for a cellular telephone system based on outages reported by operator's staff was studied. The failure data from two high-performance computing sites was studied in [SG10] which provides the mean time to failure and repair and the root cause of failures. In our work the failure effect on the services offered by a GSM/UMTS network are analyzed. The GSM/UMTS overall system architecture and functionality are well described in 3GPP standards, see e.g. [TS210a].

The main contributions of this paper are:

- Failures are categorized into operator, leased services and power related. The failure classification is based upon the logs reported by the operator's staff. The analysis of failures based upon this categorization gives new insight of potential dependencies between the different operators and their contribution to the overall failure intensity. The analysis shows similar failure periodicity for the three failure categories.
- The failure intensity is provided for rural and urban areas. This provides new insight of how failures impact on the actual services offered to the customers in rural and urban areas.
- An analysis of failures with common root cause, shows that restoration times for affected services are not identical. This is contrary to the common assumption in dependability analysis.
- The number of changes in the network is significant compared with the number of failures. This emphasizes that it is important to understand the continuous deployment and evolution of the network when performing dependability analysis. An analysis of changes vs. failures did not unveil correlation between these.

The rest of the paper is organized as follows. Section 2 gives an introduction to the operation and maintenance processes, which generate the data analyzed.

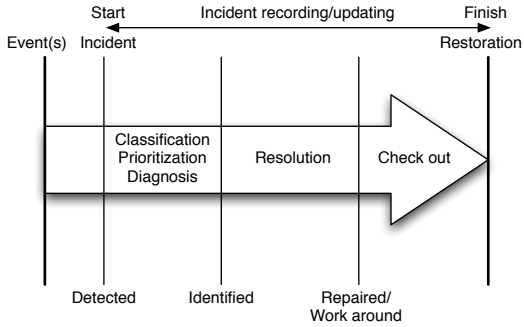

Figure 1. Handling of an incident with activities relatively to time.

In Section 3 we describe the data set used in the study. Section 4 describes the results of service failures vs. population density, and in Section 5 the periodicity of the failures are shown and briefly discussed. Section 6 presents the results regarding how common root cause failures affect the restoration time for the affected Base Transceiver Stations (BTSs) and NodeB. In Section 7 we present the correlation between changes and failures in the data set analyzed. Section 8 concludes the paper.

2. Operation and management processes

For a better understanding of the data set analyzed, the operation and maintenance processes of the operator are described in the following. The operator has adapted the Information Technology Infrastructure Library (ITIL) as framework for the operation and maintenance processes. The British Governments Central Computer and Telecommunications Agency developed ITIL in the 1980s. The objectives of ITIL are to provide high quality services as defined by the business, at acceptable cost facilitated by defined processes and best practices. The ITIL framework can be adapted and used by any business and organization. ITIL has been the basis for the ISO/IEC 20000 Information technology service management [iso05]. ITIL has five domains, of which we will focus on the incident and change management processes within the service operation [Off07a] and service transition [Off07b] domains.

The incident management process' objectives are to restore the service or system as soon as possible after detection of an incident. An incident is defined as a deviation, which may cause an interruption in the future, of the standard operation of the service or system. The main procedures and activities of the incident process are: detection, recording, classification, prioritization, diagnosis, escalation, resolution and check out. Fig.1 shows the relative time line from event(s) triggering an incident to the restoration of the service or system. The incidents are triggered by some events, possibly

correlated, detected by some monitoring means of the system. All kinds of actions, including temporary fixes and workarounds, might be used to restore the service or system. An incident record is created by the operator's staff at detection time and is updated until the check out and closure of the incident. The incident records contain several pre-defined fields necessary for description, diagnosis and resolution of the incidents, such as start times, services affected, classification and priority. The initial classification of an incident is just for a first support in finding the cause and might be changed during the diagnostic and resolution activities through the organization and potential escalation procedures. The incident's priority is based on the impact on business and customers. The duration of an incident is from detection to restoration of the service/system. The classification and prioritization are often used for categorizing the Key Performance Indicators (KPIs) used for monitoring, steering and improving the incident management process.

The change management process shall ensure that all requested changes are efficiently handled by standardized procedures and documentation to improve the operation of the service or system and to minimize change related incidents. One change operation may impact several resources in the network. An incident could initiate a change to be implemented in the network for restoration or to replace a temporary work-around. A change is any modification in the network, such as e.g. SW or HW configuration. Change records contain the objectives, scope and the actual actions needed for deployment of the change. In addition, change records keep all information needed for risk assessment, acceptance of implementation, scheduling of implementation, implementing details and reviewing/control after implementation. Scheduling of the implementation of changes are controlled and coordinated. Every change is reviewed to ensure fulfillment of objectives after implementation.

3. Data set analyzed

In dependability analyses of networks the common approach has been to use some basic failure logs, see e.g. [MIB+08] and [OS07]. The challenges are that these failure logs do not necessarily provide all information needed, and more important, they might neither reveal the network structure, nor how the services and customers are affected by the failures. The network might go through several changes and small/big evolutionary steps during the time period analyzed. The root cause identifications of failures require in depth knowledge of the complete system. It is important to understand the inter-operator dependencies, e.g., leasing of services, when analysing the failures. A failure correlation based purely on comparing start and finish times of events do not capture the root cause or all its succeeding failures.

In this paper we use a data set covering approximately 1000 consecutive days from a cellular network operator. The data set contains information from incident and change records regarding the access network, from BTS and NodeB to the Base Station Controller (BSC) and Radio Network Controller

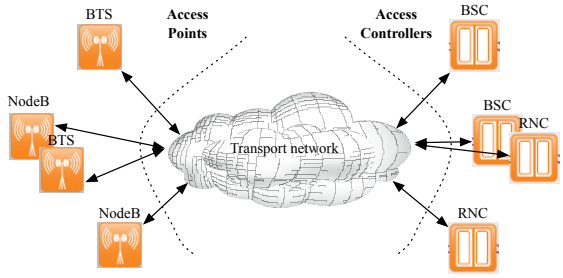

Figure 2. Schematic figure of a GSM/UMTS access network.

(RNC), as recorded by the operator's staff. The operator has a GSM/UMTS network with several thousands of BTS/NodeB site locations. Fig.2 shows a schematic overview of a GSM/UMTS access network. A site location may contain a BTS, a NodeB or both. The transport network connects the access points with the access controllers (RNC or BSC). The transport network represents all technology used, such as for Asynchronous Transfer Mode (ATM) and Synchronous Digital Hierarchy (SDH).

The usage of incident records give valuable information for dependability analyses, since the underlying events are collectively kept in the diagnosis and recording of the handling of the incident. The operator's staff, at all organizational support levels, has used and recorded all available information and network knowledge at the time of incident detection to the closure of the incident. The incident records give information of the affected services and provides implicit the network structure. The granularity of start and finish times in incidents records are seconds. The classification and priority logged by the operators's staff in the incident record are used to identify the failures that degrade the services offered to the customers. Failures are related to HW, SW, cable cuts, configuration, capacity, work etc. Examples of impact on services are degraded quality, reduced capacity or functionality, no service at all, etc. Relative to the ITIL definition of incident, this failure definition, i.e. the one we have used, excludes incidents with possible service interruptions in the future. Incidents from central equipment at RNC/BSC locations are not included in the analysis. Note that customers may be offered services from several BTS/NodeB site locations, where each may be offering GSM and/or UMTS. The data set include all BTS/NodeB locations that have been operational during the whole or parts of observation period.

The change records give valuable information of changes performed in the network. These records are used by the operators' staff to identify risk associated with the change, its reason and the required implementation effort. A change might be related to one resource only (e.g. adding a new carrier to a NodeB) or a cascade of changes of several resources (e.g. reconfiguration of

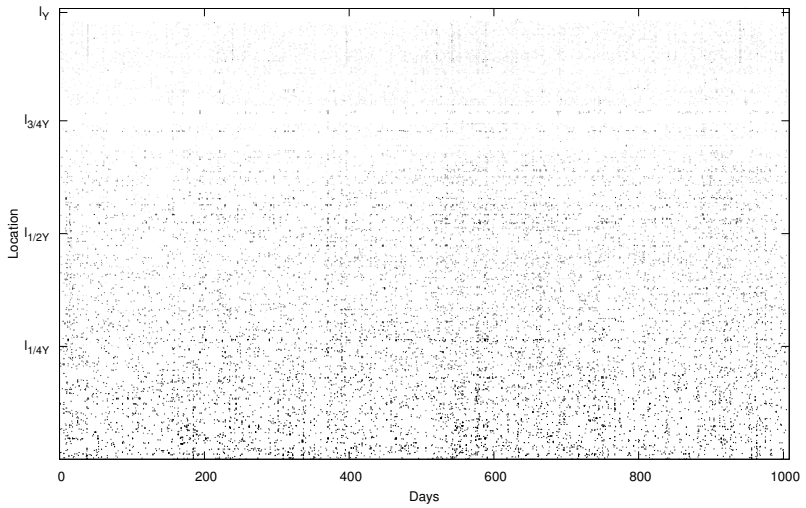

Figure 3. Time of occurrence of failures and the affected BTS/NodeB locations l_y. The population density grows going up the y-axis. The grey scaling is given by (2).

the transmission from a NodeB to the RNC). All change records, as classified by the operator, which modify the access network are included in the data set. The granularity of start and finish times logged in the change records are in days.

4. Service failures vs. population density

From the incident data set, as described in Section 3, the impact on the services offered from a BTS/NodeB site location can be identified. We use the classification and prioritization as logged by the operator's staff to identify all failures that have immediately impact on the services offered from the BTS/NodeB locations. A BTS/NodeB location can contain several physical and logical BTSs and NodeBs dependent on capacity, configuration, equipment type etc. All failures, also including consequences of planned work, are mapped to the affected BTS/NodeB locations. For instance, a failure in the transport network could reduce the transmission capacity for several BTS/NodeB locations.

Fig.3 shows time of occurrence of failures and the affected BTS/NodeB locations. The locations are indexed according to population density, to distinguish between rural and urban areas. How to obtain the density index is described in the following. The operator's total coverage is divided into a number of geographical areas, where an area i has extent a_i. Within each area we are able to track the number of inhabitants, h_i. For simplicity we assume that the number of customers of the operator is proportional to the

number of inhabitants in each area, and that the operator covers 100% of the inhabitants. Each BTS/NodeB location is mapped to one of these areas based on its GPS position. If there are more, say b_i, BTS/NodeB locations in one area, it is assumed that the customer density are the same for all, i.e. h_i/a_i. The BTS/NodeB locations, in total Y, are ordered by increasing customer density, from the lowest to highest. Within each area, the BTS/NodeB location l_y was ordered by its name/id. Hence, if BTS/NodeB location z is located in area j and BTS/NodeB location y is located in area i we have that $l_z > l_y \Rightarrow h_j/a_j \geq h_i/a_i$. The failure intensity, $f(t_x, l_y)$ is defined in terms of affected customers at location l_y during time slot t_x (the slot length is one day) as:

$$f(t_x, l_y) = \frac{h_i}{b_i} n(t_x, l_y) \tag{1}$$

where $n(t_x, l_y)$ are the number of failures at location l_y during slot t_x. To visualize the failure intensity in the scatter plot, the failure intensity $f(t_x, l_y)$ was given a grey scale value $g[f(t_x, l_y)]$ proportional to the percentile of the intensity. More precise, if $G(t_x, l_y)$ is the number of observations less or equal to $f(t_x, l_y)$ and the total number of observations is $\mathbf{G} = Y \cdot t_{max(x)}$, then $g[f(t_x, l_y)]$ is as follows.

$$g[f(t_x, l_y)] = \frac{G(t_x, l_y)}{\mathbf{G}} \tag{2}$$

From Fig.3 it can easily be seen that failures in the access network are daily events that the operator's staff has to manage. In the period between 550 and 600 days the scatter plot is most dense. The failure intensities per inhabitant are seemingly higher in areas with the lowest customer density. The normalization of failures per inhabitants given by $g[f(t_x, l_y)]$ is in this context conservative, since it is independent of the actual BTS/NodeB location configuration and how the failure affect the services offered. A typical BTS/NodeB location in an urban area has more cells, higher capacity, more infrastructure and equipment installed than an average rural location. Hence, a failure of urban locations will affect less of the location's total service than in a rural location. The scatter plot also displays some vertical lines indicating failures affecting several BTS/NodeB locations. Such failures could be due to common root causes in the transmission network, power distribution, planned work etc. The vertical shades in Fig.3 also indicate a non constant overall failure rate.

The distribution of the percentage of failures over the period for the affected BTS/NodeB locations were plotted in Fig.4. In the figure the BTS/NodeB locations have been divided into area groups, $g_j, j = (1, 2, ..., 7)$. Each area group has approximately the same number of inhabitants. Area group g_1 contains all the areas with the lowest customer density, whereas area group g_7 contains areas with the highest customer density. The number of failures for

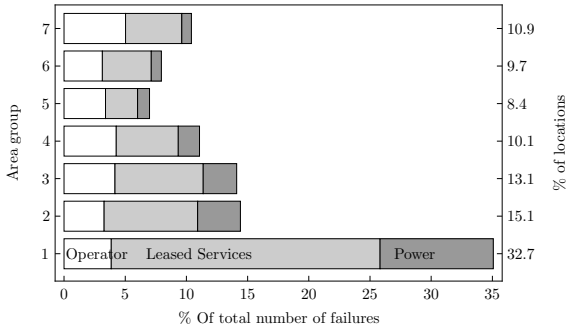

Figure 4. Distribution of percentage of failures within each group of areas. Each group of areas contains approximately the same number of inhabitants.

each area group is calculated as;

$$n_{g_j} = \sum_{\forall l_y \in g_j} \sum_{i=1}^{max(x)} n(t_i, l_y) \tag{3}$$

The failures classifications logged by the operator's staff are used to categorize the failures into three main failure classes denoted; power, leased services and operator. The power failure class contains all failures related to the electricity distribution, battery, Uninterruptible Power Supply (UPS), rectifiers etc. The leased service failure class is related to all equipment and service leased/hired from 3rd parties. Failures that are not categorized into leased service or power belong to the operator failure class.

Fig.4 shows the percentage of the total BTS/NodeB locations in each area group. The number of locations is highest in the least customer dense area group. Area group g_1 has 32,7 percentage of the total locations Y. Note however, that a typical BTS/NodeB location in an urban area has more cells, higher capacity, more infrastructure and equipment installed than an average rural location. Fig.4 shows that the number of failures is higher in areas with small number of inhabitants. Also here the difference is conservatively shown, as noted earlier, since all failures are counted as equal and independent of the BTS/NodeB location configuration and how the failure in concern affects the actual BTS/NodeB. Hence, a failure of urban locations will affect less of the location's total service than in rural locations.

The relative amount of failures categorized as leased service and power are much higher in the rural area groups than in the urban area groups as shown in Fig.4. Other access operators can use leased services and power in the same areas and thereby increase the dependencies between the operators. In rural areas dependencies between access operators are higher due to more limited infrastructure and less economical incitements to build their own infrastructure.

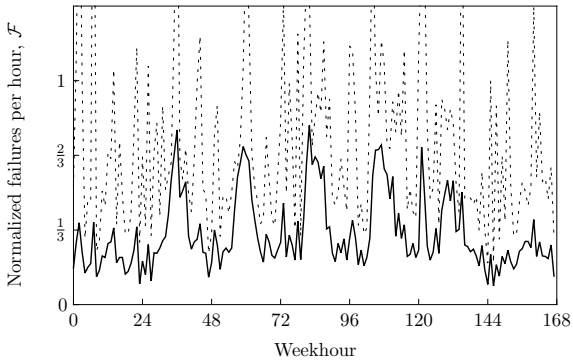

Figure 5. Mean (tick line) normalized number of failures, using unit $\mathcal{F}$, per week hour and the standard deviation (dotted line). The 24 first hours belong to Sundays, the last 24 hours belong to Saturdays.

5. Periodicity of failures

The failures in a network are not entirely random but are also believed to be dependent on the changes and work performed in the network. These assumptions are also supported by analyses performed in [LAJ99] and [MVM02]. From the relatively large data set, covering more than 1000 consecutive days as described in Section 3, we identify the start time of failures that affect services offered from the BTS/NodeB locations. Incidents as consequences of planned work by the operator and leased services operators are included to capture potential failures due to work in the network.

Fig.5 shows the mean number of failures per week hour (tick line) and the standard deviation. The first 24 hours of a week belong to Sundays, next 24 hours are Mondays and so on. The mean number of failures per week hour and the standard deviation have been normalized using an undisclosed constant. This normalization unit, $\mathcal{F}$, is used throughout this paper to avoid revealing sensitive data and for the anonymity of the operator. The mean number of failures per week hour, for the data set covering total W weeks, is obtained as;

$$n_h(s) = \frac{1}{\mathrm{W}} \sum_{w=1}^{\mathrm{W}} \sum_{\forall l_y} n(s + (w-1) \cdot 24 \cdot 7, l_y), \qquad (4)$$
$$s = 0, 1, ..., 167$$

The first observation, i.e., $s = 0$, is immediately after midnight on Sunday and $n(t, l_y)$ are number of failures at location l_y during slot t of length one hour, as defined in Section 4.

From the plot in Fig.5 it can be seen that the failure intensity is highest between 10AM and 02PM each working day. In addition, the failure intensity

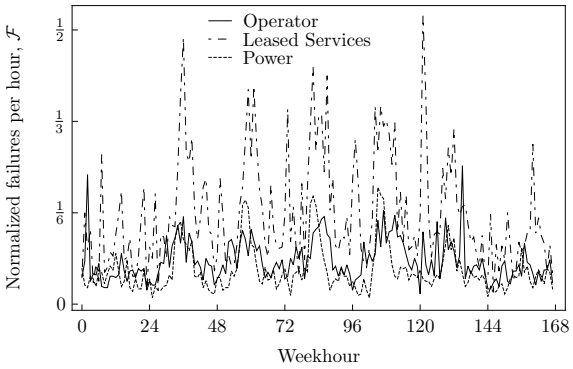

Figure 6. Mean of normalized number of failures, using unit $\mathcal{F}$, per week hour for the failure categories operator, leased services and power. The 24 first hours belong to Sundays, the last 24 hours belong to Saturdays.

is relatively high around 01AM, especially in the night between Thursday and Friday. The time periodicity is quite striking even though the standard deviation is larger than the mean value. Keep in mind that all BTS/NodeB locations affected by common root cause are included, which will increase the standard deviation.

In Section 4 we categorized the failures into three failure classes; operator, leased services and power. In Fig.6 the mean number of normalized failures, $\mathcal{F}$, for each failure category are plotted. Note that the most dense failure periods for all categories are overlapping.

The overall time periodicity of the failures per hour is analyzed by performing a Discrete Fourier Transform (DFT), counting from the first hour of day one to the last hour, T, in the data set. The start time of the failures from the incident records is used to map the failures to the hours. Fig.7 shows the spectrogram of DFT of the failures per hour, using absolute value of the magnitude of each of the frequencies without the mean (also known as the constant component). In the plot we have only shown the frequencies up to $1/2 * j/T$ since $F(T-j) = F^*(j)$ because they are complex conjugate. The DFT, $F(j)$, of the total failures per hour is calculated as:

$$F(j) = \frac{1}{T}\sum_{h=0}^{T} n(t)e^{-i\frac{2\pi}{T}t}, j = 0, 1, 2, ..., T \tag{5}$$

Where $n(t)$ is the total number of failures during slot t of length of one hour according to;

$$n(t) = \sum_{\forall l_y} n(t, l_y), t = 0, 1, 2, ..., T \tag{6}$$

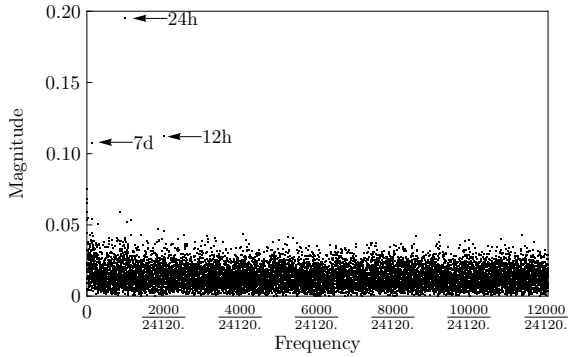

Figure 7. Spectrogram of the Fourier analysis of failures per hour showing the absolute value of the magnitude of each of the frequencies without the constant component (the mean value).

In Fig.7 we find three frequencies (without the constant component) with significantly higher magnitude than the other frequencies that appear more like noise. The linear trend, $l(t)$, has been removed from the set of $n(t)$ before performing the DFT. The three dominant frequencies represent sinusoidal with frequencies of 24 hours,12 hours and 7 days in order of decreasing magnitude. The spectrogram in Fig.7 gives a strong indication that high failure intensity in the night between Thursday and Friday, as shown in Fig.5, is most probably due to some major incidents with common root cause or planned work.

The inverse DFT of the failures per hour will give the exact same number of total failures per hour as given by the incident records. In general the inverse DFT gives the number of failures as;

$$n(t) = \frac{1}{T}\sum_{j=0}^{T} F(j)e^{+i\frac{2\pi}{T}jt}, t = 0, 1, 2, ..., T \tag{7}$$

The spectrum diagram shown in Fig.7 shows that three frequencies plus the constant component are by far the most dominant. Using these limited frequencies, we can derive an approximation of the time dependent failure density as follows;

$$\hat{n}(t) = \frac{1}{T}\sum_{j\in d} F(j)e^{+i\frac{2\pi}{T}jt} + l(t), t = 0, 1, 2, ..., T \tag{8}$$

Where d is the set of the three dominant frequencies and their complex conjugates plus the constant component and $l(t)$ is the linear trend that was removed before performing DFT.

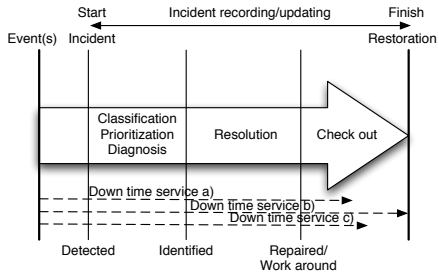

Figure 8. An incident affecting several services/system where the down times for each service/system are different.

6. Failures with common root cause

In dependability analyses it is usually assumed that all failures having the same root cause occur and are rectified at the same time. The same is assumed for dependent services loosing their resources. These assumptions do not take into account that the actual repair process of the common root cause might be gradually performed, where the dependent services/systems are restored at different times based on priority or service level agreements. Similarly, the dependent services/systems could require different restore times after resources are again available due to higher layer protocols and/or applications.

The time periodicity of the failure categories operator, leased services and power as shown in Fig.6 indicates potential dependencies between access operators. The same leased services and power are possibly used by other access operators. In Fig.4 the relatively high number of failure categorized as leased services and power, especially in rural areas, further indicates that the dependencies between access operators might be significant. From the incident data described in Section 3, the effect of a common root cause, as logged by the operator's staff, on the BTS/NodeB is identified. In the analysis we identify the start time when the affected BTS/NodeB does not provide any services due to a common root cause and the finish time when it is restored. A common root cause failure affects minimum two BTS/NodeB. Failures due to planned work are also included in this analysis. Fig.8 shows the relative time line from event(s) triggering a common root cause failure to the restoration of affected services. In the figure the common root cause failure affects three services, a), b) and c). In this example all services are affected at the same time, but the down times for the services are different.

From the data set we analyze the time difference between when the first affected BTS/NodeB is restored and the restoration times for the other BTS/NodeBs affected by the same common root cause. Let the number of affected BTS/Node B be p_c by common root cause failure c. Then each BTS/NodeB in the set of affected nodes, b_c, counts for $1/p_c$ of the affected

BTS/NodeBs. Denote the time BTS/NodeB i in the set b_c is restored by t_i and let $t_{(i)}$ denote the ordered sequence of these, i.e., $t_{(i)} \leq t_{(i+1)}$. For each BTS/NodeB brought back into normal operation, the restored proportion is increased by $1/p_c$. Denote $r_c(\tau)$ the restored proportion of failed BTS/NodeBs due to root cause c at time τ. Formally

$$r_c(\tau) = \frac{1}{p_c} \sum_{i=1}^{p_c} I(t_{(i)+} - t_{(1)-} > \tau), \forall c \tag{9}$$

where $I(\ldots)$ is the indicator function that takes value 1 if the argument is true and 0 otherwise.

Let number of common cause failures we have observed be m, i.e. $c = 1, \ldots, m$. Introduce an ordering of the $r_c(\tau)$ at τ the ordering $r_{(1)}(\tau) \leq r_{(2)}(\tau) \leq \ldots \leq r_{(m)}(\tau)$. Note that the ordering among the cs may change with τ. The q quantile is then given by;

$$R_q(\tau) = \begin{cases} r_{(m(1-q))}(\tau), & \text{if m(1-q) is an integer} \\ r_{(\lfloor m(1-q)+1 \rfloor)}(\tau), & \text{if m(1-q) is not integer} \end{cases} \tag{10}$$

The $R_q(\tau)$ gives the q quantile of the restored proportion of affected BTS/NodeB for common root causes at τ after the first restored BTS/NodeB. Note that we have used the term (1-q) in (10) since the ordering of $r_c(\tau)$ is by increasing value, while we are interested in the quantile of common root causes that are most recovered at time τ. The mean of the proportion of affected BTS/NodeB restored at the time τ is given by;

$$\bar{R}(\tau) = \frac{1}{m} \sum_{c=1}^{m} r_c(\tau) \tag{11}$$

Fig.9 shows the mean, median ($R_{50\%}(t)$), $R_{25\%}(t)$, $R_{75\%}(t)$ and $R_{90\%}(t)$ for the restored proportion of affected BTS/NodeB for common root causes as logged by the operator's staff. As can be observed in the figure the median starts at 50% with a horizontal line until point B, at approximately 10 seconds, where it starts increasing and reaches 100% around 20 seconds. This means that 50% of all common root causes have restored 50% of the affected BTS/NodeB with no time difference for the affected BTS/NodeB, and after 20 seconds 50% of all common root causes have restored all its affected BTS/NodeB. The $R_{25\%}(t)$ is a horizontal line at 100%, which means that 25% of all common root causes are restored with no time difference for the affected BTS/NodeB. The $R_{90\%}(t)$ starts at 25% with a horizontal line until point A, at approximately 11 seconds, where it starts increasing and reaches 50% around 150 seconds (point C). This means that 90% of all common root causes have restored 25% of the affected BTS/NodeB with no time difference for the affected BTS/NodeB, and after 150 seconds 90% of all common root causes have restored 50% of the affected BTS/NodeB. At point D in the figure at approximately 200 seconds,

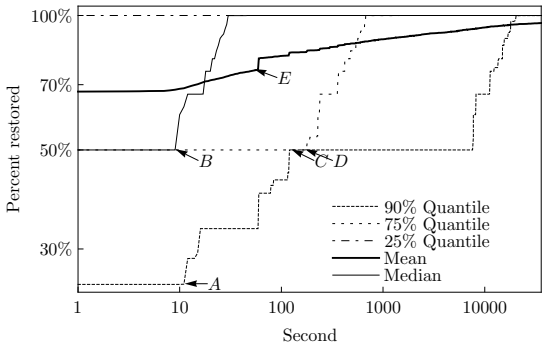

Figure 9. Mean, $R_{25\%}(t)$, $R_{50\%}(t)$ or median, $R_{75\%}(t)$ and $R_{90\%}(t)$ of the restored proportion of affected BTS/NodeB for common root causes as logged by the operator's staff.

75% of all common root causes have restored at least 50% of the affected BTS/NodeB. The mean is also shown in the figure. The mean represents the expected proportion of the affected BTS/NodeB restored at the time in concern. For instance, at point E in the figure, the expected proportion of restored BTS/NodeB at time 70 seconds is 75%.

In the analysis described in Sections 4 and 5 all BTS/NodeB failures caused by common root causes have been included. With the identification of the common root causes for failures as logged by the operator's staff more insight in the failure analysis can be given. E.g. in the scatter plot in Fig.3 a significant proportion of the observable vertical lines are due to common root causes for the affected BTS/NodeB locations. Similarly, the peak of the number of failures between Thursday and Friday night in Fig.5 and Fig.6 are due to a common root cause.

7. Correlation of failures and changes

The evolutions of networks introduce changes to be implemented, from small to significant. Examples of evolution steps in the cellular networks are introduction of GPRS/EDGE, UMTS/HSPA and LTE. Evidently these evolution steps imply big changes in the network, not only in the BTS/NodeB (HW/SW platform and/or supplier) but also for transmission solutions towards the BSC/RNC. Not to forget the necessary changes needed in the core networks.

In Section 5 the periodicity of the failures were analyzed based on the start time of the logged incidents. When analysing the periodicity of the changes we use the finish time in the change records as logged by the operator's staff. A change is not fulfilled before all needed implementations, possibly affecting several resources in the network, are deployed in the network. A change covers also the radio configuration of the BTS/NodeB. The finish time granularity in change records are days. For leased services we include the changes reported

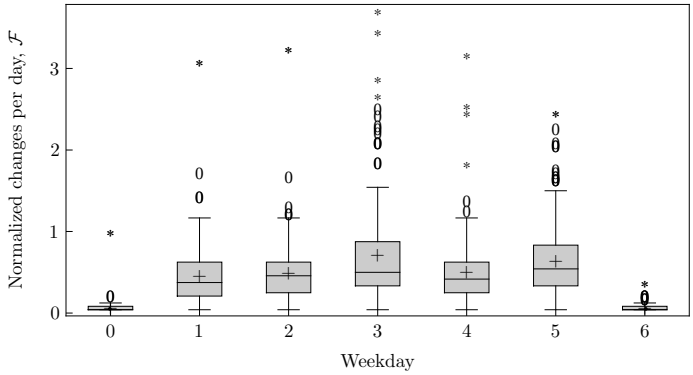

Figure 10. Boxplot for normalized number of changes, using unit $\mathcal{F}$, on weekdays with median (the horizontal line in each box), mean value (+), near outliers (o) , far outliers ($*$) and the IQR covering 50% middle of the data. The week starts on Sunday (0) and ends on Saturday (6).

by the 3rd party to the operator. We do not include changes related to repair activities and exclude all changes on central equipment (BSC/RNC).

Fig.10 is a boxplot of normalized numbers, unit $\mathcal{F}$ (from Section 5) of changes per weekday. The weekday is captured from the finish time of the changes. The boxplot shows the median value (the horizontal line within each box), mean value (+), near outliers (o), far outliers ($*$) and the Inter Quartiles Range (IQR) covering 50% middle of the data. Weeks are starting on Sundays and ends on Saturdays. The plot in Fig.10 shows that the change intensity is highest during working days. This corresponds to the failure intensity per weekday as plotted in Fig.5. Since the granularity of changes are given in days, we cannot identify the actual time of the day for the deployment. Even though the number of included changes count only the change objectives, and not the actual number of resources changed, the number of changes are significantly compared with the number of failures described in Section 5. Note that the number of failures in Section 5 includes all failures due to a common root cause that affect several BTS/NodeB.

When trying to analyse the correlation between changes and failures we have to consider both the time lag and set of changes and failures to be included in the analysis. The time lag is the time between the change is deployed in the network and when the possible failures are discovered as a consequence of the change. Note that this is also highly dependent on the change process at the operator. According to the ITIL definition, every change will be carefully monitored and possible rollback will be performed immediately if found necessary by the operator's staff. Further, changes undergo reviews and risk analyses before deployment to minimize failures. In the analysis of the correlation between

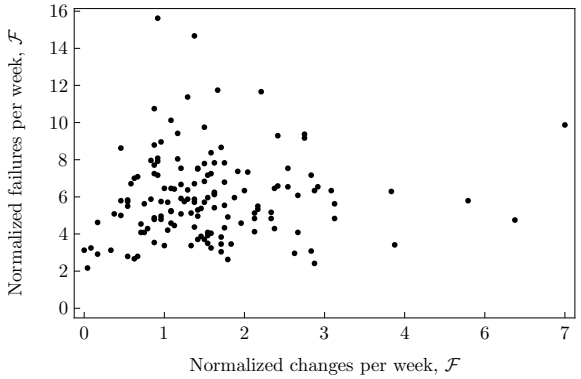

Figure 11. Normalized number, using unit $\mathcal{F}$, of changes and failures correlation within same week where time slot is week. All radio failures and changes are excluded.

changes and failures we have divided the access network into two main parts denoted; radio part and fixed part based upon the classification done by the operator's staff. The radio part is the interface between the BTS/NodeB and the user equipment. Changes like e.g. cell neighbor definitions are defined as radio part. The fixed part is related to everything except the radio part. In the correlation analysis we used the non-radio changes and failures The correlation between changes, C_u, and failures, N_u, per slot time u for non-radio parts are calculated according to the Pearson product moment correlation coefficient $\rho(c(u), n(u))$ defined as:

$$\rho(C_u, N_u) = \frac{\mathrm{cov}(C_u, N_u)}{\sigma_{C_u}\sigma_{N_u}} = \frac{E\{(C_u - \mu_{C_u})(N_u - \mu_{N_u})\}}{\sigma_{C_u}\sigma_{N_u}} \tag{12}$$

Where σ_{C_u} and σ_{N_u} are the standard deviation and μ_{C_u} and μ_{N_u} are the mean for the changes and failures per time slot u respectively. The $\rho(C_u, N_u)$ is calculated using time slot of both days and weeks. The time lag has been varied from 0 to 6 days and 0 and 1 week. The $|\rho(C_u, N_u)|$ was less than 0.20 in all cases. We are not able to identify correlation between changes and failures. In Fig.11 a scatter plot for changes and failures is shown where time slot length is a week, time lag is zero (i.e. within same week) and where all changes and failures related to radio are excluded. Only root cause failures are counted. The normalized number of changes and failures are using unit $\mathcal{F}$ and is the same unit defined in Section 5.

Acknowledgment

We acknowledge the valuable help from the Incident Manager, the OSS Manager and the OSS System Administrator at the operator.

8. Conclusion

In this paper we have studied the failures and changes from the access network from a GSM/UMTS operator. With the large data set covering more than 1000 consecutive days as logged by the operator's staff, new insight into the failure and changes characteristics is provided. The study shows that service failures at the BTS/NodeB locations are higher in rural areas than in urban areas and that the service failures have a strong time periodicity with highest failure intensity during working hours. Dependencies between operators might be significant as the failure classes leased services and power give major contribution to the failure intensity. Change records as used by the operator's staff have been used to study whether there are any correlation between changes and failures. The study did not identify any correlations. The operator logged common root causes exhibit different restoration times for the affected BTS/NodeB locations. The time differences can be more than several minutes and assuming that all affected services are restored at the same time can be wrong.

References

[FH09] E. L. Følstad and B. E. Helvik. Managing availability in wireless inter domain access. In *Proc. International Conference on Ultra Modern Telecommunications Workshops ICUMT '09*, pages 1–6, October 12–14 2009.

[IEE08] IEEE 802.21,D11; Draft standard for local and metropolitan area networks: Media indepenedent handover services, 2008.

[iso05] ISO/IEC 20000-1 Information technology service management part 1: Specification, and part 2: Code of practice, December 2005.

[LAJ99] C. Labovitz, A. Ahuja, and F. Jahanian. Experimental study of Internet stability and backbone failures. In *Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing, 1999. Digest of Papers*, pages 278–285, June 15–18 1999.

[MIB+08] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot. Characterization of failures in an operational IP backbone network. *IEEE/ACM Transactions on Networking*, 16(4):749–762, August 2008.

[MVM02] S. M. Matz, L. G. Votta, and M. Malkawi. Analysis of failure and recovery rates in a wireless telecommunications system. In *Proc. International Conference on Dependable Systems and Networks DSN 2002*, pages 687–693, June 23–26 2002.

[Off07a] Office of Government Commerce (OGC). *ITIL Core Books, Service Operation*. The Stationery Office (TSO), May 2007.

[Off07b] Office of Government Commerce (OGC). *ITIL Core Books, Service Transition*. The Stationery Office (TSO), May 2007.

[OS07] A. Oliner and J. Stearley. What supercomputers say: A study of five system logs. In *Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2007*, pages 575–584, Edinburgh, UK, June 25–28 2007.

[SG10] B. Schroeder and G. Gibson. A large-scale study of failures in high-performance computing systems. *IEEE Transactions on Dependable and Secure Computing*, 7(4):337–351, October/December 2010.

[SK01] C. Simache and M. Kaaniche. Measurement-based availability analysis of Unix systems in a distributed environment. In *Proc.12th International Symposium on Software Reliability Engineering ISSRE 2001*, pages 346–355, Hong Kong, November 27–30 2001.

[TS210a] 3GPP TS 23.002; Network architecture, December 2010.

PAPER D

Towards Risk-aware Communications Networking

Piotr Chołda, Eirik Larsen Følstad, Bjarne E. Helvik, Pirkko Kuusela, Maurizio Naldi and Ilkka Norros

Reliability Engineering & System Safety

vol. 109, pp. 160-174. January 2013

TOWARDS RISK-AWARE COMMUNICATIONS NETWORKING

Piotr Chołda[1], Eirik Larsen Følstad[2], Bjarne E. Helvik[2], Pirkko Kuusela[3], Maurizio Naldi[4], Ilkka Norros[3]

[1] *AGH University of Science and Technlolgy*
Kraków, Poland
{piotr.cholda}@agh.edu.pl

[2] *Centre for Quantifiable Quality of Service in Communication Systems*
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@q2s.ntnu.no

[3] *VTT, Technical Research Centre of Finland*
Helsinki, Finland
{Pirkko.Kuusela, Ilkka.Norros}@vtt.fi

[4] *Dipartimento di Informatica Sistemi Produzione (DISP)*
Università di Roma "Tor Vergata",
Roma, Italy
{naldi}@disp.uniroma2.it

Abstract We promote introduction of risk-awareness in the design and operation of communications networks and services. This means explicit and systematic consideration of uncertainties related to improper behavior of the web of inter-dependent networks and the resulting consequences for individuals, companies and a society as a whole. Central activities are the recognition of events challenging dependability together with the assessment of their probabilities and impacts. While recognizing the complex technical, business and societal issues, we employ an overall risk framing approach containing risk assessment, response and monitoring. Our paradigm gathers topics that are currently dispersed in various fields of network activities. We review the current state of risk-related activities in networks, identify deficiencies and challenges, and suggest techniques, procedures, and metrics towards higher risk-awareness.

Keywords: dependability, network design, recovery, reliability, risk, Service Level Agreement (SLA), survivable networks

1. Introduction

It is a generally recognized fact that people depend more and more deeply on a complex web of interdependent communications networks, in particular the Internet. Risks associated to the failures of electronic communications reverberate directly across society. We must be aware of those risks and decide how to face them.

The literature dealing with risk is extensive, ranging from Lowrance's classic [Low76] to the recent [GMWD06, Hai09, Ave11, pot11]. Looking only into a few papers recently published in RESS like [Ave10b, GSA11, UHV11, TA11, LHTC12], we can see that the topic is gaining momentum in various contexts, also in networking. Most of the risk literature is, however, either general or focused on industries in which life danger or societal consequences of failures are spectacularly high (e.g., safety of energy provisioning, aviation, railways, or oil drilling platforms). In contrast, the context of communications networks is underrepresented, although the inclusion of risk in reliability analyses has been advocated in some papers (e.g., in [BM90] for networks or [SCK04] for dependable computing). With this paper we intend to promote the issue of networking risk in a comprehensive way, and illustrate possible approaches.

Lowrance [Low76] defined risk as 'a measure of the probability and severity of adverse effects.' Kaplan and Garrick [KG81] specified the notion of risk as a triplet consisting of a risk scenario (including the event sequence leading to the unfortunate event), the likelihood of that scenario, and the consequences of the scenario (damage created). Along these lines, we consider that also in networking there are three basic components that should be considered to properly address risk:

- clear recognition of *events that challenge network dependability*,
- assessment of their *probability* (conditioned on available information, thus often subjective/Bayesian) and *extent*, trying to take into account uncertainties involved, and
- assessment of their *impact*, an element mostly neglected in our context so far.

However, as we will discuss extensively in this paper, the dependability problems of communication networks and the associated risks are to a large extent different from those in the fields traditionally considered safety-critical or risk-prone. One of the main challenges is that the rhythm of innovation in communications is now so fast that the networks must be considered as continuously changing. We can still recognize the usage of technical innovations as proceeding through three phases: from being a technological *toy* to becoming an *alternative* to the devices and services in place, to finally representing the *dominant solution*. In the world of Internet applications, the progress from a toy to a dominant way of acting happens often at very fast pace. Moreover, networking paradigms are changing — consider, e.g., the current trend towards cloud computing.

So far, risk in network design and operation has been present mainly implicitly, while here we emphasize the need to deal with it explicitly. Nowadays, a typical approach to reliability is technology-oriented. The occurring failures are classified according to their roots, frequencies, and time durations. Granting full connectivity and survivability to those failures is the ultimate end in itself. For that purpose, recovery methods are introduced, with a basic focus on connectivity restoration, assessment of actual downtimes incurred before traffic can be sent again, and optimization of backup resources. However, in practice we must recognize that there are a number of higher-level issues that require a finer attention to the consequences of failures and the people or companies affected by them. We can identify both business and societal issues. The service provided by an operator is typically just a part in a longer service chain, so that the service provider has to cooperate with the other providers supplying other rings of the chain. At the same time that service belongs with a service portfolio offered by the operator to customers of different relevance and profile, where each service has different technical needs. Service disruptions do not have all the same business consequences.

The liability of a network operator if the service provided to its customers degrades is defined in SLA. They typically include performance bounds on some basic service parameters (e.g., the minimum guaranteed bitrate), but generally do not go much beyond granting a basic degree of dependability in terms of service features like Quality of Service (QoS), availability and security [Hel04]. However, communications services are nowadays so pervasive that a number of human activities, sometimes vital, rely on them: the influence of critical infrastructures to people's lives (and the consequences of catastrophes) is so heavy that they are typically supervised by state authorities, and go quite beyond the simple business relationship between service provider and customer. Therefore, evaluation of services just through some technical dependability parameters leads to a very narrow viewpoint. Adopting a *risk-aware networking* approach allows us to consider and reconcile both technical and higher-level perspectives.

Although dependability can be affected by intentional attacks on the network, in this paper we limit our interest to risks related to service disruptions due to network failures that are not caused by malicious actions[1], considering all unintentional events after which some network elements (hardware, software, protocols) cease to work properly. We structure our discussion adopting notions of NIST Special Publication 800-39 [80011] on the management of information security risk in a company, which is the most relevant level of responsibility in this context. This recommendation divides the risk management process into the following four activities:

[1]This topic has been described quite well, see for instance [Whe11].

- Risk framing: the umbrella action that produces a whole risk management strategy for the organization, where assumptions on challenging events are enumerated and the three points below are accomplished.
- Risk assessment: to identify possible problems, and estimate their frequencies and impact, first qualitatively and then quantitatively.
- Risk response: to determine reactions to predicted risk, where basic options include acceptance, avoidance, mitigation, sharing, or transfer.
- Risk monitoring: to check whether the selected responses have performed well, and provide feedback to re-evaluate and update response policies.

Unfortunately, the development of scientific methods to assess networking risks is still in progress. Although there are many notable activities contributing to this area, some already with a long history and a considerable maturity (see Sections 3–5), the entire view has not been grasped yet in a sufficiently comprehensive and organized way. Rather, a lot of work has been done concerning the risk-aware paradigm we are advocating, but it is dispersed in many various regulatory, standardization, research, planning, operational and maintenance as well as infrastructure resilience activities. They should be recognized and promoted as a whole, so that each part would really add to the meaning and significance of the others in the context of the risk-aware networking.

Our emphasis is somewhat different from that of complex systems science, where new theoretical tools are developed for better understanding of emergent features and phenomena of large networks (see, e.g., [NBW06]). Such insights can be valuable for understanding general relations like scaling laws, and perhaps even for rough evaluation of some risks. For example, it is a mathematical fact that if the distribution of node degrees is appropriately heavy-tailed, then even a random placement of links yields a 'softly hierarchical' network topology with short connections and high robustness [NR08]. We, however, are calling for higher risk-awareness of all players in actual, practical communications networking. Properly understood, it includes awareness of theoretical advances in complex network research.

In this paper, following the description of the risk management process recalled above, we investigate four realms of interest for risk-aware networking. In Section 2 about *methodology*, we claim that risk-aware networking needs a methodology (risk framing) that reflects the multi-faceted nature of the subject. In Section 3 about *techniques*, we show that there are several techniques of mostly mathematical character that are essential for assessing network dependability and risk. In Section 4 on *recovery methods*, we show that the main technical response to risk is its mitigation when we design the network aiming at its survivability, and risk sharing combined with service differentiation when the agreements between the service provider and its customer implicitly include a trade-off between cost and quality. Finally, in Section 5 on *practices*, we claim that network design and operation practices must be adapted to cater for proper risk monitoring, an indispensable part of risk-awareness.

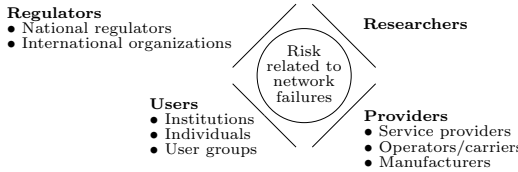

Figure 1. Different classes of actors in the field of network risk.

We conclude by expanding the view to the whole ecosystem of networking companies, and emphasizing the role of regulators in defining the responsibilities and accountability of network and service providers.

2. Risk Framing: on the Methodology of Risk-Aware Networking

The current Internet is both large and extremely complex. It is based on an ecosystem of continuously evolving technical organizations and companies providing communications facilities and services. Its design is based on the work of practitioners and scientists, while various rules for its construction and use, as well as guidelines for its evolution, are set by national and international regulation authorities[2]. While discussing the risk due to failures of this communication infrastructure, we have at least four classes of actors playing a role, and having different points of view, as shown in Fig. 1. The four actor classes differ as to their interests and the threats they face, as well as for their range of action, see Table 1. The class represented by network and service *providers* is the only one that is able to directly influence the network and modify it, and therefore it is natural that the *provider*'s point of view slightly dominates the risk perspective. The aim of *researchers* is mostly to find algorithms and computational techniques for tasks like resilient design and efficient monitoring. In this paper we also seek to contribute to high-level understanding of the complexity of risk-related issues and support risk-aware networking. The achievement of this goal is valuable for the *providers* and *regulators*, and eventually for the *users*.

2.1 Risk Management Cycle

Even the hardware-centric world of providers ought to study the network as a compound socio-technical system, functioning on one hand within human societies and on the other hand in a natural physical environment. A system approach is necessary, but detailed system-theoretic modeling is possible only

[2]For instance, re-shaping of the Internet top-level governance from its US-centric origin to a global entity has undergone a long discussion among Internet authorities, governments, international organizations and other stakeholders.

Table 1. Actor classes and their characteristics relevant for network risk.

Actors	Interests	Threats	Actions
Providers	• Profit • Customer satisfaction	• Penalties • Loss of customers	• Care for dependability • Enterprise risk management
Users	• Availability • Quality and price	• Loss of connectivity or service • Business or life consequences	• SLA adjustment • Choice of a provider
Regulators	• Common benefit and societal needs • Competition	• Anarchy and monopoly • Breakdown of critical infrastructures	• Regulations • Collection of statistics
Researchers	• Innovative solutions • Understanding	• Lack of funding • Lack of focus	• Public promotion of ideas • Standardization

for well-defined sub-systems. For more vaguely characterized systems, and in particular when human factors have a prominent role, one could prefer methods like Checkland's Soft Systems Methodology [Che99]. According to this approach, the researcher does not see the world as a set of well-distinguished systems, but as a realm of complex purposeful activities for which models are constructed within a learning process aimed also at improving those activities.

In this spirit, we consider risk-aware networking, seen principally from the *provider*'s viewpoint, as a control cycle presented in Fig. 2. An existing network is continuously *observed* (by monitoring, customer feedback...), and some kind of a *picture* of its dependability status is maintained. However, when speaking of *risk* monitoring, special attention should be directed to failures with potentially severe consequences, and losses experienced by users should also be monitored as far as possible. Various degrees of analysis and processing of the raw observation data may be required here. On the basis of the observed status, decisions on network changes, including those of network support systems and relations to external networks, are taken. An important task here is the adequate assessment of risks related to the network. While risk factors related to 'normal' failures can, at least in principle, be estimated quantitatively on the basis of failure and loss statistics, thorough qualitative analyses may reveal system vulnerabilities with still a high level of risk. Many other factors than dependability-related ones influence the decisions, but we do not deal with them here.

Note that the inner cycle of Fig. 2 could basically apply to any network provider, whereas the tasks of analysis and risk assessment require additional expertise and are often neglected. The consequence of this is that the 'picture' and the risk response can be unfounded. Contrary to the current state, they should be mandatory in risk-aware networking. The most relevant techniques and practices related to those tasks will be discussed in detail in Sections 3 and 5, respectively.

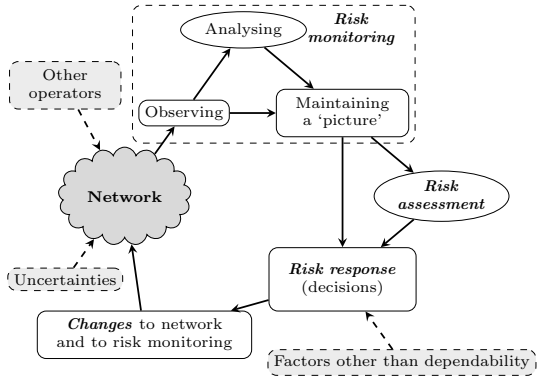

Figure 2. The care-taking cycle of risk-aware networking of a provider.

2.2 Risk Framing for Communications Networks

There is a tendency to see the network as a single entity, but this is far from reality. The network is composed by a number of autonomous subnetworks, which may provide services at different layers, and be owned and operated by a number of different parties. In this context an autonomous subnetwork is to be intended as capable of taking its decisions independently of other players, e.g., concerning its design, its operations, its interconnection, its purchase of services, its cooperation on a peer-to-peer basis. Those subnetworks interact in a complex manner to provide end-user services. It is more correct to regard the network as an ecosystem of networking companies, where each of them has its own business model and a place in the value chain. In this setting, each actor simultaneously competes and co-operates with other market actors. A typical example of the inter-relationships in this context is illustrated in Fig. 3. In that picture each cloud represents an autonomous entity, while the clouds depicted within each dotted box represent entities belonging to the same company (i.e., companies A, B, and D), with a common governance and coordination.

The end *service providers* deliver services (e.g., cellular telephony) to end users. These co-operate for roaming and interconnection, but concurrently they may compete for the same subscribers. In Fig. 3, companies A and B have their own *service platforms* for delivery, while company C leases all its delivery services from company A. The latter is a vertical provider, operating all facets of the service delivery. However, also for this kind of providers, it is common to rent the housing and transport capacity from others. The transport capacity may be provided either as links/leased lines or through the use of virtual routers owned and operated by another party. The fact that the different technology layers may be owned and operated by different entities hinders a global view. A *specialized service provider*, which may play a role of a

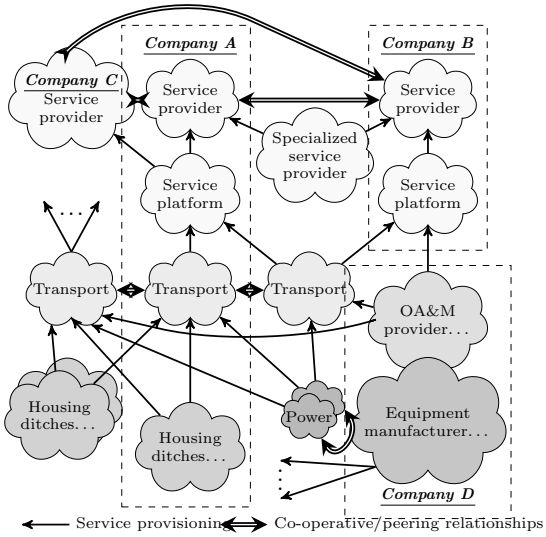

Figure 3. Example of dependencies between autonomous market actors resulting from their co-operation.

location provider or clearing house, is also indicated. It is foreseen that in the future there will be an increasing number of such providers, forming a complex value chain for a compound end user service. In this context, it should also be reminded that end users may be served by several access networks and a number of intermediate Autonomous Systems to reach the service platform of a provider they are looking for.

In the risk assessment context we should also take into account that networks that may appear as completely independent of each other, may in fact share strong commonalities in their environment. For example,

- power to networks or components that should act as backup of each other may be provided by the same supplier;
- cables owned by different carriers may be placed in the same cable duct or ditch;
- equipment operated by different provides may reside in the same housing facility.

For instance, it is quite common for the cellular access that the base stations of different operators, possibly using various technologies, are co-located. The last but not least player that should be mentioned in this networking ecosystem, is the equipment manufacturer. Usage of homogeneous equipment and software throughout the network is a recognized source of common mode logical and

design failures and should be accounted for in a risk analysis. Apart from this fact, there is a trend among network operators to outsource the operation and maintenance of their networks to companies associated with the manufacturers, see for instance [O'B09]. This is also a source of dependencies between services delivered by apparently independent providers and should be addressed in a risk analysis. See also a discussion on theoretical aspects of this issue below in Section 3.2.

Fig. 4 collects the major aspects of Internet networking that should be considered at the risk framing stage. The three dimensions of complexity are:

- horizontal sectioning;
- vertical layers of network technology/protocol;
- market elements related to the commercially optimized sharing of resources within the system of different network providers.

While developing the methodologies supporting risk-awareness, we may take guidance from networking systems, such as aviation and railways, where risk assessment methodologies are more mature. The field of communications shares some properties with those, since:

- there can be many competing providers sharing their resources,
- business solutions are networked,
- outsourcing is used, and
- there is a continuous adaptation to new technologies.

However, there are major differences. We point out that:

- communications networking does not have any central control unlike the ones used for common airspace,
- in communications networking the availability is rarely sacrificed if problems arise (to stop unsafe services), and
- the challenge in the communications risk assessment is the incomparably fast, heterogeneous development of technologies, components, and network usage patterns.

Thus, on the whole, communications networks are heterogeneous and fast moving objects for risk assessments and a large flexibility is needed in the methodology. On the other hand, when time scales and focus are narrowed and targets restricted, we become closer to a well-defined homogeneous (sub-)system.

A risk-aware network operator has also to take into consideration diverse techniques and practices related to causes of failures, network fault-resilience, failure statistics and the estimation of losses, together with their underlying assumptions and limitations. Moreover, the difference of the *user*, *provider* and *regulator* viewpoints highlights the need for various system methods and models according to the particular requirements of risk assessment, starting from a *user*'s interests up to the *regulator*'s concerns on the dependability of the communication infrastructure as a whole. Note that the network recovery with respect to 'normal failures' is not unrelated to the occurrence of big crashes and resilience against them. Serious disturbances may result from

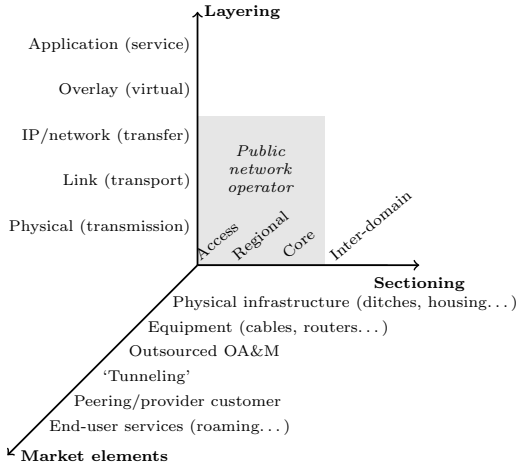

Figure 4. Network aspects that influence the Internet risk.

unexpected coincidences or from hidden vulnerabilities, but both cases can be counteracted (although never totally prevented) by continuous care for network dependability, e.g., through:

- resilient network design,
- research on the functioning of algorithms and software,
- tracking of vulnerabilities, and
- high safety culture at core network facilities.

3. Risk Assessment and Modeling Techniques

First, we elaborate on mechanisms used for dealing with failures as the main factors responsible for increasing risk related to telecom operations. Then, we present the extent of dangers related to failures occurrence along with problems of gathering meaningful statistics, giving a global view of this phenomenon. Afterwards, we sketch foundations of the theoretical aspects of risk modeling. All of the presented techniques can be used for quantification of the design and prediction of the resilient network behavior.

3.1 Network Reliability

The reliability of a network is typically evaluated by the probability that two nodes are (physically) connected through a communications chain. A more effective approach would include the evaluation of the actual capacity provided to carry the customer's traffic. Two nodes may be connected but with a traffic capacity between them inadequate to provide the desired services. In short, it can be said that a satisfactory level of QoS or even Quality of Experience

(QoE) are the sufficient conditions for successful networking, while connectivity is only a necessary one.

When neither repairs nor recovery methods are taken into account[3], the *reliability function* can however be used as the basic measure for a single network element (e.g., a node or a link). It determines the probability that an element operates properly beyond an assumed mission time t, starting at time 0. Any single element alternates therefore between up and down states. The uptime, i.e., the period of the uninterrupted work, can be taken as a measure of failure frequencies[4], and is usually estimated by its mean, MUT. Similarly, we measure the average duration of downtimes, MDT. Since the downtime can be viewed as the time needed for the element to recover from its failed state, MDT and MUT are equivalent to the mean time to recovery, $MTTR$, and the mean time to (first) failure, $MTTF$, respectively. Despite the fact that we have many theoretical and advanced models related to the network reliability theory, commonly applied network modeling of repairable systems has been limited to steady-state availability analysis, which combines the information on mean up- and downtimes.

Turning from single elements to connections (or services), we may define the availability A of a connection as the probability that the connection is up, expressed through the ratio $A = MUT/(MUT + MDT)$. An important property of these metrics is that they might be directly perceived by an end user. From the viewpoint of risk assessment however, availability alone is not sufficient as a risk assessment basis. It can be misleading, since it is an average and does not account for the possibly wide dispersion around the average. Additionally, it does not allow to recover the frequency and impact of failures, since it provides just the ratio of the up- and downtimes. Therefore, a quantitative approach focused on service continuity is necessary [CMHJ09].

Reliability metrics can be included in networking risk assessment using Kaplan and Garrick's [KG81] triplets (s_i, p_i, c_i), where s_i represents the event, p_i is the probability of that event, and c_i is the impact (consequence) of that event. In the networking context, we can say that for instance: s_1 = fault of link 1; p_1 = unavailability of link 1, or $MTTF$ for this link; and c_1 is traffic loss related to the failure of link 1, provided an assumed recovery method is applied, etc. Alternatively, c_i may be expressed in a way that is more relevant for the provider's business or the customer's satisfaction, e.g., as penalties due to SLA violation (in money units), as customer churn rates, or through quality deterioration metrics (increase of download times, decrease of streaming video QoE, etc.).

[3]Practically, repairs and recovery procedures are carried out as a response to reduce the risk, and they should be taken into account. See Section 4.1.

[4]In the case of contemporary multi-layer recovery, faults in some layers (e.g., IP) can be masked by fast survivability procedures triggered in layers beneath (e.g., optical), and then the higher-layer service perceived by a client is not broken, allowing for treatment of such a situation as an uninterrupted working time.

3.2 Failure Statistics

A network operator is risk-aware if it is able to credibly predict failure probabilities and their impact. Measurements of up- and downtimes are needed not only for direct computing of performance indicators but also for forming adequate modeling assumptions. Better models would help reliability prediction, and consequently risk assessment, of future networks. Two issues are challenging in this context:

- dependencies between failure events,
- the non-Markovian character of failure processes.

Moreover, we assume that many large operators assume risk-aware policies that require high-availability networks. Therefore, single points of failure should be avoided. This raises the crucial problem of a proper modeling of multiple failures. So far, the most commonly applied approach to reliability considered failures as independent events despite there are some notable scientific contributions going beyond it, for instance the hazard potential approach [BCCS00]. Other generic models for correlated failures include Markovian models [Spr77, HTHB97], a martingale approach to failure dynamics [AN91], and a recent general framework based on normal copulas [ND08]. The independence assumption is very useful for mathematical convenience to decrease complexity, but it is generally false. In fact, measurements [MIB+08, GHHK10] indicate that failures in communications networks may often be correlated. Overlooking this would result in dangerous overestimation of the actual reliability [Joh05], which leads to undervaluation of the actual risk incurred.

Measurements on the operational Sprint network [MIB+08] indicate that about 30% of failures take place either simultaneously or within a few seconds of one another on different links. Assuming independent link failures would suggest that joint ones be extremely rare. In addition to sheer chance, reasons behind a multiple failure may fall in the following three categories:

- *structural*: two systems share a common service or component;
- *dynamic*: a failure of one component increases the stress on another;
- *epistemic*: the first failure remains unobserved until the second occurs.

The last case means that if network monitoring is not implemented carefully and thoroughly, single faults may go unnoticed, hidden by automatic recovery, and only multiple faults will lead to a system failure. As regards structural reasons, one can point to common equipment among providers, common physical infrastructure among carriers and between seemingly diverse access networks, common operation and maintenance activities among providers, and other commonalities along the market elements in Fig. 4.

The analysis of network failure data suggests that assuming failure processes to be Markovian—memoryless, possessing exponentially distributed up- and downtimes—may not be justified. Downtime durations of network elements have been reported to be sub-exponential or heavy-tailed. Thus, long failure durations are more frequent than what simple Markovian models suggest, and

Table 2. Summary of models and methods on statistical network failures, basic results.

Data	Model or analysis method, outputs	Reference
Large IP backbone; links, routers, PoP	Overlapping failures, failure classes; number of events: power-law; time between failures: typically Weibull	[MIB+08]
IP-core and regional network, node and link failures	Distance-dependent correlation between failures of network elements.	[GHHK10]
Small IP-core, node failures	Router model with exponential uptime and Pareto downtime durations	[KN10]
Small IP-core, node and link failures	Nodes and local links, Weibull uptimes; long haul links, gamma uptimes	[GH12a]
Access network, node and link failures	Spatial and temporal localities, impact of a link failure to a node outage, impact of network design on outages	[CSKM07]
Wireless network, software/hardware failure data	Typically Weibull distribution for $MTTR$ or $MTTF$	[MVM02]
Large IP network	Failure clustering	[LL06]

this should be taken into account during risk assessment in relation to the events impact. A summary of statistical network failure modeling and analysis methods appearing in recent literature is presented in Table 2.

Unfortunately, appropriate failure measurement data are rarely publicly accessible, with [UNI11] as one of few positive exceptions. Still, any up and downtime data are valuable in developing reliability modeling as it prompts for more practical models and reveals areas in which the current data collection needs to be improved. Even with simple data and network information it is possible to provide estimates of the experienced availability for network customers [KN10] widening the scope of network planning and management.

3.3 Loss Estimation

Loss is a major metric to evaluate the impact of risk-incurring events on the service layer, and is easily perceived by customers. There is a whole chain of losses at different levels in a communications network. At the bottom (the Layering-axis of Fig. 4), there are losses of data at the physical layer. But, because of unsuccessful recovery or lack of retransmission mechanisms, such losses propagate to higher layers, resulting in application losses, the ones that generate real harm to a service. The proper context for risk assessment is therefore located at the application layer. In fact, the same amount of traffic loss at the physical layer can result in different service disruptions for the customer: compare for instance a loss of single private voice call vs. emergency call. At the design stage, we can set an upper bound for losses under the reference design conditions, and obtain therefore a conservative estimate. Two groups of losses can be identified as follows.

- *Direct losses*: related to the accumulated unfinished work due to failure occurrence [JT03, HT09], that is traffic lost by being sent to NULL interfaces

or traffic that would be carried if a connection were not broken[5]. Exact modeling of this type of losses has rarely been used. Instead, the loss is assumed to be proportional to downtime and transfer rate. This is not an extensively studied phenomenon; as far as the authors know, [GHW06] is the only paper that discusses this group of losses. Sometimes, experimental data are analysed to fit known distributions, as in [KN10].

- *Indirect losses*: generated by secondary effects, e.g., when traffic flows are re-routed from failed paths and can cause congestion and buffer overflows on the paths that have received the re-routed traffic. Though the customer is not affected directly, QoS/QoE is decreased (a negative externality). This category of losses is typically not taken into account. Its evaluation has to, however, consider current and dynamic network conditions as topology, load, and routing.

3.4 Risk Metrics and Networking Business

Previously, we dealt with the statistical characteristics of network failures. However, a new dimension should be added to the reliability issue, by moving beyond the operational view and considering the business risk for the service providers, society and consumer activity associated with downtimes. Here we delineate a mathematical risk theory for networks, drawing from non-networking contexts.

A mathematical risk theory, providing models for the economical losses associated with adverse events, is well developed in the contexts of the finance [MFE05] and insurance business sectors [DC04]. In the former, the aim is to analyze the variation of the value assigned to a portfolio of securities consisting of stocks or bonds, as the market conditions change. Downturn events may result in the fall of the value of a stock (the market risk) or in the default of a money borrower (the credit risk). On the other hand, in the case of insurance, the best known method for risk transfer, the aim is to evaluate the economical losses associated with an insurance policy, should the insured-against event take place (e.g., the loss of an asset or the occurrence of damages), and correspondingly, to set the insurance premium.

The aim of a mathematical risk theory for networking would be to provide mathematical tools to associate a risk measure with the overall set of downturns that may affect the network service, for instance: failures, indirect traffic losses, or malfunctioning. The introduction of a mathematical risk theory may also provide a different view of the protection means against such downturns.

We first consider the issue of direct risk metrics. Above all, the translation of the risk concept to the networking context calls for the identification of risk in this case. In the insurance/banking context the risk is naturally expressed in

[5]This amount is by definition unobservable, since it is not produced by customers who notice failures and stop sending traffic. Nevertheless, this unsent amount of traffic is not charged and represents a loss of potential revenues to an operator, thus also being a failure impact.

monetary units. This is not the case in the networking context. Here the risk is related to the failure to provide services as embodied in the operator-customer relationship. But such a failure is typically expressed through reliability-related events, and namely in network-centric units. For example, we are used to consider the network connectivity, the failure occurrence rate and its duration, the degradation in the Quality of Service (loss rate, packet delay). Therefore, we need to convert those reliability or QoS metrics into economical losses. Examples of network downturns that may be converted into monetary expressions are:

- the amount of lost traffic when the Quality of Service is degraded,
- the amount of lost traffic when the customer's connection is broken,
- the penalty paid by the operator to its customer (individual or institutional) under SLA or a threat of judiciary actions;
- the effort that has to be spent to restore the service, both as capital expenditures for purchase of new equipment to replace the failed one and as operational expenditures on a maintenance team.

A proposal to assess the economic value of some of these downturns is reported in [INSZ09] in the context of an economics-based traffic management system, where the penalties stated in SLA and the market price of leased lines are used to evaluate the economical damage associated with traffic loss. We can note that the relationship between reliability and economical losses is not a straightforward one: for instance, in [Tod06] it has been shown that a system with a larger reliability level is not necessarily characterized by smaller losses caused by failures.

In network operations, losses are not isolated cases concerning a single point of failure and a single customer. They occur quite continuously (luckily, on a small scale, most of the time) and involve a number of customers each time. In the finance context the risk for a security owner is determined by the aggregation of the securities it holds, that is, its portfolio of securities, some of which may lose money and others do not. An analogous situation takes place in the banking context for the credit risk of a money lender, and in the insurance context for the portfolio of insurance policies held by an insuring company. A similar approach holds for the networking context as well, where we may consider a portfolio composed of customers/services (an approach proposed in [ND08]) and the losses associated with such a portfolio.

We need anyway a method to map the adverse events occurring on the network into a quantity characterizing the economic risk incurred by the network operator. As hinted above, this is actually a two-step process. First, we convert the network-centric measure of service disruption into an economic measure representing the losses associated to the service disruption, and then we compute a single metric summing up the overall effect of those losses. If we indicate the random variable representing the losses by X, an overall measure of risk on X is a functional $\rho(X)$ that maps the probability distribution of the random variable X into a positive real number. The most common

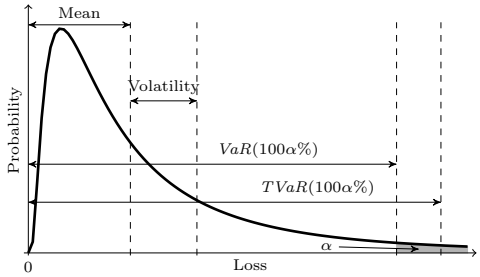

Figure 5. Basic risk measures.

measure of risk developed in the contexts recalled above is the *Value-at-Risk* (*VaR*) [MFE05]:

$$VaR(\alpha) = F_X^{-1}(\alpha), \tag{1}$$

where $F_X^{-1}(\cdot)$ is the inverse probability distribution function of X. $VaR(\alpha)$ represents the maximum loss incurred with probability α (the probability that the loss is greater than the $VaR(\alpha)$ value is $1-\alpha$). Despite being widely used as a reference metric in many risk management environments, *VaR* has received a considerable criticism (see [Sze05], where alternative measures of risk are also surveyed, and [Ave10a] for a more general critical analysis of risk measures). A major problem with *VaR* is that it does not consider the potential extreme losses exceeding the *VaR* itself. At least this shortcoming can be avoided if we employ the alternative metric *Tail Value-at-Risk*, also known as *Conditional Value-at-Risk* (*TVaR* or *CVaR*), which measures the expected value of the losses larger than *VaR* (hence, it is larger than *VaR*):

$$TVaR(\alpha) = \mathbb{E}\left[X | X \geq VaR(\alpha)\right] = \frac{1}{1-\alpha}\int_{\alpha}^{1} VaR(\xi)\,\mathrm{d}\xi. \tag{2}$$

When α is very close to 1, the resulting $TVaR(\alpha)$ or $VaR(\alpha)$ can be taken as proxies for the maximum loss to be expected. Both measures are shown for comparison in Fig. 5, where a sample probability density function of X (e.g., the losses incurred during a time period of one month) is reported. The *Volatility* is a measure of the dispersion of losses around the average value (in practice, the standard deviation of losses in the reference period of time).

Both *VaR* and *TVaR* represent *univariate* measures of risk, since they provide a single value. They are the metrics of choice when all the risk facets can be aggregated, possibly after a preliminary conversion into the same unit of measure, e.g., monetary value. However, it may happen that different sources of risk need to be considered separately, so that the joint value of different risk components is of interest rather than the aggregated risk. Another situation arises when one wishes to consider risk components that are not amenable to a monetary expression, for instance by considering at the same time QoS,

security, and monetary loss metrics. In those situations we may resort to multivariate risk measures, such as those analyzed for instance in [CM07].

Though so far we have relied a lot on metrics derived from the finance context, some caution needs to be exercised when translating those metrics in the networking area. A major difference is that the events of interest in finance or insurance industries are point events, such as the default of a company or the disaster occurrence to the insured company. Instead, in the networking context most events of interest have an associated duration (e.g., the time needed to repair a failure), and losses grow with the duration of the event. Therefore, we need to associate a time dimension to the risk measure, so that we should refer the *Value-at-Risk* to a specified time period, e.g., *VaR* over a year. An example of the application of the *VaR* metric in the networking context is provided in [ND08].

The evaluation of any risk metric in networks is, however, a difficult task for a number of reasons. In fact, as it was said in Section 3.3, a relevant component of the risk incurred during failures is the traffic loss when QoS or QoE is degraded or the connectivity is lost, with all associated problems. In addition, the computation of the risk measure often involves correlated variables. There are two reasons for this:

- many failures are correlated or depend on a common source of failures (see Section 3.2);
- even if correlated failures are neglected, risks associated to SLAs are correlated since they may refer to the same network region.

Finally, downturns are typically rare and their evaluation in a complex environment is likely to call for a simulation-based evaluation where we have to resort to variance reduction techniques.

3.5 Techniques for Assessment Integration

In addition to the mathematical techniques recalled in the previous sections, which allow us to evaluate the impact of risky events under precise modelling assumptions, there are semi-formal methods that may be useful in risk assessment even when the network system as a whole is not modeled formally. An example is represented by *dependability cases*, which are defined in [DK04] as 'a documented body of evidence that provides a convincing and valid argument that the network is adequately dependable, taking all aspects of dependability into account, for a given application in a given environment.' A basic structure of the dependability case consists of three key elements, whose chain of relationships can be illustrated as follows:

$$\textit{Evidence} \quad \rightarrow \quad \textit{Arguments} \quad \rightarrow \quad \textit{Claims}$$

Those elements are characterized as:

- the available *evidence*, i.e., all kinds of documented facts about the network, including maintenance procedures, failure data etc.; and

- the stated goals, or *claims* about different aspects of dependability; they are usually subdivided into a hierarchy of subclaims; as well as
- explicitly formulated *arguments*, which provide support to the claims on the basis of evidence.

The above scheme is an adaptation of the definition of so-called *safety cases* used in the safety assessment of large systems like nuclear power plants [BB98, Kel98]. A dependability case gathers dependability-related information on a complex system in one document (or document structure), organized according to the claim-argument-evidence logic.

Although an experimental dependability case of the Finnish University Network was reported in [NKS08], network risk assessment has not been approached yet with the 'case' methodology, as far as we know. However, we would like to point out at this possibility for the future.

4. Risk Response: Recovery Methods and Service Differentiation

We divide approaches to risk response into two groups. The first of them has a long tradition in designing a network so that it applies mechanisms that provide survivability to failures. What is new, is the emphasis laid on necessity for introduction of differentiated mechanisms suited for various types of services in order to properly address many levels of risks related to them. The second group has an economical character and paradoxically can be in many cases a quick win option for an operator that does not has sufficient resources to effectively use technical means or assumes additional methods of protecting its value chain.

4.1 Technical Means

Unintentional outages due to failures represent the main risk in communications networks. Thus, *risk mitigation* is achieved mainly by making networks resilient in the face of failures (fault-tolerant, survivable), through recovery mechanisms that automatically adopt redundancy (spare resources, backup) to switch the traffic affected by failures. Various recovery mechanisms can also be employed to introduce service differentiation. It represents a form of *risk sharing*, since the customer and the network operator may use the SLA to agree on the respective levels of responsibility in the presence of service degradation.

We can adopt either of two approaches to network resilience against failures: the *engineering* approach focused on the implementation of technically available mechanisms, and the *operations research* approach emphasizing optimization goals or the pursuit of mechanisms meeting requirements related to selected network services. The first approach can be treated as a bottom-up one: the choice of network technology limits the set of available recovery methods that can be used; then the resulting costs and quality is influenced by that choice.

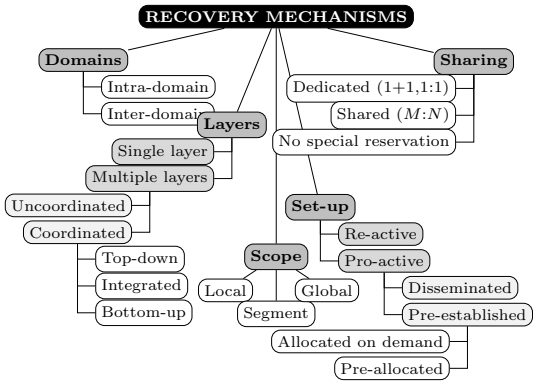

Figure 6. Classification of network recovery mechanisms. The prefix *pre-* is used to mean that the process is performed before a failure occurs, i.e., with a pro-active approach.

On the other hand, the application of the operations research approach, i.e., an approach not restricted by what is present in the equipment or standards, is top-down: first a designer assumes some constraints, for instance related to the quality, and then tries to select an optimized recovery method from a broad spectrum of possibilities. A typical goal is the minimization of cost. In this case, the set of recovery methods is usually loosely limited, and sometimes quite unrealistic options are treated as available (e.g., optical layer re-routing). Now, with the advent and implementation of sophisticated recovery methods, e.g., supported by the automatic control plane under Generalized Multiprotocol Label Switching in fixed networks, the engineering and operations research perspectives converge and enable the adoption of applicable cost- and risk-optimized recovery methods, making risk response feasible.

In order to facilitate the design process, several classifications of possible recovery methods have been introduced. They have a twofold meaning: (1) a presentation of the spectrum of possible methods to mitigate risk, i.e., an educational role; and (2) an indication of the degrees of freedom associated to each method, so as to allow for a preliminary rough design selection. The classifications typically adopt some rule of thumb that includes cost and quality features, and allow for service differentiation (and the subsequent risk sharing). Here we report a quite comprehensive classification, which includes five dimensions [CJ10]. That classification is also sketched in Fig. 6:

(I) **Domains**, involved in recovery operation (see the Sectioning-axis in Fig. 4): (1) intra-domain (single domain): fast (i.e., decreasing impact), but enabling only local optimization, and (2) inter-domain (multiple domains): assuring global optimization, but slower, hardly enabling quality control, and prone to operator's resistance to reveal sensitive information.

(II) **Layers** in which the recovery operates, (see the Layering-axis in Fig. 4): (1) *single layer* based, where the recovery may take place either at lower layers—fast but usually expensive—or at higher layers—slower but potentially cheaper and more flexible (enabling better service differentiation due to the involved connection granularity)—and (2) *multiple layers* based, with the actions on multiple layers being either uncoordinated—simple but costly—or coordinated—potentially cheaper, but complex.

(III) **Scope** of recovery, defining which part(s) of the end-to-end connection are to be recovered (the scope is typically limited to intra-domain recovery): (1) *local* (single link, node): fast but involving complex optimization and potentially expensive, (2) *global* (path, end-to-end): slower, easier to optimize, and (3) *segment*: intermediate between the two above.

(IV) **Set-up** method of recovery resources, which defines the timing relationship between the failure and the determination of the recovery action, with the two basic cases being: (1) *re-active*, computed on demand (known as *restoration* or *re-routing*), coming from the IP world, being flexible but slow, and (2) *pro-active*, pre-computed (called *protection*), which is robust and fast, but rather costly, typical for connection-oriented fixed telecommunications networks (SONET/SDH, MPLS), having many sub-types dependent on the technology applied.

(V) **Sharing** of recovery resources, which defines the degree of sharing of the redundant resources adopted for recovery: (1) *dedicated*: very costly but fast, (2) *shared*: quite robust and with a reasonable cost, and (3) with *no special reservation* of resources, relevant for all types of re-active methods, flexible and cost-efficient but slow.

The options associated to each dimension employed in the classification allow for a very wide range of risk-aware choices, which affect both network design and management, with implications on several time-scales. Most typically, we have three levels of actions, with their own time horizon. We have *dimensioning* activities, which are accomplished with years-long perspectives. We have *routing*, that allocates existing resources for time periods lasting months or days. And on the smallest time-scale we have *traffic engineering*, where decisions are taken hour-by-hour.

Since the engineering and the operations research approaches have somewhat different goals, their outcomes are expected to be diverse. While the former, directed at operational goals, aims at reducing disruption, the latter tries to minimize costs. The optimization solutions that consider thresholds on quality parameters agreed in an SLA are quite rare, although some works have recently been published [MH09, Bai10, XTMM11, ON11, VTA13]. However, the disruption is usually considered statically, and the aim is the minimization of the mean downtime or steady-state probability of unsuccessful recovery. But the perceived disruption, impacting QoE, is not the recovery time reduction itself, but either the simulated loss of traffic or the delay incurred due to

failures. The divergence of results obtained through the two approaches stems also from the fact that cost-optimized methods tend to involve sharing and a larger scope of recovery (global or segment), while fast recovery, minimizing disruption, is achieved through dedication of resources and acts on a local level. Methods combining cost-effectiveness and limitation of failure impact should rearrange a connection after a performance threshold is exceeded (e.g., concerning the maximum number of failures), but they intrinsically involve difficult dynamic optimization algorithms. Additionally, when we consider the layer at which the recovery action takes place, higher layer methods are better from the cost viewpoint due to their finer granularity, while coarse lower layer methods are fast and expensive as they operate on bulky data but do not allow for differentiation. All those aspects should be taken into account by a risk-aware network designer.

In order to introduce a risk-aware approach and allow for risk sharing, it should be avoided to take into account just the operator's perspective and neglect the customer's perception of the service. In fact, the customer is directly affected by failures and is the party mostly interested in the correct evaluation of their impact. Risk assessment without taking into account the customer's role leads to a very partial view. Reliability, risk, and costs are linked by the service features agreed on in the SLA, which represents a relevant tool to enforce a fully risk-aware view by the network operator. For example, the customer's perspective can be included when a broad portfolio of service classes is considered, with different levels of resilience, and the associated various levels of risk sharing [CMH+07]. Although the existing SLA are quite general from this viewpoint (they typically take into account just the steady-state availability), even the existing standardization and recommendation solutions envisage a very large set of metrics that can constitute a base for service differentiation. Aside from measures inspired by the reliability theory, we can find metrics as various as QoE or the number of concurrent failures [CTC+09]. With the adoption of a risk-aware approach, it is time to use such a broad set of metrics as a basis to set performance thresholds and define penalties for their violation in SLA.

4.2 Market Means

A risk management approach to reliability allows us to consider risk mitigation and hedging strategies as accompanying the network-related ones, such as redundancy or fast recovery provisioning. In fact, we can adopt protection measures at a management level, not relying on the operator's own network. We can classify such risk mitigation measures under the following two categories:

- *expansive strategies*, where we aim to preserve the revenue stream;
- *protective strategies*, where we aim to recover the damage due to failures.

The former category includes those measures by which the operator keeps the service going for its customers, though relying on the networks of other operators rather than its own. If the operator keeps the service going, it keeps

cashing on the traffic delivered for its customers, though it will have to pay the alternative operator for that. In order to have this alternative available at the sudden and unpredictable time of failure, the operator must have bought rights of usage on other networks in advance. Buying such rights on demand could not be possible, because the alternative network is not available, or could prove to be too expensive when the offering party uses its dominant position, taking advantage of the urgent need of the provider having outage problems in its network. A preventive purchase of usage rights is represented by the option for leasing spectrum examined in [MN11b].

On the other hand, the operator may choose to accept the loss resulting from the failure of its network, but recovering at least part of its loss by subscribing to an insurance policy. In that case the operator pays a premium against network-related disasters, and receives the compensation on the occurrence of failures. An example of this strategy is the one against security risks on the Internet, proposed in [BL08]. An alternative form of protection is that guaranteed by the so-called CAT bonds (CAT is for 'catastrophe'), issued for natural disasters as well as for man-made and malicious attacks [Kun02]. Here the time sequence of money exchanges is reversed with respect to classical insurance policy. In an insurance policy the network operator pays a premium upfront and receives a compensation if and when the insured-against event takes place. In CAT bond the operator issues a bond, which is bought by investors wishing to take on the risk faced by the operator. Though the operator receives the price paid by the investors upfront, it is then compelled to pay a periodic coupon to compensate them for their risk-taking. However, if the event that is insured against by the bond takes place before the bond's expiry time, the provider is not obliged to pay the principal back to the investors, who then suffer the risk related to the failure.

5. Risk Monitoring and Related Practices

In this section we discuss some issues related to the operation of networks and provisioning of services that will have great impact on the risk associated with networking. Practical models should cope when confronted with some of the real problems:

- absence of single entity to control the network;
- limitation of the insight into underlaying failures and fault handling processes; or
- the network is under constant change and evolution, in fact times between equipment and topology changes in communications networks have the same order of magnitude as times between severe failures.

The most important issues are discussed below. Firstly, we emphasize the relationships of Internet market players. Secondly, we position the role of regulators in this market. Thirdly, practical aspects of network operation are discussed, with the emphasis put on human factors. And at the end of the

section, we give an overview of current practices and identify the challenges in collecting and using data for active risk monitoring.

5.1 Communications Networking Marketplace and Regulators

Fig. 3 illustrates just a few of the inter-relationships for a tiny fraction of the network. The overall set of relationships is large and immensely complex, and has not been mapped yet, as far as the authors know. If we limit ourselves to view the Internet as an interconnection of Autonomous system (AS), a substantial effort has been spent to map the network of AS, as for instance in [IRR11, CAI11, Ker11]. However, even for this limited case, no one claims to have a complete map.

Hence, performing an adequate risk treatment of communications networks is extremely challenging, also because of missing information about:

- the propagation of the consequences of network failures through value chains and peering relationships between market actors;
- an extensive number of commonalities among market actors due to mutual provisioning of underlaying services, common infrastructure, common Operations, Administrations, and Maintenance (OA&M) procedures, etc.

An example of an attempt to help the end user managing the risk associated with these commonalities in a multi-provider, multi-technology mobile access setting, is represented by the suggestion to extend the media independent handover databases of the IEEE 802.21 standard with information about equipment supporting the individual access points and their dependability characteristics [FH09]. Such an approach is, however, far from sufficient to allow an overall risk assessment of services provided in a complex market.

In fact, regulators enforce international and domestic laws to determine requirements on operators providing public service. Two examples of the regulators' activities are the EU Directive on universal service [EUu02] at the European level, and the body of telecommunications regulations defined by the FCC (Federal Communications Commission) in the US [Tit11]. The aim of such regulations is to ensure the availability to the end users of affordable, good quality, and future-oriented services in a competitive framework. We can note that enabling risk assessment and risk management should also be one of the aims. We expect such regulation to define the operators obligations relevant to risk management. Note also that the requirements set by the regulators have significant impact on the ecosystem of networking companies, and thereby on the risk associated with the services provided. Such impact is not always a risk-reducing one. For instance, the regulation on operators with a significant market power reduces the duplication of infrastructure, contributing to the overall efficiency of the telecommunication system. But such reduction makes the infrastructure more liable to failures and less available, with a subsequently increased risk. On the other hand, the regulators might use means to manage the social impact through special requirements for services related to national

safety and provided to prioritized users. For example, in the FCC's National Broadband Plan [FCC10], the reliability and resiliency of communications networks are treated as important issues and will be addressed.

A number of ongoing activities in national and international bodies will have a significant impact on the risk associated with communications networks and services, e.g., by the FCC on network neutrality [FCC05], JAIPA (Japan Internet Providers Association) on packet shaping [Jap08], and ICANN (Internet Corporation for Assigned Names and Numbers) on Internet governance and addressing. Unfortunately, the risk issues are often not explicitly dealt with.

We must finally note that addressing the risks associated with communication networking in a societal context requires information about the network structure, about operational and commercial cooperation among service providers, and operational statistics to be available outside the individual market actors that originally own them. This is contrary to their current practice, which keeps much of this information confidential. Its diffusion will also cause additional costs, so that a resistance may be expected from the service providers themselves. Hence, if the public aim is controlling those risks, a firm and decisive approach from national and international bodies is required. This must be followed up by the standardization bodies in defining which information shall be disseminated, how, and by which format.

5.2 Network Design and Operation Practices

The usage of planning, operational and surveillance tools is quite often reflected by the maturity of the operator and, of course, by his economy. The tools depend on the technologies used and the services provided, as well as the operators organization. The varieties of tools support all parts of the network, like infrastructure (e.g., buildings), the logical and physical network elements and structures, as well as service management and provision. In order to assess and monitor risks, we need the total view of the network structure coming from all the tools, and all the information obtained from the working equipment and operations support systems. Dimensioning, scalability and effective dependability of a network are the result of the balance among conflicting requirements, due for example to the expected market structure, the user behavior, economical aspects, or risk issues (both investment and operational expenses). Most operators use quite simple rules of thumb for dimensioning and design to get the desired level of robustness in their networks (recall for instance the classification of recovery mechanisms given in Section 4.1).

For risk-aware networking the insight into the operation and maintenance processes used by the network operator is important.

5.3 The Human Factor in Operations

It is a common view in the networking domain that a high percentage of network failures is caused by human errors [Kuh97]. Therefore, it is highly

relevant for risk-aware networking to understand, how human operators keep the 'invisible' infrastructure functioning. As one of very few studies in this area, we cite results of [NNLS13]. Twenty representatives of the staff operating the networks of a large national operator were interviewed and the answers were analyzed with the methodology described in [Nor04]. The special work demands in high-tech environments that are intrinsically implied by features of the work domain can be generally classified as being related either to its (1) dynamics, (2) complexity, or (3) uncertainty. These three dimensions covered and structured well also the features of the present domain.

Dynamics appears due to the network nature itself, that is: (i) high frequency of faults and disturbances, implied by the size of the network; (ii) continuous renewal of technology; (iii) network growth caused by new services, and as requirements for fast action of the staff. A reason for urgency may be the scale of disturbance, the criticality of the failure, and a strict SLA. The criticality of a fault must be found out quickly, and actions are often needed before the root cause of the disturbance is identified.

Complexity appears first as related to technologies: the staff of a large operator have to master a large set of technical concepts, products and versions. In addition to this, the operators must manage the historically produced complexity of the existing networks, including ownership and management relations.

Uncertainty is encountered on one hand as a technical constraint related for instance to the wear-out of hardware, hidden errors in software, differences in the implementation of standards and impossibility of exhaustive testing. On the other hand, the operators must often act on the basis of incomplete or flawed information, where additionally all effects of change at the network cannot be known beforehand. The uncertainty is escalated by activities changing the network where modifications are carried out simultaneously at several sites.

Erroneous acts were found at two levels: individual and organizational processes. As regards the work of an individual network staff member, haste, stress, handling several tasks simultaneously and night work, were identified as factors increasing the vulnerability of work performance. Two error types identified in work performances were: lapses and confusions, in particular during configuration and subcontractors works. The vulnerability of performance at organizational level seems to be caused by factors related to habit and culture, for example: meaningless repetitions, slackening of attention during work, neglecting of knowledge or instructions, as well as weakening of interest and motivation. In summary, the human factor in OA&M is an important risk factor and should be taken into account at the risk monitoring stage.

5.4 Data Collection for Risk Monitoring

Collection of dependability-related information for risk monitoring is of utmost importance for network operators. Though all operators collect huge amounts of data, the collection is aimed neither at reliability prediction nor

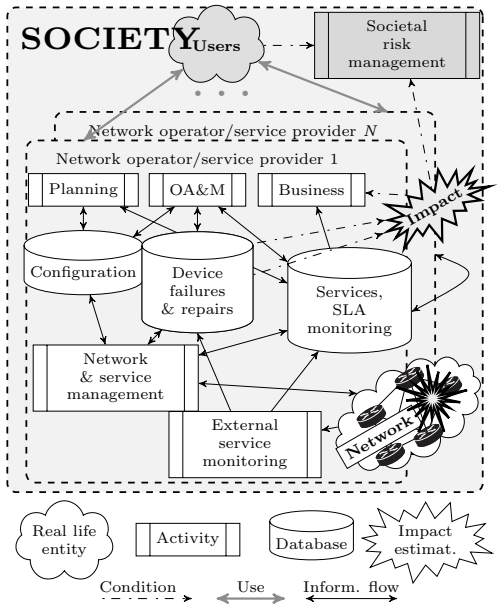

Figure 7. Network risk related data flow.

at risk monitoring and assessment. Rather, this data is used for network and service provisioning, management, and OA&M tasks. In addition, there is no common approach in failure data collection among network operators and service providers. And, naturally, this data is not made available in the public domain. Hereafter, we provide a general description of the current state of data collection, based on our insight, and some guidelines on its requirements under a risk-aware approach.

Fig. 7 is a simplified sketch of the risk-related data flow between networking market players and the users. The inter-relationships between the network operators and service providers illustrated in Fig. 3, are depicted in Fig. 7 with the cloud crossing several network providers. The services are internal (delivered by the operator to its own end users) as well as external (provided to other operators).

As said in Section 3.3, service failures are a major source of risk in communications networks. The impact of failures for the service provider is determined by their multi-faceted consequences: lost traffic and corresponding revenues, penalties incurred by not meeting the SLA, or other indirect costs related to the operator's reputation. However, in a societal context, the impact of communication failures may be far larger than that suffered by the provider of the service. In Fig. 7 the impact is shown spanning several network providers

and the society. Consequences beyond the scope of the operator are very difficult to assess, since they are tightly linked to individual users and the context in which the services are used. The expenses associated with impact, and its measurement, may differ significantly among the users. Furthermore, not all consequences can be measured by monetary terms.

Under a risk-aware approach, statistics of performance and faults in the network serve as the basis for service monitoring and strategic decisions on company operations, like the re-assessment of the risk framework. In many cases the collection of those statistics is defined by regulations, contracts, or agreements. Several sources collectively separated into internal and external ones are used for data collection. The configuration databases represent the physical and logical network and service provisioning of the planned and current state of the network. They must be maintained to make the information on network topology accessible and to reflect the interdependencies among resources in the network. The performance and faults statistics are stored in provisioning databases and provide information on the behavior of the network over time. Not only the network internal observations are sources for such data, but also interconnected networks and customers are relevant data sources. Careful attention must be paid to which data should be collected and stored, to balance the needed information against the amount of data to be stored and analyzed.

Using the collected data for risk monitoring bears considerable challenges. As noted in Section 3.2, dependencies between failure events are likely and the failure processes have a non-Markovian character. If the correlations between failures are to be analyzed, a lot of information is needed, including network topology, traffic handling or recovery mechanisms. Unfortunately, such information is fragmented among different data collection systems stemming from various operational requirements. In addition, data from different market actors must be considered jointly.

A minimal *failure event record* contains the following information pieces about the event:

- equipment identifier,
- start time of the failure, and
- repair time of the failure.

In order to analyze the failures and possible correlations, the event data must be put into the context in which the event takes place. The context (network topology, etc.) should also be stored. The role of meta-data, that is the data crucial for the correct interpretation of the fault data, is underestimated and it is seldom stored in a comprehensive way. To properly address risk, one needs to have information about the process that gives rise to the failure statistics.

If network operators provide *incident information*, such as classification, root cause identification or priority, this data needs to be linked to the failure events.

Such incident information is obtained under the most complete knowledge[6] and it cannot be reconstructed afterwards.

In data collection, one needs also to be aware of certain challenges that may be encountered in the analysis of the reliability data. One issue is that the most interesting data may be difficult to distinguish from erroneous information. For example, if downtime durations indicate heavy-tailed distribution (see Section 3.2), then the longest observed downtimes are very important observations. However, a long downtime duration may also result from an error in parsing the event information, or just from missing data. A fundamental problem is that network monitoring is typically implemented by using the very same network it is monitoring: its performance degrades if the underlying network degrades.

Physical equipment, software modules and system configurations are replaced, modified or changed quite frequently to meet traffic demands and functional requirements. This results in short unaltered periods of the systems compared to the time constants in their failure processes. Similarly, for cost efficiency and competitiveness, operation and maintenance have to adapt to new equipment/technology and the services provided. These continuous changes, add challenges to data analysis and risk management.

For the assessment of correlation and interdependencies, so important in risk analysis, the physical network topology can be extracted from the various databases, but the logical topology might be difficult to obtain. This makes it difficult to maintain a correct network view to correlate failures triggered by error propagation of common conditions/events. There are several commercial systems on the market to perform tasks in data collection and in failure correlation, such as for example Hewlett-Packard OpenView and TeMIP or IBM Tivoli. However, none of them makes data easily accessible for risk assessment or enables (semi)automated risk management.

6. Conclusions

Throughout this work, we have characterized, with varying levels of maturity, risk-related approaches for the design and operation of dependable networks. We claim that the basic needs to be addressed by the research community to serve the industry, business, and society are the following:

Establishment of studies on risk-aware communications networks. Table 3 presents different networking aspects from this standpoint.

Multi-level approach to risk management (e.g., multi-carrier, multi-technology, multi-service, multi-metric). Risk-awareness is not limited only to the design of the operator's own infrastructure. It must take into account different building blocks of the service, where various dimensions are

[6]No pre-programmed intelligence can fully detect anomalies or root causes as this may require information about abnormal events in the outside world at that very moment.

Table 3. Goals on the way to risk-aware networking.

Overall objective				**Intermediary steps**
Objective	**Features, indicator(s)**	**Baseline**	**Target**	
Design, planning & assessment taking into account risk-awareness	Assumed level of risk	Qualitative treatment of risk at best	Risk (event-frequency-impact) in a goal function	Extension of a set of parameters involved in network design and SLA construction, risk as a constraint
Proper risk assessment	Used reliability metrics	Availability as an implicit measure of risk/loss (in the services context)	A set of explicit measures of risk (frequency of events and their severity, along with the assessment of their uncertainty)	Definition of the relation between network reliability and risk assessment
		Mainly connectivity assessment	Quantification of the network ability to provide services with required QoS levels	Inclusion of QoS/QoE measures in reliability assessment
		Loss measured at the traffic level	Loss assessed at the service level	Development of proper loss models taking into account layering and indirect impact
	Used risk metrics	Risk expressed implicitly as selected reliability metrics	Rich set of explicit risk metrics actively applied and induced by business and societal conditions	Definition of adequate risk measures for communications networking
Risk-aware data collection	Analysis-friendly collection of failure data	Detailed failure data utilized almost only re-actively, for repair purposes	Analysis of failure data as a continuous activity; results are used in risk assessment and network design	Working on existing data to improve monitoring and to reveal improper assumptions related to risk assessment
	Modeling of dependencies	Basing on the independence assumption	Correlations between failures taken into consideration	Collection of more detailed data

represented. For example, operational aspects to be covered involve: roaming agreements, multi-homing issues, CAT bonds usage, or even maintenance of the user equipment as a part of the network[7].

Complex value chain. The proper risk-aware design of networks involves a very large set of interacting partners. The complexity of those interactions makes it difficult to determine the details of their cooperation, especially as it is desirable that the risk-aware attitude is adopted not only by an individual player, but by the whole community of operators. The issue is hindered by the fact that risk-awareness is related to the steadily ongoing cyclic process of risk

[7]A paradoxical example of the last issue is the massive provision of software patches to users of mobile phones of a popular brand, which had to be accomplished by the operator, rather than by the equipment manufacturer, to avoid risk of misconfiguration and loss of services to the customers.

framing, assessment, response, and monitoring. Such difficulties are reflected, for example, in the definition of SLAs, where we have a variety of approaches to service provisioning guarantees against an abstract umbrella that is determined by regulatory or standardization bodies. Introduction of risk-awareness would involve emphasis also on development of more sophisticated SLA if necessary.

Acknowledgments

The authors would like to thank Andrzej Jajszczyk, Przemysław Pawełczak, and Rafał Stankiewicz for their help while working on this paper.

References

[80011] Managing information security risk. organization, mission, and information system view. NIST Special Publication 800-39, March 2011.

[AN91] E. Arjas and I. Norros. Stochastic order and martingale dynamics in multivariate life length models: a review. In K. Mosler and M. Scarsini, editors, *Stochastic Orders and Decision under Risk. IMS Lecture Notes—Monograph Series*, volume 19, pages 7–24. Institute of Mathematical Statistics, Hayward, CA, 1991.

[Ave10a] T. Aven. *Misconceptions of Risk*. Statistics in Practice. John Wiley & Sons, Inc., Chichester, UK, 2010.

[Ave10b] T. Aven. On how to define, understand and describe risk. *Reliability Engineering and System Safety*, 95(6):623–631, June 2010.

[Ave11] T. Aven. *Quantitative Risk Assessment. The Scientific Platform*. Cambridge University Press, Cambridge, UK, 2011.

[Bai10] S. R. Bailey. Disaster preparadness and resiliency. In C. R. Kalmanek, S. Misra, and Y. R. Yang, editors, *Guide to Reliable Internet Services and Applications*, chapter 14, pages 517–543. Springer-Verlag Ltd., London, UK, 2010.

[BB98] P. Bishop and R. Bloomfield. A methodology for safety case development. In F. Redmill and T. Anderson, editors, *Industrial Perspectives of Safety-critical Systems: Proc. 6th Safety-critical Systems Symposium, Birmingham 1998*, pages 194–203. Springer-Verlag, 1998.

[BCCS00] K. Brady, J. Chandra, Y. Cui, and N. D. Singpurwalla. Hazard potentials and dependent network failures. In *Proc. 33rd Hawaii International Conference on System Sciences HICSS-33*, Wailea Maui, HI, January 4-7 2000.

[BL08] J.-C. Bolot and M. Lelarge. A new perspective on Internet security using insurance. In *Proc. 27th IEEE Conference on Computer Communications INFOCOM 2008*, Phoenix, AZ, April 15-17 2008.

[BM90] G. Brush and N. Marlow. Assuring the dependability of telecommunications networks and services. *IEEE Network*, 4(1):29–34, January 1990.

[CAI11] The cooperative association for Internet data analysis CAIDA: Macroscopic Internet topology data kit (ITDK). `http://www.caida.org/data/active/internet-topology-data-kit/`, 2011.

[Che99] P. Checkland. *Systems Thinking, Systems Practice: Includes a 30-Year Retrospective*. John Wiley & Sons, Inc., New York, NY, 1999.

[CJ10] P. Chołda and A. Jajszczyk. Recovery and its quality in multilayer networks. *IEEE/OSA Journal of Lightwave Technology*, 28(4):372–389, February 15, 2010.

[CM07] I. Cascos and I. Molchanov. Multivariate Risks and Depth-trimmed Regions. *Finance and Stochastics*, 11(3):373–397, July 2007.

[CMH+07] P. Chołda, A. Mykkeltveit, B. E. Helvik, O. J. Wittner, and A. Jajszczyk. A survey of resilience differentiation frameworks in communication networks. *IEEE Communications Surveys & Tutorials*, 9(4):32–55, 2007.

[CMHJ09] P. Chołda, A. Mykkeltveit, B. E. Helvik, and A. Jajszczyk. Continuity-based resilient communication. In *Proc. 7th International Workshop on the Design of Reliable Communication Networks DRCN 2009*, Washington, D.C., October 25-28 2009.

[CSKM07] B.-Y. Choi, S. Song, G. Koffler, and D. Medhi. Outage analysis of a university campus network. In *Proc. 16th International Conference on Computer Communications and Networks ICCCN 2007*, Honolulu, HI, August 13-16 2007.

[CTC+09] P. Chołda, J. Tapolcai, T. Cinkler, K. Wajda, and A. Jajszczyk. Quality of resilience as a network reliability characterization tool. *IEEE Network*, 23(2):11–19, March/April 2009.

[DC04] M. Denuit and A. Charpentier, editors. *Mathématiques de l'Assurance Non-Vie*, volume 1, Principes Fondamentaux de Théorie du Risque. Economica, Paris, France, 2004.

[DK04] G. Despotou and T. Kelly. Extending the safety case concept to address dependability. In *Proc. 22nd International System Safety Conference ISSC 2004*, Providence, RI, August 2-6 2004.

[EUu02] The European Parliament Council: Directive on universal service and users' rights relating to electronic communications networks and services, March 7, 2002.

[FCC05] Federal Communications Comission: Internet policy statement, September 23, 2005.

[FCC10] Federal Communications Commission: Connecting America: The national broadband plan. Directive 2002/22/EC, March 16, 2010.

[FH09] E. L. Følstad and B. E. Helvik. Managing availability in wireless inter domain access. In *Proc. International Conference on Ultra Modern Telecommunications Workshops ICUMT '09*, pages 1–6, October 12–14 2009.

[GH12a] A. J. Gonzalez and B. E. Helvik. Analysis of failures characteristics in the UNINETT IP backbone network. *International Journal of Space-Based and Situated Computing*, 2(1):3–11, 2012.

[GHHK10] A. J. Gonzalez, B. E. Helvik, J. K. Hellan, and P. Kuusela. Analysis of dependencies between failures in the UNINETT IP backbone network. In *Proc. 16th Pacific Rim International Symposium on Dependable Computing PRDC 2010*, Tokyo, Japan, December 13-15 2010.

[GHW06] Q. Gan, B. E. Helvik, and O. Wittner. Refined classification of service unavailability for comparison: Shared path protection vs. rerouting. In *Proc. 2006 International Conference on Communication Technology ICCT 2006*, Guilin, China, November 27-30, 2006.

[GMWD06] A. V. Gheorghe, M. Masera, M. Weijnen, and L. J. De Vries. *Critical Infrastructures at Risk. Securing the Eutopian Electric Power System*, volume 9

of *Topics in Safety, Risk, Reliability and Quality*. Springer, Dordrecht, The Netherlands, 2006.

[GSA11] T. O. Grøtan, F. Størseth, and E. Albrechtsen. Scientific foundations of addressing risk in complex and dynamic environments. *Reliability Engineering and System Safety*, 96(6):706–712, June 2011.

[Hai09] Y. Y. Haimes. *Risk Modeling, Assessment, and Management*. Wiley Series in Systems Engineering and Management. John Wiley & Sons, Inc., Hoboken, NJ, 2009.

[Hel04] B. E. Helvik. Perspectives on the dependability of networks and services. *Telektronikk*, 100(3):27–44, 2004.

[HT09] P. E. Heegaard and K. S. Trivedi. Network survivability modeling. *Computer Networks*, 53(8):1215–1234, June 2009.

[HTHB97] M. Hecht, D. Tang, H. Hecht, and R. W. Brill. Quantitative reliability and availability assessment for critical systems including software. In *Proc. 12th Annual Conference on Computer Assurance COMPASS'97*, Gaithersburg, MD, June 16-19 1997.

[INSZ09] P. Iovanna, M. Naldi, R. Sabella, and C. Zema. Economics-driven short-term traffic management in MPLS-based self-adaptive networks. In *Proc. IFIP 4th International Workshop on Self-Organizing Systems IWSOS 2009*, Zurich, Switzerland, December 9-11 2009.

[IRR11] Merit Nnetwork, inc.: Internet routing registry, 2011.

[Jap08] Japan Internet Provers Aassociation (JAIPA), Telecommunications Carrears Association (TCA), Telecom Services Association (TELESA) and Japan Cable and Telecommunications Association (JCTA): Guideline for packet shaping, May 2008.

[Joh05] D. M. Johnson. QoS control versus generous dimensioning. *BT Technology Journal*, 23(2):81–96, April 2005.

[JT03] B. Jæger and D. Tipper. Prioritized traffic restoration in connection oriented QoS based networks. *Computer Communications*, 26(18):2025–2036, December 2003.

[Kel98] T. P. Kelly. *Arguing Safety. A Systematic Approach to Safety Case Management*. PhD thesis, Department of Computer Science, University of York, York, UK, September 1998.

[Ker11] T. Kernen. Public route server and looking glass list. `http://www.traceroute.org/`, 2011.

[KG81] S. Kaplan and B. J. Garrick. On the quantitative definition of risk. *Risk Analysis*, 1(1):11–28, March 1981.

[KN10] P. Kuusela and I. Norros. On/off process modeling of IP network failures. In *Proc. 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2010*, pages 585–594, Chicago, IL, June 28 – July 1 2010.

[Kuh97] D. R. Kuhn. Sources of failure in the public switched telephone network. *IEEE Computer*, 30(4):31–36, April 1997.

[Kun02] H. Kunreuther. The role of insurance in managing extreme events: Implications for terrorism coverage. *Business Economics*, 37(2):6–16, April 2002.

[LHTC12] G. Levitin, K. Hausken, H. A. Taboada, and D. W. Coit. Data survivability vs. security in information systems. *Reliability Engineering and System Safety*, 100:19–27, April 2012.

[LL06] J. Lepropre and G. Leduc. Inferring groups of correlated failures. In *Proc. 2nd Conference on Future Networking Technologies CoNEXT'06*, Lisbon, Portugal, December 4-7 2006.

[Low76] W. W. Lowrance. *Of Acceptable Risk: Science and the Determination of Safety.* William Kaufmann, Inc., Los Altos, CA, 1976.

[MFE05] A. J. McNeil, R. Frey, and P. Embrechts. *Quantitative Risk Management: Concepts, Techniques and Tools.* Princeton University Press, Princeton, NJ, 2005.

[MH09] A. Mykkeltveit and B. E. Helvik. Adaptive management of connections to meet availability guarantees in SLAs. In *Proc. IFIP/IEEE 11th International Symposium on Integrated Network Management IM 2009*, Long Island, NY, June 1-5 2009.

[MIB+08] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot. Characterization of failures in an operational IP backbone network. *IEEE/ACM Transactions on Networking*, 16(4):749–762, August 2008.

[MN11b] L. Mastroeni and M. Naldi. Options and overbooking strategy in the management of wireless spectrum. *Telecommunication Systems*, 48(1-2):31–42, October 2011.

[MVM02] S. M. Matz, L. G. Votta, and M. Malkawi. Analysis of failure and recovery rates in a wireless telecommunications system. In *Proc. International Conference on Dependable Systems and Networks DSN 2002*, pages 687–693, June 23–26 2002.

[NBW06] M. Newman, A.-L. Barabási, and D. J. Watts. *The Structure and Dynamics of Networks.* Princeton University Press, Princeton, NJ, 2006.

[ND08] M. Naldi and G. D'Acquisto. A normal copula model for the economic risk analysis of correlated failures in communications networks. *Journal of Universal Computer Science*, 14(5):786–799, March 2008.

[NKS08] I. Norros, P. Kuusela, and P. Savola. A dependability case approach to the assessment of IP networks. In *Proc. 2nd International Conference on Emerging Security Information, Systems and Technologies SECUWARE 2008*, Cap Esterel, France, August 25-31 2008.

[NNLS13] L. Norros, I. Norros, M. Liinasuo, and K. Seppnen. Impact of human operators on communication network dependability. *Cognition, Technology & Work*, 15:363–372, November 2013.

[Nor04] L. Norros. *Acting under Uncertainty. The Core-Task Analysis in Ecological Study of Work.* VTT Technical Research Centre of Finland, Espoo, Finland, 2004. VTT Publications: 546.

[NR08] I. Norros and H. Reittu. Network models with a 'soft hierarchy': A random graph construction with loglog scalability. *IEEE Network*, 22(2):40–46, March/April 2008.

[O'B09] K. J. O'Brien. Ericsson and Nokia Siemens are managing just fine. *The New York Times*, April 12, 2009.

[ON11] N. Ogino and H. Nakamura. Telecommunications network planning method based on probabilistic risk assessment. *IEICE Transactions on Communications*, E94-B(12):3459–3470, December 2011.

[pot11] M. R. potentialsnd. *Risk Assessment. Theory, Methods, and Applications.* John Wiley & Sons, Inc., Hoboken, NJ, 2011.

[SCK04] D. P. Siewiorek, R. Chillarege, and Z. T. Kalbarczyk. Reflections on industry trends and experimental research in dependability. *IEEE Transacions on Dependable and Secure Computing*, 1(2):109–127, April/June 2004.

[Spr77] J. Spragins. Dependent failures in data communication systems. *IEEE Transactions on Communications*, COM-25(12):1494–1499, December 1977.

[Sze05] G. Szegö. Measures of risk. *European Journal of Operational Research*, 163(1):5–19, May 2005.

[TA11] J. Tømmerås and T. Aven. A framework for reliability and risk centered maintenance. *Reliability Engineering and System Safety*, 96(2):324–331, February 2011.

[Tit11] Text of code of federal regulations/e-CFR: Title 47 telecommunication, 2011.

[Tod06] M. T. Todinov. Reliability analysis based on the losses from failures. *Risk Analysis*, 26(2):311–335, April 2006.

[UHV11] I. B. Utne, P. Hokstad, and J. Vatn. A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering and System Safety*, 96(6):671–678, June 2011.

[UNI11] The norwegian research network UNINETT: Downtime statistics. `http://drift.uninett.no/downs/`, 2011.

[VTA13] K. Vajanapoom, D. Tipper, and S. Akavipat. Risk based resilient network design. *Telecommunication Systems*, 52(2):799–811, 2013.

[Whe11] E. Wheeler. *Security Risk Management*. Syngress, Waltham, MA, 2011.

[XTMM11] M. Xia, M. Tornatore, C. U. Martel, and B. Mukherjee. Risk-aware provisioning for optical WDM mesh networks. *IEEE/ACM Transactions on Networking*, 19(3):921–931, June 2011.

PAPER E

Reliability modelling of access point selection and handovers in heterogeneous wireless environments

Eirik Larsen Følstad and Bjarne E. Helvik

Proceedings of the 9th International Workshop on Design of Reliable Communication Networks (DRCN)

Budapest, Hungary, March 2013

RELIABILITY MODELLING OF ACCESS POINT SELECTION AND HANDOVERS IN HETEROGENEOUS WIRELESS ENVIRONMENTS

Eirik Larsen Følstad, Bjarne E. Helvik
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@q2s.ntnu.no

Abstract It is generally recognized that wireless access is getting more and more the preferred way to interact with services. For critical services the reliability of the service session is crucial. We propose a modelling approach for prediction of the reliability of a session in a multi operator multi technology wireless environment. The model allows comparison of different trajectories of access points and handovers along a projected route when the user service is dual homed. We propose to extend the Media Independent Handover (MIH) framework to support the collection of measurement reports from user equipments and signalling in the networks for prediction of session reliability. The proposed model can be used to find the optimal access point selection and handovers for a dual homed service, where the session reliability is basis for the handover decision.

Keywords: Wireless networks, reliability, availability, measurement, evaluation

1. Introduction

The coming 4G networks are assumed to be a mixed environment with different access technologies and several operators all integrated into IP based networks. With lower price, and improved throughput and QoS deployed, further incitements are promoting use of wireless access. The user equipment has become a powerful computing device supporting a number of wireless access technologies like GSM/UMTS, LTE, WLAN and WiMAX. Key challenges in wireless networks are to timely and seamlessly change the point of attachment of the user equipment as the user moves.

In this paper we propose a modelling approach for prediction of the reliability of session in a multi operator multi technology wireless environment where both the coverage and handover failures are taken into account. In our proposal the geographical area is divided into a number of virtual cells with radio coverage

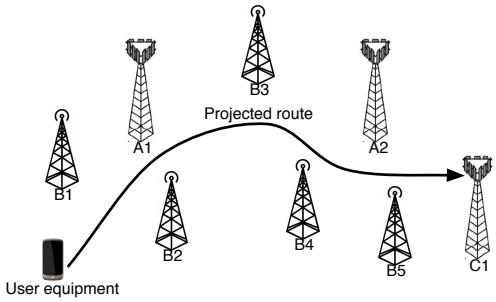

Figure 1. A projected route for a user where several access points can be used. Access point selection and timely handovers are essential to ensure service continuity.

from access points of several wireless access technologies operated by network operators. With the virtual cells defined, the session reliability can be predicted for a projected route. For critical services, this prediction allows to compare session reliability for different trajectories for a projected route. A trajectory, S_{ij}, is defined as the series of access points used in the virtual cells by the two connections i and j from the user equipment to the network. The reliability of the service session is crucial for critical services, like e.g. emergency handling, health care services, energy control and surveillance/monitoring. Reliability is a metric for service continuity, formally $R_{S_{ij}}(t_m) = P(T_{FF} > t_m)$ where T_{FF} is time to first failure and t_m is the mission time. For critical services $R_{S_{ij}}(t_m)$ should be close to 1, i.e., $1 - P(T_{FF} > t_m) \ll 1$, to ensure high probability of uninterrupted service.

Fig.1 shows an example network with several access points and a projected route for a user. Depending on the radio coverage of the access points, there exists several possible trajectories of access points and corresponding handovers. Different network operators own the access points using various wireless access technologies. In [GJ03] the concept of Always Best Connected is defined. This definition covers aspects such as e.g., personal preferences, QoS requirements, available network resources and network coverage. Our contribution is how the reliability of the session for the projected route can be included in the Always Best Connected concept. In the wired access networks, multi homing is used to increase the reliability of the services. This is a possibility in the wireless environment as well, but the mobility of the users make it more complicated. Handover algorithms have to address the decision and execution of change of point of attachment.

A significant research effort has been put into how to make the handover algorithms more reliable and effective. In [YSN10] a survey of vertical handover decision algorithms is presented. Handovers are classified into four groups based upon the handover decision criteria and methods; 1) RSSI based, 2) bandwidth based, 3) Cost function based and 4) combination algorithms. Our contribution

presented in this paper could be part of combination handover algorithms. There exist several proposals of mechanisms to improve handover performance, like pre-authentication [DDF+07] [CIRG09] and provisioning and activation of resources in the target network [NFS+09]. The approaches in [DDF+07], [CIRG09] and [NFS+09] use Media Independent Handover (MIH) [IEE08] as framework. MIH is an emerging standard allowing the user equipment to perform the handover decision based on information provided by the network about the possible access points in the area. We also propose to use MIH focused on how to predict the session reliability for a projected route.

In [FH09] a solution is proposed where MIH was used to build and distribute network topology information with availability estimates. In [FL09] it is described principles for how measurement reports from user equipments can be used to resolve problems and network performance issues. We propose to extend MIH to support the collection of measurement reports from user equipments and signalling in the networks for prediction of session reliability.

The rest of the paper is organized as follows. First in Section 2 we present the system description and in Section 3 an analysis of the robustness of the size of proposed virtual cells are performed. Section 4 describes how the reliability of a dual homed session may be modelled as a phased mission, and approximation suited for optimization is derived. The accuracy of the approximation is analysed in Section 5. Some comparisons between local hop-by-hop and global projected route based handover decisions are compared in Section 6, while detailed information on optimization methods and comparisons are presented in [FH13a]. Section 7 concludes the paper.

2. System description

Our proposal is motivated by how cellular and wireless radio optimization and handover are performed in operational networks. One of the underlying handover mechanisms is the instantaneous experienced quality of some indicators like e.g. signal strength and signal quality. For radio link optimization customer complains and drive-tests are typically basis for optimization. Similarly, the handover decision has primarily been based upon the radio link quality experienced by the user equipment in concern. The goal is to execute the handover in due time before the used radio link cannot be used due to some constraint.

Handover algorithms are typically local hop-by-hop based decisions, i.e., they do not focus on the total session that necessitates several handovers. For critical services, where the service continuity is essential, the seemingly best local hop-by-hop based decision can have a fatal consequence later in the session. For critical services, a global projected route based handover mechanism is favourable since all necessary handovers throughout the session time is taken into account.

The usage of the MIH framework is proposed extended to enable reliability prediction of the service session. The MIIS database is used for requesting

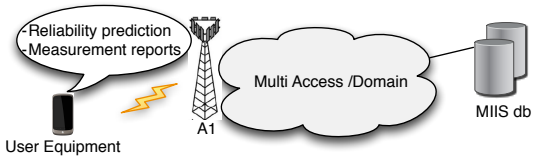

Figure 2. Sketch of MIIS usage for prediction of session reliability. Measurement reports from user equipment populate MIIS database. Such information provides means to select optimal selection of access points and handovers.

network information and provides media independent mechanisms for sending measurement reports. In Fig.2 the user equipment attached to access point $A1$ can send measurement reports and request network information from the MIIS database. The measurement reports contain experienced radio conditions for the given geographical areas. By combining measurement reports and signalling from networks, MIIS identifies limited geographical areas where the radio conditions, like e.g. coverage failure intensity, recovery rate, handover failure probabilities between access points, are homogenous. These limited geographical areas are defined as virtual cells.

Referring to Fig.1, a user has to traverse a number of virtual cells along the projected route. The user requests the MIIS database for information that provide means to find the optimal trajectory as series of access points for each of the two connections in the dual homed session. In this paper we will describe how to predict the reliability for a trajectory given that the virtual cells are defined.

Trustworthy third-party agents must operate the MIIS databases. For network providers the MIIS information is sensitive because it provides detailed dependability parameters and deep insight into the network. For users, the privacy is a concern, since the measurements reports provide information about their movements. Likewise, the integrity of the measurement reports must be validated to ensure trustworthy information. Accurate positioning methods are needed to identify the geographical area for measurement reports and location for virtual cell boundaries.

The measurement reports contain information that could be user equipment specific. For instance, a car-mounted device has better receiving capabilities than the same device without such mounting. Likewise, the capabilities in terms of access technologies and number of active interfaces supported differ between user equipment types. In addition, the speed of the user has impact on e.g. handover success probabilities. We have assumed that a user equipment supports up to two active interfaces. Without loss of generality, user equipments are identical and have the same velocity through a virtual cell. The content of measurement reports are influenced by e.g. traffic load and interference. We

assume that time stamps of the measurement reports are used to find time of day dependent virtual cell parameters.

The handover decisions and executions are essential mechanisms to ensure service continuity for a mobile user. The mechanisms for handover decision and execution can be located in the user equipment or in the network. Multi homing capabilities may be used to provide higher reliability of the session. In our proposal, the provisioning, i.e. activation and deactivation of the interfaces are performed at layer 1 and layer 2, whereas the multi homing handling are provided at higher layers, such as network and transport layers. Mobile Stream Control Transmission Protocol (SCTP) [SXM+00] and its extensions cellular SCTP [ASS03] are examples of multi homing protocols at transport layer. Mobile IPv6 (MIPv6) [PJA10] and Site Multihoming by IPv6 Intermediation (SHIM6) [EN09] are examples of multi homing protocols at network layer. In our proposal, a prerequisite is a dual homing mechanism that provides seamless usage of the two connections if one connection is failing.

3. Robustness of virtual cell boundaries

The concept of virtual cells is essential in our proposed reliability modelling of a trajectory. Analysis of the robustness of where the virtual cell boundaries are located will be performed later in this section. First, the reliability of a dual homed session is predicted by a continuous time discrete space Markov model, where handovers can be performed at any time. From this, a discretized model is described where the handover implications on reliability are calculated only at the virtual cell boundaries.

3.1 Homogeneous model with Poisson handover process

Assume that all virtual cells are homogeneous regarding radio conditions and handover executions. This is an oversimplification of the real world, but the purpose is to validate the robustness where the virtual cell boundaries are located. For a projected route, e.g. as shown in Fig.1, the user will traverse through a number of virtual cells. The following behaviour and parameters are used to model a dual homed session for a trajectory;

- A multi homing mechanism ensures usage of the dual homed session and provide seamless service continuity if one of the two connections fails.
- A connection to an access point has a constant radio coverage failure intensity λ. The coverage from different access points fail independently.
- When a connection to an access point has been lost, the time to recover is n.e.d with mean $1/\mu$.
- The sojourn time in a virtual cell is n.e.d with mean $1/\lambda_d$ and the probability for a handover is p_h for each connection of the dual homed session. The Markov properties yield a handover intensity of $\lambda_d p_h$ which is constant irrespective of the average size of a virtual cell. E.g. if cells sizes are halved yield expected sojourn time $1/(2\lambda_d)$ and handover probabilities $p_h/2$.

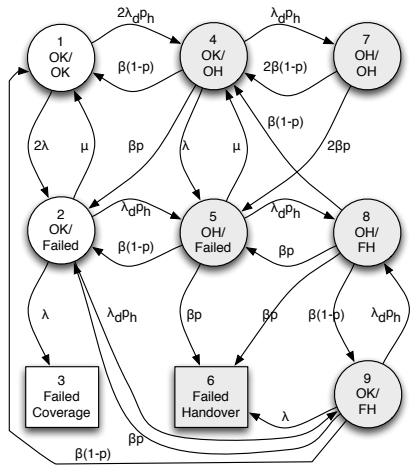

Figure 3. State transition diagram for dual homed session. Grey shaded states are handover states, others are coverage states. Rectangular states shaped represent that both connections are failed.

- The duration of a handover is n.e.d. with mean $1/\beta$ and may fail with a failure probability of p. In case of dual handovers, the handovers fail independently
- A connection that has failed can perform either a recovery or a handover. A failed connection has same handover intensity and handover failure probability as for a working connection.

In Fig.3, a state transition diagram for a dual homed connection is shown. This model represents a continuous time discrete space Markov model where the virtual cells for the projected route are homogenous and the two connections are symmetrical, i.e., transition intensities are identical for the two connections in all cells.

In this simplified model, handovers may take place at any time, in spite of the virtual cell consent, due to the Markov assumptions. The objective of the model is to be a basis for "discretization" to distinct cells borders, see subsection 3.2, but where the results obtained are robust to cell size used.

In Fig.3 handover states Ω_H are shaded grey, while the white ones are coverage states Ω_C since loss of radio connection is the main cause of failure within a virtual cell. We have $\Omega = \Omega_H \bigcup \Omega_C$ and $\Omega_H \bigcap \Omega_C = \emptyset$. In the handover states, $\Omega_H = \{4, 5, 6, 7, 8, 9\}$ at least one of the connection is executing a handover. In the coverage states, $\Omega_C = \{1, 2, 3\}$ no handover is carried out. Rectangular states shaped in the figure, $\Omega_F = \{3, 6\}$, represent that the session has failed, whereas the circled constitute working states, $\Omega_W = \Omega \bigcap \overline{\Omega}_F$. There

is no transition intensities out of failed states, since we are interested in finding the reliability of a session of time t_m, i.e. $R(t_m)$. The working states are named according to the state of each of the two connections. For example, the state named OK/OK shows that both connections are working and the state FH/OH shows that one connection has a failed connection executing handover while the other connection has a working connection while executing a handover.

The transition intensity matrix for Fig.3 is organized as

$$\Lambda = \begin{bmatrix} \Lambda_{CC} & \Lambda_{HC} \\ \Lambda_{CH} & \Lambda_{HH} \end{bmatrix} \tag{1}$$

where Λ_{CC} is the transition intensity matrix between the coverage states and Λ_{HH} is the transition intensity matrix between the handover states, and finally Λ_{CH} and Λ_{HC} represent the transition intensity matrixes between the coverage and handover states and vice versa respectively. Let q_{xy} denote the transition intensity in Λ from state x to state y where $x, y \neq x \in \Omega$ and $q_{xx} = -\sum_{\forall y, y \neq x} g_{xy}$. The transient state probability vector $p(t) = [p_1(t), p_2(t), .., p_9(t)]^T$ where $p_1(t), p_2(t)$ and $p_3(t)$ represent the coverage states and $p_4(t), p_5(t), .., p_9(t)$ represent the handover states. The transient state probability vector is found with the initial condition $p(0) = [1, 0, 0, 0, 0, 0, 0, 0, 0]^T$ by

$$\Lambda p(t) = \frac{d}{dt} p(t) \tag{2}$$

The probability for service continuity up to time t, i.e. that the service has not been disconnected caused by handover or coverage failures, is given by the reliability function

$$R(t) = 1 - \sum_{i \in \Omega_F} p_i(t) \tag{3}$$

where $p_3(t)$ represents the transient probability for the Failed Coverage state and $p_6(t)$ the Failed Handover state at time t. $R(t)$ will be used as a reference in the next subsection where the robustness of where the cell boundaries are analyzed.

3.2 Virtual cell's boundaries

In Section 3.1 a continuous model was derived for a dual homed service were handovers are performed at any time instant given by the handover intensity $\lambda_h p_h$. Here we will investigate the sensitiveness of where the cell boundaries are defined. As introduced in Section 2 the virtual cell sizes are dependent on the radio conditions i.e., the quality and strength of the signal received. Thus, the cell sizes are dependent on all access points' radio conditions.

Consider for a given projected route when transitions between Ω_C and Ω_H take place only at equidistant time instants. The equidistant time instants are given by the sojourn time in the homogenous virtual cells. Assume that the time in virtual cells is $\Delta = \lambda_d^{-1}$ and handovers take effect at $t = i\Delta, i \in \mathbb{N}$. The

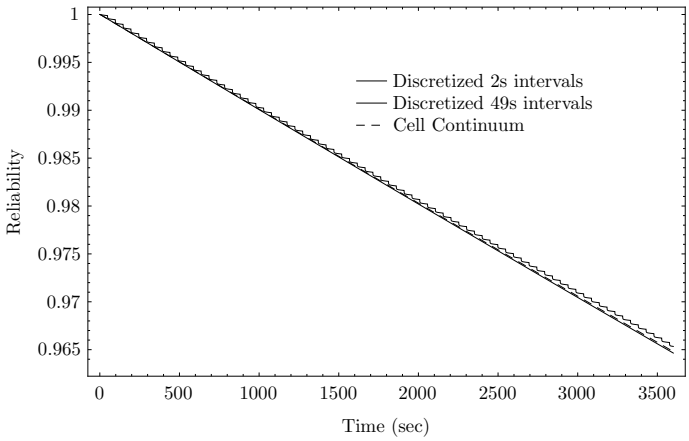

Figure 4. Comparison between $R(t)$ and $\dot{R}(t)$ where the equidistant interval $\Delta = \{2s, 49s\}$ using parameter values given in Table 1.

time between handovers is no longer n.e.d $\lambda_d p_h$, but is a geometrical distributed number of handovers with parameter p_h. The aim is to find a model where the constant virtual cell sizes can be adjusted and still have the reliability function $\dot{R}(t)$ close to $R(t)$ of (3) and preserves this property irrespective of the choice of Δ. Such robustness gives improved precision on estimated parameters and flexibility to adjust virtual cell sizes according to the estimations. Within a virtual cell, only coverage states are considered given by the transition intensity matrix

$$\Lambda_C = \begin{bmatrix} \Lambda_{CC} & 0 \\ 0 & 0 \end{bmatrix} \tag{4}$$

Note that in Λ_C $q_{xy} = 0, \forall x \in \Omega_H$. The transient state probability vector just prior a handover is $\dot{p}((i+1)\Delta_-)$[1]. The $\dot{p}((i+1)\Delta_-)$ is derived from

$$\Lambda_C \dot{p}(t) = \frac{d}{dt}\dot{p}(t) \tag{5}$$

with the initial condition $\dot{p}(i\Delta_+)$ just after a handover and $\dot{p}(0) = p(0)$. By assuming that the handover time is negligible the transition probabilities are used at the virtual cell boundaries. The transition probabilities are given by

$$\Pi_H = -\Lambda_H / q_{xx} + I, \text{ where } \Lambda_H = \begin{bmatrix} 0 & \Lambda_{HC} \\ 0 & \Lambda_{HH} \end{bmatrix} \tag{6}$$

[1]The notations Δ_- and Δ_+ are used to indicate instants immediately before and after the handover that takes place.

Table 1. Reference parameter values

.

Parameters	λ λ_{i_d} λ_{j_d}	μ μ_{i_d} μ_{j_d}	$\lambda_d p_h$	β $\beta_{i_d i_{d+1}}$ $\beta_{j_d j_{d+1}}$	p $p_{i_d i_{d+1}}$ $p_{j_d j_{d+1}}$
Value	1/998	1/2	1/100	4	6/100
Units	s^{-1}	s^{-1}	s^{-1}	s^{-1}	

In (6) $q_{xx} = 0, \forall x \in \Omega_C$. The transient state probabilities just after handover is $\dot{p}(i\Delta_+) = \Pi_H^{\infty} \dot{p}(i\Delta_-)$. To have a model that is insensitive to the choice of Δ, we have to preserve a constant average handover intensity, given that the connection is working irrespective of the choice of Δ. Although $p_h \lambda_d = p_h/\Delta$ we have to compensate for moving all handovers to the cell border, since the probability of being in the coverage states is decaying in the continuous case. We do this by introducing an effective cell time Δ^* that ensures that the expected number of handovers are same in the two cases, i.e. $\dot{p}(i\Delta_+)\mathbf{1_C} p_h = \int_{i\Delta}^{i\Delta+\Delta^*} \lambda_h p_h \dot{p}(t) 1_C dt$ using that $\Delta = \lambda^{-1}$ yields

$$\dot{p}(i\Delta_+)\mathbf{1_C}\Delta = \int_{i\Delta}^{i\Delta+\Delta^*} \dot{p}(t) 1_C dt \tag{7}$$

where $1_C = [1,1,1,0,0,0,0,0,0]$. The intensity from the coverage to the handover states at time t is $\alpha(t) = \Lambda_C \dot{p}(t) 1_H$ where $1_H = [0,0,0,1,1,1,1,1,1]$. If we use that $\dot{p}(i\Delta + t)1_C \approx \dot{p}(i\Delta)1_C e^{-\alpha(i\Delta)t}$ the effective cell time Δ^* is found by

$$\Delta = \int_0^{\Delta^*} e^{-\alpha(i\Delta)t} dt = \frac{1 - e^{-\alpha(i\Delta)\Delta^*}}{\alpha(i\Delta)} \tag{8}$$

which gives

$$\Delta^* = \frac{-\ln\big(1 - \Delta\alpha(i\Delta)\big)}{\alpha(i\Delta)} \tag{9}$$

The probability for service continuity up to time $t = i\Delta_+$, i.e. the service has not been disconnected caused by handover or coverage failures, is given by the reliability function

$$\dot{R}\big((i+1)\Delta_+\big) = 1 - \dot{p}(i\Delta + \Delta^*)1_F \tag{10}$$

In Fig.4 comparison between $R(t)$ and $\dot{R}(t)$ are shown for the parameters values as given in Table 1. For $\dot{R}(t)$ there is plotted two cases where the virtual cell sizes (Δ) is set to 2s and 49s respectively. The figure shows very good approximation for $R(t)$ with $\Delta = 2s$ for $\dot{R}(t)$. Even for $\Delta = 49s$ the approximation is acceptable at time t=3600s. If $\Delta \geq 50s$ the expected number

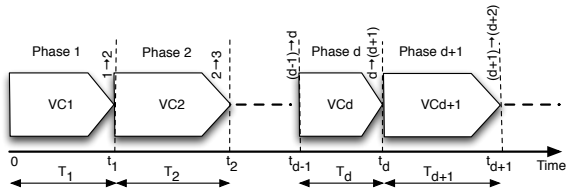

Figure 5. Projected route as a phased mission, where traversal of each virtual cell including handover to next cell is one phase.

of handovers for the dual homed session in the time interval $[i\Delta, (i+1)\Delta]$ is more than one given by the handover intensity in Table 1. From $\Delta \geq 50s$ the approximation does not hold. This implies that the model is insensitive to where the virtual cell boundaries are defined as long as handover probability is preserved. Maximum cell sizes are given by the handover intensity.

4. Phased mission

In our proposed model, handovers are only executed at the virtual cell boundaries. There exist several possible trajectories of a projected route for a dual homed session where the reliabilities of trajectories can be significantly different.

A session following a given trajectory can be considered as a phased mission, where each phase corresponds to the traversal of one virtual cell including handover to the next virtual cell if a handover takes place at the cell boundary. The phased mission is illustrated in Fig.5, where the change from phase d to $d+1$ takes place at t_d. The sojourn time of phase d is T_d. In the following a continuous time discrete space Markov model is used to model each of the phases a heterogeneous environment. In the next subsection, an approximation for optimization is derived.

4.1 Heterogeneous environment

In a phased mission system the parameters describing the various events, e.g. cell sojourn time and failure/repair rates differ between the phases. The reliability of each phase depends on the preceding phase's operational state and the time to spent in the phase. Each phase can be described as a continuous time discrete space Markov model with time independent parameters.

Without loosing generality we may index the virtual cells in the order they are visited from 1 to m, i.e. following the phases for the mission. Denote the set of all access points covering virtual cell d as b_d. A trajectory may be given as a serie of pair of access points to use in each virtual cell and can be written as $S_{ij} = \{(i_1, j_1), \ldots, (i_d, j_d), \ldots, (i_m, j_m)\}$ where $i_d \in b_d$ and $j_d \in b_d$ and $i_d \neq j_d$. In Fig.6 the state transition diagram for phase d of the trajectory S_{ij} is modelled. The diagram is based upon Fig.3 with some refinements that

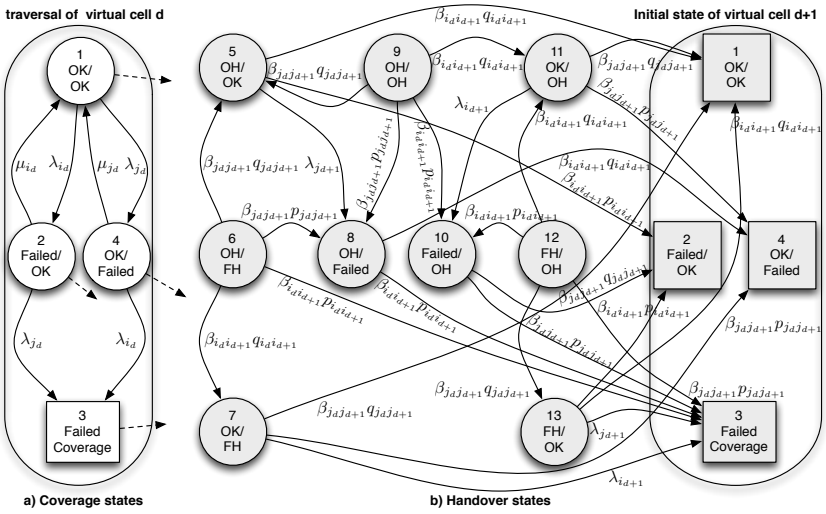

Figure 6. State transition diagram for phase d of S_{ij}. White coloured states represent the traversal of a virtual cell. The absorbing handover states represent the initial conditions for phase $d+1$. Transitions from coverage states to handover states are modelled as instantaneous transition of probability given S_{ij}.

will described in the following. The name of each state contains the status of each of the two connections in the dual homed session. In the figure the handover states $\ddot{\Omega}_H$ also include absorbing states. These are the initial states of phase $d+1$. An access point may cover several virtual cells. In each virtual cell the access point is modelled with different transition rates and parameters, e.g. like $\lambda_{id,d}$. To keep the notation simple, we will in the rest of the paper use the index i_d for dependability parameters and attributes for an access point i_d in a virtual cell d, i.e. $\lambda_{id,d} \rightarrow \lambda_{id}$.

In Fig.6 transition intensities and parameters have indexes. Single indexes represent an access point, e.g. λ_{i_d} represents coverage failure intensity for access point i_d for virtual cell d. Double indexes represent relations between two access points in different virtual cells, where e.g. $p_{i_d i_{d+1}}$ represents the handover failure probability from access point i_d to i_{d+1} and success is given by $q_{i_d i_{d+1}} = 1 - p_{i_d i_{d+1}}$. Transition intensities from the coverage states $\ddot{\Omega}_C$ to the handover states $\ddot{\Omega}_H$ is modelled as instantaneous transitions. The probabilities of the transitions are given the trajectory to follow. In the event of a coverage failure while executing handover, no recovery is modelled. This can be justified since the recovery time much longer than the duration of a handover.

The transition intensity matrix for Fig.6 is used to find the transient probabilities $\ddot{p}(T_{d_-})$ for virtual cell traversal with the initial condition $p(0) = \ddot{p}(t_{d-1_+})$.

For the first virtual cell $\ddot{p}(0) = [1,0,0,0,0,0,0,0,0,0,0,0,0,0]^T$.

$$\ddot{\Lambda}\ddot{p}(t) = \frac{d}{dt}\ddot{p}(t), \text{ where } \ddot{\Lambda} = \begin{bmatrix} \ddot{\Lambda}_{CC} & \ddot{\Lambda}_{HC} \\ 0 & \ddot{\Lambda}_{HH} \end{bmatrix} \tag{11}$$

For the trajectory S_{ij} the handover performed from virtual cell d to $d+1$ is given by elements $\{i_d, j_d\}$ and $\{i_{d+1}, j_{d+1}\}$. If $i_d = i_{d+1} \in b_d \bigcap b_{d+1}$ no handover takes place for connection i. Similar is defined for connection j. Define an indicator function representing the handover to perform between virtual cell d and $d+1$ as $I(t_d) = \{|i_d \cap i_{d+1}|, |j_d \cap j_{d+1}|\}$, i.e. $I(t_d) = \{1,1\}$ defines no handover.

By neglecting the handover time the transition probability matrix for handover is given

$$\ddot{\Pi}_H = -\ddot{\Lambda}_H/\ddot{q}_{xx} + I, \text{ where } \ddot{\Lambda}_H = \begin{bmatrix} 0 & \ddot{\Lambda}_{HC} \\ 0 & \ddot{\Lambda}_{HH} \end{bmatrix} \tag{12}$$

The transient state probabilities just after handover is $\ddot{p}(T_{d_+}) = (\ddot{\Pi}_H)^3 \ddot{p}(T_{d_-}|I(t_d))$ that becomes initial condition for phase $d+1$. Only 3 operations are necessary since there is no loops in the matrix and 3 is the largest path from an initial to an absorbing state. Given that just prior handover $\ddot{p}(T_{d_-}) = [\ddot{p}_1, \ddot{p}_2, \ddot{p}_3, \ddot{p}_4, 0,0,0,0,0,0,0,0,0,0]^T$ the instantaneous transition of probability from the coverage states to the handover states, as indicated in Fig.6 depends on the indicator function $I(t_d)$

$$\begin{aligned} &\dot{\ddot{p}}(T_{d_-}|I(t_d) = \{1,1\}) = \ddot{p}(T_{d_-}) \\ &\dot{\ddot{p}}(T_{d_-}|I(t_d) = \{0,1\}) = [0,0,\ddot{p}_3,0,\ddot{p}_1,0,0,\ddot{p}_4,...,0,0,\ddot{p}_2]^T \\ &\dot{\ddot{p}}(T_{d_-}|I(t_d) = \{1,0\}) = [0,0,\ddot{p}_3,0,0,0,\ddot{p}_4,0,0,\ddot{p}_2,\ddot{p}_1,0,0]^T \\ &\dot{\ddot{p}}(T_{d_-}|I(t_d) = \{0,0\}) = [0,0,\ddot{p}_3,0,0,\ddot{p}_4,0,0,\ddot{p}_1,0,0,\ddot{p}_2,0]^T \end{aligned} \tag{13}$$

where $\ddot{p}_1 = \ddot{p}_1(T_{d_-}), \ddot{p}_2 = \ddot{p}_2(T_{d_-}), \ddot{p}_3 = \ddot{p}_3(T_{d_-})$ and $\ddot{p}_4 = \ddot{p}_4(T_{d_-})$. For a dual homed session modelled as a mission with m phases, the reliability is given by the probability for being in the working states in the last phase, i.e., we have

$$\ddot{R}_{S_{ij}}(t_{m_+}) = \ddot{p}_1(T_{m_+}) + \ddot{p}_2(T_{m_+}) + \ddot{p}_4(T_{m_+}) = 1 - \ddot{p}_3(T_{m_+}) \tag{14}$$

4.2 Approximation of service continuity probability calculation

In Section 4.1 it was pointed out that the initial state of phase $d+1$ is obtained from the end state of phase d. The service reliability is given by the probability for being in the working states in the last phase. Here we will describe how to derive an approximation of the reliability where the initial state of a phase is only dependent on the actual handover from the previous phase. Such an approximation facilitates finding the optimal trajectory for the projected route.

A prerequisite for the commencement of phase d is that $T_{FF} > t_{d-1}$, i.e. phase $d-1$ has been successfully completed, therefore

$$\ddot{R}_{S_{ij}}(t_{d_+}) = \ddot{R}(t_{d-1_+})\ddot{R}(T_{d_+}|T_{FF} > t_{d-1}) \tag{15}$$

In obtaining $\ddot{R}(T_{d_+}|T_{FF} > t_{d-1})$ in (15) we use the state probabilities at the end of phase $d-1$ as described in Section 4.1. We want to find an approximation for these normalized probabilities without solving (11). Based on the generic solution of (11), it may be shown that the ratios between the probabilities of being in the working states approaches a limit, i.e., $\ddot{p}_4(t)/\ddot{p}_1(t) \to c_4$ and $\ddot{p}_2(t)/\ddot{p}_1(t) \to c_2$. We refer these as the stabilized ratios. If $\ddot{p}_4(T_{d-1_+})/\ddot{p}_1(T_{d-1_+}) \approx c_4$ and $\ddot{p}_2(T_{d-1_+})/\ddot{p}_1(T_{d-1_+}) \approx c_2$, we may approximately find the initial condition for phase d without finding the actual probabilities, but finding c_4 and c_2 instead.

Time needed to achieve the stabilized ratio is a measure of how fast the memory of the initial state decays. To find the time to achieve the stabilized ratio the eigenvalues $\gamma_1, \gamma_2, \gamma_3$ and γ_4 of the intensity matrix $\ddot{\Lambda}_{CC}$ are used. These are the four roots of

$$\det(\ddot{\Lambda}_{CC} - \Gamma) = 0 \tag{16}$$

where $\gamma_1 = 0$. To find the tree other roots a third degree polynomial has to be solved. The polynomial can be written as $\gamma^3 + a_2\gamma^2 + a_1\gamma + a_0 = 0$ where a_0, a_1 and a_2 are coefficients representing expressions of entries of $\ddot{\Lambda}_{CC}$. From the model we know that the eigenvalues are only real roots. One real root is significantly smaller (absolute value) than the two others when $\mu_{i_d}, \mu_{j_d} \gg \lambda_{i_d}, \lambda_{j_d}$. The two other eigenvalues represent the time constant of how fast the stabilized ratios are approached. To find an approximation of these two eigenvalues, we set root $\gamma_2 = 0$ and the third degree polynomial is factorized and reduced to $\gamma^2 + a_2\gamma + a_1 = 0$. Approximate values of γ_3 and γ_4 can be found to be $-\mu_{i_d}$ and $-\mu_{j_d}$. The interpretation of this is that the short term memory of the initial state decays with the time constant of the largest of $1/\mu_{i_d}$ and $1/\mu_{j_d}$. If the time spent in a virtual cell is more than the largest of $4/\mu_{i_d}$ and $4/\mu_{j_d}$ the ratios between the working probabilities are close to c_4 and c_2.

To find the stabilized ratio between the working states of $\ddot{\Omega}_{CC}$ we reduce the state space to $\ddot{\Omega}_{CC_-} = \{1, 2, 4\}$ where the transition towards state 3 is removed. The eigenvalues of this system can be found and approximated to $\{0, -\mu_{i_d}, -\mu_{j_d}\}$, i.e. same as for the $\ddot{\Omega}_{CC}$. For this reduced $\ddot{\Omega}_{CC_-}$ the node equations is used to get the stabilized ratios as $\ddot{p}_4(t) \approx \ddot{p}_1(t)\lambda_{j_d}/\mu_{j_d}$ and $\ddot{p}_2(t) \approx \ddot{p}_1(t)\lambda_{i_d}/\mu_{i_d}$, i.e., $c_4 \approx \lambda_{j_d}/\mu_{j_d}$ and $c_2 \approx \lambda_{i_d}/\mu_{i_d}$.

Now consider the trajectory S_{ij} with m phases. The approximated normalized transient probability vector just prior a handover is $\ddot{p}(T_{d_-}) = [\mu_{i_d}\mu_{j_d}, \lambda_{i_d}\mu_{j_d}, 0, \lambda_{j_d}\mu_{i_d}, 0, 0, 0, 0, 0, 0, 0, 0, 0]^T/(\mu_{i_d}\mu_{j_d} + \lambda_{i_d}\mu_{j_d} + \lambda_{j_d}\mu_{i_d})$. The approximated probability vector $\dot{\ddot{p}}(T_{d_+}|I(t_d))$ just after a handover that only dependent on the number of handovers to perform as given by (13) and we get

an approximation of the reliability as

$$\hat{R}_{S_{ij}}(t_{m_+}) = \ddot{R}_1\left(T_{1_+}\right) \prod_{n=2}^{m} \hat{R}_d\left(T_{n_+} | T_{FF} > t_{n-1}\right) \tag{17}$$

This approximation is very useful for finding the optimal trajectory since each of the phases can be derived with only knowledge of previous phase's dependability parameters.

5. Accuracy of approximation

We will address the approximation of $R_{S_{ij}}(t_{m_+})$ by $\hat{R}_{S_{ij}}(t_{m_+})$ and the implications of the found trajectory. A user will follow a projected route as depicted in Fig.1 with five virtual cells. Say that the best trajectory found is given by $S_{ij} = \{(B1, A1), (B2, A1), (B3, A1), (B4, A1), (B5, A1)\}$, and we have $I(t_d) = \{0, 1\}, d = 1, \ldots, 5$. Sojourn time in each virtual cell $T_d = 14$s.

Fig.7 shows $\ddot{R}_{S_{ij}}(t_{5_+}) - \hat{R}_{S_{ij}}(t_{5+})$ for different parameter sets, where the volumes of the bubbles are proportional to the difference. White bubbles indicate $\ddot{R}_{S_{ij}}(t_{5_+}) \geq \hat{R}_{S_{ij}}(t_{5_+})$ otherwise they are grey. For a parameter set, all virtual cells have the same parameter set. The ratios between the parameters between connection i and j are given by the axes. When the ratio is negative, connection i has reference value otherwise connection j has the reference value. The reference values are given in Table 1. In Fig.7 the maximum difference, i.e., the largest bubble, is $2.52 \cdot 10^{-5}$ for $\ddot{R}_{S_{ij}}(t_{5_+}) = 0.98952$ when $4/\mu_{i_d} > 14s$ or $4/\mu_{j_d} > 14s$. As long as the $4/\mu_{i_d} < 14s$ or $4/\mu_{j_d} < 14s$ the difference is in the range of $4.3 \cdot 10^{-6}$ or less. For $I(t_d) = \{0, 0\}$ and $I(t_d) = \{1, 1\}$ the same tendency can be found. This implies that the approximation of (14) provides good results as long as the time spent in a virtual cell is more than the four times than the largest of the expected recovery time.

6. Comparison of handover decisions

In this section comparison between the local hop-by-hop and global projected route based handover decisions is described.

A global route based handover decisions can use the approximation $\hat{R}_{S_{ij}}$ given in (17) to find a near-optimal trajectory. The model and approximation of $\hat{R}_{S_{ij}}$ has been implemented as an Integer Linear Programming (ILP) optimization. Details on the implementation will not be presented in this paper, but may be found in [FH13a]. Here some results will be given for providing some insights into the proposed model. Assume a local hop-by-hop handover decision that selects the combinations of access points that maximizes for surviving the immediate handover and the traversal of the next virtual cell, i.e., the reliability of traversal of virtual cell d is optimized given the access point selected in phase $d - 1$ as

$$\arg\max_{i_d j_d} \hat{R}_d(T_{d_+} | T_{FF} > t_{d-1}, i_{d-1}, j_{d-1}) \tag{18}$$

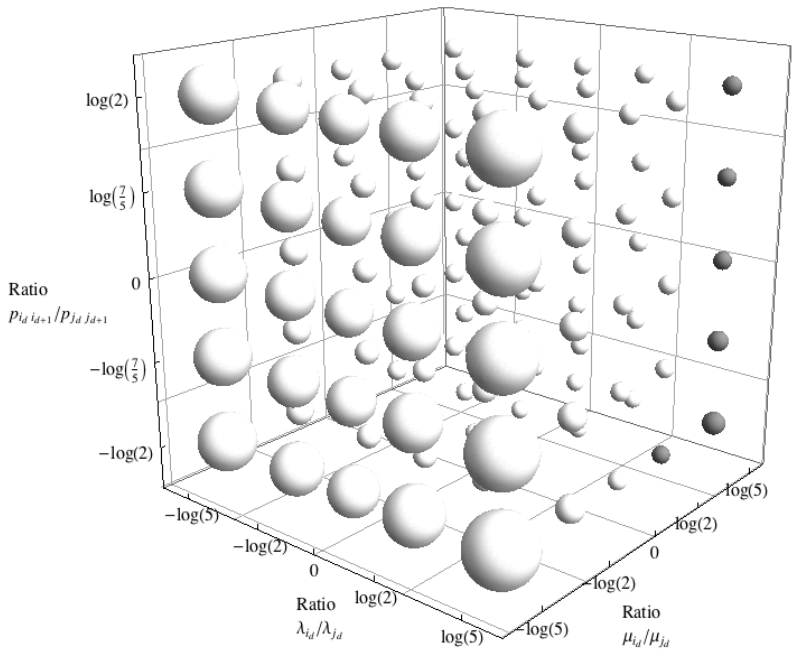

Figure 7. Difference between the approximation of $\ddot{R}_{S_{ij}}(t_{5_+})$ by $\hat{R}_{S_{ij}}(t_{5_+})$ for different parameter sets. Volumes of the bubbles are proportional to the value of $\ddot{R}_{S_{ij}}(t_{5_+}) - \hat{R}_{S_{ij}}(t_{5_+})$. White bubbles indicate $\ddot{R}_{S_{ij}}(t_{5_+}) \geq \hat{R}_{S_{ij}}(t_{5_+})$. The ratios between the parameters between connection i and j are given by the axes. When the ratio is negative, connection i has reference value otherwise connection j has the reference value according to Table 1.

where $\hat{R}_1(T_{1_+}|T_{FF} > t_0, i_0, j_0) = R_1(T_{1_+})$. Each possible combination of (i_d, j_d) given (i_{d-1}, j_{d-1}) is calculated in the same way as for phase d in (17).

To compare the reliability of the trajectories found by ILP and local hop-by-hop optimizations different scenario-instances are created. The basics for all scenario-instances are four access network operators and 15 virtual cells with i.i.d. $T_d \sim$ uniform $[20, 30]$, see Table 2. Operator A and C have coverage in all virtual cells whereas B and D cover 6 successive virtual cells each where the first virtual cell is randomly selected. A network operator has at most one access point covering any virtual cell, though one access point may cover several successive virtual cells. Define b_d^A, b_d^B, b_d^C and b_d^D as the access points for the respectively operators for virtual cell d and we have $b_d = b_d^A \bigcup b_d^B \bigcup b_d^C \bigcup b_d^D$ where $|\bigcup_{d=1}^{15} b_d^A| \sim$uniform$[5, 8]$, $|\bigcup_{d=1}^{15} b_d^B| = 3$, $|\bigcup_{d=1}^{15} b_d^C| = 2$ and $|\bigcup_{d=1}^{15} b_d^D| \sim$uniform$[3, 6]$. For instance, operator D has from 3 to 6 access points for a given scenario-instance where one access point may

Table 2. Dependability parameters for scenario-instances

	Parameters	Values			
		$i_{d+1} \in b^A_{d+1}$	$i_{d+1} \in b^B_{d+1}$	$i_{d+1} \in b^C_{d+1}$	$i_{d+1} \in b^D_{d+1}$
	$\lambda_{i_{d+1}}$	$U[1/998, 2/998]$	$U[2/998, 5/998]$	$U[1/998, 3/998]$	$U[1/998, 2/998]$
	$\mu_{i_{d+1}}$	$U[1/4, 1/2]$	$U[1/4, 1/2]$	$U[1/4, 1/2]$	$U[1/4, 1/2]$
$i_d \in b^A_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.02]$	$U[0.01, 0.04]$	$U[0.01, 0.03]$	$U[0.01, 0.04]$
	$\beta_{i_d i_{d+1}}$	$U[4, 8]$	$U[2, 4]$	$U[4, 8]$	$U[2, 4]$
$i_d \in b^B_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.04]$	$U[0.01, 0.03]$	$U[0.01, 0.04]$	$U[0.01, 0.05]$
	$\beta_{i_d i_{d+1}}$	$U[3, 6]$	$U[4, 8]$	$U[3, 6]$	$U[3, 6]$
$i_d \in b^C_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.03]$	$U[0.01, 0.04]$	$U[0.01, 0.04]$	$U[0.01, 0.04]$
	$\beta_{i_d i_{d+1}}$	$U[2, 4]$	$U[4, 8]$	$U[4, 8]$	$U[2, 4]$
$i_d \in b^D_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.04]$	$U[0.01, 0.02]$	$U[0.01, 0.02]$	$U[0.01, 0.03]$
	$\beta_{i_d i_{d+1}}$	$U[3, 6]$	$U[3, 6]$	$U[2, 4]$	$U[4, 8]$

provide coverage for one or two virtual cells. A total of 100 scenario-instances are created with the dependability parameters as defined in Table 2, where all parameters have identical independent uniform distributions. Note that handover parameters $p_{i_{d-1}i_d}$ and $\beta_{i_{d-1}i_d}$ is only valid when $i_{d-1} \neq i_d$ otherwise $p_{i_{d-1}i_d} = 0$ and $\beta_{i_{d-1}i_d} = 0$.

In Fig.8 the difference between $\hat{R}_{S_{ij}}(t_{m_+})$ found by ILP optimization and $\hat{R}_{S_{xy}}(t_{m_+})$ found by local hop-by-hop optimization is shown. The scenario-instances are ordered according to the differences from smallest to largest. As can be observed the ILP optimization provides the trajectory with the highest reliability for all scenario-instances. In the figure the absolute value of $\hat{R}_{S_{ij}}(t_{m_+})$ for each scenario-instance is also shown. This shows relative large variations between the reliability of trajectories found for the different scenario-instances. The correlation coefficient between $\hat{R}_{S_{ij}}(t_{m_+}) - \hat{R}_{S_{xy}}(t_{m_+})$ and $\hat{R}_{S_{ij}}(t_{m_+})$ for the scenario-instances is -0.239 indicating a weak correlation. For all the scenario-instances the difference between $R_{S_{ij}}(t_{m_+})$ and the approximation $\hat{R}_{S_{ij}}(t_{m_+})$ is in the range $7.0 \cdot 10^{-6}$ or less, where $R_{S_{ij}}(t_{m_+}) > \hat{R}_{S_{ij}}(t_{m_+})$.

7. Conclusion

In this paper we have proposed a reliability model of a trajectory defined as the series of access points used in the virtual cells for a dual homed session. Central in the model is the concept of virtual cells defined on basis on the measurement reports and signalling from networks. We have shown that the model is insensitive to where the virtual cell boundaries are defined as long as handover probabilities are preserved. The proposed model is suited for optimization where the trajectory with highest reliability is basis for handover decision. The potential with such a global route based handover decision is

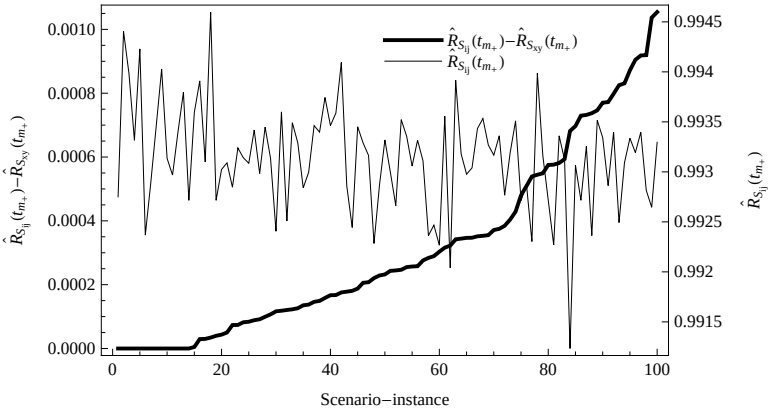

Figure 8. Difference between $\hat{R}_{S_{ij}}(t_{m_+})$ found by ILP optimization and $\hat{R}_{S_{xy}}(t_{m_+})$ found by local hop-by-hop optimization. The scenario-instances are ordered according to the differences from smallest to largest. The ILP optimization provides the trajectory with the highest reliability for all scenario-instances. The absolute value of $\hat{R}_{S_{ij}}(t_{m_+})$ for each instance is also shown.

provided with a comparison with a local hop-by-hop handover decision strategy.

References

[ASS03] I. Aydin, W. Seok, and C. C. Shen. Cellular SCTP: a transport-layer approach to Internet mobility. In *Proc. 12th International Conference on Computer Communications and Networks ICCCN 2003*, pages 285–290, Dallas,USA, October 20–22 2003.

[CIRG09] C. Christakos, A. Izquierdo, R. Rouil, and N. Golmie. Using the media independent information service to support mobile authentication in fast mobile IPv6. In *IEEE Wireless Communications and Networking Conference WCNC 2009*, pages 1–6, Budapest, Hungary, April 2009.

[DDF+07] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardo, R. Lopez, T. Kodama, and H. Schulzrinne. Seamless proactive handover across heterogeneous access networks. *Wireless Personal Communications*, 43(3):837–855, June 28, 2007.

[EN09] M. B. E. Nordmark. Shim6: Level 3 multihoming shim protocol for IPv6. IETF network working group, 2009.

[FH09] E. L. Følstad and B. E. Helvik. Managing availability in wireless inter domain access. In *Proc. International Conference on Ultra Modern Telecommunications Workshops ICUMT '09*, pages 1–6, October 12–14 2009.

[FH13a] E. L. Følstad and B. E. Helvik. Optimizing service continuity in a multi operator multi technology wireless environment. In *Proc. 9th International Conference on the Design of Reliable Communication Networks DRCN 2013*, pages 111–118, Budapest, Hungary, March 4–7 2013.

[FL09] A. Freedman and M. Levin. Virtual drive test: an in-situ method for network measurements and optimization. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, IWCMC '09, pages 1433–1437, New York, NY, USA, June 21–24 2009. ACM.

[GJ03] E. Gustafsson and A. Jonsson. Always best connected. *IEEE Wireless Communications*, 10(1):49–55, February 2003.

[IEE08] IEEE 802.21,D11; Draft standard for local and metropolitan area networks: Media indepenedent handover services, 2008.

[NFS+09] P. Neves, F. Fontes, S. Sargento, M. Melo, and K. Pentikousis. Enhanced media independent handover framework. In *Proc. 69th IEEE Vehicular Technology Conference VTC Spring 2009*, pages 1–5, Barcelona, Spain, April 26–29 2009. IEEE.

[PJA10] C. Perkins, D. Johnson, and J. Arkko. Mobility support in IPv6. IETF mobile IP working group Internet-draft obsoletes: 3775 (if approved), 2010.

[SXM+00] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. RFC2960: Stream control transmission protocol, 2000.

[YSN10] X. Yan, Y. A. Sekercioglu, and S. Narayanan. A survey of vertical handover decision algorithms in fourth generation heterogeneous wireless networks. *Computer Networks*, 54(11):1848–1863, 2010.

PAPER F

The cost for meeting SLA requirements; implications for customers and providers

Eirik Larsen Følstad and Bjarne E. Helvik

Reliability Engineering & System Safety

vol. 145, pp. 136-146, January 2016

THE COST FOR MEETING SLA REQUIREMENTS; IMPLICATIONS FOR CUSTOMERS AND PROVIDERS

Eirik Larsen Følstad, Bjarne E. Helvik
Department of Telematics, Norwegian University of Science and Technology (NTNU)
O.S. Bragstads plass 2B,
Trondheim, Norway
{eirik.folstad, bjarne}@q2s.ntnu.no

Abstract A Service Level Agreement (SLA) describes the service, the Service Level Objectives (SLOs), the price the customer should pay and the compensation if the SLOs are not met. There is a trade-off for the provider between the costs for improving the deployed service quality vs. probability of paying compensation. We propose how to estimate the provider's optimal service deployment. We show that the optimal deployed service quality is dependent on the SLOs, deployment cost, compensation and observation interval. A service deployment based on cost optimization results in targeted dependability objectives values that are significantly better than stated in the SLOs. The proposed approach provides valuable insight for an aggregator, who buys services from other providers, to negotiate adequate SLOs, price and compensation from the providers to make a valuable offer for its own customers.

Keywords: Service Level Agreement, Dependability, Service deployment, Optimization, Evaluation

1. Introduction

Our society is dependent on critical infrastructures where failure free operations are of utmost importance. Examples of critical infrastructures are telecommunications, water supply systems, electrical power systems and banking and finance. Typical for providers of critical infrastructures is that they are part of compound service deliveries, where each of the parties is commercially and technically autonomous. The interdependencies between such parties are discussed in several papers, see e.g. [BBC+10, MZB+13, YGB14, Ouy14, NSG15].

It is important to control the service dependability through the delivery chain of several autonomous parties with legally binding agreements. The delivery of the services between parties and the related economic transactions may be regulated through SLAs, see for instance [E-806, Har05, WB10, TBvdZ04]. SLAs for controlling the service dependability have been used in telecommuni-

cations and cloud computing, but little in conjunction with compound service deliveries provided by several critical systems and parties.

One aspect in an SLA is the specification of the quality of the service that shall be delivered. This is commonly specified as values of service-level objectives (SLOs). In setting up the SLAs, a fact that is paid surprisingly little attention, is that there are few failures during the typical observation interval for the SLOs, e.g., one year. Hence, due to the stochastic fluctuations of the failure and repair processes, what is observed may deviate significantly from the values representing the asymptotic average behavior of the service. The probability of not meeting the availability SLO requirement during a finite observation interval was first dealt with by Goyal and Tantawi [GT88].

This paper investigates the relation between the dependability related SLOs, and the asymptotic values of these a service must be designed for. The objective is to provide insight that enables SLAs to be means for a cost quality trade-off beneficial to all parties that may be agreed upon. For the provider, it is a trade-off between the risk of paying compensation to the customer for not meeting the SLOs, and the investment in equipment and operations to improve the service dependability. For the service customer, it is a matter if risk sharing, where the consequences he will experience if the provider does not meet the agreed SLO are compensated by the provider with a penalty stated in the SLA. Dependent on the kind of application or type of infrastructure this compensation may be significant. Since a number of interwoven techno-economic relations are sought captured by a few SLOs, there are a number of pitfalls, and the use of SLAs may turn out to be counterproductive [SBM09, TT05].

From the following items in the SLA: (i) the observation interval, (ii) the number of acceptable failures, (iii) the maximum number of down times that may exceed a threshold, (iv) the accumulated down time, (v) the non-compliance compensation paid to the customer, and generic models proving a certain failure intensity and a tightly controlled repair handling time, a parameterization of a semi-Markov on-off model for the service provision is deduced. The on state defines when the service is delivered according to the temporal performance SLOs (in terms of provided functionality, response times, etc.) and off otherwise. This forms a basis for an understanding of how the SLOs and the cost parameters impact the actual service delivered as well as the economy of the service provision.

Most other quantitative analysis related to the dependability aspects of SLAs concentrate on the service availability. Specifying SLOs for the actual services having control with the failure intensity and down time duration may be just as important and is a salient aspect of this study.

Some work take into account that providers need to over-dimension, i.e. have a safety margin, in the service provision relative to what is specified in the dependability SLOs, to ensure good earnings on a service with penalties. The safety margin is addressed in [ZG05, MC08, GH10, SWG10] with relation to the known asymptotic unavailability and how the safety margin for the

provider is depended on the duration of the observation interval. Both [GH10] and [SWG10] pinpoint how the safety margin is sensitive to the tail of the repair process. A methodology is presented in [Sch11] to set the unavailability safety margin according to the tolerated customer compensation for a given observation interval. In [Fra12] a framework is proposed for modeling the optimal investment for availability for a two state semi-Markov modelled system where the customer compensation is depending on the down time duration and its variance. A similar trade-off is formalized as an optimization problem in [LHD13] with the objective to minimize the total cost of system improvements and compensations. A two-state Markov model is analyzed in [MN11a] where an upper bound for an insurance premium is calculated based upon the dependability related SLOs number of failures, cumulative down time duration and number of down times longer than a defined threshold. In our work we identify the optimal safety margin with respect to the same dependability SLOs as in [MN11a] for an observation interval, investments and operational procedures and customer compensation. We propose to model investments and operational procedures to change the behavior of the failure and repair processes.

With detailed information of a system numerical methods may be used for dependability analysis for the modelled system with a finite set of states, see e.g. [RT88, RS95]. However, such detailed information and models causes the computing effort to be too demanding for studying the aspects in this paper.

An additional issue not included in this paper is how to manage the system to meet the SLOs for the offered service. Some discussions regarding SLA management may be found in e.g. [BSC01, BHK$^+$04, LHD13, GH12b].

The rest of the paper is organized as follows. In Section 2 we present the on-off model in more detail. Section 3 deals with the SLA, its items (i)-(v) listed above and the generic cost models. In Section 4 the probability of violating the SLOs is derived. Based on this, Section 5 describes how a provider may operate the system so it maximizes his profit for the service. Section 6 describes how aggregated on-off models may be used to deal with compound service delivery systems. In Section 7 we present some case scenarios and discuss the influence of SLO items (i)-(v) on the inherent/asymptotic behavior of the service provision and vice versa. Section 8 concludes the paper.

2. The on-off model

The behavior of the system is modelled by an on-off semi-Markov model. This is of course a gross simplification relative to the behavior of the real system, but is the most complicated model we may build based on the three dependability related SLOs, i.e., items (ii) to (iv) as introduced in Section 1 for a given observation interval. For more detailed models, more information has to be included in the SLA combined with in depth knowledge of the provider's system and operational procedures. Note that often just one dependability related SLO is found in SLAs for cloud and communication services, typically

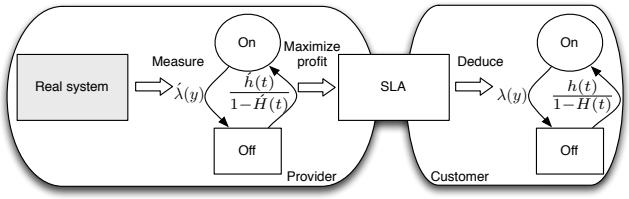

Figure 1. A two state semi-Markov model deduced from the SLA offering from a provider.

the availability, see e.g. [Ama13, Mic13, Nex13, Cen13, Ver13], but here we favor additional dependability related SLOs to better describe the system requirements.

For the on-off semi-Markov model the system alters between the two states described by a failure process and a repair process. The failure process describes the event where the service delivered drops below the satisfactory performance level. Similarly, the repair process describes the event that combinations of fault handling mechanisms and operational procedures have restored the service to a satisfactory performance level. The performances SLOs define the satisfactory service delivery.

Since the failure process is an aggregate of many underlying failures, e.g. originating from hardware and software in the sub systems, causing a non satisfactory service delivery, we assume that it is a non-homogeneous Poisson process (NHPP), cf. Palm-Khintchine's theorem, with an intensity $\lambda(y)$ where y is the calendar time. The NHPP is a generalization of a homogeneous Poisson process (HPP), which enables us to model seasonal, weekly and daily variations in the failure intensity, as well as trend and change due to change in load or operational conditions. The expected number of failures in an observation interval τ is $\Lambda(\tau) = \int_0^\tau \lambda(y)dy$ and the number of failures observed $N(\tau)$ is Poisson distributed

$$P(N(\tau) = n) = \Lambda(\tau)^n/n! \cdot e^{-\Lambda(\tau)} \tag{1}$$

The repair process is assumed to be any arbitrary process with independent and identically distributed restoration times, D with probability density function (PDF) $h(t)$ and cumulative distribution function (CDF) $H(t)$. This model of the failure and repair processes defines a semi-Markov process. Fig. 1 illustrates how to deduce a two state model from the SLOs in the SLA between a provider and a customer. Inherent parameters in the system are denoted $\hat{x}$, while the estimated are, to keep the notation simple, untagged.

As described earlier in this section we have proposed to use three dependability related SLOs where one of them is related to failure intensity. With three dependability related SLOs we can therefore at most describe the repair time distribution with two parameters. In the rest of the paper we

have used the gamma distribution with shape parameter α and scale parameter β, i.e., $H(t) = \Gamma(\alpha, t/\beta)/\Gamma(\alpha)$ where $\Gamma(\alpha) = \int_0^\infty e^{-x}x^{\alpha-1}dx$ and $\Gamma(\alpha, t/\beta) = \int_{t/\beta}^\infty e^{-x}x^{\alpha-1}dx$. The expected down time is $E[D] = \alpha\beta$ and its coefficient of variation $\sqrt{Var[D]}/E[D] = 1/\sqrt{\alpha}$. Note that if an alternative model for the repair process with two adjustable parameters is available, e.g. based on operational data from a provider, the gamma distribution may be replaced by this, likely at the cost of an increased computational complexity.

Denote the accumulated time spent in the off state during the observation interval τ by $\Omega(\tau)$. In an on-off model, the number of failures $N(\tau)$ and $\Omega(\tau)$ will not be independent. However, in the context of highly dependable systems where the accumulated time spent in the off state is very short compared to the observation interval τ, independence is a good approximation. Hence, when

$$\lambda(y) \ll 1/E[D], \forall y \in [0, \tau] \tag{2}$$

holds, we assume that

$$P(\Omega(\tau) \leq \omega, N(\tau) = n) \approx P(N(\tau) = n) \cdot H^{\otimes n}(\omega) \tag{3}$$

where $P(N(\tau) = n)$ is given in (1) and $H^{\otimes x}(t)$ is the CDF of an n-fold convolution of the down time duration. This may in general be derived with the recursion $H^{\otimes x}(t) = \int_0^\infty H^{\otimes(x-1)}(t-y)h(y)dy$. A validation of this approximation relative to the exact joint distribution is given in Appendix A.

3. The SLA and the provider's cost model

In a rational market with competition, a provider has to deliver services that are competitive and attractive with respect to quality and price. The SLA formalizes the service to be delivered, price and compensation, and should reflect the deployed service quality such that the (estimated) business for the provider in the long run is attractive for its stakeholders.

3.1 Dependability related service-level objectives

The SLOs defined in an SLA must be measurable over a finite period. In SLAs and in most research, the contracted unavailability (or availability) has been the most dominant dependability related SLO. In contrast to this, the service requirements and SLOs are most likely different for different usage of the service. For some customers the mean time between failures may be the most important dependability attribute, while for others restrictions on long outage times might be the most critical requirement.

Fig. 2, adapted from [E-806], shows parts of an SLA that provides relevant information referred in this paper. Besides the commercial parts, the criteria for satisfactory service are defined. These criteria should describe the performance requirements for the service as well as the usage limitations the customer must comply with. The dependability SLOs define the agreed deviations for the

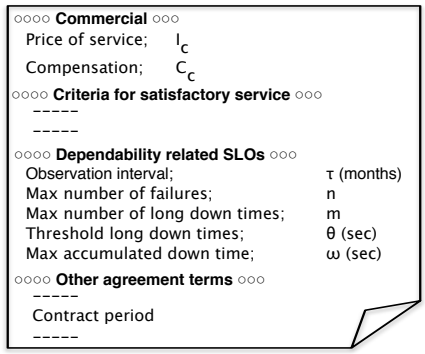

Figure 2. Example of parts of SLA content adapted from [E-806].

service delivery. The dependability SLOs are independent of the underlying failure and repair processes, and do not require a stationary failure process.

Note that there is a distinct difference between the SLA contract period and the observation interval. The contract period defines the legal commitment of the validity period of the SLA, whereas the observation interval is the agreed time interval(s), during which the dependability SLOs are calculated. Within a contract period there may exist several observation intervals. In this paper the same observation interval is used for all the dependability SLOs.

We denote the number of failures during the observation interval, τ, by $N(\tau)$, the number of down times during the interval that exceeds θ by $M(\tau)$, and accumulated down time during the interval by $\Omega(\tau)$. These are dependent stochastic variables. The dependability related SLOs for the finite observation interval τ are then;

- $N(\tau) \leq n$; maximum number of failures.
- $M(\tau) \leq m_\theta$; maximum number of down times longer than the threshold θ. In the rest of the paper we will use m for m_θ since m is always related to a threshold defined by θ.
- $\Omega(\tau) \leq \omega$; maximum accumulated down time.

Fig. 3 illustrates relations between some dependability related SLOs. During the observation interval τ, we will get an average time between failures $\tau/N(\tau)$ and an average down time $\Omega(\tau)/N(\tau)$, which represents a point in the plane. The bold dashed line represents the maximum number of failure objective τ/n. The availability objective is represented by the straight bold line representing the inverse of the observed unavailability, i.e., τ/ω. The vertical dashed lines represent requirements for maximum average down times, not discussed further in this paper, and the dash-dot curve is a projection of a limitation of a restriction on the number of long down times for a given m, θ and τ. To

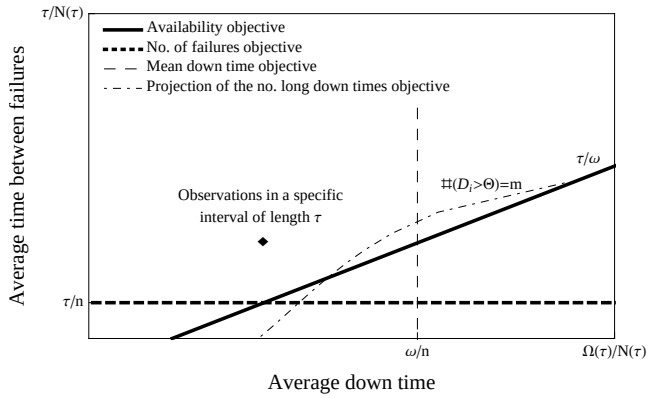

Figure 3. Illustration of dependability related SLOs.

comply with the SLOs, the point representing the observations of the system must be above and to the left of the curves representing the objectives. The optimum service deployment point will most likely be in this region, sufficiently away from the constraints represented by the objectives, to accommodate the stochastic fluctuations of the failure and repair processes for the agreed observation interval. This optimum service deployment point will be further investigated and discussed in the following sections.

3.2 Provider's cost model

To be able to offer services the provider has to use capital expenditures and operational expenses for hardware/software, implementation, maintenance etc. For simplicity, we denote these costs as deployment cost. The inherent quality in the system is dependent on the deployment cost, and increasing the quality implies increased deployment cost. Given the inherent system quality, the provider has to offer services that comply with SLOs in the SLA. If the SLOs are not fulfilled over the observation interval, the provider has to pay a compensation C_c to the customer. Here, the compensation is modelled as a fixed amount irrespective of which SLO that is violated and the severeness of the violation. We consider this as representative for commercial services, although some service providers use different compensation schemes. For instance the cloud service providers Amazon [Ama13] and Microsoft [Mic13] do only compensate for availability violations. The network communication providers Nextgen [Nex13] and CenturyLink [Cen13] have guarantees for both availability and repair times, but do only compensate for availability violations. Verizon [Ver13] guarantees 100% availability for some Internet access services and compensates violation of repair times in addition

to the availability violation. CenturyLink and Verizon also compensate for packets performance violations such as jitter and delay. For specific cases, (4) below may be modified to adopt to these.

In the following let $\hat{S}$ denote the contracted service quality, i.e., what is stated in the SLA with the values n, m and ω and S the properties of the deployed service, i.e., estimated with the parameters $\Lambda(\tau)$, α and β. A provider's profit $R(\hat{S}|S)$ may be viewed as

$$\begin{aligned} R(\hat{S}|S) &= I_{c|\hat{S}}(\tau) - C_{d|S} - C_{c|\hat{S}} P_{\hat{S}|S}(\tau) \\ &= I_{c|n,m,\omega}(\tau) - C_{d|\Lambda(\tau),\alpha,\beta} - C_{c|n,m,\omega} P_{n,m,\omega|\Lambda(\tau),\alpha,\beta}(\tau) \end{aligned} \tag{4}$$

where $C_{d|S}$ is the deployment cost, $I_{c|\hat{S}}(\tau)$ is the selling price for the service, i.e., the provider's income, and $P_{\hat{S}|S}(\tau) = P_{n,m,\omega|\Lambda(\tau),\alpha,\beta}(\tau)$ is the probability of violating the SLOs. The probability of violating the SLOs will be further explained in Section 4.

The compensation cost can be reduced at the expense of the deployment cost that affects the deployed service quality S. For the provider there is an optimum profitable service deployment where the sum of deployment and compensation costs are minimized. The estimation of the optimal deployment, described by the failure and repair processes, will be derived in the following.

4. Probability of violating service-level objectives

The provider's probability of payment of compensation is linked to the probability of violating the SLOs as defined in Section 3.1. The probability of breaching one or several of the SLOs by the provider can be expressed as

$$\begin{aligned} P_{n,m,\omega|\Lambda(\tau),\alpha,\beta}(\tau) &= P[N(\tau) > n \cup M(\tau) > m \cup \Omega(\tau) > \omega] \\ &= P[N(\tau) > n] + P[M(\tau) > m \cap N(\tau) \leq n] \\ &+ P[\Omega(\tau) > \omega \cap N(\tau) \leq n \cap M(\tau) \leq m] \end{aligned} \tag{5}$$

The probability $P_{n,m,\omega|\Lambda(\tau),\alpha,\beta}(\tau)$ separates into three disjoint sets of events. Each of these disjoint events will be derived in the following.

4.1 Maximum number of failures

Having defined the semi-Markov process, cf. Fig. 1, the number of failures during an observation interval is equal to the on/off transitions. Assuming that the down times may be negligible with respect to the up times, the probability of violating the number of failure occurrences during the observation interval may be expressed as

$$P[N(\tau) > n] = 1 - \sum_{i=0}^{n} \frac{\Lambda(\tau)^i}{i!} e^{-\Lambda(\tau)} \tag{6}$$

where $\Lambda(\tau)$ is the expected number of failures during the observation interval τ.

4.2 Maximum number of long down times

The repair process is modelled as any arbitrary process with independent and identically distributed restoration times as described in Section 2. In an environment with highly dependable systems the provider's probability of violating the maximum number of long down times may be expressed with independent Bernoulli variables yielding the approximation

$$\begin{aligned} & P[M(\tau) > m \cap N(\tau) \leq n] \\ & = \sum_{i=0}^{n} P[M(\tau) > m | N(\tau) = i] P[N(\tau) = i] \\ & = \sum_{i=m+1}^{n} \frac{(\Lambda(\tau))^i}{i!} e^{-\Lambda(\tau)} \left(1 - \sum_{j=0}^{m} \binom{i}{j} (1 - H(\theta)^j H(\theta)^{i-j}) \right) \end{aligned} \tag{7}$$

where $H(\theta)$ is the estimated probability of a down time duration less or equal to the threshold θ. In (7) the probability of the number of failures that may violate the maximum number of long times are from $m+1$ to n since (6) already has counted for violating the number of failures. Last summation of (7) expresses the probability of the combinations of down times for the given number of failures that do not violate the maximum number of long down times.

4.3 Maximum accumulated down time

Takacs [Tak57] derived the probability of violating the accumulated down time $P[\Omega(\tau) \leq t]$ for a two state system with $\hat{G}(t)$ and $H(t)$ as the CDFs of times between failures and duration of down times respectively as

$$P[\Omega(\tau) \leq \omega] = \sum_{n=0}^{\infty} H^{\otimes n}(\omega) [\hat{G}^{\otimes n}(\tau - \omega) - \hat{G}^{\otimes n+1}(\tau - \omega)] \tag{8}$$

where $\otimes$ is the convolution operator and $H^{\otimes x}(t)$ is the x-fold convolution of a given CDF of the distribution of the down times. In the case by Takacs the failure process $\hat{G}(t)$ is homogeneous. In our case, the estimated failure process is non-homogeneous where $G(t) = 1 - e^{-\Lambda(t)}$. Further more, closed form solutions exist only when $H(t)$ is negative exponential or deterministic. Hence, an approximation is needed.

As motivated at the end of Section 2 and validated in Appendix A, we may use (3) to get the following approximation for highly dependable systems

$$P[\Omega(\tau) \leq \omega] \approx \sum_{n=0}^{\infty} H^{\otimes n}(\omega) P[N(\tau) = n] \tag{9}$$

The conditional probability that the provider violates the maximum accumulated down time becomes

$$
\begin{aligned}
&P[\Omega(\tau) > \omega \cap N(\tau) \leq n \cap M(\tau) \leq m] \\
&= \sum_{i=0}^{n} \sum_{j=0}^{Min[i,m]} P[\Omega(\tau) > \omega | M(\tau) \leq j \cap N(\tau) \leq i] \\
&\cdot P[M(\tau) \leq j | N(\tau) = i] P[N(\tau) = i] \\
&= \int_{\omega}^{\infty} \Big[\sum_{i=0}^{n} \frac{(\Lambda(\tau))^i}{i!} e^{-\Lambda(\tau)} \sum_{j=0}^{Min[i,m]} \binom{i}{j} (1 - H(\theta))^j H(\theta)^{i-j} \\
&\cdot h^{\otimes j}(t|t > \theta) \otimes h^{\otimes (i-j)}(t|t \leq \theta) \Big] dt
\end{aligned} \tag{10}
$$

where $h^{\otimes n}(t)$ is the n-fold convolution of the estimated PDF of duration of down times. The first summation in (10) expresses the probability of the number of failures that may contribute to violating the accumulated down time, yielding a maximum of n failures, since (6) already has counted for violating the number of failures. Only the probabilities of combinations of down times that do not violate the maximum number of long down times are included, given by the second summation in (10) going from 0 to the minimum of i and m, since (7) counts for violating the number of long down times.

The convolutions of mixtures of right-truncated $h(t|t > \theta)$ and left-truncated $h(t|t \leq \theta)$ distributions of down times are numerically obtained by discretization and using the discrete Fourier transform. For efficiency, the summation in (10) is performed in the Fourier (frequency) domain. The accuracy obtained is validated. Note that this approach is flexible, as it allows us to use arbitrary $H(t)$ in the model.

Inserting (6), (7) and (10) into (5) yields the probability $P_{n,m,\omega|\Lambda(\tau),\alpha,\beta}(\tau)$ of not complying with the SLOs.

5. Optimizing providers profit

To maximize (4), i.e., the providers profit, we need a relation between the deployment cost $C_{d|S}$ and the asymptotic service quality S. To illustrate, to get insights and to obtain indicative results, we introduce a generic relationship, that captures the salient factors, but which is not claimed to be exact. In cases where specific design, configuration and/or operation options are available, the generic relations may be replaced by these and a corresponding (integer) optimization performed.

The deployment cost consists of two parts, one related to the asymptotic unavailability, $C_{du|S}$, of the service and one part related to the coefficient of variation of the duration of down times, $C_{dcv|S}$. This yields the deployment cost $C_{d|S} = C_{du|S} + C_{dcv|S}$.

The profit given by (4) may be refined with the probability of violating the SLOs given by (5) and the cost models to estimate the optimal deployment as

$$R_{n,m,\omega|\lambda,\alpha,\beta}(\tau) = I_{c|n,m,\omega}(\tau) - \underset{\lambda,\alpha,\beta}{\arg\min}\left(C_{du|\lambda,\alpha,\beta} + C_{dcv|\alpha,\beta} + C_{c|n,m,\omega}P_{n,m,\omega|\lambda,\alpha,\beta}(\tau)\right) \tag{11}$$

where we, to keep the illustration simple, use an HPP for the failure process, i.e., $\lambda(y) = \lambda$, $y \in [0, \tau]$.

To establish an aggregated cost vs. availability model, we introduce a reference unavailability U_0 and a degree of replication δ. In simple single element systems, duplication corresponds to $\delta = 2$, triplication to $\delta = 3$, etc. The obtained unavailability U is then modelled as $U = U_0^{\delta}$, which yields

$$\delta = \frac{\ln U}{\ln U_0} \approx \frac{\ln(\lambda E[D])}{\ln U_0} \tag{12}$$

The deployment cost typically increases slightly faster than δ, say δ^{ν}, since spare routes etc. tend to be more costly than the primary, i.e., ν is close to, but a little larger than 1. For instance, Telenor [Tel14a] offers a spare route at a higher price than the primary while Amazon [Ama13] offers virtual computing instances at the same price, but if two instances are in different availability zones an additional cost is introduced for data transfer between the independent zones. Hence, a simple aggregated relation between asymptotic unavailability cost and model parameters becomes

$$\begin{aligned} C_{du|\lambda,\alpha,\beta} &= \left(\frac{-\ln U}{-\ln U_0}\right)^{\nu} C_0 \\ &= \Big(-\ln(U)\Big)^{\nu} C_{du0} \approx \Big(-\ln(\lambda\alpha\beta)\Big)^{\nu} C_{du0} \end{aligned} \tag{13}$$

where C_{du0} is the reference deployment cost for the reference unavailability U_0.

If the provider wants to reduce the variance of the duration of down times, more money has to be put in deployment and operations. The variance of the duration of the down times expresses the providers' knowledge, preparations and processes for keeping the duration of the down times within certain limits, as well as the deployed systems' mechanisms for failure corrections. To model the aggregated cost vs. variance of the duration of down times we introduce the reference cost C_{dcv0} for a reference coefficient of down time durations and a degree of reduction η. The deployment cost increases with reduced variation, and deployment cost for reducing the coefficient of variation of the service interruption may be modelled as

$$C_{dcv|\alpha,\beta} = C_{dcv0}\left(\frac{E[D]}{\sqrt{Var[D]}}\right)^{\eta} = C_{dcv0}\alpha^{\frac{\eta}{2}} \tag{14}$$

Table 1. SLOs and commercial terms as regulated in an example SLA with the assumed deploy cost parameters.

Group	Parameter	Symbol	Value
Commercial	Cost (income for provider)	$I_\tau(n,m,\omega)$	400
	Compensation Cost	C_c	1000
SLO	Observation interval (months)	τ	12
	Max number of failures	n	3
	Max number long down times	m	1
	Threshold long down time (sec)	θ	1800
	Max acc. down time (sec)	ω	4500
Deploy cost	Deploy Cost, unavail reference	C_{du0}	18
	Deploy Cost, unavail cost factor	ν	1,25
	Deploy Cost, CV reference	C_{cv0}	5
	Deploy Cost, CV cost factor	η	3
Optimized	Failure intensity, Possion (1/sec)	λ	$2.46 \cdot 10^{-8}$
	Duration outage, Gamma	α (shape)	1.40
	Duration outage, Gamma (sec)	β (scale)	642

Telstra [Tel14b] offers customers to buy different SLA premium restoration services to reduce the time to repair dependent on time of the day. This example illustrates how a change of the repair process with the aim to reduce the not only the mean, but also the variance has a cost.

To illustrate how the compensation and deployment cost for asymptotic availability, $A = (\lambda\alpha\beta + 1)^{-1}$ is depending on different failures intensities, Fig. 4 depicts an example where the down times are gamma distributed with $\alpha = 6$ and $\beta = 300$ s for SLOs and costs found in Table 1. Note that there is a distinct minimum of the total cost. Likewise, Fig. 5 illustrates an example of compensation and deployment cost for different coefficient of variation for gamma distributed down time durations where $E[D] = 1800$ s.

6. Aggregation of several on-off models

In this section we describe how to find the properties of an aggregated system from a number of SLAs. An aggregated system provides services composed of sub-services from the underlying systems. Each underlying system is operated by an autonomous service provider that delivers its sub-service in accordance with an SLA with the set of SLOs defined in Section 3.1.

A structure function may be used to describe the aggregated system as composed of underlying systems, see e.g. [BP75] for an introduction. In the following denote the set of underlying systems as $\mathcal{J}$, the number of minimal cuts sets as k and the set of underlying systems in minimal cut set x as J_x where $x \in 1, ..., k$.

In [KN10] the Palm distribution of the duration of down times for an aggregated system is derived. With the assumptions that the underlying systems are independent, and that only one cut-set of the aggregated system yields system failure at any time, which is permissible for a highly available system, the Palm distribution of the aggregated system's down time duration

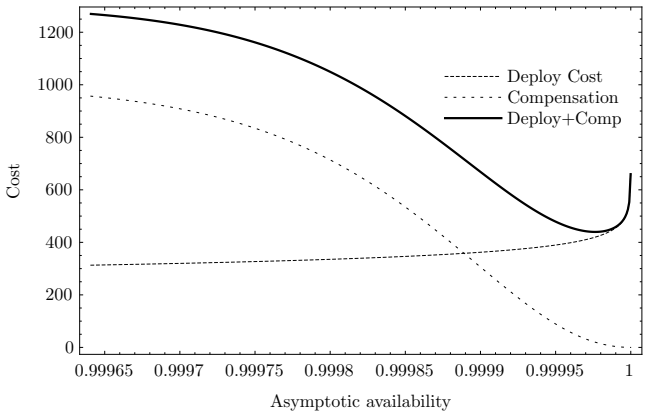

Figure 4. Deployment for asymptotic availability vs. cost for different failures intensities (λ) and gamma distributed duration of down times with $\alpha = 6$ and $\beta = 300$ s for SLOs and costs found in Table 1. A minimum cost may be observed.

is

$$1 - H_A(t) = \sum_{x=1}^{k} \frac{\Lambda_x}{\sum_{r=1}^{k} \Lambda_r} \left[1 - H_x(t)\right] \tag{15}$$

where Λ_x and $H_x(t)$ represent failure intensity and cumulative duration of down time distribution for minimal cut-set x respectively. In [KN10] the derivations of Λ_x and $H_x(t)$ may be found as

$$\Lambda_x^{-1} = \frac{\left(\prod_{i \in J_x} E[D_i]/(E[D_i] + E[S_i])\right)^{-1} - 1}{\sum_{i \in J_x} E^{-1}[D_i]} \tag{16}$$

and

$$1 - H_x(t) = \sum_{i \in J_X} \frac{E^{-1}[D_i]}{\sum_{j \in J_x} E^{-1}[D_j]} \left[1 - H_i(t)\right] \cdot \prod_{j \in J_x \setminus \{i\}} \frac{\int_t^\infty \left[1 - H_j(s)\right] ds}{E[D_j]} \tag{17}$$

where $E[S_i]$ is the expected time between failures for the underlying system i and $E[D_i]$ is its expected duration of down times with CDF $H_i(t)$. See Section 2 for relations to the model parameters.

Assume that a duration of down time caused by cut-set J_x is followed by the state where all systems in the cut-set are again functional. This implies an approximation of the intensity of failures for the cut-set in concern. With this

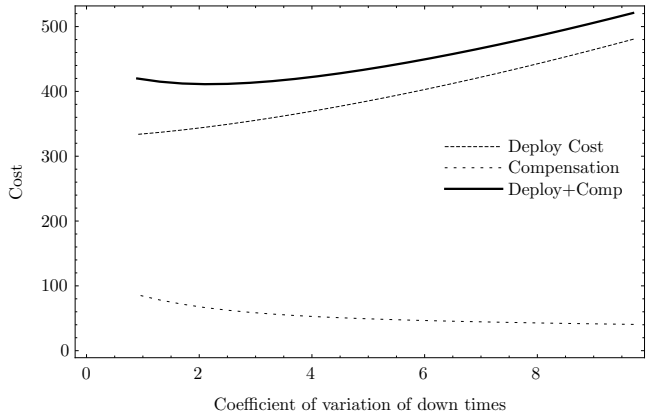

Figure 5. Deployment for coefficient of variation of down times vs. cost for different value of shape parameter of a gamma distributed duration of down times for SLOs and cost found in Table 1. $E[D] = 1800$ s. A minimum cost may be observed.

approximation the distribution of the time between failures for the aggregated system can be given as

$$g_A(t) \approx \Lambda_A e^{-\Lambda_A t}, \text{where } \Lambda_A = \sum_{x=1}^{k} \Lambda_x \tag{18}$$

With the time between failures and duration of down time distributions derived for the aggregated system, an aggregator may form relations between its own SLA and the SLAs for the set of underlying sub systems $\mathcal{J}$ as

$$\begin{aligned} R_{n,m,\omega|\Lambda_A,H_A(t)}(\tau) &= I_{c|n,m,\omega}(\tau) \\ &- \sum_{\forall j \in \mathcal{J}} \left(I_{c_j|n_j,m_j,\omega_j}(\tau) - C_{c_j|n_j,m_j,\omega_j} P_{n_j,m_j,\omega_j|\lambda_j,\alpha_j,\beta_j}(\tau) \right) \\ &- C_{c|n,m,\omega} P_{n,m,\omega|\lambda,\alpha,\beta}(\tau) \end{aligned} \tag{19}$$

Note that the deployment cost in (19) is related to the price for the services delivered by underlying systems reduced with the expected compensations.

7. Case scenarios

In this section we exemplify the on-off model deduced from the SLA and other parameters as described in Sections 4-6. A discussion of the sensitivity of the parameters is provided.

First we want to recall the main approximations and assumptions used. Appendix A validates the approximation of the independence of number of

failures and the accumulated down times and discusses the insensitivity to fluctuations in the failure intensity. The main assumptions are related to the dependability SLOs given in Section 3.1. Note that SLAs typically define the maximum number of failures. In Sections 7.1 and 7.2 we deal with the problem under the assumption of a constant failure intensity, i.e., a homogeneous failure process. In Section 7.4 the result from a simulation study is shown, demonstrating that the results obtained are insensitive to fluctuations in the failure intensity. The model of the deployment cost is as given in Section 5. A compensation is assumed to be paid if one or several of the SLOs are violated during an observation interval as described Section 4.

7.1 Reference scenario

In Table 1 the assumed values of the SLOs, commercial terms and deployment cost parameters are given as a reference scenario. The values of the SLOs are realistic for a highly dependable system, whereas the deployment cost parameters are examples to show how these impact the estimated deployed dependability quality of the system.

Mathematica [Wol11] is used to solve the numerical optimization. The optimal case, i.e., assuming operator behaviour from (11) is obtained, corresponding to the values for λ, α and β are included in Table 1.

To study the parameters' sensitivity of estimated failure and repair processes on the operators profit a 3D plot for the profit for a range of values of λ, α and β is given in Fig. 6. The plotted ranges enclose the optimal values yielding the maximum profit 26.2. In the figure the profit is proportional to the volume of the bubble, i.e., the bubble with the largest volume is the most profitable combination of λ, α and β. As indicated by Fig. 6 the profit has a global optimum and is not very sensitive to the plotted range of parameter values. The asymptotic availability based on the parameter values of the failure and repair processes is given by the grey tones of the bubbles in Fig. 6. As may be found in the figure, a high profitable deployed service does not correspond to the highest availability.

7.2 Deployed vs. required quality

A refinement of Fig. 3 is provided in Fig. 7 where the requirements are the contracted SLOs given by Table 1. The maximum number of failures objective and maximum unavailability objective are represented in the figure, derived from n/τ and $1/U = \tau/\omega$ respectively. There is no mean duration of down time SLO, but the maximum down time threshold θ puts constraint on the mean duration of down times. In the figure three lines are illustrating how θ influences the mean duration of down times depending on the providers control of the repair process. These lines are named; fixed, controlled and uncontrolled repair time to associate the provider's capability to manage the repair process in terms of coefficient of variation, i.e., $1/\sqrt{\alpha}$, of the repair time.

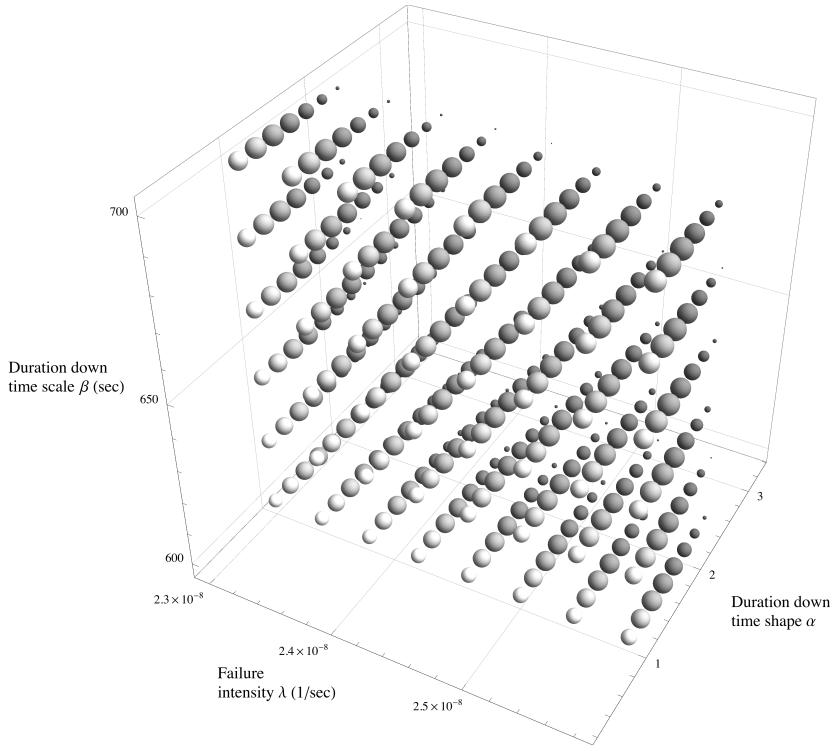

Figure 6. Providers' profit is dependent on failures intensity (λ) and shape (α) and scale (β) parameters of the distribution down time. The volumes of the bubbles are proportional to the profit. The whitest bubble indicates the highest availability and darkest indicates the lowest availability.

As an example the values of $\alpha = \{100, 5, 1\}$ have been used for illustrating the fixed, controlled and uncontrolled repair time and for each the following is solved with respect to β

$$1 - \frac{\Gamma(\alpha, \theta/\beta)}{\Gamma(\alpha)} = \frac{\gamma}{\tilde{\lambda}} \tag{20}$$

where $\gamma = m/\tau$ is the intensity of the long down times and $\tilde{\lambda}$ is the intensity of service failures. The equations are solved for different values of $\tilde{\lambda} > \gamma$. The higher the shape parameter α gets, representing a fixed repair time, the closer will $E[D]$ get the to threshold θ.

To investigate how the deployed dependability qualities are dependent on the SLOs and cost parameters a number of different values are studied for the

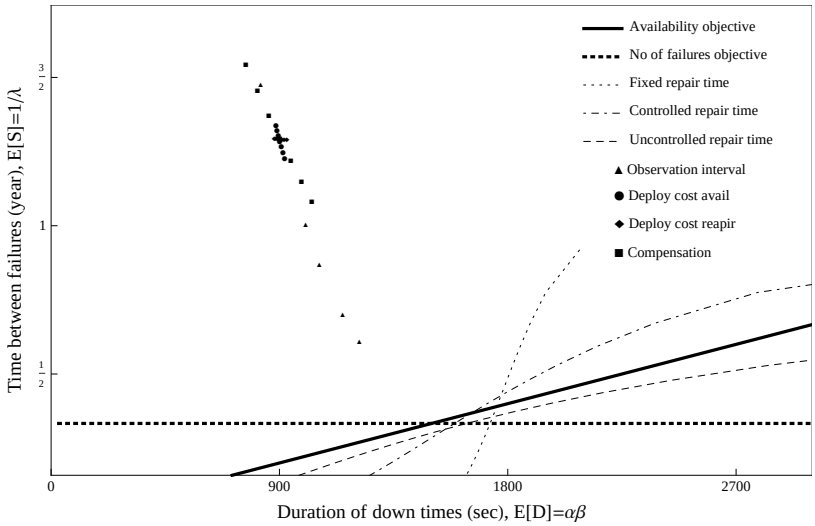

Figure 7. Optimal system deployment for the given SLOs with variations in cost parameters and observation interval. Cost parameters are changed with ±15% compared with values given in Table 1. Observation interval = $\{8, 12, 24, 36, 72, 120\}$ months with scaled requirements from Table 1.

parameters. As a reference scenario the parameters and cost as given in Table 1 is used. From this reference point one of the parameters is changed and the corresponding optimal service quality deployment is derived and depicted in Fig. 7. For the parameters compensation (C_c), deployment cost unavailability factor (ν) and deployment cost repair (η) the changes are ±15% in steps of ±5%, while for the observation interval (τ) we have used $\{4, 8, 12, 24, 36, 72, 120\}$ months. The SLOs n, m and ω and costs are scaled in proportion with the observation interval. For the number of long outages, $m = 1$ at 12 months, this is not feasible. Hence, for $\tau = \{4, 8\}$ we use $m = 1$.

Both compensation and deployment cost affect the deployed dependability qualities as indicated in Fig. 7. When the compensation (C_c) is decreased, the deployed dependability qualities approach the SLOs. Similarly, the higher the deployment cost gets, the further away is the deployed dependability quality the SLOs. The interpretation is that the lower deployment cost gets relative to the expected compensation, the better it is for the provider to deploy better dependability qualities for the service. For the observation interval (τ) the deployed dependability quality tends to get closer to the SLOs when the interval gets longer as indicated in Fig. 7. When the observation interval is four months, the service failure intensity gets very low ($4.02 \cdot 10^{-9}$), while the mean duration of down time gets very high (more than 10.000 sec), not shown in the

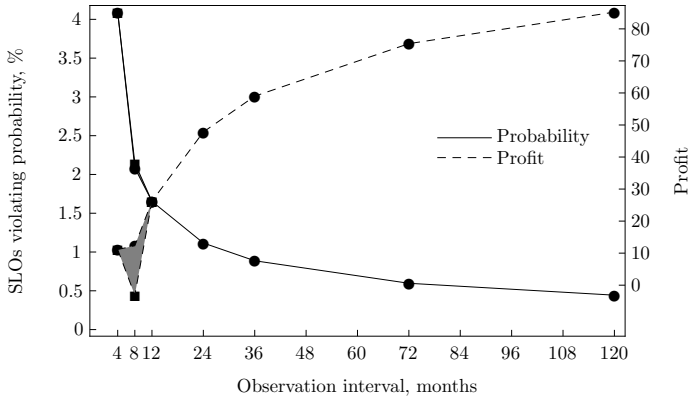

Figure 8. Sensitivity of the observation interval for violating SLOs and the profit per year for the values given in Table 1.

figure. The model provides a good insight on how the observation interval, in particular how a relative short interval, affects the optimal deployment.

The observation interval is known to have a significant effect on the probability of violating the availability SLO [CBB+05, ZG05]. In the more complex setting discussed here, Fig. 8 shows probability of violating the SLOs and the provider's profit for optimized values of λ, α and β for the actual observation interval. It is clearly indicated that the probability of violating the SLOs is higher for a short observation interval than for the longer intervals. In addition, the figure illustrates that the profit is higher with longer observation interval, which implies that the provider should use an observation interval that is equal the contract period of the SLA.

The shaded area in Fig. 8 provides a probability zone caused by the scaling of the maximum number of long down times. For the intervals of $\tau = 4$ and $\tau = 8$ months curves for both $m = 0$ and $m = 1$ are plotted. As can be observed, the $m = 0$ requirement is a more demanding than $m = 1$ for an observation interval of 8 months, while it has no effect when the observation interval is 4 months, since the maximum accumulated down time is the most demanding requirement in both cases.

7.3 Negotiation of service-level objectives

It may be unfeasible in practice to control the failure rates and repair times distributions in a continuous way for a system as assumed in the previous sections. However, this kind of analysis may also be a useful tool in the negotiations between the service provider and the customers. Fig. 9 depicts the provider's profit for a range of values of the SLOs parameters n, ω and θ,

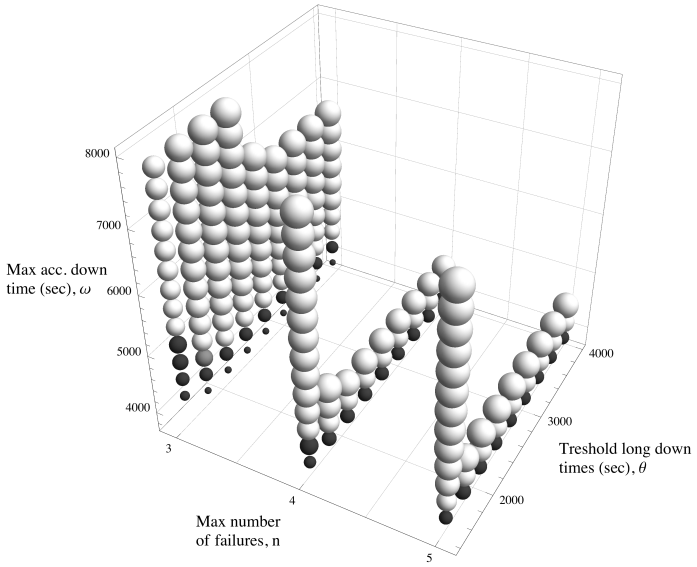

Figure 9. The maximum provider's profit, represented as the volume of the bubbles, for a range of values of the SLOs n, ω and θ. All other parameters kept at the values in Table 1. The medium grey bubble indicates the profit of the reference scenario in Table 1. Dark grey bubbles indicate less profit than this scenario, light grey larger.

while the income from the service is kept constant. Starting with the reference scenario of Table 1 (the medium grey bubble), it may be seen how the potential profit from the service may change as the service requirements are strengthened or weakened by altering the SLO parameters n, ω and θ. If the customer has a similar relation between the value of the service to him, i.e., what he is willing to pay as $I_{c|n,\omega,\theta}$, and the parameter values, this may help to find a set of SLO parameters that yields a better trade-off for both, tentatively Pareto optimality.

7.4 Non-homogeneous Poisson failure process

Earlier in Section 7 the probability of violating the dependability SLOs, i.e., the quantity $P_{n,m,\omega|\lambda,\alpha,\beta}(\tau) \to P_{\text{opt}}(\tau)$ in (5), was obtained as a key quantity in finding the optimal operational parameters for a system. These parameters were obtained for an HPP failure process. SLAs do not typically have any requirement for the failure process, just the values observed over the given interval. In this section, we will investigate whether fluctuations in the failure process has any significant influence on the result obtained, as long as the requirement of short down times, i.e., (2) is met. This is done by performing

a simulation study where the probability of violating the SLOs is compared between HPP and NHPP failure processes for the reference scenario as given in Table 1 with the optimal operational parameters. If this probability, $P_{\text{obs}}(\tau)$, is nearly the same as $P_{\text{opt}}(\tau)$, cf. (11), the optimal operation point is insensitive to fluctuations in the failure process. The simulations are performed without neglecting down times in the failure generation process, so the robustness of the assumption in (3) is demonstrated as well.

An NHPP failure process may have a variety of different time varying failure intensities. For instance, in [FH11] a data set for covering more than 1000 consecutive days from a cellular network operator was analyzed and it was found that the failure intensity had strong cyclic effects of 12 hours, 24 hours and 7 days. The following model may be used for the variations of failure intensity for an NHPP failure process with multiple cyclic and trend effects

$$\lambda(y) = \sum_{i=0}^{s} \psi_i y^i + \sum_{j=1}^{k} \rho_j \sin(\varpi_j y + \varrho_j) \tag{21}$$

where y is the calendar time and the periods of the cyclic effects are given by $2\pi/\varpi_j$.

For the reference scenario as given in Table 1 the optimized HPP failure intensity, λ, is $2.46{\cdot}10^{-8}$ for gamma distributed down times with the parameters $\alpha = 1.40$ and $\beta = 642$. As may be found in Fig. 8 the probability of violating the SLOs is $P_{\text{opt}}(\tau) = 1.652\%$. To compare this result with an NHPP with the same expected number of failures in the observation interval τ the failure intensity fulfills $\Lambda(\tau) = \int_0^\tau \lambda(y)dy = \lambda\tau$.

The simulator was implemented in Mathematica 8 [Wol11] running on a Mac with 2.5GHz Intel Core 2 Duo CPU with 4 GB memory and OS X version 10.6.8. A total of 400,000 years were simulated, i.e., equal 400,000 observation intervals.

In Table 2 the estimated probabilities, P_{obs}, with the 95% confidence intervals are found by simulation for the HPP case without neglecting down times (first line) and three different NHPP cases where the cyclic effects are given in hours or days. Note for the three NHPP cases the phase shifts, ϱ_j, are 0. The probability of violating the SLOs by simulation for the three NHPP cases and HPP are found to be very similar and close to the calculated optimal value. This demonstrates the insensitivity to fluctuations in the failure process, as well as the approximation in (3).

7.5 Aggregated systems

Assume a system consisting of several underlying systems as depicted in Fig. 10. This scenario describes how an aggregator may combine offerings from several providers to be able to offer a new service. The aggregated system consists of a certain structure of services provided by independent network operators, named N_1 and N_2, and independent data centre providers,

Table 2. Simulation results for the probability of violating the SLOs for the reference scenario in Table 1 for the HPP (first line) and three NHPP failure processes with the same expected number of failures during the observation interval τ. The $\varrho_j = 0$ for all NHPP.

ψ_0	ψ_1	ρ_1	ϖ_1	ρ_2	ϖ_2	P_{obs} [%]
$2.46 \cdot 10^{-8}$	0	0	0	0	0	1.655 ± 0.038
$3.0 \cdot 10^{-8}$	$-3.43 \cdot 10^{-16}$	$0.5 \cdot 10^{-8}$	24h	$0.2 \cdot 10^{-8}$	7d	1.667 ± 0.051
$3.0 \cdot 10^{-8}$	$-3.49 \cdot 10^{-16}$	$1.5 \cdot 10^{-8}$	30d	$0.2 \cdot 10^{-8}$	7d	1.608 ± 0.040
$2.8 \cdot 10^{-8}$	$-2.18 \cdot 10^{-16}$	$1.5 \cdot 10^{-8}$	90d	$0.5 \cdot 10^{-8}$	7d	1.665 ± 0.035
$2.46 \cdot 10^{-8}$	From optimization procedure: $P_{\text{opt}}(\tau)$					1.652

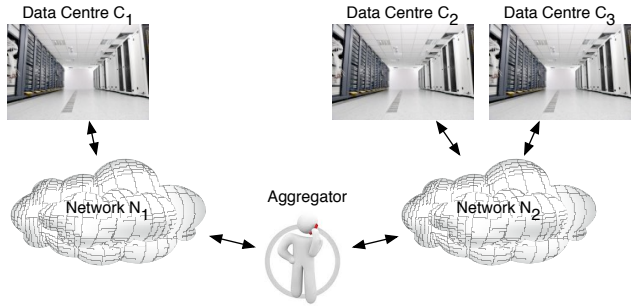

Figure 10. An aggregated system consisting of underlying systems described by the structure function $\Phi = \Big(N_1 \cap C_1\Big) \cup \Big(N_2 \cap (C_2 \cup C_3)\Big)$.

named C_1, C_2 and C_3 respectively. As indicated in Fig. 10, the on-state of the aggregated system depends on one data centre and its connected network to be in the on-state. The aggregated system is described by the following structure function

$$\begin{aligned}\Phi &= \Big(N_1 \cap C_1\Big) \cup \Big(N_2 \cap (C_2 \cup C_3)\Big) \\ &= (N_1 \cup N_2) \cap (N_2 \cup C_1) \\ &\cap (N_1 \cup C_2 \cup C_3) \cap (C_1 \cup C_2 \cup C_3)\end{aligned} \tag{22}$$

The aggregator's mechanisms for providing a fault tolerant system of the underlying systems are not counted for. For instance, a replication procedure may be needed to ensure that data is replicated to all the data centres. The SLAs for the underlying systems are defined in Table 3. In the table the estimated optimized values for the underlying systems as λ_i, α_i and β_i are also included.

In the informed case the aggregated system's failure intensity and its mean down time may be found using the estimated optimized values for each of the underlying systems by using (15) and (18) as described in Section 7.5. As

Table 3. SLOs and costs with the assumed deploy cost parameters as regulated by multiple SLAs for a scenario as depicted in Fig. 10.

	Parameter	N_1	N_2	C_1	C_2	C_3
Commercial	$I_\tau(n,m,\omega)$	400	400	300	200	200
	C_c	1000	1000	650	400	400
SLO	τ (months)	12	12	12	12	12
	n	3	3	21	30	30
	m	1	1	7	10	10
	θ (sec)	1800	1800	1800	1800	1800
	ω (sec)	4500	4500	32500	40000	40000
Deploy cost	C_{du0}	18	18	15	15	15
	ν	1,25	1,25	1,25	1,25	1,25
	C_{cv0}	5	5	4	4	4
	η	3	3	3	3	3
Optimized	$\lambda \cdot 10^{-7}$ (1/sec)	0.246	0.246	3.435	5.504	5.504
	α	1.404	1.404	0.935	0.802	0.802
	β (sec)	642.2	642.2	1281.7	1414.9	1414.9

described in Section 7.2, each of the providers of the underlying systems has added a safety margin for not violating their agreed SLOs. The aggregated system's failure intensity is found to be in the range of $1.9 \cdot 10^{-11}$ with mean duration of down time of approximately 508 seconds (using Palm's identity for $\int_0^\infty (1 - H(t))dt$. In the naive case, where the SLOs form the basis for the computation, failure intensity is found to be $1.6 \cdot 10^{-10}$ and mean down time to be 1070 seconds using the n_i and ω_i for each of the underlying systems only. The optimized system is an undoubted over dimensioned system. An aggregator may use this as an opportunity to obtain lower prices for the services provided by the underlying providers combined with lower SLOs or reduced compensations. This in turn will be the aggregator's added value to his customers, since the aggregated service price gets lower than the sum of the prices for all underlying services.

8. Conclusion

It is shown how an on-off model of a service from a provider may be obtained from the parameters of a service level agreement (SLA) between provider and customer. SLAs are expected to be an increasingly important and used means, when a chain of autonomous partners provides critical services. The price of the service, observation interval, service level objectives (SLOs), deployment cost and compensation in case the SLOs are not met, are taken into account. The SLOs considered are number of failures, accumulated down time and number of severe outages over an observation period. It is also shown how aggregated systems may be handled. This approach provides valuable insights into the cost vs. quality (in terms of dependability SLOs) trade-off for the provider and the customer. One such insight is obtaining the risk sharing in providing important infrastructure services.

It is also demonstrated that having short observation periods, as a part the agreement, will incur a significantly increase in cost relative to longer observation intervals. The model may be used by the service provider to find an approximately cost optimal inherent deployed dependability. This will be significantly different from the naive approach using the dependability related SLOs directly. However, the approach for obtaining the optimal inherent deployed dependability is based on a continuous set of solutions using idealized relations between cost, failure intensities and repair processes. In a real system, there will be a discrete set of options for providing the service, both in terms of system designs and/or configurations, as well as maintenance strategies. How to deal with this discrete set of solutions in obtaining the optimal designs and strategies are for future research.

Acknowledgment

We acknowledge the input and discussions with the researchers Astrid Undheim and Andres González at Telenor and the professors Yuming Jiang and Poul Heegaard at Institute of Telematics at NTNU. We would like to thank the anonymous reviewers for their comments and suggestions which have lead to a significant improvement of the paper.

Appendix A. Assessing the error of approximation

In this appendix, we validate the approximation introduced in (3). First we validate the approximation of neglecting the down times when counting the failures from an HPP failure process and then when the failure process is NHPP.

A.1 The effect of neglecting down times

To obtain the simultaneous probability for the accumulated down time and the number of failures $P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x]$ we follow the line of reasoning in Takacs' [Tak57]. Let $\{\xi_1, \xi_2, \xi_3, \ldots\}$ and $\{\vartheta_1, \vartheta_2, \vartheta_3, \ldots\}$ denote the times spent on-state and off-state respectively where $\zeta_x = \sum_1^x \xi_x$ and $\chi_x = \sum_1^x \vartheta_x$. The system starts in on-state at time $t = 0$ and alternates between the on-state and off-state until ending in either on-state or off-state at the end of the observation interval and we may write

$$
\begin{aligned}
&P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x] \\
&\quad = P[\chi_x \leq \omega, \zeta_x + \chi_x \leq \tau < \zeta_{x+1} + \chi_x] \\
&\quad + P[\zeta_x \geq \tau - \omega, \zeta_x + \chi_{x-1} \leq \tau < \zeta_x + \chi_x] \\
&\quad = P[\zeta_x \leq \tau, \zeta_x < \tau - \omega] - P[\chi_x \leq \omega, \zeta_{x+1} < \tau - \omega] \\
&\quad + \Upsilon(\tau, x, \omega) - \Upsilon(\tau, x + 1, \omega)
\end{aligned} \tag{A-1}
$$

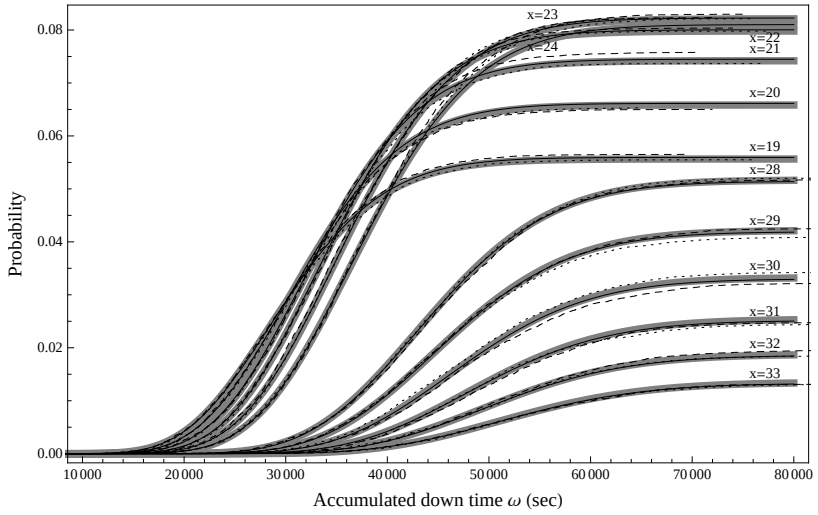

Figure A-1. $P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x]$ (thin lines) and $P[\Omega(\tau) \leq \omega, N(\tau) = x]$ (thick lines) are depicted for the parameters $\lambda = 7.504 \cdot 10^{-7}\text{s}^{-1}, \alpha = 0.8, \beta = 2000$ s and $\tau = 12$ months for an HPP failure process. Note that differences are small for all cases though only some are shown in the figure. $P[\Omega(\tau) \leq \omega, x]$ is less than $P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x]$ for $x \leq 23$ while higher otherwise. The simulated HPP (dashed) and NHPP (dotted) show also very small effect of neglecting the down time and that the variations in the failure intensity of an NHPP is very small as well.

where

$$\begin{aligned}\Upsilon(\tau, x, \omega) &= \int_{y=0}^{\omega} P\Big[\zeta_x \geq \tau - \omega, \zeta_x \leq \tau - y | \chi_{x-1} = y\Big] \\ &\quad \cdot P[y \leq \chi_{x-1} < y + dy] dy \\ &= \int y = 0^{\omega} h^{\otimes(x-1)}(y) \cdot \Big(\hat{G}^{\otimes x}(\tau - y) - \hat{G}^{\otimes x}(\tau - \omega)\Big) dy \\ &= \Theta(\tau, x, \omega) - \hat{G}^{\otimes x}(\tau - \omega) \cdot H^{\otimes(x-1)}(\omega) \end{aligned} \tag{A-2}$$

Substitution of (A-2) into (A-1) yields

$$\begin{aligned}P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x] &= \Big(H^{\otimes x}(\omega) - H^{\otimes(x-1)}(\omega)\Big) \\ &\quad \cdot \hat{G}^{\otimes x}(\tau - \omega) + \Theta(\tau, x, \omega) - \Theta(\tau, x + 1, \omega) \end{aligned} \tag{A-3}$$

where $\hat{G}(t)$ is a homogeneous failure process. Further, $\Theta(\tau, x, \omega) = \int_0^{\omega} h^{\otimes(x-1)}(y) \hat{G}^{\otimes x}(\tau - y) dy$, $\Theta(\tau, 0, \omega) = 1$ and $\Theta(\tau, 1, \omega) = \hat{G}(\tau)$. For gamma

distributed down times and an HPP failure process this may be written as

$$\begin{aligned}
\Theta(\tau,x,\omega) &= H^{\otimes(x-1)}(\omega) - \frac{e^{-\lambda\tau}}{\beta^{(x-1)\alpha}\Gamma(x-1)\alpha} \\
&\cdot \sum_{i=0}^{x-1} \frac{\lambda^i}{i!} \int_0^{\omega} y^{(x-1)\alpha-1} \cdot (\tau-y)^i e^{(-\beta+\lambda)y} dy \\
&= H^{\otimes(x-1)}(\omega) - \frac{e^{-\lambda\tau}\sum_{i=0}^{x-1}\lambda^i/i!}{\Gamma((x-1)\alpha)\beta^{(x-1)\alpha}} \\
&\cdot \sum_{j=0}^{i} \tau^j (-\omega)^{i-j} \omega^{(x-1)\alpha} \cdot (\omega(1/\beta-\lambda))^{-i+j+(1-x)\alpha} \binom{i}{j} \\
&\cdot \Big(\Gamma(i-j+(x-1)\alpha) \\
&- \Gamma(i-j+(x-1)\alpha, \omega(1/\beta-\lambda))\Big)
\end{aligned} \tag{A-4}$$

where $\hat{G}(\tau) = 1 - e^{-\lambda\tau}$. We now have an expression (A-3) of the exact simultaneous probability and we may assess the error of the approximation of neglecting the down times as the difference between $P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x]$ and $P[\Omega(\tau) \leq \omega, N(\tau) = x]$ where $P[\Omega(\tau) \leq \omega, N(\tau) = x] = H^{\otimes x}(\omega)P[N(\tau) = x]$. The differences will be higher the higher the density of failures become and with increased expected down time. In Fig. A-1 $P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x]$ (thin lines) and $P[\Omega(\tau) \leq \omega, N(\tau) = x]$ (thick lines) are depicted for the parameters $\lambda = 7.504 \cdot 10^{-7}\text{s}^{-1}, \alpha = 0.8, \beta = 2000$ s and $\tau = 12$ months representing a system behavior that provoke higher differences than used in this paper. The difference is hardly noticeable for the depicted number of failure in the figure and is less than 2% for all cases. As may be observed, $P[\Omega(\tau) \leq \omega, N(\tau) = x]$ is less than $P[\hat{\Omega}(\tau) \leq \omega, N(\tau) = x]$ for $x \leq 23$ while higher otherwise. The approximation may also be shown to be valid for a NHPP as long as time varying failure intensity $\lambda(y) \ll 1/E[D], \forall y \in [0, \tau]$, where for gamma distributed down times $E[D] = \alpha\beta$.

A.2 The effect of neglecting variations in the failure intensity

For an NHPP failure process with multiple cyclic and trend effects, the model in (21) may be used for the variations of failure intensity. In (A-3) an HPP failure process is assumed. To investigate the effects on the approximation when there is an NHPP failure process we have performed a simulation study.

The on-off system is simulated without neglecting the down period. For the intensity we have used (21) for $s = 1$ and $k = 2$ where $\psi_0 = 7.504 \cdot 10^{-7}, \psi_1 = 2.55 \cdot 10^{-16}, \rho_1 = 1.5 \cdot 10^{-7}, \rho_2 = 0.2 \cdot 10^{-7}$ and ϖ_1 and ϖ_0 represent periods of 24 hours and one week respectively. The phase shifts, ϱ_1 and ϱ_2 are both set to 0. The excepted number of failures during the observation interval τ is equal for the HPP and NHPP failure processes where $\Lambda(\tau) = \int_0^{\tau} \lambda(y)dy = \lambda\tau$.

A total of 60,000 years were simulated, i.e., equal 60,000 observation intervals. Results from this simulation study are shown in Fig. A-1 for HPP and NHPP failure processes. These results combined with the result in Table 2 confirm that the effect of neglecting down times, cf. (3) is very small, and that variations in the failure intensity, i.e., the effect of an NHPP failure process, is very small as well.

References

[Ama13] Amazon Web Services. Amacon EC2 service level agreement. `http://aws.amazon.com/ec2/sla/`, June 2013.

[BBC+10] A. Bobbio, G. Bonanni, E. Ciancamerla, R. Clemente, A. Iacomini, M. Minichino, A. Scarlatti, R. Terruggia, and E. Zendri. Unavailability of critical SCADA communication links interconnecting a power grid and a telco network. 95(12):1345–1357, 2010. 19th European Safety and Reliability Conference on reliability.

[BHK+04] L.-O. Burchard, M. Hovestadt, O. Kao, A. Keller, and B. Linnert. The virtual resource manager: an architecture for SLA-aware resource management. In *IEEE International Symposium on Cluster Computing and the Grid, CCGrid 2004*, pages 126–133, April 19-22 2004.

[BP75] R. Barlow and F. Proschan. *Statistical theory of reliability and life testing: probability models*. Holt, Rinehart and Winston New York, 1975.

[BSC01] P. Bhoj, S. Singhal, and S. Chutani. SLA management in federated environments. *Computer Networks*, 35(1):5–24, January 2001.

[CBB+05] R. Clemente, M. Bartoli, M. Bossi, G. D'Orazio, and G. Cosmo. Risk management in availability SLA. In *Proc. 5th International Workshop on the Design of Reliable Communication Networks DRCN 2005*, pages 411–418, Lacco Ameno, Island of Ischia, Italy, October 16–19 2005.

[Cen13] CenturyLink. Savvis SLA attachment. `http://www.centurylinktechnology.com/legal/sla`, 2013.

[E-806] ITU-T E.860; Framework of a service level agreement, February 2006.

[FH11] E. L. Følstad and B. E. Helvik. Failures and changes in cellular access networks; a study of field data. In *Proc. 8th International Workshop on the Design of Reliable Communication Networks DRCN 2011*, pages 132–139, Krakow, Poland, October 10–12 2011.

[Fra12] U. Franke. Optimal IT service availability: Shorter outages, or fewer? *IEEE Transactions on Network and Service Management*, 9(1):22–33, March 2012.

[GH10] A. J. González and B. E. Helvik. Guaranteeing service availability in SLAs; a study of the risk associated with contract period and failure process. *IEEE (Revista IEEE America Latina) Latin America Transactions*, 8(4):410–416, August 2010.

[GH12] A. J. Gonzalez and B. E. Helvik. System management to comply with SLA availability guarantees in cloud computing. In *Proc. 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom) 2012*, pages 325–332, Tapei, China, December 3–6 2012.

[GT88] A. Goyal and A. Tantawi. A measure of guaranteed availability and its numerical evaluation. *IEEE Transactions on Computers*, 37(1):25–32, January 1988.

[Har05] K. L. Hartley. Defining effective service level agreements for network operation and maintenance. *Bell labs technical journal*, 9(4):139–143, 2005.

[KN10] P. Kuusela and I. Norros. On/off process modeling of IP network failures. In *Proc. 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2010*, pages 585–594, Chicago, IL, June 28 – July 1 2010.

[LHD13] P. Leitner, W. Hummer, and S. Dustdar. Cost-based optimization of service compositions. *IEEE Transactions on Services Computing*, 6(2):239–251, 2013.

[MC08] H. Maciejewski and D. Caban. Estimation of repairable system availability within fixed time horizon. *Reliability Engineering & System Safety*, 93(1):100–106, January 2008.

[Mic13] Microsoft. Windows azure cloud services, virtual machines, and virtual network service level agreement (SLA). `http://www.microsoft.com/en-us/download/details.aspx?id=38427`, 2013.

[MN11a] L. Mastroeni and M. Naldi. Network protection through insurance: Premium computation for the on-off service model. In *Proc. 8th International Workshop on the Design of Reliable Communication Networks DRCN 2011*, pages 46–53. IEEE, October 2011.

[MZB+13] D. S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic. Smart power grid and cloud computing. *Renewable and Sustainable Energy*, 24:566–577, 2013.

[Nex13] Nextgen group. Service level agreement (SLA). `http://www.nextgennetworks.com.au/about/service-management-centre/service-level-agreement/`, 2013.

[NSG15] S. Ntalampiras, Y. Soupionis, and G. Giannopoulos. A fault diagnosis system for interdependent critical infrastructures based on HMMs. *Reliability Engineering & System Safety*, 138:73–81, 2015.

[Ouy14] M. Ouyang. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 121:43–60, 2014.

[RS95] G. Rubino and B. Sericola. Interval availability analysis using denumerable markov processes: application to multiprocessor subject to breakdowns and repair. *IEEE Transactions on Computers*, 44(2):286–291, February 1995.

[RT88] A. Reibman and K. Trivedi. Numerical transient analysis of markov models. *Computers & Operations Research*, 15(1):19–36, 1988.

[SBM09] J. Sauvé, C. Bartolini, and A. Moura. Looking at business through a keyhole. In *Proc. IFIP/IEEE International symposium on integrated network management-workshops IM*, pages 48–51, New York, NY, June 1–5 2009.

[Sch11] F. Schulz. Decision support for business-related design of service level agreements. In *Proc.2nd IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pages 35–38, Beijing, China, July 15–17 2011.

[SWG10] A. Snow, G. Weckman, and V. Gupta. Meeting SLA availability guarantees through engineering margin. In *Proc. 9th International Conference on Networks (ICN)*, pages 331–336, Menuires, France, April 11–16 2010.

[Tak57] L. Takács. On certain sojourn time problems in the theory of stochastic processes. *Acta Mathematica Hungarica*, 8(1):169–191, 1957.

[TBvdZ04] J. Trienekens, J. Bouman, and M. van der Zwan. Specification of service level agreements: Problems, principles and practices. *Software Quality Journal*, 12(1):43–57, 2004.

[Tel14a] Telenor. Prisliste for kapasitetsprodukt. https://www.jara.no/produkter/kapasitet/priserogavtaler/, June 2014.

[Tel14b] Telstra. Standard restoration and SLA premium. http://www.telstra.com.au/customer-terms/business-government/other-services/restoration-sla-premium/, June 2014.

[TT05] R. Taylor and C. Tofts. Death by a thousand SLAs: a short study of commercial suicide pacts. *Forschungsbericht, Hewlett-Packard Labs*, 2005.

[Ver13] Verizon. European service level agreement for: Verizon Internet dedicated, Internet DSL office and Internet DSL solo. http://www.verizonenterprise.com/terms/emea/at/sla/, 2013.

[WB10] L. Wu and R. Buyya. Service level agreement (SLA) in utility computing systems. *Arxiv preprint arXiv:1010.2881*, 2010.

[Wol11] Wolfram Research, Inc. Documentation centre. http://reference.wolfram.com/mathematica/guide/Mathematica.html, 2011.

[YGB14] M. Yigit, V. C. Gungor, and S. Baktir. Cloud computing for smart grid applications. *Computer Networks*, 70:312–329, 2014.

[ZG05] L. Zhou and W. Grover. A theory for setting the "safety margin" on availability guarantees in an SLA. In *Proc. 5th International Workshop on the Design of Reliable Communication Networks DRCN 2005*, pages 403–409, Lacco Ameno, Island of Ischia, Italy, October 16-19 2005.

PAPER G

Optimizing service continuity in a multi operator multi technology wireless environment

Eirik Larsen Følstad and Bjarne E. Helvik

Proceedings of the 9th International Workshop on Design of Reliable Communication Networks (DRCN)

Budapest, Hungary, March 2013

OPTIMIZING SERVICE CONTINUITY IN A MULTI OPERATOR MULTI TECHNOLOGY WIRELESS ENVIRONMENT

Eirik Larsen Følstad, Bjarne E. Helvik
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@q2s.ntnu.no

Abstract Our every day life is getting more and more dependent on wireless access to the desired private, business or machine-to-machine related services and applications. Among these, critical services put the highest requirement on service continuity, i.e., the probability of obtaining an uninterrupted service should be as close to one as possible. Multi homing can be used to increase the service continuity. We propose methods for how to derive the optimal trajectory of access points for a dual homed session in a multi operator multi technology wireless environment where the service continuity of the radio conditions is basis for the handover decisions.

Keywords: Wireless networks, reliability, availability, measurement, evaluation

1. Introduction

The wireless connectivity has become important for the society for a large variety of services and applications such as e.g. infotainment, machine-to-machine communication, business and health care services. Future networks are assumed to be a mixed environment with different access technologies and several operators all integrated into an IP based network. In such an environment key challenges are the selection of the access points to use and timely execution of handovers.

For critical services, like emergency handling, health care and surveillance/monitoring, the continuity of the service is crucial. Multi homing solutions may improve the reliability of the services by utilizing disjoint resources. In this paper we propose how to find the optimal trajectory for a dual homed session in a multi operator multi technology wireless environment, where the reliability of the radio connections is basis for handover decisions. A trajectory is defined as series of access points, S_{ij}, to use by the two radio connections i and j between the user equipment and the network along a projected route.

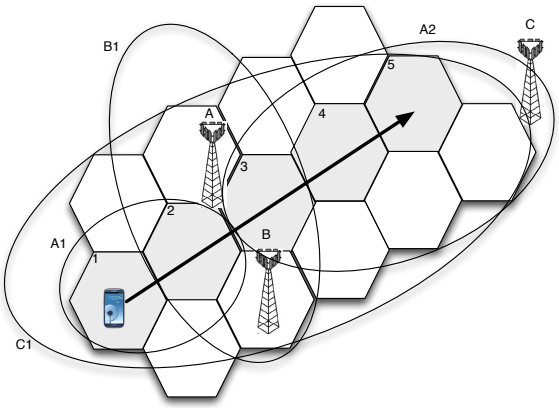

Figure 1. Example network with operators A, B and C with access points coverage (ellipses) and virtual cells (hexagons).

How to derive the projected route is not covered in this paper, but may be given by means of navigation tools or physical constraints.

For a projected route, i.e. the physical transport, there exists huge number of trajectories of access points and corresponding handovers. In [FH13b] a model for prediction of service continuity of a dual homed session for a projected route is described as a phased mission based upon the concept of virtual cells. Virtual cells are defined as limited geographical areas where the radio conditions are homogenous. Here, we extend this work by methods for finding which access points to use in each virtual cell for each connection that maximizes the service continuity. Reliability is a metric for service continuity, formally $R_{S_{ij}}(t_m) = P(T_{FF} > t_m)$ where T_{FF} is time to first failure and t_m is the mission time. For critical services $R_{S_{ij}}(t_m)$ should be close to 1, i.e. $1 - P(T_{FF} > t_m) \ll 1$, to ensure high probability of uninterrupted service. Our method ensures that the series of access points S_{ij} defines disjoint access points in each cell for the two connections. Multi homing protocols can utilize the S_{ij} for achieving the optimal service continuity, i.e. $\max_{\forall S_{ij}} R_{S_{ij}}(t_m)$.

Fig.1 shows an example network with three access network operators, named A, B and C. Access coverages are shown as ellipses in the figure. Operator A has two access points, named $A1$ and $A2$. Operators B and C have one access point each, identified as $B1$ and $C1$ respectively. The arrow shows the projected route. Looking into the projected route, the user will traverse five different virtual cells shown as hexagons. We propose methods for how to find the access points to be used in each virtual cell to maximize $R_{S_{ij}}(t_m)$ for a

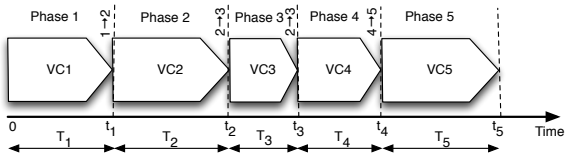

Figure 2. Session modelled as phased mission for the projected route in Fig.1.

dual homed session. The proposed methods supports a global projected route based handover mechanism where all handovers throughout the session time is taken into account and not only as local hop-by-hop based decisions.

To find the optimal service continuity the feasible trajectories are represented by a graph, e.g as in Fig.3 for the example above. Graph models have often been used to describe optimization algorithms. The Bellman-Ford algorithm [Bel56] finds the shortest path between a given pair of vertices in a graph model using the cost of the edges for calculation. Bhandari [Bha99] and Suurballe [Suu74] provide algorithms for diverse routing in networks, described by vertices and edges in graph models. Both Bellman-Ford and Bhandari/Suurballe algorithms may be used to find a trajectory for a dual homed session, but it is not necessary the optimal solution in terms of $\max R_{S_{ij}}(t_m)$. We propose combination of heuristic optimizations based upon shortest path algorithms and Bhandari where edges are allocated dependability metrics, e.g. reliability and availability, related to the access points and handovers to find a near-optimal trajectory.

Minimal cut-sets and minimal path-sets are often used in network reliability evaluations. However, as the number of minimal cut-sets and path-sets easily gets quite large and reduction techniques have to be included [SR93]. Integer Linear Programming (ILP) is a powerful technique to solve optimization problems. However, finding the optimal solution is often NP-hard and therefore some relaxations are needed. For probabilistic link failures [AS08], [LML10] and [CSK02] describe optimization models to find a pair of paths between a source and a destination having minimum joint failure probability where reduction of number of minimal cuts-sets is one of the relaxation techniques. In this paper we formulate problem of finding the optimal trajectory as an integer linear program based upon the continuous time discrete space Markov model proposed in [FH13b]. This model captures the dynamics of failures and restorations between the selected access points in the trajectory.

The rest of the paper is organized as follows. In Section 2 the proposed model is presented. The reliability model is presented in Section 3 that is used as basis for the integer linear programming and heuristic optimizations as described in Section 4 and Section 5. The optimization methods are compared in Section 5. We conclude this paper in Section 7.

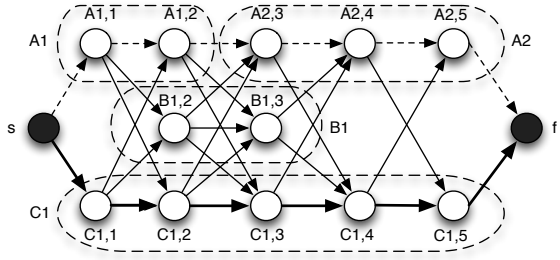

Figure 3. Graph representing the mission phases of the projected route in Fig.1. Optimal trajectory is shown by the bold and dashed edges.

2. Model

For a user that requires access to critical services in a multi operator multi technology wireless environment the reliability of the service is crucial. For a projected route there exists a number of possible different trajectories of access points. To increase the reliability of the service, dual homing is used. In the following we describe how the reliability can be predicted and optimized.

In [FH13b] the reliability for a dual homed session is described as a phased mission. The model allows prediction of the reliability for a given trajectory along a projected route. The Media Independent Handover (MIH) [IEE08] framework is proposed extended with capabilities to enable reliability prediction. The Media Independent Information Service (MIIS) database is used for requesting network information and provides media independent mechanisms for sending measurement reports. Measurement reports contain experienced radio conditions for the given geographical areas. By combining measurement reports from user equipments and signalling from networks, MIIS identifies limited geographical areas where the radio conditions, like e.g. coverage failure intensity, recovery rate, handover failure probabilities between access points, are homogenous. These limited geographical areas are defined as virtual cells. The optimization task may be performed in a powerful user equipment or in a server in combination with the MIH.

As described in [FH13b] each phase corresponds the traversal of one virtual cell including an optional handover to the next virtual cell. Fig.2 shows the different phases of the projected route as depicted in Fig.1. The phased mission is illustrated in Fig.2 where change from phase d to $d+1$ takes place at time t_d and the sojourn time of phase d is T_d.

To find the optimal trajectory we describe the phased mission as a directed graph $G = (V, E)$. Vertices, V, represent radio coverage from access points in virtual cells and edges, E, as handover between pairs of access points. The phased mission depicted in Fig.2 is described by the graph model shown in

Fig.3 that contains all possible trajectories. The vertices $s \in V$ and $f \in V$ are representing the start (s) and final destination (f) of the projected route. Without loosing generality we may index the virtual cells in the order they are visited from 1 to m, i.e., following the phases for the mission.

To generalize the naming of vertices $i_d \in V, i_d \notin \{s, f\}$ in the graph model let the i_d represent an access point identifier prefixed with the identification of the operator and the access technology (e.g. GSM, UMTS) covering virtual cell d. Denote the set of all access points covering virtual cell d as b_d. For instance, for the example in Fig.3 $b_2 = \{A1, B1, C1\}$. A trajectory may be given as a serie of pair of access points to use in each virtual cell and can be written as $S_{ij} = \{(i_1, j_1), \ldots, (i_d, j_d), \ldots, (i_m, j_m)\}$ where $i_d \in b_d$ and $j_d \in b_d$ and $i_d \neq j_d$. In the figure the optimal trajectory $S_{ij} = \{(A1, C1), (A1, C1), \ldots, (A2, C1)\}$ is shown by the bold and dashed edges.

The user moves through a virtual cell and then performs a handover to the next virtual cell. The time spent in each virtual cell is dependent on a variety of parameters, one of them is the velocity. However, the time spent in each virtual cell is independent of the access point selected. The above definitions allows several visits to the same virtual cell, where each visit is assigned a new index d. Handovers take place in the transition from one virtual cell to another. For a trajectory S_{ij} no handover takes place if $i_d = i_{d+1} \in b_d \bigcap b_{d+1}$ and $j_d = j_{d+1} \in b_d \bigcap b_{d+1}$.

With the naming convention of the access point identifier type of handover can be identified. A handover given by $(i_d, i_{d+1}) \in E$ is said to be horizontal if the same access technology is used by i_d and i_{d+1}, otherwise it is a vertical handover. Vertical handover is the term used to change the point of attachment from one access technology (e.g. GSM) to one another (e.g. UMTS). If the point of attachment is within the same operator, it is an intra-domain handover, otherwise it is an inter-domain handover.

3. Reliability model and analysis

To assign the graph model with dependability parameters used by optimization methods the model and parameters as proposed in [FH13b] is the basis. The state transition diagram in Fig.4 from [FH13b] shows the model for traversal of virtual cell d including the handover to cell $d + 1$ for trajectory S_{ij}. Each phase is modelled as a continuous time discrete space Markov model. Handover states Ω_H are grey, while the white ones are coverage states Ω_C since loss of radio connection is the main cause of failure within a virtual cell. The working states are named according to the state of each of the two connection in S_{ij}. For example, the state named OK/OK shows that both connections are working and the state FH/OH shows that connection i has a failed radio connection and executing handover while connection j has a working radio connection and executing a handover. Transitions from Ω_C to Ω_H are only indicated. These transitions are modelled as instantaneous transitions described in the following.

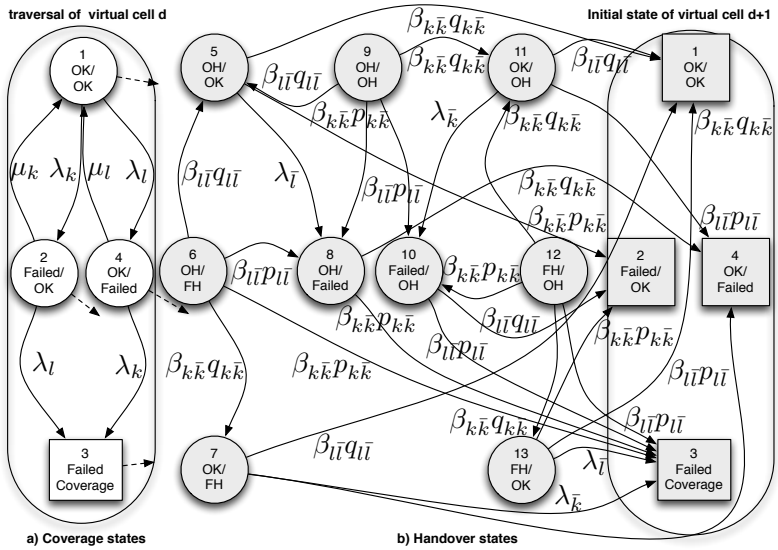

Figure 4. State transition diagram for phase d for trajectory S_{ij}. To simplify the notation in the figure the index $k = i_d$, $\bar{k} = i_{d+1}$ and $l = j_d$, $\bar{l} = j_{d+1}$. Absorbing handover states (gray shaded) represent the initial conditions to the next phase. Transitions into handover states are modelled as instantaneous transition given by S_{ij}.

In Fig.3 it is shown that an access point may provide radio coverage to a number of virtual cells, like e.g. $A2$ that covers cells $3, 4$ and 5. In each of these virtual cells the access point may have different characteristics modelled as parameters in a transition diagram, e.g. like $\lambda_{id,d}$. To keep the notation simple, we will in the rest of the paper use the index i_d for dependability parameters and attributes for an access point i_d in a virtual cell d, i.e. $\lambda_{id,d} \rightarrow \lambda_{id}$.

In Fig.4 the index $k = i_d$, $\bar{k} = i_{d+1}$ and $l = j_d$, $\bar{l} = j_{d+1}$. A radio connection between a user equipment and an access point i_d covering virtual cell d has a constant radio coverage failure intensity λ_{i_d}. The radio coverage from different access points fail independently. When a radio connection to access point i_d has been lost, the time to recover is n.e.d with mean $1/\mu_{i_d}$ in cell d. Handover from i_d to i_{d+1} is n.e.d. with mean $1/\beta_{i_d i_{d+1}}$ and may fail with a probability of $p_{i_d i_{d+1}}$ where $q_{i_d i_{d+1}} = 1 - p_{i_d i_{d+1}}$. In case of dual handovers, the handovers fail independently.

Based on the model presented in Fig.4 and the results from [FH13b], the reliability of a dual homed session can be written as

$$R_{S_{ij}}(t_{m_+}) = R_1\left(T_{1_+}\right) \prod_{d=2}^{m} R_d\left(T_{d_+} | T_{FF} > t_{d-1}\right) \tag{1}$$

where $R_d(T_{d_+}|T_{FF} > t_{d-1})$ represents the reliability of phase d. The notations t_{d_-} and t_{d_+} are used to indicate instants immediately before and after the handover that takes place. Transition intensity matrices for Fig.4 may be organized as

$$\Lambda_C = \begin{bmatrix} \Lambda_{CC} & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \Lambda_H = \begin{bmatrix} 0 & \Lambda_{HC} \\ 0 & \Lambda_{HH} \end{bmatrix} \tag{2}$$

where Λ_{CC} is the transition intensity matrix for Ω_C, Λ_{HH} is the transition intensity matrix for Ω_H and Λ_{HC} is the transition intensity matrix for intensities from Ω_H to Ω_C. By neglecting the handover time the end state for phase d is given as $p(T_{d_+}) = (\Pi_H)^3 p(T_{d_-}|I(t_d))$ where Π_H is the transition probability matrix of Λ_H and the handover indicator function $I(t_d) = \{|i_d \cap i_{d+1}|, |j_d \cap j_{d+1}|\}$. Only 3 operations are necessary since 3 is the largest path from an initial to an absorbing state.

Reliability of phase d is $R_d(T_{d_+}|T_{FF} > t_{d-1}) = 1 - p_3(T_{d_+})$ and the initial state for phase d+1 is $p(0) = \{p_1(T_{d_+}), p_2(T_{d_+}), 0, p_4(T_{d_+}), 0, \ldots, 0\}^T / (p_1(T_{d_+}) + p_2(T_{d_+}) + p_4(T_{d_+}))$. The traversal of cell d is given by $\Lambda_C \dot{p}(t) = d\dot{p}(t)/dt$ with the initial condition $p(0)$. For first phase $p(0) = \{1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}^T$. The instantaneous transitions from Ω_C to Ω_H are given by

$$\begin{aligned} p(T_{d_-}|I(t_d) = \{1,1\}) &= \dot{p}(T_{d_-}) \\ p(T_{d_-}|I(t_d) = \{0,1\}) &= [0, 0, \dot{p}_3, 0, \dot{p}_1, 0, 0, \dot{p}_4, ..., 0, 0, \dot{p}_2]^T \\ p(T_{d_-}|I(t_d) = \{1,0\}) &= [0, 0, \dot{p}_3, 0, 0, 0, \dot{p}_4, 0, 0, \dot{p}_2, \dot{p}_1, 0, 0]^T \\ p(T_{d_-}|I(t_d) = \{0,0\}) &= [0, 0, \dot{p}_3, 0, 0, \dot{p}_4, 0, 0, \dot{p}_1, 0, 0, \dot{p}_2, 0]^T \end{aligned} \tag{3}$$

where $\dot{p}_1 = \dot{p}_1(T_{d_-})$, $\dot{p}_2 = \dot{p}_2(T_{d_-})$, $\dot{p}_3 = \dot{p}_3(T_{d_-})$ and $\dot{p}_4 = \dot{p}_4(T_{d_-})$. As described in [FH13b], an approximation of the reliability may be derived where the initial state of a phase is only dependent on handovers performed in the previous phase. The approximated normalized transient probability of working states just prior handover is given as $\hat{\dot{p}}(T_{d_-}) = \{\mu_{i_d}\mu_{j_d}, \lambda_{i_d}\mu_{j_d}, 0, \mu_{i_d}\lambda_{j_d}, 0, 0, 0, 0, 0, 0, 0\}^T / (\mu_{i_d}\mu_{j_d} + \lambda_{i_d}\mu_{j_d} + \mu_{i_d}\lambda_{j_d})$. The approximated probability vector $\hat{p}(T_{d_+}|I(t_d))$ is only depended on the number of handovers to perform, similar as given by (3), and we get an approximation of the reliability as

$$\hat{R}_{S_{ij}}(t_{m_+}) = R_1\left(T_{1_+}\right) \prod_{d=2}^{m} \hat{R}_d\left(T_{d_+}|T_{FF} > t_{d-1}\right) \tag{4}$$

In the following section we will describe how the model and dependability parameters are used in the different optimization methods.

4. Integer linear programming optimization

The optimal trajectory based upon the reliability prediction can be derived from an Integer Linear Programming (ILP) formulation. The ILP is formulated

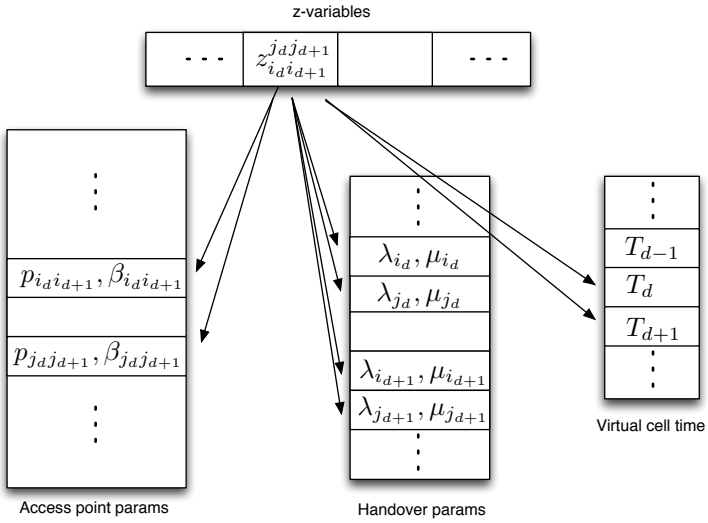

Figure 5. Sketch of the relations between the $z_{i_d i_{d+1}}^{j_d j_{d+1}}$ variables and the dependability parameters shown in Fig.4.

with an objective function for the reliability to be maximized given a set of constraints to be fulfilled. An ILP formulation offers great deal of flexibility for the objective function and constraints on the behalf on complexity. Since ILP formulations only permit linear relations between the variables, special attention has to be put into how create the objective functions and constraints.

In (4) a phase is defined as the traversal of one cell including the handover to the next cell. This is an approximation of the reliability and therefore the trajectory found may not be the optimal. By letting the phase definition be the handover into the cell including the cell traversal, the reliability of one phase is made independent of previous handovers caused by the stabilized ratio between the working states and we get

$$\hat{R}_{S_{ij}}(t_{m-}) = \hat{R}_1(T_{1-}) \prod_{d=2}^{m} \hat{R}_d \left(T_{d-} | T_{FF} > t_{d-1} \right) \tag{5}$$

where the difference from (4) is that handover is performed before the cell traversal and not after.

From (5) we want to derive an ILP formulation with the objective to minimize $1 - \hat{R}_{S_{ij}}(t_{m-})$. Immediately we see that the product form of (5) cannot be used directly in the objective function, but this can be solved by using logarithmic values of $\hat{R}_1(T_{1-})$ and $\hat{R}_d(T_{d-}|T_{FF} > t_{d-1})$ which transforms the product form to a sum form. As a trajectory $S_{ij} = \{(i_1, j_1), \ldots, (i_d, j_d), \ldots, (i_m, j_m)\}$

it is seen that that we may let a binary variable $z_{i_d i_{d+1}}^{j_d j_{d+1}}$ represents a given combination of used access points in phase d and $d+1$ for the two connections. Fig.5 shows a sketch of the relations between the $z_{i_d i_{d+1}}^{j_d j_{d+1}}$ and the dependability parameters in Fig.4. The dependability parameters are grouped into access point parameters, handover parameters and virtual cell sojourn times T_d. Handover parameters constitute the $\beta_{i_d i_{d+1}}$ and $p_{i_d i_{d+1}}$ while the access point parameters constitute λ_{i_d} and μ_{i_d}.

The structure of the objective function related to (5) is given as

$$\min \sum_{\substack{\forall i,j \\ d=1,\ldots,m}} -\ln\Big(\hat{R}_d(T_{d\_}|T_{FF} > T_{d-1})\Big) z_{i_{d-1} i_d}^{j_{d-1} j_d} \tag{6}$$

where $-\ln(\hat{R}_1(T_{1\_}|T_{FF} > T_0)) z_{i_0 i_1}^{j_0 j_1} = -ln(\hat{R}_1(T_{1\_})) z_{i_0 i_1}^{j_0 j_1}$.

For optimizing the objective function we need to define the following constraints

$$\sum_{\substack{\forall i_{d+1} \\ d=0,\ldots,m}} x_{i_d i_{d+1}} - \sum_{\substack{\forall i_{d-1} \\ d=1,\ldots,m+1}} x_{i_{d-1} i_d} = \begin{cases} 1, & i_0 = s \\ -1, & i_{m+1} = f \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

$$\sum_{\substack{\forall j_{d+1} \\ d=0,\ldots,m}} y_{j_d j_{d+1}} - \sum_{\substack{\forall j_{d-1} \\ d=1,\ldots,m+1}} y_{j_{d-1} j_d} = \begin{cases} 1, & j_0 = s \\ -1, & j_{m+1} = f \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

$$\sum_{\substack{\forall i_d \\ d=1,\ldots,m-1}} (x_{i_d i_{d+1}} + y_{i_d i_{d+1}}) \leq 1 \tag{9}$$

$$\sum_{\substack{\forall i_d \\ d=1,\ldots,m-1}} (x_{i_d i_{d+1}} + y_{i_d i_{d+1}}) \leq 1 \tag{10}$$

$$z_{i_d i_{d+1}}^{j_d j_{d+1}} \geq x_{i_d i_{d+1}} + y_{j_d j_{d+1}} - 1, d = 0, \ldots, m \tag{11}$$

$$z_{i_d i_{d+1}}^{j_d j_{d+1}}, x_{i_d i_{d+1}} \text{ and } y_{j_d j_{d+1}} \text{ are binary variables.} \tag{12}$$

where the constraints (7) and (8) provide connections of edges from vertex s to vertex f for both connection in S_{ij}. Constraints (9) and (10) ensure disjoint vertices for S_{ij} in each phase. To keep a linear relation between the x and y variables we use the result from [Wat67] which states that any product of two binary variables can be replaced by a single new binary variable as given by the constraint given by (11).

Once the trajectory S_{ij} is found by the objective function (6) the the exact reliability can be calculated with (1) and we denote this as $R_{S_{ij}}(t_{m_+})_{ILP}$.

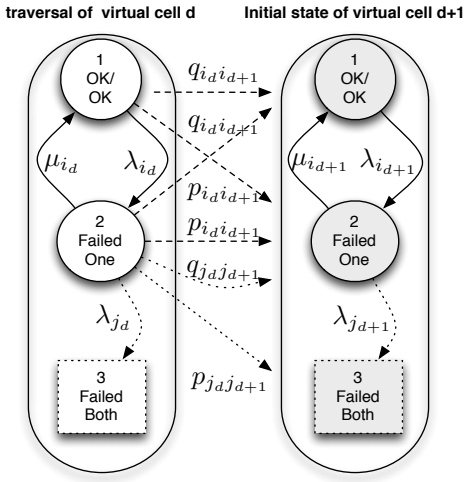

Figure 6. Simplified state transition diagram for phase d for heuristic optimization focused on the series of access points S_i used by one of the two connections. Dependencies to the other connection are only indicated with dotted states and transition intensities.

5. Heuristic optimizations

In this section some heuristic optimizations will be proposed to find near-optimal solutions with lower computational effort than the ILP optimization. Since finding the optimal solution with ILP algorithm may need considerable computation effort, heuristic optimizations are means to solve large systems. First, we will describe how well known shortest-path algorithms can be utilized where different global strategies are followed to find the series of access points S_i used by connection i. Then we describe heuristic optimizations that use the information of S_i as basis for finding the series of access points S_j used by the connection j.

5.1 Single access point selection method

Well known simple algorithms for finding the shortest path between a source and destination in a graph are Dijkstra [Dij59] and Bellman-Ford [Bel56]. For Dijkstra/Bellman-Ford the shortest path is defined as the minimum sum of weight of edges used from source to destination. A simplified state transition diagram for phase d is shown in Fig.6 focused on the access points S_i used by connection i. In this simplified model the dynamics between the two connections are only indicated with dotted states and transitions. This model

will be used by heuristic optimizations based on shortest-path algorithms for deriving a near-optimal trajectory.

Since the objective is to maximize the reliability of the dual homed session, it is intuitively to maximize the reliability for each connection. For a single connection the reliability function of $R_{S_i}(t_m)$ is the serialized structure of the number of phases;

$$R_{S_i}(t_{m\_}) = \prod_{d=1}^{m} e^{-\lambda_{i_d} T_d}(1 - p_{i_{d-1} i_d}) \tag{13}$$

where $p_{i_0 i_1} = 0$. To assign the dependability parameters let the weight of an edge (i_{d-1}, i_d) be

$$w_{Ri_{d-1}i_d} = -\ln(e^{-\lambda_{i_d} T_d}) - \ln(1 - p_{i_{d-1} i_d}), \forall i_d \tag{14}$$

where $d = 1, \ldots, m$ and $w_{Ri_m i_{m+1}} = 0$. This makes the weights of the edges additive and favours the most reliable series of access point S_i.

The reliability function only utilizes the failure intensity and handover failure probability. To also include the recovery rate the availability metric is used. The rationale is to reduce the time the dual homed session is at risk for failure caused by the failure intensity of S_i. Consider the traversal of a virtual cell for one connection, i.e. considering only state 1 and 2 in Fig.6. The instantaneous availability at time t is given the probability of being in state 1 at time t found by

$$dp_1(t)/dt = -\lambda_l p_0(t) + \mu_l p_1(t) \tag{15}$$

with the initial condition given by stabilized ratio between stationary solution between the two states of previous phase given the handover to perform. If $i_{d-1} = i_d$ then the initial condition for phase $d + 1$ is $p(0) = \{\mu_{i_{d-1}}, \lambda_{i_{d-1}}\}/(\mu_{i_{d-1}} + \lambda_{i_{d-1}})$, otherwise $p(0) = \{p_{i_{d-1} i_d}, 1 - p_{i_{d-1} i_d}\}$. For a single connection the availability $A_{S_i}(t_{m\_})$ is the serialized structure of the number of phases;

$$A_{S_i}(t_{m\_}) = \prod_{d=1}^{m} 1/T_d \int_0^{Td} p_1(t)dt \tag{16}$$

Since the instantaneously availability at time of handover is lower it is set to $1 - p_{i_{d-1} i_d}$ the dependability parameters are used to derive the weight of an edge (i_{d-1}, i_d) as

$$w_{Ai_{d-1}i_d} = -\ln\Big(1/T_d \int_0^{Td} p_1(t)dt\Big) - \ln(1 - p_{i_{d-1} i_d}), \forall i_d \tag{17}$$

where $d = 1, \ldots m$ and $w_{Ai_m i_{m+1}} = 0$. This makes the weights of the edges additive and favours the series of access point S_i with highest availability.

A local hop-by-hop handover decision selects the combinations of access points that maximizes for surviving the immediate handover and the traversal

of the next virtual cell, i.e., the reliability of traversal of virtual cell d is optimized given the access point selected in phase $d-1$ as. Assume that the series of access point defined by S_i was known in advance. Then by using the definition given by (5) in Section 4 the weights are calculated to hold the reliability for the actual phase as;

$$w_{Mj_{d-1}j_d} = -\ln \hat{R}_d(T_{d\_}|T_{FF} > t_{d-1}) \tag{18}$$

where $j_d \bigcap i_i = \emptyset$ for $d = 1, \ldots, m$ and $w_{Mj_mj_{m+1}} = 0$.

5.2 Dual access point selection method

Here we will describe three different heuristic optimizations to find near-optimal S_{ij}. Two global heuristic optimizations find S_{ij} based upon S_i using the weights as described in Section 5.1. The third is a local heuristic optimization.

The first heuristic optimization is a pure greedy heuristic based on Dijkstra [Dij59] or Bellman-Ford [Bel56]. To ensure that $i_d \bigcap j_d = \emptyset$ for $d = 1, \ldots, m$ for S_{ij} all edges directed towards the vertices in S_i are removed except for the final destination f. Then Dijkstra [Dij59] or Bellman-Ford [Bel56] algorithm is run again to find S_j. This greedy heuristic allows to use any of the weights described in Section 5.1 in the second round. Pure greedy heuristic might not find S_{ij} where $i_d \bigcap j_d = \emptyset$ for $d = 1, \ldots, m$ even such exists. This is the so-called trap-problem. The Dijkstra algorithm runs in $O(|E| + |V| \log |V|)$ time while Bellman-Ford uses $O(|E||V|)$, where $|V|$ and $|E|$ are the number of vertices $V \in G$ and edges $E \in G$ respectively. Even though the Dijkstra/Bellman-Ford algorithms are time efficient, the results achieved are not necessarily the optimal trajectory caused by simplified model not capturing the dynamics between the two connections as shown in Fig.4.

The second heuristic optimization use the Bhandari algorithm described in [Bha99] that finds the vertex-disjoint shortest pair of paths. The big differences from Dijkstra/Bellman-Ford algorithms are how the Bhandari algorithm uses a vertex splitting technique and edge modifications governed by the shortest path found in the first run to create a modified graph to be used in the second run of shortest-path algorithm. Details can be found in [Bha99]. After the edge modifications it is not given that S_i holds the shortest path in the modified graph. To avoid negative cycles we add the weight of each edge found in the first round to the edges in the same phase. For typical applications where the Bhandari algorithm is used the round trip view is advantage over the greedy algorithms. However, when the costs of the edges are representing probabilities, the non-use of the shortest path might turn into a disadvantage. This is exemplified if the shortest path is a non failing path, i.e. $P(T_{FF} > t_m) = 1$ for a mission of duration t_m and the Bhandari algorithm does not select this path since the algorithm optimizes the round trip path. The Bhandari vertex-disjoint algorithm runs in $O(|V + m|^2)$ time where $|V|$ number of vertices $V \in G$ and $|m|$ is the number of phases in the graph. The third heuristic optimization is a local greedy heuristic that selects the combinations of disjoint access points

Table 1. Heuristic optimizations to find near-optimal trajectory

	Method			
Heuristic	Dual	S_i	S_j	Reliability
G-RR	Dijkstra	Single reliability (13)	Single reliability (13)	$R_{S_{ij}}(t_{m_+})_{GRR}$
G-RM	Dijkstra	Single reliability (13)	Phase reliability (18)	$R_{S_{ij}}(t_{m_+})_{GRM}$
G-AM	Dijkstra	Single availability (17)	Phase reliability (18)	$R_{S_{ij}}(t_{m_+})_{GAM}$
G-LM	Greedy	Local phase reliability (19)		$R_{S_{ij}}(t_{m_+})_{GLM}$
B-RR	Bhandari	Single reliability (13)	Single reliability (13)	$R_{S_{ij}}(t_{m_+})_{BRR}$
B-RM	Bhandari	Single reliability (13)	Phase reliability (18)	$R_{S_{ij}}(t_{m_+})_{BRM}$
B-AM	Bhandari	Single availability (17)	Phase reliability (18)	$R_{S_{ij}}(t_{m_+})_{BAM}$

that optimize the reliability of each of the phases for the dual homed session. The reliability for phase d is optimized given the access point selected in phase $d-1$ as

$$\arg\max_{i_d j_d} \hat{R}_d(T_{d\_}|T_{FF} > t_{d-1}, i_{d-1}, j_{d-1}) \tag{19}$$

where $\hat{R}_1$ starts with $i_0 = s$ and $j_0 = s$. Each possible combination of (i_d, j_d) given (i_{d-1}, j_{d-1}) is calculated in the same way as for phase d in (5).

In Table 1 the different combinations of heuristic optimizations are summarized. For instance, the heuristic named G-RM use the Dijkstra algorithm to find S_i with weights of edges as defined by ((13). Then after removal of all towards the vertices identified with S_i the weights are calculated according to (18) and Dijkstra algorithm is run again. Once the trajectory S_{ij} is found by the optimization the reliability can be calculated with (1) and denoted according to the heuristic optimization as e.g. $R_{S_{ij}}(t_{m_+})_{GRM}$ for the G-RM heuristic.

6. Comparison of results from optimizing methods

Even though the concept of virtual cells is introduced to make the number of possible trajectories finite, this number will still be quite large. The objective functions used by the ILP and heuristic optimizations are different, and different "best" trajectory may be found. To compare the results from the methods a number of scenario-classes are defined. From these scenario-classes, a number of scenario-instances are generated. A graph model, e.g. like the one in Fig.3, represents each scenario-instance.

6.1 Scenario classes and instances

We define six scenario classes, each with a defined number of virtual cells along the projected route and network operators providing radio coverage. A network operator may provide radio coverage for all or only a part of the virtual cells. The total radio coverage from a network operator is provided for successive virtual cells. If a network operator provides only a part of the virtual cells, the first virtual cell is randomly selected. For the scenario classes

Table 2. Scenario-classes and operator access coverage

		Characteristics							
		Coverage Operator A		Coverage Operator B		Coverage Operator C		Coverage Operator D	
Class	Cells	cells per AP	total cells	cells per AP	total cells	cells per AP	total cells	cells per AP	total cells
1	5	U[2,3]	5	2	2	5	5		
2	10	as class 1	10	as class 1	4	as class 1	10		
3	15	as class 1	15	as class 1	6	as class 1	15		
4	5	U[2,3]	5	2	2	5	5	U[1,2]	2
5	10	as class 4	10	as class 4	4	as class 4	10	as class 4	4
6	15	as class 4	15	as class 4	6	as class 4	15	as class 4	6

defined a network operator has only one access point covering any virtual cell. One access point may cover several successive virtual cells, where the number of virtual cells is i.i.d.

Define b_d^A, b_d^B, b_d^C and b_d^D as the set of access points for the different network operators covering virtual cell d, where $b_d = b_d^A \bigcup b_d^B \bigcup b_d^C \bigcup b_d^D$. Scenario-class definitions are given in Table 2. E.g for scenario-class 5, the access points of network operator D provide coverage for a number of successive virtual cells, where the number is i.i.d. $\sim$ uniform$[1, 2]$. This means that for scenario-instances created from scenario-class 5 network operator D may have $2, 3$ or 4 access points covering 4 virtual cells. If network operator D has 4 access points in a scenario-instance created from scenario-class 5, this gives $b_d^D \neq b_{d+1}^D \neq b_{d+2}^D \neq b_{d+3}^D \neq \emptyset$ for it's successive coverage starting from a randomly selected virtual cell d.

From each scenario class in Table 2 it is created 100 scenario instances with dependability parameters as defined in Table 3 where all parameters have identical independent uniform distributions. Note that handover parameters $p_{i_{d-1}i_d}$ and $\beta_{i_{d-1}i_d}$ is only valid when $i_{d-1} \neq i_d$ otherwise $p_{i_{d-1}i_d} = 0$ and $\beta_{i_{d-1}i_d} = 0$. Sojourn time T_d in each virtual cell is i.i.d. $\sim$ uniform$[20, 30]$.

6.2 Results

For each graph, representing the scenario instance defined in Section 6.1, the greedy, Bhandari and ILP optimizations are used to find the series of access points S_{ij} given by their objective functions. We have used Mathematica 8 [Wol11] to implement the greedy and Bhandari optimizations. Mathematica computations were performed on a PowerEdge M610 blade with 2.67GHz quad-core CPU with 24GB memory running 64 bits Linux. For the ILP optimization we used the modelling language AMPL, version 20110302, with the commercial solver gurobi, version 4.0. The ILP optimization was solved on a virtual machine running Unix on a vmware server. The virtual machine was allocated 2GB memory (never a bottleneck for the scenarios) and two 2.4GHz CPUs.

The objective of the optimization is to find the optimal trajectory measured with the reliability metric $R_{S_{ij}}(t_{m_+})$ given in (1). Fig.7 shows boxplots of the differences between the algorithm with the highest $R_{S_{ij}}(t_{m_+})$ and each of the optimization methods for each scenario instance per scenario class.

Table 3. Dependability parameters for scenario-instances

		Values			
	Parameters	$i_{d+1} \in b^A_{d+1}$	$i_{d+1} \in b^B_{d+1}$	$i_{d+1} \in b^C_{d+1}$	$i_{d+1} \in b^D_{d+1}$
	$\lambda_{i_{d+1}}$	$U[1/998, 2/998]$	$U[2/998, 5/998]$	$U[1/998, 3/998]$	$U[1/998, 2/998]$
	$\mu_{i_{d+1}}$	$U[1/4, 1/2]$	$U[1/4, 1/2]$	$U[1/4, 1/2]$	$U[1/4, 1/2]$
$i_d \in b^A_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.02]$	$U[0.01, 0.04]$	$U[0.01, 0.03]$	$U[0.01, 0.04]$
	$\beta_{i_d i_{d+1}}$	$U[4, 8]$	$U[2, 4]$	$U[4, 8]$	$U[2, 4]$
$i_d \in b^B_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.04]$	$U[0.01, 0.03]$	$U[0.01, 0.04]$	$U[0.01, 0.05]$
	$\beta_{i_d i_{d+1}}$	$U[3, 6]$	$U[4, 8]$	$U[3, 6]$	$U[3, 6]$
$i_d \in b^C_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.03]$	$U[0.01, 0.04]$	$U[0.01, 0.04]$	$U[0.01, 0.04]$
	$\beta_{i_d i_{d+1}}$	$U[2, 4]$	$U[4, 8]$	$U[4, 8]$	$U[2, 4]$
$i_d \in b^D_d$	$p_{i_d i_{d+1}}$	$U[0.01, 0.04]$	$U[0.01, 0.02]$	$U[0.01, 0.02]$	$U[0.01, 0.03]$
	$\beta_{i_d i_{d+1}}$	$U[3, 6]$	$U[3, 6]$	$U[2, 4]$	$U[4, 8]$

For the scenario classes the mean of $R_{S_{ij}}(t_{m_+})_{ILP}$ as determined by the ILP optimization is shown above the boxplot for ILP in figure. The G-AM heuristic outperforms the G-RR and G-RM heuristic and is slightly better than the G-LM heuristic with respect to reliability of the trajectory found. Both the G-AM and G-LM take more of the dependability parameters into account than the G-RR and G-RM. For the Bhandari heuristic the B-RR is significant better than the other Bhandari heuristic optimizations. While the greedy heuristic improved with utilizing more of the dependability parameters, the Bhandari heuristic optimizations suffer. This is due to the way the edge weights are changed before the edge modifications are performed. But the B-AM performs better than the B-RM in the same manner as G-AM compared with G-RM. In the figure the optimization named G&B refers to the greedy or Bhandari heuristic that provides the highest reliability for a given scenario-instance. As can be observed, this combined heuristics shows a significant improvement of the reliability of the trajectory found. Both the greedy and Bhandari heuristic optimizations get worse compared to the ILP optimization when the number of virtual cells traversed and operators that may be used, i.e. the number of vertices and edges in the graph, gets larger. As can be seen in Fig.7, the ILP algorithm does provide the best reliability for any of the scenario instances since the boxplot for ILP has only value 0. But it must be noted that ILP optimization uses an approximation of the reliability, as objective function and thus, may not find the optimal trajectory.

In Fig.8 a boxplot is showing the time usage for the different algorithms to provide insight into to the computational effort of the methods. Note the log scale used on the ordinate. The exact time consumption is not of the main interest, but how the computation effort changes with increased number of vertices and edges in the graph. The time usage for ILP and

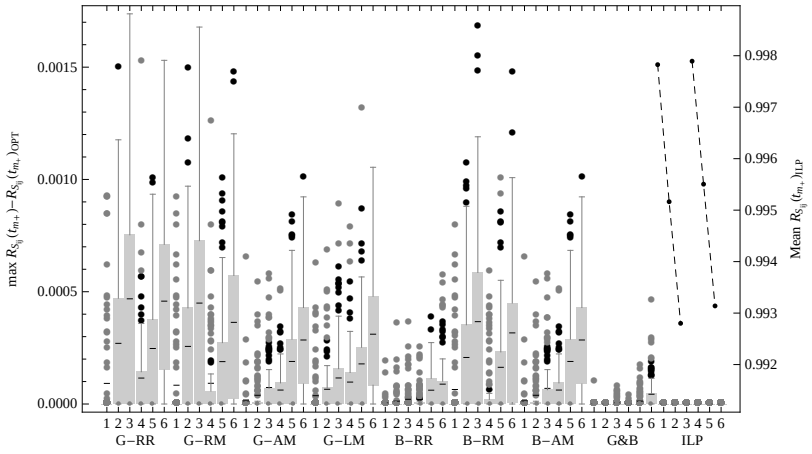

Figure 7. Reliability comparison is between the highest reliability found by any of the optimization methods for the scenario instance. G&B in the graph refers to the best of the greedy and Bhandari algorithms. Above the boxplot for ILP, the mean of $R_{S_{ij}}(t_{m_+})_{ILP}$ is shown for each scenario-class.

heuristic optimizations are not directly comparable since the optimizations were performed on different HW. However, when computing the ILP optimization with Mathematica and same HW as the heuristics optimizations the average time usage for scenario-class 3 and 6 increased approximately four times. As expected the time consumption of ILP optimization is extremely sensitive to number of vertices and edges in the graph, with the benefit of finding a trajectory with best reliability of the optimization methods.

A common heuristic in managing connectivity in wireless networks is to minimize the number of handovers. Handovers are not explicitly addressed in any of the optimizations in this paper. However the optimizations have used the reliability as the main criterion where reliability of handovers are taken into account. As such a handover is only performed when this gains the reliability. On this background it is interesting to regard and compare the number of handovers used by the optimizations. Fig.9 shows the number of handovers for each scenario-class for the different methods as distribution charts. Each distribution chart is drawn as histogram bars for the number of handovers for scenario-instances. The width of a histogram bar represents the number of scenario-instances with the same number of handovers. For the algorithm named G&B the number of handovers are taken from the greedy or Bhandari heuristic that provides the highest reliability. In case a tie, the lowest number of handovers is chosen. The number of handovers is reduced when the availability is used to find S_i for the heuristic optimization compared with

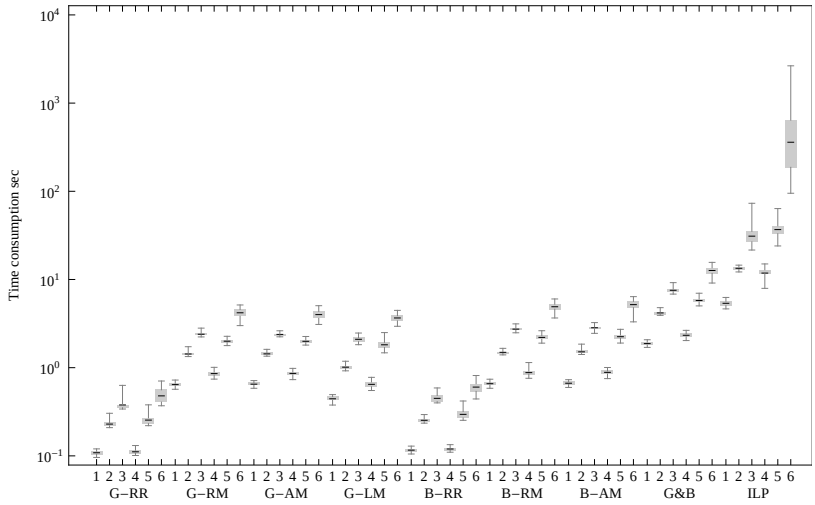

Figure 8. Time usage for finding trajectory given the objective functions for the optimization methods. Note that the ILP and the heuristic optimizations were performed on different HW configurations. Computing ILP optimization with Mathematica and same HW as the heuristics optimizations increased the average time four times for scenario-class 3 and 6.

use of reliability since G-AM and B-AM find trajectories with less number of handovers than G-RR, G-RM, B-RR and B-RM. In addition, G-AM and B-AM find trajectories with higher reliability than G-RR, G-RM, B-RR and B-RM as shown in Fig.7. As can be observed in Fig.9 the ILP optimization, from an overall perspective, performs quite well also for the number of handovers as metric.

7. Conclusion

For critical services the reliability is crucial. We have proposed methods for finding the near-optimal trajectory for a dual homed session that can be used by multihoming protocols. The optimization methods utilize in different ways the dynamics and dependencies modelled with a continuous time discrete space Markov model for traversal virtual cells along the projected route. With global handover strategy, i.e. considering the total projected route of an user, a significantly improved reliability can be achieved compared with local hop-by-hop handover decisions. ILP optimization finds the trajectory with the highest reliability compared with the greedy and Bhandari heuristic optimizations for any scenario-instance. However, using the trajectory with the highest reliability found by any of the greedy or Bhandari heuristic optimizations shows a significant improvement of the reliability compared with the ILP for any

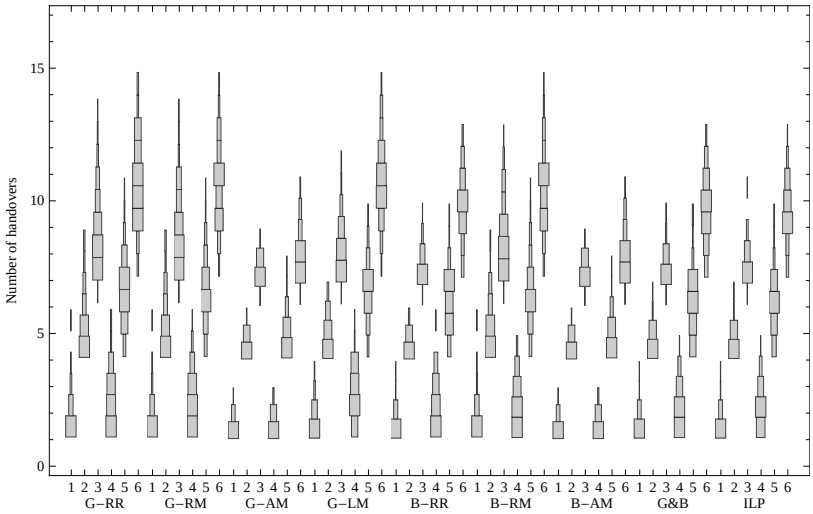

Figure 9. Distribution chart of number of handovers for trajectories found by the optimization methods. The width of a histogram bar represents the number of scenario-instances with the same number of handovers.

scenario-instance. The computational effort of ILP is still much higher than all greedy and Bhandari heuristic optimizations together for any scenario-instance. It is also observed that, from an overall perspective, the ILP optimization has the lowest overall number of handover performed which is accordance with current practice in operations of cellular networks.

References

[AS08] A. Andreas and J. Smith. Mathematical programming algorithms for two-path routing problems with reliability considerations. *INFORMS Journal on Computing*, 20(4):553–564, 2008.

[Bel56] R. Bellman. On a routing problem. *NOTES*, 16(1), 1956.

[Bha99] R. Bhandari. *Survivable networks: algorithms for diverse routing.* Kluwer Academic Pub, 1999.

[CSK02] W. Cui, I. Stoica, and R. Katz. Backup path allocation based on a correlated link failure probability model in overlay networks. In *Proc. 10th IEEE International Conference on Network Protocols*, pages 236–245, Paris, France, November 12–15 2002.

[Dij59] E. W. Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1:269–271, 1959. 10.1007/BF01386390.

[FH13b] E. L. Følstad and B. E. Helvik. Reliability modelling of access point selection and handovers in heterogeneous wireless environment. In *Proc. 9th International*

Conference on the Design of Reliable Communication Networks DRCN 2013, pages 103–110, Budapest, Hungary, March 4–7 2013.

[IEE08] IEEE 802.21,D11; Draft standard for local and metropolitan area networks: Media indepenedent handover services, 2008.

[LML10] H.-W. Lee, E. Modiano, and K. Lee. Diverse routing in networks with probabilistic failures. *IEEE/ACM Transactions on Networking*, 18(6):1895–1907, December 2010.

[SR93] S. Soh and S. Rai. Experimental results on preprocessing of path/cut terms in sim of disjoint products technique. *IEEE Transactions on Reliability*, 42(1):24–33, 1993.

[Suu74] J. W. Suurballe. Disjoint paths in a network. *Networks*, 4(2):125–145, 1974.

[Wat67] L. J. Watters. Reduction of integer polynomial programming problems to zero-one linear programming problems. *Operations Research*, 15(6):1171–1174, 1967.

[Wol11] Wolfram Research, Inc. Documentation centre. `http://reference.wolfram.com/mathematica/guide/Mathematica.html`, 2011.

PAPER H

Using genetic algorithms for optimizing the reliability of dual homed wireless sessions

Eirik Larsen Følstad and Bjarne E. Helvik

Proceedings of the 6th International Workshop on Reliable Networks Design and Modeling (RNDM)

Barcelona, Spain, November 2014

USING GENETIC ALGORITHMS FOR OPTIMIZING THE RELIABILITY OF DUAL HOMED WIRELESS CRITICAL SERVICES

Eirik Larsen Følstad, Bjarne E. Helvik
Department of Telematics
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@item.ntnu.no

Abstract The wireless access to any service in different contexts is nowadays taken for granted. However, the dependability requirements are different for various services and contexts. Critical services put high requirement on the service reliability, i.e., the probability of no service interruption should be close to one. Dual homing may be used to increase the service reliability in a multi technology, multi operator wireless environment, where the user's mobility necessitates access point selections and handovers. To allow the user to assess the risk of the service session, a prediction of the service reliability is necessary. This prediction must fulfil the need for the optimal sequence of access point selections and handovers with regard to service reliability and being computation efficient to accomplish the need for the real-time operation. We demonstrate how Genetic Algorithm (GA) may be used to predict and to improve the (near) optimal service reliability by fast and simple heuristics, far more computationally efficient than an Integer Linear Programming (ILP) optimization.

Keywords: Critical services, wireless networks, reliability, genetic algorithms, optimization

1. Introduction

The evolution of wireless technologies, such as e.g., local area network (WLAN), High Speed Data Access (HSPA) and Long Term Evolution (LTE) combined with the widespread use of smartphones [BGC12] have made the wireless the preferred access service. Various contexts and services demand different dependability requirements.

For critical services, like emergency handling, health care services, energy control and surveillance/monitoring, the service reliability is crucial. In such contexts, the probability of no service interruption should be close to one. Dual homing protocols, such as mobile stream control transmission protocol [SXM+00] and Site Multihoming by IPv6 Intermediation (SHIM6) [EN09], may

be used to increase the service reliability where the diversity of the wireless accesses are utilized across different technologies and network operators.

Networks are evolving and network topologies change rapidly. As critical services may be started at any location there is a need at run-time to predict and to identify the access points and handovers along a projected route to allow the user to assess the risk before starting the critical service. A projected route is the physical movement of the user. Optional routes may for instance by found by means of navigation tools. For each of these there is a probability that the service may be completed without failures, i.e., no interrupts. A model for prediction of service reliability of a dual homed critical service is established [FH13b].

The objective of this paper is to show that genetic algorithms (GA) may be used to effectively combine simple and fast heuristics to find an optimal or near optimal route. This approach closes the gap between the service reliability obtained by straightforward heuristics and the optimal obtained by Integer Linear Programming (ILP) optimization, which is computationally too demanding in an operational system.

A trajectory is defined as series of access points used for each of the two radio connections for a dual homed critical service along a projected route. Most handover algorithms and dual homing protocols use local hop-by-hop based decisions and do not consider all handovers during a service session. The use of the optimal trajectory may be considered as a global based handover strategy optimized for service reliability.

The service reliability is measured by the metric $R(t_m) = P(T_{FF} > t_m)$ where T_{FF} is time to first failure and t_m is the mission time. Assume a network scenario as depicted in Fig.1. Planned access coverage, indicated by ellipses, is provided by three operators named A, B, and C with their access points $A1$, $A2$, $B1$ and $C1$ respectively. The access points may provide coverage from different technologies. An arrow in Fig.1 represents the projected route. At the starting location, the objective is at run-time to derive the trajectory with (near) optimal service reliability.

The work in this paper is based on model for prediction of service reliability of a dual homed critical service in a multi technology, multi operator wireless environment, [FH13b], briefly outlined in Section 2. This prediction model defines the concept of virtual cells as limited geographical areas where the radio conditions are homogenous. Handovers are performed between the virtual cells and effectively limit the number of trajectories for a projected route. Virtual cells are indexed according to the order they are visited from 1 to m along the projected route. Access points covering virtual cell d is identified with the set b_d. Let a trajectory be identified by $S_{ij} = \{(i_1, j_1), \ldots, (i_d, j_d), \ldots, (i_m, j_m)\}$ where $i_d, j_d \in b_d$, $i_d \neq j_d$ and i and j are the two connections for the dual homed critical service. The user will traverse a number of virtual cells, shown as hexagons in Fig.1, along the projected route. The objective of this paper is

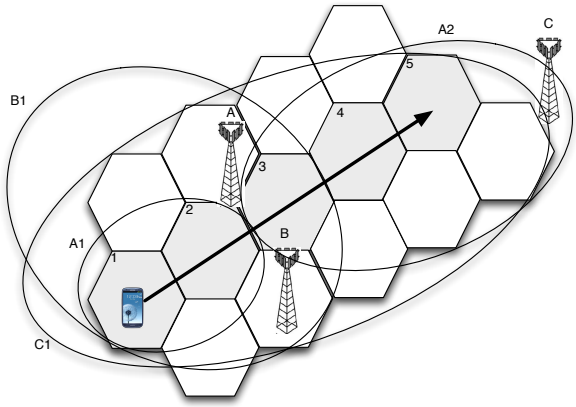

Figure 1. Example network with three network operators (A, B and C) and their access points (A1 and A2, B1 and C1 respectively), with planned access coverage (ellipses). Along a projected route (arrow) the user moves through a number of virtual cells (hexagons).

to efficiently find the trajectory with the (near) optimal service reliability, i.e.,

$$\arg\max_{S_{ij}} R_{S_{ij}}(t_m) \tag{1}$$

In [FH13a] the optimal trajectory was derived by ILP optimization using the model from [FH13b]. It was shown that increased service reliability might be obtained with global handover strategy compared with a local hop-by-hop strategy when reliability is being optimized. Heuristics were proposed based on Dijkstra [Dij59] and Bhandari [Bha99] for computation efficiency on behalf of the optimality of the trajectory. We use GA combined with results of the heuristics in [FH13a] to improve the (near) optimal trajectory while still being computational efficient compared with an ILP optimization.

The term genetic algorithm was coined by Holland [Hol92]. An introduction to GA may be found in [Ree10]. In [DAS97a] it is proposed how GA may be used for finding (near) optimal all-terminal network topology considering cost and reliability. A variable-length chromosome and population sizing are presented in [AR02] for shortest path routing. Both [DAS97a] and [AR02] pinpoint the challenges for efficient fitness function and control parameters. It is possible to identify the optimal GA control parameters for the desired optimization, but this may itself be a time demanding task [Gre86]. Repair functions are described in [AR02] and [DAS97b] for chromosomes representing infeasible paths in networks. We propose a GA where chromosomes have identical length for a projected route, and the initial population is initialized with chromosomes

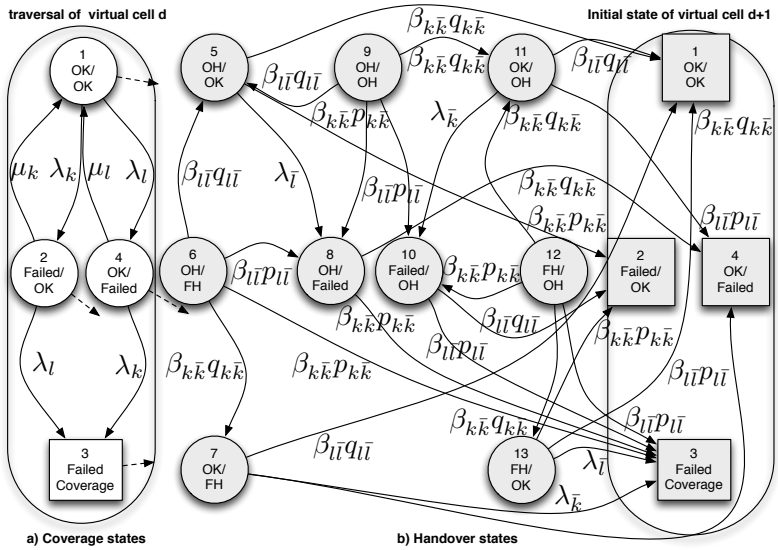

Figure 2. State transition diagram for traversal of virtual cell d and handover to cell $d+1$. Absorbing handover states (grey shaded) represent the initial conditions for traversal of cell $d+1$. Transitions into handover states are modelled as instantaneous transition given by S_{ij}.

from heuristics to allow fast convergence. The chromosome structure and the fitness function allow efficient crossover and mutation procedures without complex repair.

The rest of the paper is organized as follows. First in Section 2 we present the proposed model, while Section 3 describes the proposed GA and functionality. Several network scenarios are described and generated in 4 with stochastic characteristics for verifying the performance of the GA in Section 5. Section 6 concludes the paper.

2. Dependability model of a trajectory

In the following we describe how the reliability of a trajectory of a dual homed critical service is predicted. The reliability will be used as the basis for fitness value for the chromosomes in the GA.

In [FH13a] the reliability modelling of a trajectory is described as a phased mission. Each phase corresponds to handover from previous cell $d-1$ and traversal of virtual cell d, modelled as a continuous time discrete space Markov model as given in Fig.2. The names of the states are according to the state of the two connections of a trajectory S_{ij}. For instance, the state OK/OK indicates that both connections are working and the state FH/OH indicates that connection i has a failed radio connection and executing handover while

connection j has a working radio connection and executing a handover. The dependability parameters and attributes are obtained from measurement reports for user equipment and signalling in the networks, as explained in [FH13b]. Handover states $\Omega_H = \{5, 6, ..., 13\}$ are grey, while the white ones are coverage states $\Omega_C = \{1, 2, 3, 4\}$ since loss of radio connection is the main cause of failure within a virtual cell. Transitions into Ω_H are modelled as instantaneous transition given by S_{ij} and will be described later in this section. The change from phase d to $d+1$ takes place at time t_d and the sojourn time of phase d is T_d.

To keep the notation simple, we will in the rest of the paper use the index i_d for dependability parameters and attributes for an access point i_d in a virtual cell d, i.e., $\lambda_{id,d} \rightarrow \lambda_{id}$. In Fig.2 the indexes $k = i_d$, $\bar{k} = i_{d+1}$ and $l = j_d$, $\bar{l} = j_{d+1}$. A radio connection between a user equipment and an access point i_d covering virtual cell d has a constant radio coverage failure intensity λ_{i_d}. The radio coverage from different access points fail independently. When a radio connection to access point i_d has been lost, the time to recover is n.e.d with mean $1/\mu_{i_d}$ in cell d. Handover time from i_d to i_{d+1} is n.e.d. with mean $1/\beta_{i_d i_{d+1}}$ and may fail with a probability of $p_{i_d i_{d+1}}$ where $q_{i_d i_{d+1}} = 1 - p_{i_d i_{d+1}}$. In case of dual handovers, the handovers fail independently.

Based on the model and results from [FH13a], the reliability of a trajectory may be written as

$$\hat{R}_{S_{ij}}(t_{m\_}) = \hat{R}_1(T_{1\_}) \prod_{d=2}^{m} \hat{R}_d \left(T_{d\_} | T_{FF} > t_{d-1}\right) \tag{2}$$

where $\hat{R}_d(T_{d\_}|T_{FF} > t_{d-1})$ represents the reliability of phase d. The notations $t_{d\_}$ and t_{d_+} are used to indicate instants immediately before and after the handover that takes place. Transition intensity matrices for Fig.2 may be organized as

$$\Lambda_C = \begin{bmatrix} \Lambda_{CC} & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \Lambda_H = \begin{bmatrix} 0 & \Lambda_{HC} \\ 0 & \Lambda_{HH} \end{bmatrix} \tag{3}$$

where Λ_{CC} is the transition intensity matrix for Ω_C, Λ_{HH} is the transition intensity matrix for Ω_H and Λ_{HC} is the transition intensity matrix for intensities from Ω_H to Ω_C. As described in [FH13b], the approximated normalized transient probability of working states $\hat{p}(T_{d\_}|T_{FF} > t_d) = \{\dot{p}_1, \dot{p}_2, 0, \dot{p}_4, 0, 0, 0, 0, 0, 0, 0\}^T$, where $\dot{p}_2 = \dot{p}_1 \lambda_{i_d}/\mu_{i_d}$ and $\dot{p}_4 = \dot{p}_1 \lambda_{j_d}/\mu_{j_d}$ and $\dot{p}_1 + \dot{p}_2 + \dot{p}_4 = 1$. The approximation holds as long as time spent in virtual cell T_d is more than the largest of $4/\mu_{i_d}$ and $4/\mu_{j_d}$.

By neglecting the handover time, the state just after handover is given as $p(T_{d_+}) = (\Pi_H)^3 p(T_{d\_}|T_{FF} > t_d, I_d)$ where Π_H is the transition probability matrix of Λ_H and $I_d = |i_d \cap i_{d+1}||||j_d \cap j_{d+1}|$ is the indicator function for the handovers. Only 3 operations are necessary since 3 is the largest path from an initial to an absorbing state in Ω_H. The instantaneous transitions from Ω_C to

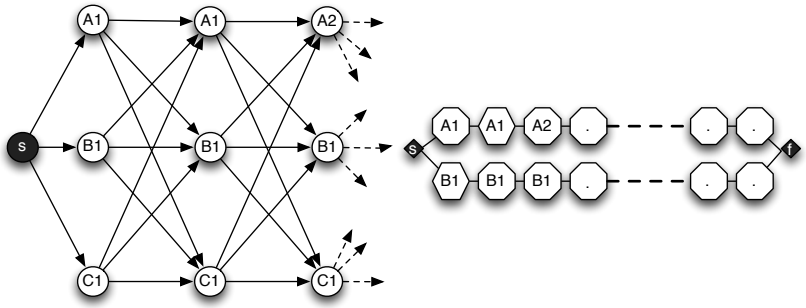

Figure 3. A graph model of the example network in Fig.3 with sketch indicating all possible trajectories and a chromosome representing one specific trajectory.

Ω_H are given by

$$
\begin{aligned}
&p(T_{d\_}|T_{FF} > t_d, I_d = 11) = \dot{p}(T_{d\_}|T_{FF} > t_d) \\
&p(T_{d\_}|T_{FF} > t_d, I_d = 01) = [0, \ldots, \dot{p}_1, 0, 0, \dot{p}_4, 0, 0, 0, 0, \dot{p}_2]^T \\
&p(T_{d\_}|T_{FF} > t_d, I_d = 10) = [0, \ldots, \dot{p}_4, 0, 0, \dot{p}_2, \dot{p}_1, 0, 0]^T \\
&p(T_{d\_}|T_{FF} > t_d, I_d = 00) = [0, \ldots, \dot{p}_4, 0, 0, \dot{p}_1, 0, 0, \dot{p}_2, 0]^T
\end{aligned} \tag{4}
$$

The traversal of cell d is given by $\Lambda_C p(t) = dp(t)/dt$ with the initial condition $p(0)$. For first phase $p(0) = \{1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}^T$ and for phase d is $p(0) = \{p_1(T_{d-1_+}), p_2(T_{d-1_+}), p_3(T_{d-1_+}), p_4(T_{d-1_+}), 0, \ldots, 0\}^T$. This yields the reliability of phase d

$$
\hat{R}_d(T_{d\_}|T_{FF} > t_{d-1}) = 1 - p_3(T_{d\_}) \tag{5}
$$

When the (near) optimal trajectory is found by using the approximation given by (5), the actual trajectory reliability , $R_{S_{ij}}(t_{m\_})$, may be calculated by using $\hat{p}(T_{d\_}|T_{FF} > t_d) = \{p_1(T_{d\_}), p_2(T_{d\_}), 0, p_4(T_{d\_}), 0, 0, 0, 0, 0, 0, 0\}^T$.

In the following we will describe how $\hat{R}_{S_{ij}}(t_{m\_})$ is used by GA.

3. Description of GA

Each of the main procedures in GA will now be described along with the use of the heuristics in [FH13a] to improve the (near) optimal trajectory for a dual homed critical services. First the chromosome structure and the related fitness value are introduced.

3.1 Chromosome and fitness

It is seen that we may let the trajectory S_{ij} represents a chromosome, where (i_d, j_d) being the d'th gene-pair. The example network in Fig.1 is represented

by a graph model as shown in Fig.3 that indicates all possible trajectories. One specific trajectory is shown as a chromosome in the figure where its third gene-pair is $(A2, B1)$.

A chromosome S_{ij} is given a fitness value according to the function

$$f_{S_{ij}} = \frac{1}{1 - \hat{R}_{S_{ij}}(t_{m\_})} \tag{6}$$

The chromosome representing the trajectory with the highest reliability is given by $\arg\max_{\forall S_{ij}} \hat{f}_{S_{ij}}$.

For making the GA computationally efficient the approximation of the reliability derived in (2) is used. The exact service reliability could be used for the chromosome fitness, but this would be far more computation demanding.

3.2 Initialization

The initialization procedure introduces a population, called generation 1 as G_1, with $|G_1| = n$ feasible chromosomes, where each chromosome S_{ij} fulfils the constraints

$$|S_{ij}| = m, \forall (i,j) \tag{7}$$

$$\forall (i_d, j_d) \in S_{ij}, \text{where } i_d, j_d \in b_d, \forall d = 1, \ldots, m \tag{8}$$

$$\forall (i_d, j_d) \in S_{ij}, \text{where } i_d \neq j_d, \forall d = 1, \ldots, m \tag{9}$$

The size of the population, n, is be kept constant during the evolution of the population.

The goal with the GA is to close the gap between the service reliability of the trajectories obtained with the heuristics and ILP optimization in [FH13a] and still be computation efficient. The initial population may therefore be initialized with chromosomes representing the trajectories obtained with heuristics (further explained in Section 5). A random initialized population may also be generated to benchmark the use of the heuristics initialization.

3.3 Selection

The selection is either a roulette or a tournament process. Both selection processes allow some chromosomes to be selected several times and others to not be selected at all.

For the roulette selection the probability $p_{S_{ij}}$ for choosing the chromosome S_{ij} from the population G_c is proportional to its relative fitness, i.e.,

$$p_{S_{ij}} = \frac{f_{S_{ij}}}{\sum_{\forall S_{kl} \in G_c} f_{S_{kl}}} \tag{10}$$

From generation G_c n chromosomes are randomly selected according to their relative fitness and constitutes the intermediate population $\hat{G}_c$.

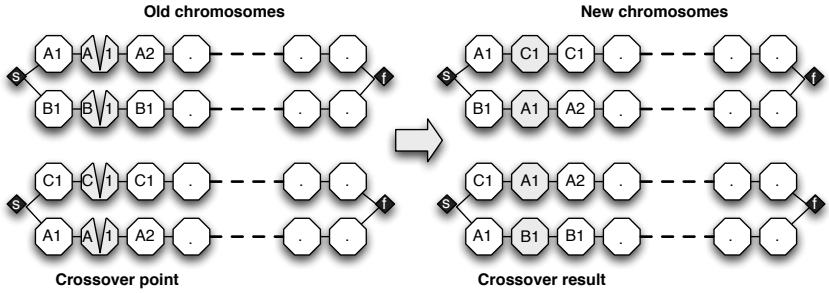

Figure 4. Example of crossover between two chromosomes of Fig.3.

For the tournament selection process, n pairs of chromosomes are compared and the chromosome with the highest fitness from each pair value is selected. A chromosome is appointed with probability $1/n$ for a tournament. The winners of all tournaments constitute the intermediate population $\hat{G}_c$.

3.4 Crossover

After the selection process described in Subsection 3.3 the intermediate population $\hat{G}_c$ undergoes a crossover procedure. From the randomly ordered set of chromosomes consecutive pairs of chromosomes are selected for crossover with an i.i. probability p_c. Say that the chromosomes S_{ij} and S_{kl} are selected for crossover. The crossover point $x \sim \text{uniform}[1, m]$ and the two new chromosomes are obtained as $S_{\hat{ij}} = \{(i_1, j_1), \ldots, (k_x, l_x), \ldots, (k_m, l_m)\}$ and $S_{\hat{kl}} = \{(k_1, l_1), \ldots, (i_x, j_x), \ldots, (i_m, j_m)\}$.

In Fig.4 the crossover operation between a pair of chromosomes from Fig.3 is depicted. At the left hand side of the figure the marked chromosomes and the gene-pair position 2 for crossover are identified. The halves defined by the crossover point are interchanged between the chromosomes, as shown at the right hand side of the figure. Note that since a handover between $i_d \in b_d$ and any $i_{d+1} \in b_{d+1}$ is possible and since $|S_{ij}| = |S_{kl}|$ there is no need for a repair after a crossover.

3.5 Mutation

After the crossover procedure the intermediate population $\hat{G}_c$ undergoes a mutation procedure. Unlike the crossover, the mutation procedure allows for mutation of multiple genes in a chromosome. Each gene of a chromosome is mutated with an i.i. probability p_m. Define an indicator function $I(ij)$ for the chromosome S_{ij} where $I(i_d) = 1$ if mutation is introduced for gene i_d of connection i. Likewise is defined for $I(j_d)$. Let's say a mutation is introduced only in

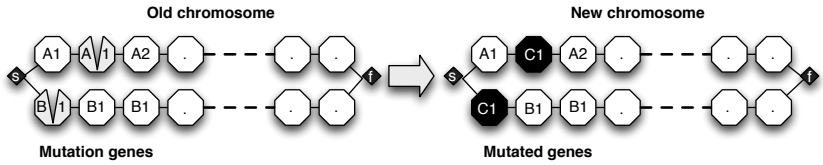

Figure 5. Example of mutation at two genes of a chromosome of Fig.3.

gene i_d of chromosome S_{ij}. If $|b_d| > 2$ the mutated chromosome, $S_{ij}^{I(ij)}$, becomes $S_{ij}^{I(ij)} = \{(i_1, j_1), \ldots, (k_d, j_d), \ldots, (i_m, j_m)\}$ where $k_d \sim$ uniform $[b_d \setminus \{i_d, j_d\}]$. For the cases where $|b_d| = 2$ then $S_{ij}^{I(ij)} = \{(i_1, j_1), \ldots, (j_d, i_d), \ldots, (i_m, j_m)\}$. This may be seen as a simple repair for not violating constraint (9).

A mutation of a chromosome S_{ij} from Fig.3 is shown in Fig.5. Here the mutations are marked at the lower half of gene-pair 1 and at the upper half of gene-pair 2, i.e., $I(j_1) = 1$ and $I(i_2) = 1$, as shown at the left hand side of the figure. At the right hand side of the figure the mutated genes are shaded black for the mutated chromosome $S_{ij}^{I(ij)}$. For instance, to mutate gene i_2 the possible access points are $b_2 \setminus \{A1, B1\}$ that reduces to $\{C1\}$ since $b_2 = \{A1, B1, C1\}$.

3.6 Elitism

In our implementation of the GA we can use none, simple or global elitism. In all cases the best fitted chromosome found in any generation is stored.

Without elitism the new population is equal the intermediate population after the crossover and mutation procedures, where $G_{c+1} = \hat{G}_c$.

When simple elitism is used the new population is the best fitted chromosomes from previous population and $n-1$ best chromosomes from intermediate population, i.e., $G_{c+1} = (S_{ij} \cup (\hat{G}_c \setminus S_{xy})$, where $S_{ij} = \arg\max f_{S_{kl}}, \forall S_{kl} \in G_c$ and $S_{xy} = \arg\min f_{S_{kl}}, \forall S_{kl} \in \hat{G}_c$.

With global elitism the new population is the n best fitted chromosomes from the previous and the intermediate population.

4. Reference cases for comparisons

To compare the reliability of the trajectory found by GA with the optimal trajectory found by ILP optimization, we define a number of scenario-classes adapted from [FH13a]. The scenario-classes are basis for scenario-instances that represent a graph model of a network, similar as shown in Fig.3.

In [FH13a] it is described six scenario-classes, each with a defined number of virtual cells and network operators providing radio coverage with maximum one access point each per virtual cell. A network operator provides radio coverage for successive virtual cells along the projected route where one access point

Table 1. Scenario-classes and operator access coverage

		Characteristics							
		Coverage Operator A		Coverage Operator B		Coverage Operator C		Coverage Operator D	
Class	Cells	cells per AP	total cells	cells per AP	total cells	cells per AP	total cells	cells per AP	total cells
1	5	U[2,3]	5	2	2	5	5		
2	10	as class 1	10	as class 1	4	as class 1	10		
3	15	as class 1	15	as class 1	6	as class 1	15		
4	5	U[2,3]	5	2	2	5	5	U[1,2]	2
5	10	as class 4	10	as class 4	4	as class 4	10	as class 4	4
6	15	as class 4	15	as class 4	6	as class 4	15	as class 4	6

Table 2. Dependability parameters for scenario-instances

	Parameters	**Values** (for λ, μ and β the unit is s^{-1}) $i_{d+1} \in b_{d+1}^A$	$i_{d+1} \in b_{d+1}^B$	$i_{d+1} \in b_{d+1}^C$	$i_{d+1} \in b_{d+1}^D$
	$\lambda_{i_{d+1}}$	$U[1/998, 2/998]$	$U[2/998, 5/998]$	$U[1/998, 3/998]$	$U[1/998, 2/998]$
	$\mu_{i_{d+1}}$	$U[1/4, 1/2]$	$U[1/4, 1/2]$	$U[1/4, 1/2]$	$U[1/4, 1/2]$
$i_d \in b_d^A$	$p_{i_d i_{d+1}}$	$U[0.01, 0.02]$	$U[0.01, 0.04]$	$U[0.01, 0.03]$	$U[0.01, 0.04]$
	$\beta_{i_d i_{d+1}}$	$U[4, 8]$	$U[2, 4]$	$U[4, 8]$	$U[2, 4]$
$i_d \in b_d^B$	$p_{i_d i_{d+1}}$	$U[0.01, 0.04]$	$U[0.01, 0.03]$	$U[0.01, 0.04]$	$U[0.01, 0.05]$
	$\beta_{i_d i_{d+1}}$	$U[3, 6]$	$U[4, 8]$	$U[3, 6]$	$U[3, 6]$
$i_d \in b_d^C$	$p_{i_d i_{d+1}}$	$U[0.01, 0.03]$	$U[0.01, 0.04]$	$U[0.01, 0.04]$	$U[0.01, 0.04]$
	$\beta_{i_d i_{d+1}}$	$U[2, 4]$	$U[4, 8]$	$U[4, 8]$	$U[2, 4]$
$i_d \in b_d^D$	$p_{i_d i_{d+1}}$	$U[0.01, 0.04]$	$U[0.01, 0.02]$	$U[0.01, 0.02]$	$U[0.01, 0.03]$
	$\beta_{i_d i_{d+1}}$	$U[3, 6]$	$U[3, 6]$	$U[2, 4]$	$U[4, 8]$

may cover several successive virtual cells. In cases where a network operator provides coverage for only a part of the projected route, the first virtual cell is randomly selected. The scenario-class definitions are given in Table 1. Note that only network operators A and C provide coverage for all virtual cells. From each of the scenario-classes 100 scenario-instances were created with dependability parameters as defined in Table 2 where all parameters are i.i.d. uniform distributions and where sojourn time T_d in each virtual cell is i.i.d. $\sim$ uniform$[20, 30]$ seconds. The access points covering a virtual cell d is given by $b_d = b_d^A \bigcup b_d^B \bigcup b_d^C \bigcup b_d^D$ where b_d^A, b_d^B, b_d^C and b_d^D are the set of access points for the different network operators covering virtual cell d.

For 80 of total 600 scenario-instances, none of the seven heuristics in [FH13a] found the optimal trajectory as identified by the ILP optimization. These 80 scenario-instances are the reference cases used for comparing the performance of GA with the heuristics and ILP. The reference cases are numbered from 1 to 80, where reference case numbered 1 belongs to scenario-class 1, references $2, \ldots, 10$ to class 3, $11, \ldots, 14$ to class 4, $15, \ldots, 36$ to class 5 and $37, \ldots, 80$ to class 6.

Table 3. Overview of total 22 different GA control parameter sets

Selection	Initialization	Crossover, p_c	Mutation, p_m	Elitism
{Roulette,Tournament}	Heuristics	0.95	0.01	{None, Simple, Global}
{Roulette,Tournament}	Heuristics	0.70	0.01	{None, Simple, Global}
{Roulette,Tournament}	Random	0.95	0.01	{None, Global}
{Roulette,Tournament}	Random	0.70	0.001	{None, Global}
{Roulette,Tournament}	Heuristics	0.95	0.03	Global

5. Results

In the following, the reliability of the trajectories for different scenario-instances found by the GAs are compared with the optimal trajectories as identified by the ILP optimization. Details of the ILP optimization are found in [FH13a].

A total of 22 different GA control parameter sets were defined and are summarized in Table 3. The sets are named according to values of the control parameters, for example R-H-95-03-G defines roulette (R) selection, heuristics (H) initialization, $p_c = 0.95$, $p_m = 0.03$ and global (G) elitism. The heuristics initialization refers to an initial population with the seven chromosomes representing the results from the seven heuristics in [FH13a] along with 93 randomly created chromosomes. All parameters sets have a population size of $n = 100$.

For each of the reference cases as defined in Section 4 100 replications of the GA are run with exit criteria of maximum 100 generations or when the difference between the max and average fitness of a generation is less than 10^{-9}. The GA was implemented in Mathematica 8 [Wol11] running on a PowerEdge M610 blade with 2.67GHz quad-core CPU with 24GB memory and a 64 bits Linux kernel.

5.1 Heuristics (H) vs. random (R) initialization

The objective is to investigate whether the initialization based on the heuristics, allows the GA to find the optimal trajectory as identified by an ILP optimization or a (near) optimal trajectory better than those found by the heuristics. A heuristics initialized GA provides at least as reliable trajectory as the best of the heuristics since the best fitted chromosome are always stored during the evolution of the population. To visualise the reliability of the trajectories obtained by the GA with the parameter set R-H-95-03-G for the different reference cases, a boxplot is presented in Fig.6. The boxplot includes the 25% and 75% quantiles with the median and outliers of the difference between reliability of the trajectories found by the each replication of R-H-95-03-G and the optimal trajectory found by the ILP optimization, i.e., $R_{S_{ij}}(t_{m\_})_{ILP} - R_{S_{kl}}(t_{m\_})_{GA}$. The reference cases within each scenario-class are sorted according to the medians of the differences. In the figure the differences between the trajectory reliability obtained by ILP optimization and the best of the heuristics are depicted as a dashed line for each reference case. The reliability of the optimal trajectory identified by the ILP optimization

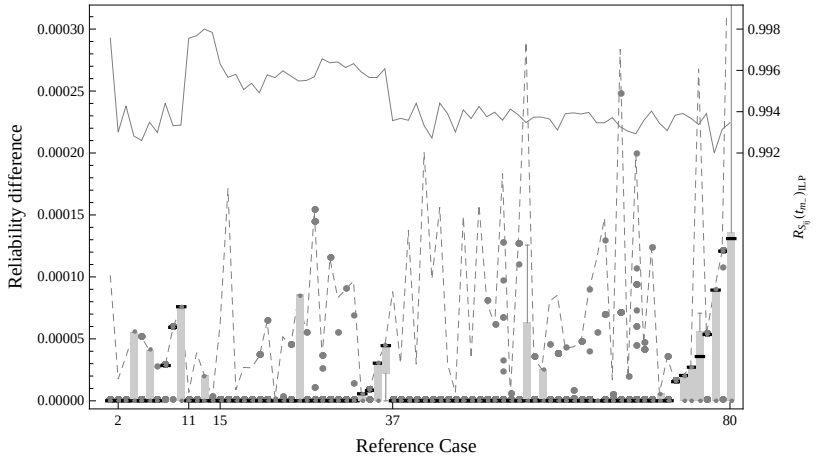

Figure 6. Boxplot of $R_{S_{ij}}(t_{m\_})_{ILP} - R_{S_{kl}}(t_{m\_})_{GA}$ with median and outliers for parameter set R-H-95-03-G. The dashed line represents the differences between the ILP optimization and the best of the heuristics. The solid line represents the reliability of the optimal trajectory identified by the ILP optimization. Observe that the optimal trajectories except for the reference case 73 are found. In addition, except for the reference case $78, 79, 80$, the 75% quantiles of the differences are less than 10^{-4}.

is represented with the solid line in the figure. As may be seen in Fig. 6, the parameter set R-H-95-03-G finds the optimal trajectories except for the reference case 73 and for the reference case other than $78, 79$ and 80, the 75% quantiles of the differences are less than $1 \cdot 10^{-4}$. As indicated in Fig. 6, the differences of the reliability of the trajectories found by ILP optimization and the set R-H-95-03-G are not directly related to the reliability of the optimal trajectory identified by the ILP optimization.

The parameter set R-H-95-03-G obtained the overall best results, determined by medians and standard deviations of the reliability of the trajectories for the reference cases, compared with other parameter sets using heuristics initialization, as classified in Table 3. It may be noted that a) GA with parameter sets using heuristics initialization without elitism obtained significantly worse results than the R-H-95-03-G while b) the sets T-H-95-03-G, R-H-95-01-G and T-H-95-01-G obtained slightly reduced results, but specific reduced results for reference case 80.

To investigate whether the global elitism combined with heuristics initialization cause the GA to converge to local optimums, the initialization based on heuristics was omitted. The resulting boxplot is shown in Fig. 7 for the set R-R-95-01-G. As may be seen, the overall results, determined by medians and quantiles for the trajectories reliabilities obtained, get significantly worse

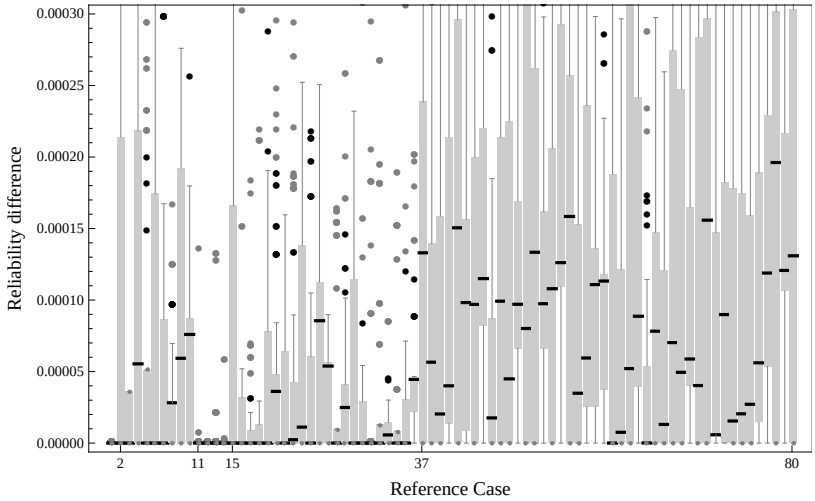

Figure 7. Boxplot of $R_{S_{ij}}(t_{m\_})_{ILP} - R_{S_{kl}}(t_{m\_})_{GA}$ with median and outliers for parameter set R-R-95-01-G. Observe that the parameter set R-R-95-01-G only rarely finds the to the optimal solution as identified by ILP optimization and significantly less frequent than the set R-H-095-03-G.

than the set R-H-95-03-G. Observe that the parameter set R-R-95-01-G only rarely finds the optimal solution as identified by the ILP optimization and significantly less frequent than the set R-H-095-03-G. For the parameter sets with random initialization without elitism the results were even significantly worse than the set R-R-95-01-G. Using simple elitism, the parameter sets T-H-95-01-S and R-H-95-01-S, improved the means and standard deviation of the trajectories reliabilities for the reference cases 78, 79 and 80, but overall they found less optimal trajectories for the other reference cases.

With the GA parameters sets and the reference cases studied these results indicate that a GA with heuristics initialization combined with global elitism is a good candidate for finding (near) optimal trajectories.

5.2 Computation effort

In Section 5.1 the reliability of a trajectory found by GA was compared with the optimal trajectory found by the ILP optimization. We now compared the computation effort of the GA compared with an ILP optimization [FH13a].

As indicated in Fig.6, a number of replications of the GA may be needed to ensure that the (near) optimal trajectory is found for each of the reference cases. The difference of the reliability of the trajectories found by ILP optimization as obtained by the percentage of all replications of the set R-H-95-03-G is

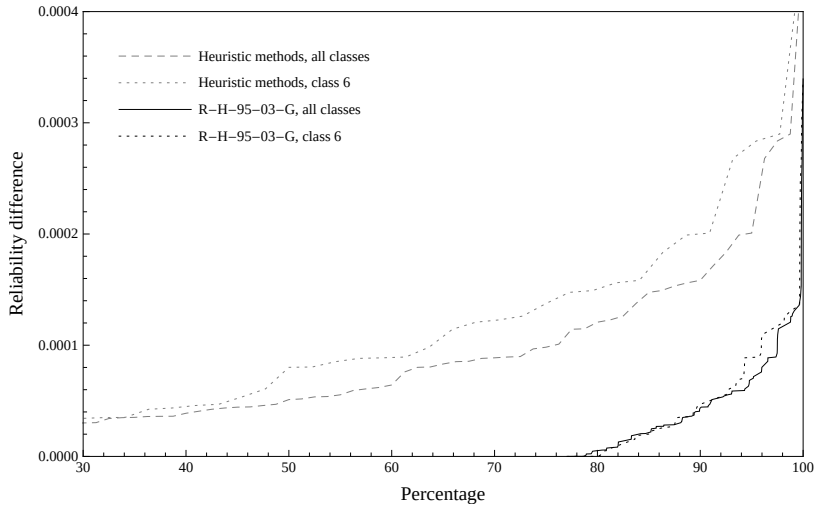

Figure 8. The difference of the reliability of the trajectories found by ILP optimization as obtained by the percentage of all replications and the set R-H-95-03-G and the best of the heuristics. Observe that approximately 80% of all R-H-95-03-G replications find the same trajectory as the ILP optimization, while 80% of the heuristics have differences of more than $1 \cdot 10^{-4}$.

depicted in Fig. 8. Similar differences are indicated for the best of the seven heuristics for each reference case. Likewise, the Fig. 8 depicts the differences for scenario-class 6 only for both the set R-H-95-03-G and best of the seven heuristics. As may be seen in the figure, approximately 80% of all R-H-95-03-G replications find the same trajectory as the ILP optimization for all scenario-classes and scenario-class 6 only. On the opposite side, approximately 80% of the heuristics have differences of more than $1 \cdot 10^{-4}$.

The exact time consumption is not of the main interest, but how the computation effort changes with increasing complexity of the scenario-instances. For having an equal HW platform for the computation effort comparisons, the ILP optimizations in [FH13a] were recomputed with the same HW as the GA implementation and the heuristics. The ILP optimizations were solved with the modelling language AMPL, version 20131213, with the commercial solver Gurobi, version 5.6.0.

The time complexity of the GA with parameter set R-H-95-03-G is analysed as follows. The heuristics initialization is dominated by the Bhandari algorithm which takes $O(b + m)^2$ time [FH13a], where $b = |\bigcup_{d=1}^{m} b_d|$. For the GA the roulette wheel selection takes $O(n \log n)$ time, crossover operation $O(n)$ time, mutation operation $O(nm)$ time and elitism $O(n \log n)$ time. Combined

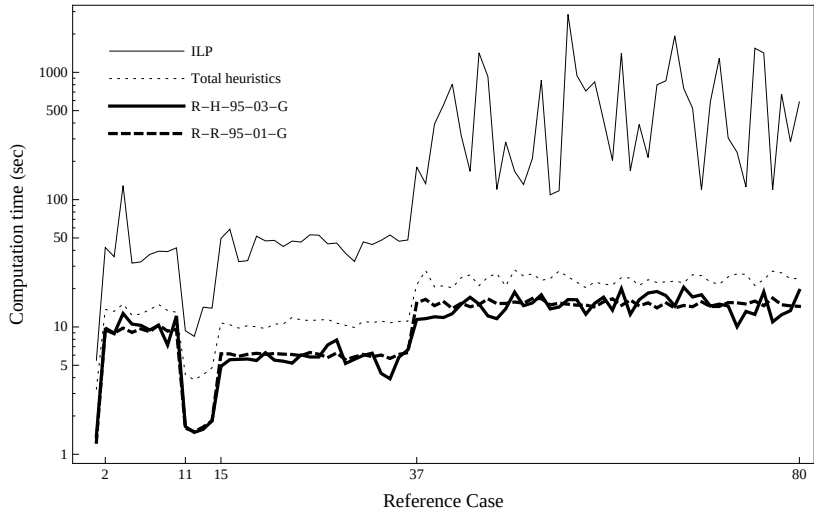

Figure 9. The mean computation effort for GA with parameter sets R-H-95-03-G and R-R-95-01-G. The computation effort for ILP optimization and total time for the heuristics are also shown. Observe that the heuristics and the GA are less sensitive to the scenario-class complexity than the ILP optimization.

together, the GA with parameter set R-H-95-03-G takes $O(b+m)^2 + O(nm)$ time, where $O(nm)$ is the time needed for each replication.

The mean computation effort for one replication of GA with the parameter sets R-H-95-03-G and R-R-95-01-G is depicted in Fig.9 for each of the reference cases. The computation time for ILP optimization and total computation time for the heuristics are also indicated. For a GA with heuristics initialization, the computation time for the heuristics is needed regardless of the number of replications. The mean computation time is comparable when using R-H-95-03-G and R-R-95-01-G. As may be observed in the figure, the computation time correlates with the complexity of the scenario-classes.

As indicated in Fig.9 the ILP optimization computation times for the scenario-class 6 reference cases have significant differences, ranging from approximately 150 seconds to more than 3000 seconds. The ILP optimization computation time is approximately five times higher for a class 5 instance than a class 4 instance, and on average approximately ten times higher for a class 6 instance than a class 5 instance. The GAs with the given parameter sets are not that sensitive to the complexity of the reference cases as the ILP optimization. For instance, the set R-H-95-03-G computation effort is approximately 2.5 times higher for a class 6 instance than a class 5 instance. When using random

initialization with no elitism the R-R-95-01-N increased the computation time with approximately five times compared with the R-H-95-03-G.

Given the mean computation time for one replication of R-H-95-03-G combined with the percentage of replications obtaining the optimal trajectory, this indicates that a better (near) optimal trajectory may be found by the GA than the heuristics alone and with less computation effort than ILP optimization. For instance, using the results depicted in Fig.8 the number of replications needed by the R-H-95-03-G to find the optimal solution may be estimated as independent Bernoulli trials with success probability of 80%.

6. Conclusion

For critical service the probability of no service interruption should be close to one. The use of the proposed GA is computationally efficient. In most cases it finds optimal or close to optimal trajectories when seeded by simple heuristics. This approach is not computationally demanding, i.e., very fast, and hence, it is extremely useful for practical implementation. A few cases are identified, where there is a notable gap between what is found by this method and the optimal trajectories. These are studied in depth, and we have not been able to get a significant improvement by using the full potential of GA, through large initial populations, many replications and parameter tuning.

The proposed method is a very good trade off between computationally efficiency and optimality of the found trajectory. It is sufficiently accurate and efficient for use in provision of dual homed wireless critical services with non stationary user equipment.

References

[AR02] C. W. Ahn and R. Ramakrishna. A genetic algorithm for shortest path routing problem and the sizing of populations. *Evolutionary Computation, IEEE Transactions on*, 6(6):566–579, December 2002.

[BGC12] H. Blodget, P. Gobry, and A. Cocotas. The future of mobile. *Business Insider*, March 22, 2012.

[Bha99] R. Bhandari. *Survivable networks: algorithms for diverse routing.* Kluwer Academic Pub, 1999.

[DAS97a] B. Dengiz, F. Altiparmak, and A. Smith. Efficient optimization of all-terminal reliable networks, using an evolutionary approach. *IEEE Transactions on Reliability*, 46(1):18–26, March 1997.

[DAS97b] B. Dengiz, F. Altiparmak, and A. Smith. Local search genetic algorithm for optimal design of reliable networks. *IEEE Transactions on Evolutionary Computation*, 1(3):179–188, September 1997.

[Dij59] E. W. Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1:269–271, 1959. 10.1007/BF01386390.

[EN09] M. B. E. Nordmark. Shim6: Level 3 multihoming shim protocol for IPv6. IETF network working group, 2009.

[FH13a] E. L. Følstad and B. E. Helvik. Optimizing service continuity in a multi operator multi technology wireless environment. In *Proc. 9th International Conference on the Design of Reliable Communication Networks DRCN 2013*, pages 111–118, Budapest, Hungary, March 4–7 2013.

[FH13b] E. L. Følstad and B. E. Helvik. Reliability modelling of access point selection and handovers in heterogeneous wireless environment. In *Proc. 9th International Conference on the Design of Reliable Communication Networks DRCN 2013*, pages 103–110, Budapest, Hungary, March 4–7 2013.

[Gre86] J. J. Grefenstette. Optimization of control parameters for genetic algorithms. *IEEE Transactions on Systems, Man and Cybernetics*, 16(1):122–128, January 1986.

[Hol92] J. Holland. Adaptation in natural and artificial systems. 1975. *Ann Arbor, MI: University of Michigan Press and*, 1992.

[Ree10] C. R. Reeves. Genetic algorithms. In M. Gendreau, J.-Y. Potvin, and F. S. Hillier, editors, *Handbook of Metaheuristics*, volume 146 of *International Series in Operations Research & Management Science*, pages 109–139. Springer US, 2010.

[SXM+00] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. RFC2960: Stream control transmission protocol, 2000.

[Wol11] Wolfram Research, Inc. Documentation centre. `http://reference.wolfram.com/mathematica/guide/Mathematica.html`, 2011.

PAPER I

Maximizing the reliability of dual homed, critical services in wireless/cellular networks

Eirik Larsen Følstad and Bjarne E. Helvik

Optical Switching and Networking

vol. 19, part 2, pp. 110-121, January 2016

MAXIMIZING THE RELIABILITY OF DUAL HOMED, CRITICAL SERVICES IN WIRELESS/ CELLULAR NETWORKS

Eirik Larsen Følstad, Bjarne E. Helvik
Department of Telematics
Norwegian University of Science and Technology,
Trondheim, Norway
{eirik.folstad, bjarne}@item.ntnu.no

Abstract In the modern society the wireless access to any service has become a commodity. However, various services have different dependability requirements. For critical services the reliability, i.e., the probability for an uninterrupted service, is utmost important. In wireless/cellular networks the execution of handover is one of the key mechanisms to provide an uninterrupted service for a mobile user. Dual homing may be utilized to increase the service reliability where disjointed access points are used for the two connections across possible different access technologies and network operators. The novelty of this paper is how a shortest path algorithm is used to efficiently find the (near-)optimal selection of access points along a projected route for a dual homed critical service. This optimization for reliability takes the radio connections, including handovers, and backhaul network into account. Backhaul network may be composed of a web of autonomous sub-networks made up of different technologies and layers, for instance SDH over an optical network layer.

Keywords: Critical services, mobile/cellular networks, backhaul networks, dual homing, optimization

1. Introduction

With the evolution of the networks and the capabilities of user equipment the access to any services through wireless means is nowadays taken for granted. A myriad of services cover a wide range of needs like e.g. infotainment, machine-to-machine communications, business and health care. Network operators provide wireless coverage with different wireless technologies such as Wireless Local Area Network (WLAN), Universal Mobile Telecommunications System (UMTS) and Long Term Evolution (LTE).

Different services have different dependability requirements. For critical services, like emergency handling and control, health care, surveillance and monitoring, the reliability is of utmost importance. For critical services there is a need, at run-time to, identify the access points and handovers along a

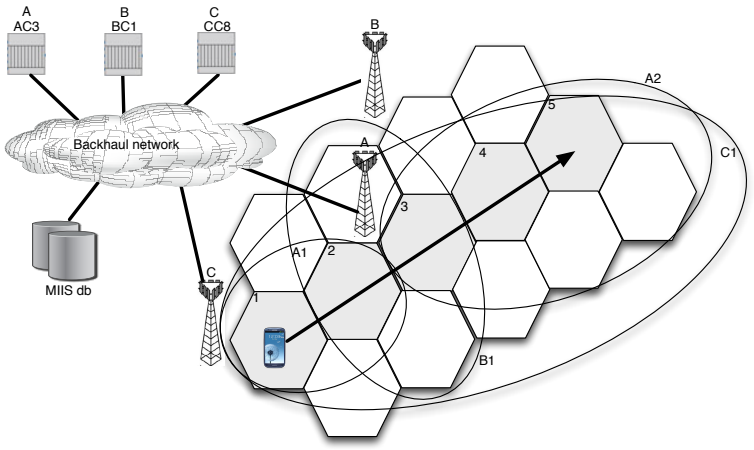

Figure 1. An example network showing the projected route for a user (the arrow) that crosses a number of virtual cells (hexagons). The access points are controlled by the access controllers AC3, BC1 and CC8 operated by the network operators A, B and C. The MIIS db is used for storing and retrieval of dependability information of access points and network topology.

projected route to allow the user to predict the service reliability. How the projected route is derived is not part of this paper, but may be given by means of navigation tools or physical constraints.

This paper presents how a shortest path algorithm may be used to efficiently find the selection of access points along a projected route for a dual homed critical service that optimizes the service reliability. The obtained optimal selection of access points may be used by handover algorithms and multi homing protocols. This reliability optimization takes the radio connections, handovers and backhaul network into account. The presented approach is a general method applicable for wireless/cellular access where the backhaul network may be composed of a web of autonomous sub-networks made up of different technologies and layers, e.g. SDH over an optical network layer. In principle the approach may be used for Line of Sight optic access between the user equipment and the access point [DYSH11], but we have focused on wireless/cellular access considered to be most appropriate technology initially.

The probability that the critical service may be completed without any interrupt is given by the metric for service reliability $R(t_m) = Pr\{T_{FF} > t_m\}$ where T_{FF} is time to first failure and t_m is the mission time. Fig. 1 depicts an example network with three network operators, named A, B and C. The access points A1, B1 and C1 are connected to the access controllers, for instance Radio

Network Controller (RNC) for UMTS, AC3, BC1 and CC8 respectively over a backhaul network. To ensure uninterrupted service in such an environment access point selection and handover execution are essential mechanisms for a user on the move.

A survey of handover decision algorithms is presented in [YSN10]. To improve the handover performance several proposals exist such as pre-authentication [DDF+07, CIRG09] and activation of resources in the target network [NFS+09]. Common for the proposals described in [DDF+07, CIRG09, NFS+09] is the usage of Media Independent Handover (MIH) [IEE08] as a framework for obtaining information of access points in the area. Typical handover algorithms are local hop-by-hop based decisions, where handover decisions are taken independently of potential future handovers. The contribution in this paper is a global route handover decision schema combined with an extension of the MIH framework that maximizes the service reliability. A global route handover decision schema takes all necessary handovers along a projected route into account.

To increase the reliability dual homing may be used, where the user equipment has radio connection with two disjointed access points. Examples of multi homing protocols are Stream Control Transmission Protocol (SCTP) [ASS03], Mobile SCTP [SXM+00], Mobile IPv6 (MIPv6) [PJA10] and Site Multihoming by IPv6 Intermediation (SHIM6) [EN09]. Similar as for handover mechanisms, one of the main challenges with multi homing protocols is the path management, i.e., which access points to use. We define a trajectory as a series of access points used for each of the two radio connections for a dual homed critical service along a projected route.

Even though dual homing is used for the radio connection, it is not given that all used resources in the backhaul network are disjoint and statistically independent. In fact, the opposite is quite common due to co-operation through (cost saving) business relations between network operators. The co-operation has evolved from site sharing and hiring leased transmission into equipment and network sharing [BS05, KKKY11]. Regard Fig. 1 where the backhaul network or parts of it is indicated as possibly shared among the operators. The Media Independent Information Service (MIIS) database, part of the MIH framework, is used for storing and retrieval of dependability information of access points and backhaul network topology.

We show how shortest path algorithms, such as Dijkstra [Dij59] or Bellman-Ford [Bel56], may be used for finding the (near-)optimal trajectory for a dual homed critical service. We will show that the trajectory found is identical to the trajectory found by an ILP optimization. Several techniques exist to improve the performance of Dijkstra algorithm, see e.g. [HSWW05, BDS+10, BDW11, DSSW09]. Even though improvements may be shown for some data sets, typical for road networks and time table information systems, they cannot be proved to be asymptotical faster than the original Dijkstra for all data sets.

The rest of the paper is organized as follows. The dependability model of a mobile user is presented in Section 2. This model is used by the shortest path algorithm as described in Section 3 for optimizing the reliability of a trajectory for a dual homed critical service. Optimization of trajectory is performed for a number of network instances and results are presented in Section 4. We conclude this paper in Section 5.

2. Dependability model of a mobile connection

In the following we describe how the reliability of a trajectory of a dual homed critical service is derived. First the problem formulation is described and then models for the dual homed radio connection and the dual homed backhaul network connection are described.

2.1 Initial problem formulation

A model for prediction of reliability for a dual homed critical service for a projected route is described in [FH13b] where virtual cells are defined as limited geographical areas, where the radio conditions are homogeneous. In Fig. 1 the projected route is indicated by an arrow and crosses several virtual cells (hexagons). Virtual cells are typical smaller than the planned service coverage for the access points (ellipses in the figure). The access points used along the projected route are described by a trajectory. Without loosing generality the virtual cells are ordered as they are visited from 1 to m along the trajectory. A trajectory S_{ij} defines the series of access points to use for the two radio connections i and j of a dual homed critical service where the set of all access points covering virtual cell d is b_d. The trajectory may be denoted as $S_{ij} = \{(i_1, j_1), \ldots, (i_d, j_d), \ldots, (i_m, j_m)\}$ where $i_d \in b_d$ and $j_d \in b_d$ and $i_d \neq j_d$.

The objective is to find the trajectory S_{ij} that maximizes session reliability, i.e,.

$$\max_{\forall S_{ij}} R_{S_{ij}}(t_m) = Pr\{T_{FF} > t_m\} \tag{1}$$

For critical services $R_{S_{ij}}(t_m)$ should be close to 1, i.e. $1 - Pr\{T_{FF} > t_m\} \ll 1$.

Here we extend the work in [FH13b] to not only consider the reliability for the radio connections, but also consider the backhaul network. To identify the resources in the backhaul network we utilize the work in [FH09] where the used backhaul resources are described by cut-sets where MIH framework is proposed extended with capabilities to enable reliability prediction. The MIIS database is used for storing and retrieval of dependability information of access points and network topology.

2.2 Dual homed radio connection

In [FH13a] the reliability modelling of access point selection and handovers in heterogeneous wireless environment for a dual homed critical service is described

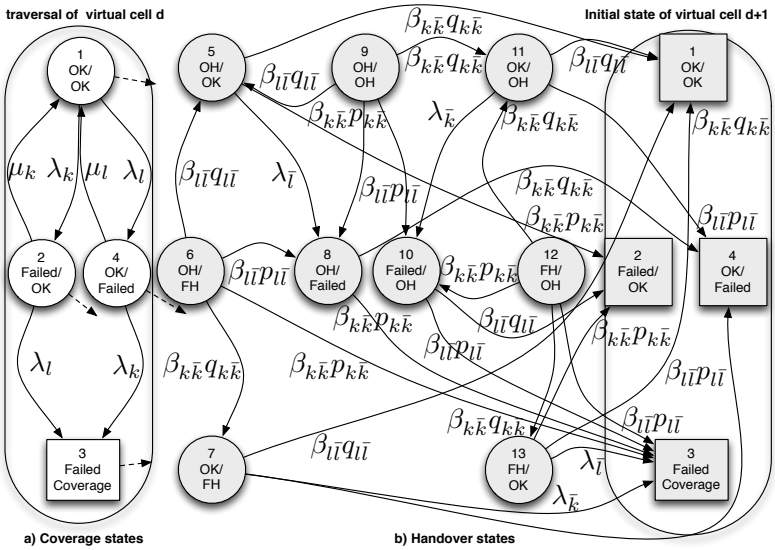

Figure 2. State transition diagram for traversal of virtual cell d and handover to cell $d+1$. Absorbing handover states (grey shaded) represent the initial conditions for traversal of cell $d+1$. Transitions into handover states are modelled as instantaneous transition given by S_{ij}.

as a phased mission. Each phase corresponds to handover from previous cell $d-1$ and the traversal of virtual cell d, modelled as a continuos time discrete space Markov model as given in Fig. 2. Handover states $\Omega_H = \{5, 6, ..., 13\}$ are grey, while the white ones are coverage states $\Omega_C = \{1, 2, 3, 4\}$ since loss of radio connection is the main cause of failure within a virtual cell. The state of the two connections of a trajectory S_{ij} is represented by the state. For instance, the state OK/OK indicates that both connections are working and the state FH/OH indicates that connection i has a failed radio connection and executing handover while connection j has a working radio connection and executing a handover. Transitions into Ω_H are modelled as instantaneous transition given by S_{ij} and will be described later in this section. The change from phase d to $d+1$ takes place at time t_d and the sojourn time of phase d is T_d.

To keep the notation simple, we will in the rest of the paper use the index i_d for dependability parameters and attributes for an access point i_d in a virtual cell d, i.e. $\lambda_{id,d} \rightarrow \lambda_{id}$. In Fig. 2 the index $k = i_d$, $\bar{k} = i_{d+1}$ and $l = j_d$, $\bar{l} = j_{d+1}$. A radio connection between a user equipment and an access point i_d covering virtual cell d has a constant radio coverage failure intensity λ_{i_d}. The radio coverage from different access points fail independently. When a radio connection to access point i_d has been lost, the time to recover is negatively exponentially distributed (n.e.d.) with mean $1/\mu_{i_d}$ in cell d. Handover from

i_d to i_{d+1} is n.e.d. with mean $1/\beta_{i_d i_{d+1}}$ and may fail with a probability of $p_{i_d i_{d+1}}$ where $q_{i_d i_{d+1}} = 1 - p_{i_d i_{d+1}}$. In case of dual handovers, the handovers fail independently.

Based on the model and results from [FH13a], the reliability of a dual homed critical service can be written as

$$\hat{R}_{S_{ij}}(t_{m_-}) = \hat{R}_1(T_{1_-}) \prod_{d=2}^{m} \hat{R}_d \left(T_{d_-} | T_{FF} > t_{d-1}\right) \tag{2}$$

where $\hat{R}_d(T_{d_-}|T_{FF} > t_{d-1})$ represents the reliability of phase d. The notations t_{d_-} and t_{d_+} are used to indicate instants immediately before and after the handover that takes place. Transition intensity matrix for Fig. 2 may be organized as

$$\Lambda_C = \begin{bmatrix} \Lambda_{CC} & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \Lambda_H = \begin{bmatrix} 0 & \Lambda_{HC} \\ 0 & \Lambda_{HH} \end{bmatrix} \tag{3}$$

where Λ_{CC} is the transition intensity matrix for Ω_C, Λ_{HH} is the transition intensity matrix for Ω_H and Λ_{HC} is the transition intensity matrix for intensities from Ω_H to Ω_C. As described in [FH13b], the approximated normalized transient probability of working states $\hat{p}(T_{d_-}|T_{FF} > t_d) = \{\dot{p}_1, \dot{p}_2, 0, \dot{p}_4, 0, 0, 0, 0, 0, 0, 0\}^T$, where $\dot{p}_2 = \dot{p}_1 \lambda_{i_d}/\mu_{i_d}$ and $\dot{p}_4 = \dot{p}_1 \lambda_{j_d}/\mu_{j_d}$ and $\dot{p}_1 + \dot{p}_2 + \dot{p}_4 = 1$. The approximation holds as long as time spent in virtual cell T_d is more than the largest of $4/\mu_{i_d}$ and $4/\mu_{j_d}$.

By neglecting the handover time the state just after handover is given as $p(T_{d_+}) = (\Pi_H)^3 p(T_{d_-}|T_{FF} > t_d, I_d)$ where Π_H is the transition probability matrix of Λ_H and $I_d = |i_{d-1} \cap i_d|||j_{d-1} \cap j_d|$ is the indicator function for the continued use of the access points, i.e. no handover . The operator $\|$ indicates the concatenation of the indicator functions for the two radio connections. For first phase $I_1 = 11$. Only 3 operations are necessary since 3 is the largest path from an initial to an absorbing state in Ω_H. The instantaneous transitions from Ω_C to Ω_H are given by

$$\begin{aligned} p(T_{d_-}|T_{FF} > t_d, I_d = 11) &= \dot{p}(T_{d_-}|T_{FF} > t_d) \\ p(T_{d_-}|T_{FF} > t_d, I_d = 01) &= [0, \ldots, \dot{p}_1, 0, 0, \dot{p}_4, 0, \ldots, \dot{p}_2]^T \\ p(T_{d_-}|T_{FF} > t_d, I_d = 10) &= [0, \ldots, \dot{p}_4, 0, 0, \dot{p}_2, \dot{p}_1, 0, 0]^T \\ p(T_{d_-}|T_{FF} > t_d, I_d = 00) &= [0, \ldots, \dot{p}_4, 0, 0, \dot{p}_1, 0, 0, \dot{p}_2, 0]^T \end{aligned} \tag{4}$$

The traversal of cell d is given by $\Lambda_C p(t) = dp(t)/dt$ with the initial condition $p(0)$. For the first phase $p(0) = \{1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}^T$ and for phase d $p(0) = \{p_1(T_{d-1_+}), p_2(T_{d-1_+}), p_3(T_{d-1_+}), p_4(T_{d-1_+}), 0, \ldots, 0\}^T$. This yields the reliability of phase d

$$\hat{R}_d(T_{d_-}|T_{FF} > t_{d-1}) = 1 - p_3(T_{d_-}) \tag{5}$$

When the (near-)optimal trajectory is found by using the approximation given by (5), the actual service continuity, $R_{S_{ij}}(t_{m_-})$, can be calculated by using $\hat{p}(T_{d_-}|T_{FF} > t_d) = \{p_1(T_{d_-}), p_2(T_{d_-}), 0, p_4(T_{d_-}), 0, 0, 0, 0, 0, 0, 0\}^T$.

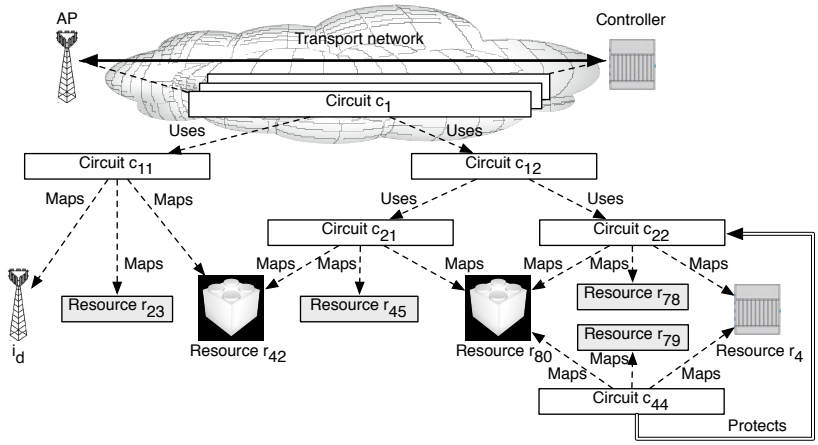

Figure 3. Some examples of relations between logical circuits, $c_\iota \in \Theta_C$, and physical resources, $r_\kappa \in \Theta_R$, between an access point i_d and the radio network controller.

In the following we will describe how $\hat{R}_{S_{ij}}(t_{m\_})$ is utilized by a shortest path algorithm to find the optimal trajectory.

2.3 Dual homed network connection

In Section 2.2 the model for the radio connections of a dual homed critical service is described. In this section we describe a model for the backhaul network infrastructure from the access points to the radio network controllers, as depicted in Fig. 3.

For dependability analysis of a system, the information about the logical and physical resources is required. This is an operational setting that only may be obtained from network operators. Such information is in practice impossible to derive without proper input from network operators. Each network operator has (a number) of Operational Support Systems (OSSs) needed for configuration, monitoring and maintenance of the network. The OSSs have the needed information of logical and physical resources. In a multi operator environment, where co-operations between operators are very likely, the logical and physical resources constitute a web of interdependent networks where none of the network operators has the total view.

Analysis of such an environment needs special attention and identification of logical and physical resources becomes critical. A model to determine the logical and physical resources and dependencies between network operators is proposed in [FH10] where information is collected from operators OSSs and stored in a MIIS database. The total view of logical and physical resources may be managed with the information in the MIIS database. Logical circuits constitute

recursive properties that allow different protocols and section networks to be nested in a technology neutral manner where the same protocol can be used at several layers. Nested logical circuits are therefore interdependent. At the lowest layer of logical circuits, the circuits are mapped to physical resources. Physical resources are assumed to be statistically independent.

In [FH10] the identifications of the logical and physical resources are based upon the principle that the owning network operator is responsible for a unique identification across operators. All necessary information of such identification and relations are collected in the MIIS database. The identification could be based upon [X.792]. In the following all logical circuits and physical resources are identified with the sets Θ_C and Θ_R respectively. Without loosing generality we may index the logical circuits $c_\iota \in \Theta_C$ and physical resources $r_\kappa \in \Theta_R$. Fig. 3 depicts examples of some relations between logical circuits and physical resources between an access point i_d and the radio network controller. In the example, there are several circuits between i_d and the controller, one of them is c_1 that use the underlying circuits c_{11} and c_{12}. At the lower layer circuits are mapped to physical resources. In the example, circuit c_{44} protects circuit c_{22}.

The structure function $\phi(i_d)$, obtained from the information stored in the MIIS database, between the access point i_d and radio network controller is defined as

$$\phi(i_d) = \begin{cases} \mathit{False}, \text{ access using } i_d \text{ fails} \\ \mathit{True}, \text{ access using } i_d \text{ operates} \end{cases} \tag{6}$$

For a dual homed critical service that uses the access points i_d and j_d, where $i_d \neq j_d$, the structure function is $\phi(i_d j_d) = \phi(i_d) \bigvee \phi(j_d)$ and provides the combinations of physical resources that make the dual homed service to fail. The general form of the structure function $\phi(i_d j_d)$ may be represented in a minimal product-of-sum form, see e.g. [BP75] for introduction. Each maxterm in a minimal product-of-sum form is a minimal cut set which yields

$$\phi(i_d j_d) = \bigwedge_{n=1}^{n_{i_d j_d}} \varphi^n_{i_d j_d} \tag{7}$$

where each maxterm $\varphi^n_{i_d j_d}$ represents one of the $n_{i_d j_d}$ minimal cut set of $\phi(i_d j_d)$. The cardinality of a minimal cut set, i.e., $|\varphi^n_{i_d j_d}|$, represents the number of failing physical resources that make the dual homed critical service to fail. To identify single points of failure in the network when using i_d and j_d we may write

$$\phi_1(i_d j_d) = \{z | z \in \varphi^n_{i_d j_d}, |z| = 1\} \forall n \tag{8}$$

which implies $\phi_1(i_d j_d) \subset \Theta_R$.

As an example assume that for Fig. 1 the structure function for $A1$ and $C1$ is given as $\phi(A1) = A1 \wedge r_{23} \wedge r_{42} \wedge r_{45} \wedge r_{80} \wedge (r_{78} \vee r_{79}) \wedge r_4$ and $\phi(C1) = C1 \wedge r_{23} \wedge r_{42} \wedge r_{55} \wedge r_{80} \wedge (r_{78} \vee r_{79}) \wedge r_7$. For the dual homed critical service we have $\phi(A1C1) = \phi(A1) \vee \phi(C1)$. The set of single points of failure in the backhaul network is $\phi_1(A1C1) = \{r_{23}, r_{42}, r_{80}\}$.

In the low-failure-probability regime in the backhaul network, i.e., $Pr\{T_{FF} < t_m\} \ll 1$ and where the network resources have a reliability of the same order of magnitude, the single point of failures will dominate the reliability. For a trajectory S_{ij} the minimal cut sets with cardinality higher than one can be neglected and the backhaul network reliability may be approximated with

$$\tilde{R}_{S_{ij}}(t_{m\_}) = \prod_{d=1}^{m} \tilde{R}_d(T_{d\_}) \approx \prod_{d=1}^{m} e^{-\lambda_{i_d j_d} T_d} \tag{9}$$

where

$$\lambda_{i_d j_d} = \sum_{\forall r_\kappa \in \phi_1(i_d j_d)} \lambda_{r_\kappa} \tag{10}$$

and where $\tilde{R}_d(T_{d\_})$ is the reliability of phase d and λ_{r_κ} is the failure intensity of the physical resource r_κ. Note that in (9) the reliability of network resources is only considered for the sojourn time in each virtual cell individually. This implies a prerequisite of an on-line notification if a network resource fails in due time before it is intended to be used. In such cases a new trajectory of the rest of the projected route may be recalculated.

3. Optimization of trajectory

In Sections 2.2 and 2.3, reliability models for the radio connection and backhaul network connection of a dual homed critical service were described. Here, we will present how these models are used in a shortest path algorithm to find the optimal trajectory.

In [FH13a] an ILP formulation was used to find the optimal trajectory for the radio connection. Since solving ILP is computationally demanding even for relative small scenarios, heuristic methods were described based upon Dijkstra [Dij59] and Bhandari [Bha99] for finding near-optimal trajectories with less computation efforts. In contrast to the heuristic methods in [FH13a] we propose an optimization method that may use any suitable shortest path algorithm for a directed graph $G = (V, E)$ between a given source $s \in V$ and a final destination $f \in V$ that always find the same trajectory as the ILP optimization in [FH13a], but with significantly less computation effort.

In the following, we will describe how a directed graph, $G = (V, E)$ is constructed from virtual cells along a projected route. Then, we describe the optimization method for the radio connection only, and later extended to also include the backhaul network connection.

3.1 Graph model

A projected route, as illustrated in Fig. 1, crosses a number of virtual cells where b_d is the set of all access points covering virtual cell d. For a dual homed critical service, assuming $|b_d| > 1$, the possible combinations of access points

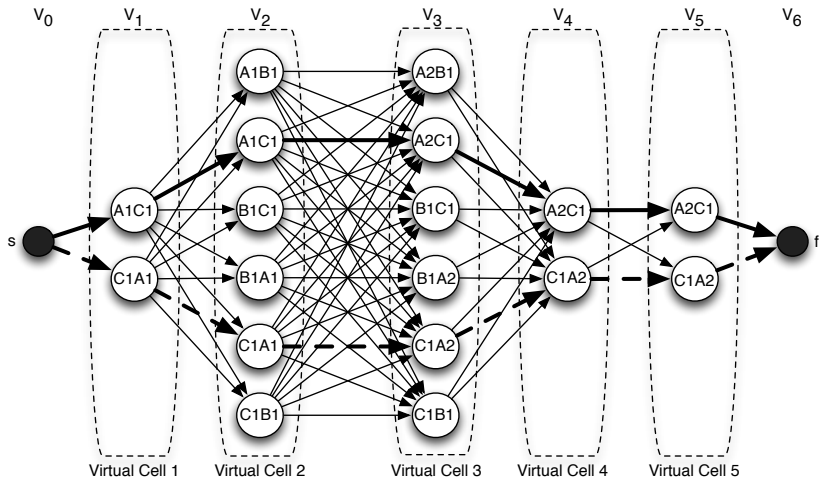

Figure 4. Directed graph, $G = (V, E)$, representing the example network in Fig. 1. Each vertex, $v_d \in V_d$ represents possible combinations of disjoint access points of the set b_d in virtual cell d. Possible handovers are represented with edges $v_d v_{d+1} \in E$.

in virtual cell d may be described as $V_d = \dot{V}_d \bigcup \ddot{V}_d$ where

$$\dot{V}_d = \{b_d \times b_d\} \setminus \{v_d | v_d = i_d i_d, i_d \in b_d\} \tag{11}$$

$$\ddot{V}_d = \{j_d i_d | i_d j_d \in \dot{V}_d\} \tag{12}$$

The cartesian product of $b_d \times b_d$, gives the ordered combinations of access points. For a dual homed critical service it is required that the access points i_d and j_d are disjoint, i.e., $i_d \neq j_d$, thus such combinations are removed from $\dot{V}_d$. To allow the opposite order of access points as of $\dot{V}_d$ these combinations are added with the set $\ddot{V}_d$. In the example network shown in Fig. 1 $b_1 = \{A1, C1\}$ which gives $V_1 = \{A1C1, C1A1\}$. Similar may be defined for all virtual cells. For the directed graph $G = (V, E)$ representing the phased mission for a projected route all access point combinations in the virtual cells are given by

$$V = \bigcup_{d=0}^{m+1} V_d, \text{ where } V_0 = \{s\}, V_{m+1} = \{f\} \tag{13}$$

The example network in Fig. 1 is represented by a directed graph $G = (V, E)$ as shown in Fig. 4 where the sets of vertices V_d are ordered according to d from 0 to $m + 1$. The number of vertices, $V \in G$ is given by

$$|V| = \sum_{d=0}^{m+1} \binom{|b_d|}{\max[|b_d| - 2, 1]} \tag{14}$$

where $b_0 = \{s\}$ and $b_{m+1} = \{f\}$.

At the virtual cell boundary of cell d, handovers may be executed to change from access point combination v_d to v_{d+1} in the next virtual cell. However, if $v_d = v_{d+1}$, where $v_d \in V_d$ and $v_{d+1} \in V_{d+1}$, no handover is executed and the same access point combination is used in both virtual cells. The edges $v_0v_1 \in E$ and $v_mv_{m+1} \in E$ are only used to make the graph connected and are not representing handovers, since $V_0 = \{s\}$ and $V_{m+1} = \{f\}$. In Fig. 4 handover possibilities are represented by directed edges $v_dv_{d+1} \in E, d = 0, \ldots m+1, \forall v_d \in V_d, \forall v_{d+1} \in V_{d+1}$. The number of edges, $E \in G$ is given by

$$|E| = \sum_{d=0}^{m} \binom{|b_d|}{\max[|b_d| - 2, 1]} \binom{|b_{d+1}|}{\max[|b_{d+1}| - 2, 1]} \tag{15}$$

3.2 Method for optimization for radio connection

For a shortest path algorithm to find the optimal trajectory between a source and final destination, metrics need to be assigned to the graph $G = (V, E)$. The Dijkstra algorithm [Dij59] finds the shortest path between a source and final destination where the sum of metrics (aka weights) for edges is minimized.

To assign the additive weights to the edges $E \in G$, we use

$$\hat{w}_{v_{d-1}v_d} = -\log \hat{R}_d(T_{d\_}|T_{FF} > t_{d-1}) \tag{16}$$

i.e., the log reliability of the radio connection of phase d, see (5), for a given combination of v_{d-1} and v_d. Note that since $i_dj_d \in V_d$ and $i_{d+1}j_{d+1} \in V_{d+1}$ the actual handover performed is given by the indicator function $I_d = |i_{d-1} \cap i_d|||j_{d-1} \cap j_d|$. For instance, the edge from $A1C1 \in V_1$ to $A1B1 \in V_2$ gives $I_2 = 10$.

3.3 Method for optimization for dual homed critical service

The reliability of phase d is not only dependent on reliability of radio connection, but also reliability of the backhaul network connection. With the prerequisites that the relevant backhaul resources are working when entering a virtual cell and that we may regard the radio connection and the backhaul connection statistically independent, the reliability for phase d is assigned to the edge weights as

$$w_{v_{d-1}v_d} = -\log\Big(\hat{R}_d(T_{d\_}|T_{FF} > t_{d-1})\tilde{R}_d(T_{d\_})\Big) \tag{17}$$

where $\tilde{R}_d(T_{d\_})$ provides the reliability of the backhaul network connection for virtual cell d, see (9).

Computations of the edge weights can utilize the fact that $w_{i_dj_di_{d+1}j_{d+1}} = w_{j_di_dj_{d+1}i_{d+1}}$ and thereby reduce the computation effort to approximate the half. In addition, the edge weights are only needed to be re-computed when there

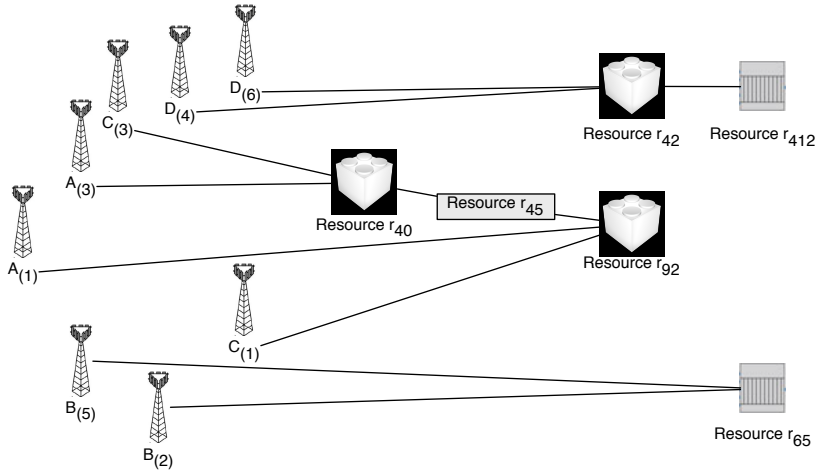

Figure 5. Network dependencies focused on single point of failures for combination of two access points belonging to given technologies.

are changes in the corresponding backhaul network, access point combinations or parameters for virtual cells.

The shortest path algorithm, like Dijkstra [Dij59], finds the optimal trajectory in the graph $G = (V, E)$. This can be viewed as a global route based handover schema. The optimal trajectory S_{ij} for a dual homed critical service is given as

$$\arg\max_{v_d,\forall d} \hat{R}_{S_{ij}}(t_m) = \arg\max_{v_d,\forall d} \prod_{d=0}^{m+1} e^{-w_{v_{d-1}v_d}} \tag{18}$$

In Fig. 4 the optimal trajectory S_{ij} is depicted with bold edges, but since $S_{ij} = S_{ji}$ the symmetric solution is also depicted with dashed edges.

If only one access point is accessible in a virtual cell d, i.e., $|b_d| = 1$, then $v_d = V_d = b_d$ and no dual homing can be established. In such cases the optimal trajectory is the concatenation of the trajectories from s to v_d and from v_d to f.

4. Results of obtaining optimal trajectory

In this section the optimal trajectory for a dual homed critical service is obtained for a number of scenario-instances. First, we describe the local hop-by-hop optimization that will be used for comparisons. Then, we describe the scenario-instances followed by discussions of the trajectories found by the optimizations.

Table 1. Scenario-class; access coverage and resources.

	Characteristics							
Operator	A		B		C		D	
Technology	1	3	2	5	1	3	4	6
Route coverage	100%	100%	40%	40%	100%	100%	40%	40%
Cells per AP	U[2,3]	5	2	2	U[2,3]	5	U[1,2]	U[1,2]
Resource, r_κ	r_{40}	r_{45}	r_{65}		r_{92}		r_{42}	r_{412}
$\lambda_{r_\kappa}(10^{-8})$ sec^{-1}	3η	3η	3η		3η		3η	3η

4.1 Local hop-by-hop optimization

For comparisons of the global route based optimization scheme we also obtain the reliability when local hop-by-hop handover decisions are performed. Local hop-by-hop decisions are typically used by handover algorithms where only the immediate next access points are considered for handover. With the information in the MIIS database, all available access points and their reliability may be used by the handover algorithm for deciding which access points to use.

A local hop-by-hop handover decision tries to maximize the surviving of the immediate handover and the traversal of the next virtual cell. The reliability of traversal of virtual cell d is optimized given the access point selected in phase $d-1$ as

$$\arg\max_{v_d,\forall d} \hat{R}_{S_{xy}}(t_m) = \arg\max_{v_d,\forall d} \prod_{d=0}^{m} e^{-w_{v_{d+1}v_d}|w_{v_{d-1}v_d}} \tag{19}$$

where $w_{v_{-1}v_1} = 0$.

4.2 Scenario-instances

To investigate how the optimal trajectory for a dual homed critical service depends on the both the radio connection and the backhaul network connection a number of scenario-instances are created. A scenario-instance is a directed graph $G = (V, E)$ that represents an example network. Each scenario-instance belongs to a scenario-class.

The scenario-classes are defined in Table 1. These represent the access coverage from the network operators together with the resources identified as single point of failures for one or several combinations of two access points. For a given operator and technology, the access points may provide coverage for successive virtual cells along projected route. For instance, in Table 1 network operator D with technology 4 covers 40% of the projected route, where each access point covers i.i.d. $\sim$ uniform$[1, 2]$ virtual cells. If the projected route traverses 30 virtual cells network operator D with technology 4 covers 12 successive virtual cells with minimum 6 and maximum 12 access points.

Denote the set of access points for network operator o with wireless technology z in virtual cell d as $b_d^{o(z)}$ where $b_d^o = \cup b_d^{o(z)}, \forall z$. All access points covering

Table 2. Scenario-instance; radio dependability parameters.

	Parameter	Values			
		$i_{d+1} \in b^A_{d+1}$	$i_{d+1} \in b^B_{d+1}$	$i_{d+1} \in b^C_{d+1}$	$i_{d+1} \in b^D_{d+1}$
	$\lambda_{i_{d+1}}\text{sec}^{-1}$	$U[1,2]/998$	$U[2,5]/998$	$U[1,3]/998$	$U[1,2]/998$
	$\mu_{i_{d+1}}\text{sec}^{-1}$	$U[1/4,1/2]$	$U[1/4,1/2]$	$U[1/4,1/2]$	$U[1/4,1/2]$
$i_d \in b^A_d$	$p_{i_d i_{d+1}}$	$U[0.01,0.02]$	$U[0.01,0.04]$	$U[0.01,0.03]$	$U[0.01,0.04]$
	$\beta_{i_d i_{d+1}}\text{sec}^{-1}$	$U[4,8]$	$U[2,4]$	$U[4,8]$	$U[2,4]$
$i_d \in b^B_d$	$p_{i_d i_{d+1}}$	$U[0.01,0.04]$	$U[0.01,0.03]$	$U[0.01,0.04]$	$U[0.01,0.05]$
	$\beta_{i_d i_{d+1}}\text{sec}^{-1}$	$U[3,6]$	$U[4,8]$	$U[3,6]$	$U[3,6]$
$i_d \in b^C_d$	$p_{i_d i_{d+1}}$	$U[0.01,0.03]$	$U[0.01,0.04]$	$U[0.01,0.04]$	$U[0.01,0.04]$
	$\beta_{i_d i_{d+1}}\text{sec}^{-1}$	$U[2,4]$	$U[4,8]$	$U[4,8]$	$U[2,4]$
$i_d \in b^D_d$	$p_{i_d i_{d+1}}$	$U[0.01,0.04]$	$U[0.01,0.02]$	$U[0.01,0.02]$	$U[0.01,0.03]$
	$\beta_{i_d i_{d+1}}\text{sec}^{-1}$	$U[3,6]$	$U[3,6]$	$U[2,4]$	$U[4,8]$

virtual cell d becomes $b_d = \cup b^o_d, \forall o$. An example of network dependencies focused on single point of failures for a combination of two access points is sketched in Fig. 5. Though the example is simple, it is used for illustration of how the network dependencies affect the optimal trajectory. In the figure $D_{(4)}$ and $D_{(6)}$, representing network operator D with technologies 4 and 6, have resource r_{42} and r_{412} as single point of failures. The failure intensities for resources are given in Table 1 where the η is a variable for backhaul network dependencies and failure intensities. Note that for $\eta = 0$ it implies no single point of failures, whereas $\eta = 1$ corresponds to approximately one failure per year on the average for a resource. The failure intensities are used for deriving the reliability of the backhaul network connection.

From the scenario-class the scenario-instances are created with radio dependability parameters as defined in Table 2. The radio dependability parameters are used for deriving the reliability of the radio connection. All parameters in the table have identical statistically independent uniform distributions. For instance the handover from an access point in virtual cell d belonging to network operator A, i.e., b^A_d to access point in virtual cell $d+1$ belonging to network operator D, i.e., b^D_{d+1} has i.i.d. $p_{i_d i_{d+1}} \sim \text{uniform}[0.01, 0.04]$ and $\beta_{i_d i_{d+1}} \sim \text{uniform}[2,4]$. Sojourn time T_d in each virtual cell is i.i.d. $\sim \text{uniform}[20,30]$. For each scenario-instance, the backhaul network dependencies and resource failure intensities are changed with the factor η to investigate how the optimal trajectory is dependent on the network resources.

4.3 Optimal trajectory

For each scenario-instance, represented by a directed graph $G = (V, E)$ defined in Section 4.2, the optimal trajectory for a dual homed critical service is identified as the trajectory with the highest reliability. For each projected route of $m = \{10, 20, 30\}$ virtual cells, 100 scenario-instances are created, giving total 300 scenario-instances. For a global route optimization, given by $\hat{R}_{S_{ij}}(t_m)$ in (18), the total session time t_m is taken into account, whereas for the local

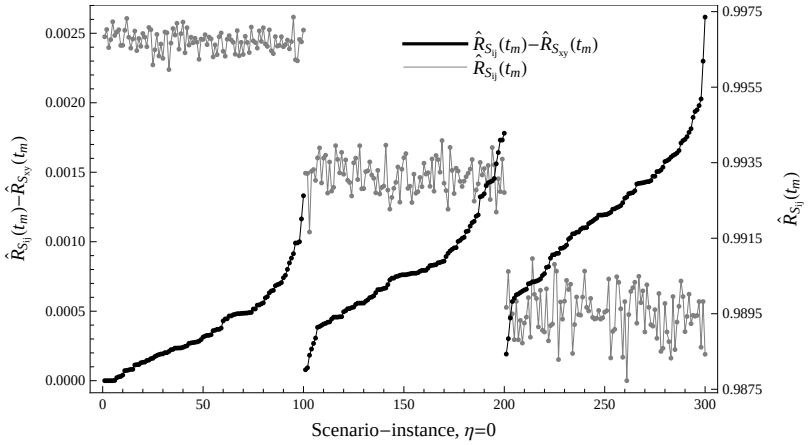

Figure 6. The reliability of global route optimization, $\hat{R}_{S_{ij}}(t_m)$ and the difference between global route optimization $\hat{R}_{S_{ij}}(t_m)$ and local hop-by-hop optimization $\hat{R}_{S_{xy}}(t_m)$ where $\eta = 0$, i.e., no backhaul network dependencies for $m = \{10, 20, 30\}$. The scenario-instances are ordered according to the difference.

hop-by-hop optimization, given by $\hat{R}_{S_{xy}}(t_m)$ in (19), maximize the reliability for each phase.

We have used Mathematica 8 [Wol11] for implementing the optimizations. Mathematica computations were performed on a PowerEdge M610 blade with 2.67 GHz quad-core CPU with 24 GB memory running 64 bits Linux.

Fig. 6 depicts the difference between the reliability of the trajectory identified global route optimization, $\hat{R}_{S_{ij}}(t_m)$, and the trajectory identified local hop-by-hop optimization $\hat{R}_{S_{xy}}(t_m)$. The difference is applicable for no backhaul network dependencies, i.e., $\eta = 0$. The scenario-instances are ordered according to the difference between $\hat{R}_{S_{ij}}(t_m)$ and $\hat{R}_{S_{xy}}(t_m)$ where instances 1 to 100 belongs to $m = 10$, 101 to 200 belongs to $m = 20$ and the rest belongs to $m = 30$. As may be observed in the figure the global route optimization provides the trajectory with the highest reliability for all scenario-instances. The local hop-by-hop optimization provides the same reliability as the global route optimization for $m = 10$ for very few instances. In the figure the absolute reliability of global route optimization, $\hat{R}_{S_{ij}}(t_m)$ is shown, where it may be observed that the difference between $\hat{R}_{S_{ij}}(t_m)$ and $\hat{R}_{S_{xy}}(t_m)$ is largest the larger m.

The mean computation effort obtaining the optimal trajectory, $S_{ij}(t_m)$ is 1.15 sec for $m = 10$, 2.82 sec for $m = 20$ and 5.05 sec for $m = 30$ with standard deviations 0.15, 0.28 and 0.46 respectively.

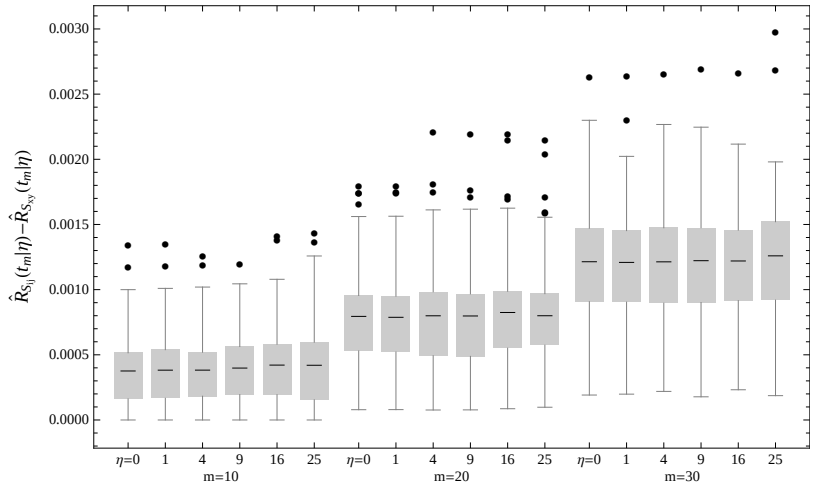

Figure 7. Difference between global route optimization $\hat{R}_{S_{ij}}(t_m)$ and local hop-by-hop optimization $\hat{R}_{S_{xy}}(t_m)$ for different backhaul network dependencies and failure intensities given by η. The boxplots show median, near and far outliers.

For backhaul network dependencies and failure intensities, given by the factor η, the difference between the reliability of the trajectory identified global route optimization, $\hat{R}_{S_{ij}}(t_m)$, and the trajectory identified local hop-by-hop optimization $\hat{R}_{S_{xy}}(t_m)$ is shown as boxplots in Fig. 7. As may be observed the differences of the reliability of the trajectories found by global route optimization and local hop-by-hop optimization are not significantly changed with different values of η.

To investigate how the reliability of a trajectory identified by a local hop-by-hop optimization is dependent on the knowledge of the backhaul network dependencies, the difference between $\hat{R}_{S_{xy|\eta=9}}(t_m)$ and $\hat{R}_{S_{xy|\eta=0}}(t_m)\tilde{R}_{S_{xy|\eta=9}}(t_m)$ is shown in Fig. 8. With knowledge of backhaul network dependencies, the trajectory is found by incorporating the reliability of the backhaul network connection for each of the phases, given by $\hat{R}_{S_{xy|\eta=9}}(t_m)$. Without this knowledge, the deriving of the trajectory does not consider the reliability of the backhaul network connection, given by $\hat{R}_{S_{xy|\eta=0}}(t_m)$ for each of the phases. However the actual reliability must be adjusted with $\tilde{R}_{S_{xy|\eta=9}}(t_m)$ a posteriori. In the figure it is quite striking that the a priori knowledge of backhaul network dependencies when deriving the trajectory using local hop-by-hop optimization does not always find a more reliable trajectory than when incorporating the backhaul network dependencies a posteriori. This is due to the fact that the

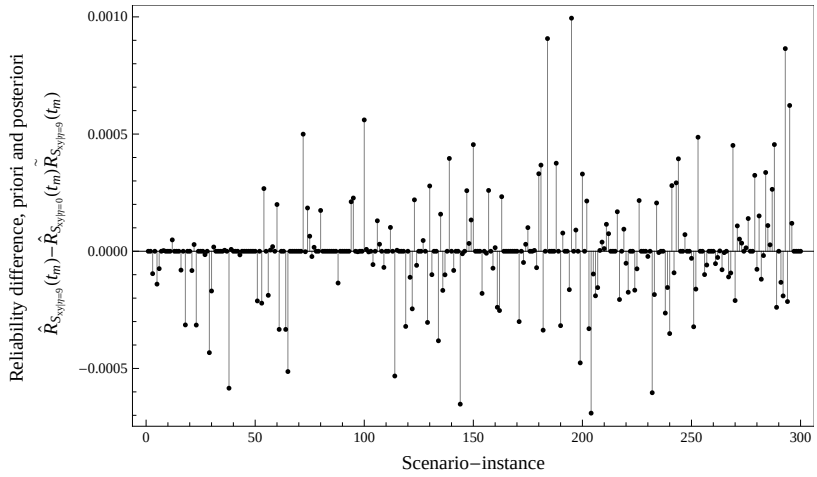

Figure 8. Difference of the reliability of a trajectory identified by a local hop-by-hop optimization with backhaul network dependencies a priori knowledge $\hat{R}_{S_{xy|\eta=9}}(t_m)$ and with a posteriori knowledge $\hat{R}_{S_{xy|\eta=0}}(t_m)\tilde{R}_{S_{xy|\eta=9}}(t_m)$ posteriori. Scenario-instances are ordered identical as for Fig. 6.

local hop-by-hop optimization rarely finds the optimal trajectory as shown in Fig. 7.

Contrary to the local hop-by-hop optimization, the global optimization with the a priori knowledge of backhaul network dependencies always provides the optimal trajectory as shown in Fig. 9.

For the backhaul network dependencies we have only included single point of failures as described in Section 2.3. As may be seen in both Fig. 8 and Fig. 9 the effect on reliability is relatively small compared to the effect of radio and handover failures, hence including cut-sets with two or more resources will not have any noticeable effect.

Fig. 8 and Fig. 9 provided insight into how the reliability of the trajectory identified with global route and local hop-by-hop optimizations are dependent on knowledge of the backhaul network dependencies. To investigate how the access points selected in each virtual cell for the trajectory obtained by a local hop-by-hop optimization is dependent on the knowledge of the backhaul network dependencies we use $|\{i_d \setminus j_d) \cup (x_d \setminus y_d) \mid \{i_d, j_d\} \in S_{ij|\eta=9}, \{x_d, y_d\} \in S_{xy|\eta=0}\}|$ as the metric. This metric provides the total number of different access points for a global route optimal trajectory $S_{ij|\eta=9}$ compared with a local hop-by-hop trajectory $S_{xy|\eta=0}$ and is depicted in Fig. 10. As may be observed, the differences are in general dependent on the number of phases, m, and get larger as m increases. Since the ordering of scenario-instances are the same as

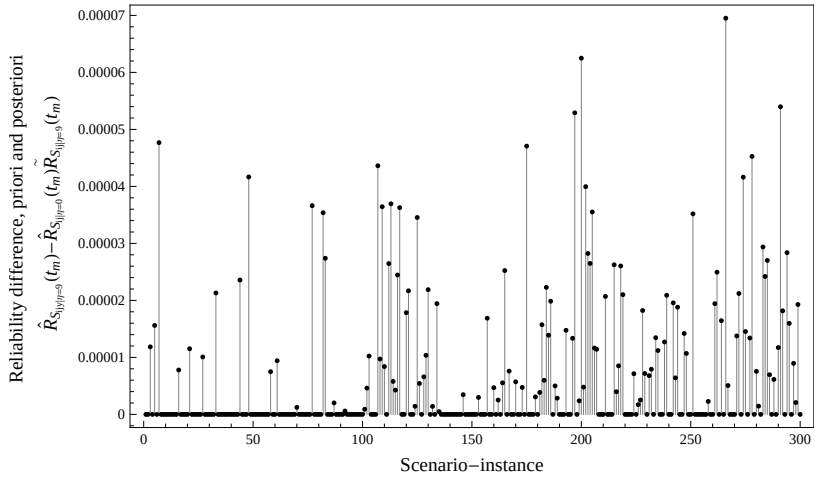

Figure 9. Difference of the reliability of a trajectory identified by a global route optimization with backhaul network dependencies a priori knowledge $\hat{R}_{S_{ij|\eta=9}}(t_m)$ and with a posteriori knowledge $\hat{R}_{S_{ij|\eta=0}}(t_m)\tilde{R}_{S_{ij|\eta=9}}(t_m)$. Scenario-instances are ordered identical as in Fig. 6.

in Fig. 6 the differences follow, from an overall perspective, the same as the difference between $\hat{R}_{S_{ij}}(t_m)$ and $\hat{R}_{S_{xy}}(t_m)$.

Similar, for the global optimization the metric $|\{i_d \backslash j_d) \cup (\backslash \tilde{i}_d \cup \tilde{j}_d) \mid \{i_d, j_d\} \in S_{ij|\eta=9}, \{\tilde{i}_d, \tilde{j}_d\} \in S_{\tilde{i}\tilde{j}|\eta=0}\}|$ is defined. The differences of the selected access points are depicted in Fig. 11. From a overall perspective, it may be observed that for the global optimization different access points selected are more frequent for larger m, i.e., larger network-instances, but the total number of different access points is not significantly higher.

5. Conclusion

In this paper we have proposed how the optimal trajectory, defined as series of access points, of a dual homed critical service, efficiently may be obtained with the Dijkstra's algorithm, where the service reliability is maximized. We have proposed how both the radio and backhaul network connections in a multi operator, multi technology environment may be included into the optimization. We have demonstrated the feasibility of finding the optimal trajectory at run-time for large networks. It is illustrated how the backhaul network connection and dependencies influence the optimal trajectory, both with respect to the reliability and the access points selected. The reliability of the optimal trajectory is mostly affected by radio and handover failures even when single points of failures exist in the backhaul network. Comparisons of the reliability

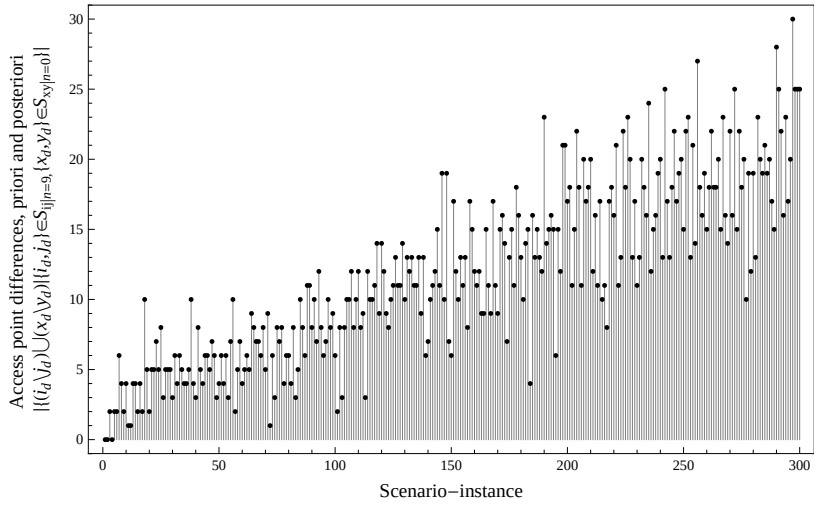

Figure 10. Total number of different access points used for a global trajectory with backhaul network dependencies a priori knowledge $S_{ij|\eta=9}$ and a local hop-by-hop trajectory with a posteriori knowledge $S_{xy|\eta=0}$. Scenario-instances are ordered identical as for Fig. 6.

of the trajectory obtained by global route optimization and trajectory obtained by a local hop-by-hop optimization are provided. These comparisons show significant gains with the use of a global route optimization. The optimal trajectory may be used by handover and multi homing mechanisms to achieve the optimized service reliability and to inform the user of the predicted service reliability of the selected route.

References

[ASS03] I. Aydin, W. Seok, and C. C. Shen. Cellular SCTP: a transport-layer approach to Internet mobility. In *Proc. 12th International Conference on Computer Communications and Networks ICCCN 2003*, pages 285–290, Dallas,USA, October 20–22 2003.

[BDS+10] R. Bauer, D. Delling, P. Sanders, D. Schieferdecker, D. Schultes, and D. Wagner. Combining hierarchical and goal-directed speed-up techniques for Dijkstra's algorithm. *J. Exp. Algorithmics*, 15:2.3:2.1–2.3:2.31, March 2010.

[BDW11] R. Bauer, D. Delling, and D. Wagner. Experimental study of speed up techniques for timetable information systems. *Networks*, 57(1):38–52, March 24 2011.

[Bel56] R. Bellman. On a routing problem. *NOTES*, 16(1), 1956.

[Bha99] R. Bhandari. *Survivable networks: algorithms for diverse routing.* Kluwer Academic Pub, 1999.

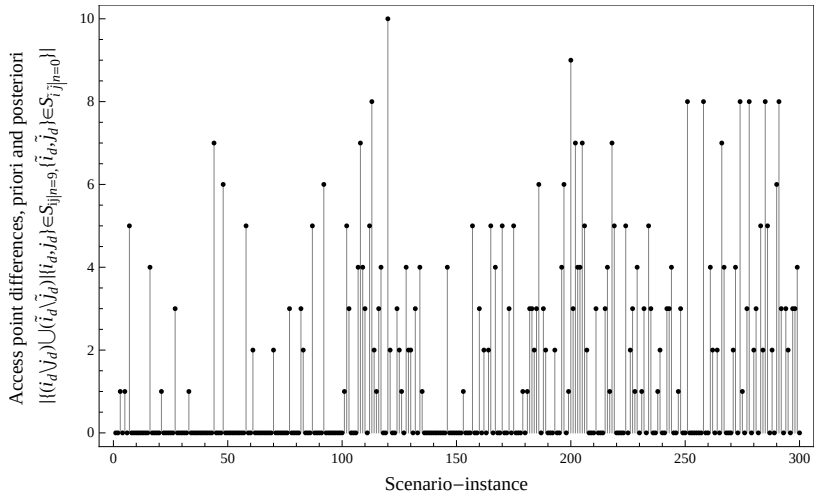

Figure 11. Total number of different access points used for a global trajectory with backhaul network dependencies a priori knowledge $S_{ij|\eta=9}$ and with a posteriori knowledge $S_{\tilde{i}\tilde{j}|\eta=0}$. Scenario-instances are ordered identical as for Fig. 6.

[BP75] R. Barlow and F. Proschan. *Statistical theory of reliability and life testing: probability models.* Holt, Rinehart and Winston New York, 1975.

[BS05] C. Beckman and G. Smith. Shared networks: making wireless communication affordable. *IEEE Transactions on Wireless Communications*, 12(2):78–85, 2005.

[CIRG09] C. Christakos, A. Izquierdo, R. Rouil, and N. Golmie. Using the media independent information service to support mobile authentication in fast mobile IPv6. In *IEEE Wireless Communications and Networking Conference WCNC 2009*, pages 1–6, Budapest, Hungary, April 2009.

[DDF+07] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardo, R. Lopez, T. Kodama, and H. Schulzrinne. Seamless proactive handover across heterogeneous access networks. *Wireless Personal Communications*, 43(3):837–855, June 28, 2007.

[Dij59] E. W. Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1:269–271, 1959. 10.1007/BF01386390.

[DSSW09] D. Delling, P. Sanders, D. Schultes, and D. Wagner. Engineering route planning algorithms. In J. Lerner, D. Wagner, and K. Zweig, editors, *Algorithmics of Large and Complex Networks*, volume 5515 of *Lecture Notes in Computer Science*, pages 117–139. Springer Berlin Heidelberg, 2009.

[DYSH11] F. Demers, H. Yanikomeroglu, and M. St-Hilaire. A survey of opportunities for free space optics in next generation cellular networks. In *Communication Networks and Services Research Conference (CNSR), 2011 Ninth Annual*, pages 210–216, Ottawa, ON, May 2–5 2011.

[EN09] M. B. E. Nordmark. Shim6: Level 3 multihoming shim protocol for IPv6. IETF network working group, 2009.

[FH09] E. L. Følstad and B. E. Helvik. Managing availability in wireless inter domain access. In *Proc. International Conference on Ultra Modern Telecommunications Workshops ICUMT '09*, pages 1–6, October 12–14 2009.

[FH10] E. L. Følstad and B. E. Helvik. Determining dependencies in multi technology inter domain wireless access; a case study. In *IEEE GLOBECOM workshops (GC Wkshps) 2010*, pages 1146–1150, Miami, FL, December 6–10 2010.

[FH13a] E. L. Følstad and B. E. Helvik. Optimizing service continuity in a multi operator multi technology wireless environment. In *Proc. 9th International Conference on the Design of Reliable Communication Networks DRCN 2013*, pages 111–118, Budapest, Hungary, March 4–7 2013.

[FH13b] E. L. Følstad and B. E. Helvik. Reliability modelling of access point selection and handovers in heterogeneous wireless environment. In *Proc. 9th International Conference on the Design of Reliable Communication Networks DRCN 2013*, pages 103–110, Budapest, Hungary, March 4–7 2013.

[HSWW05] M. Holzer, F. Schulz, D. Wagner, and T. Willhalm. Combining speed-up techniques for shortest-path computations. *J. Exp. Algorithmics*, 10:2.5:1–2.5:18, December 2005.

[IEE08] IEEE 802.21,D11; Draft standard for local and metropolitan area networks: Media indepenedent handover services, 2008.

[KKKY11] A. Khan, W. Kellerer, K. Kozu, and M. Yabusaki. Network sharing in the next mobile network: TCO reduction, management flexibility, and operational independence. *IEEE Communications Magazine*, 49(10):134–142, October 2011.

[NFS+09] P. Neves, F. Fontes, S. Sargento, M. Melo, and K. Pentikousis. Enhanced media independent handover framework. In *Proc. 69th IEEE Vehicular Technology Conference VTC Spring 2009*, pages 1–5, Barcelona, Spain, April 26–29 2009. IEEE.

[PJA10] C. Perkins, D. Johnson, and J. Arkko. Mobility support in IPv6. IETF mobile IP working group Internet-draft obsoletes: 3775 (if approved), 2010.

[SXM+00] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. RFC2960: Stream control transmission protocol, 2000.

[Wol11] Wolfram Research, Inc. Documentation centre. `http://reference.wolfram.com/mathematica/guide/Mathematica.html`, 2011.

[X.792] CCITT X.720; Information technology open systems interconnection structure of management information: Management information model, January 1992.

[YSN10] X. Yan, Y. A. Sekercioglu, and S. Narayanan. A survey of vertical handover decision algorithms in fourth generation heterogeneous wireless networks. *Computer Networks*, 54(11):1848–1863, 2010.

Bibliography

[80011] Managing information security risk. organization, mission, and information system view. NIST Special Publication 800-39, March 2011.

[ABC13] E. Ancillotti, R. Bruno, and M. Conti. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Computer Communications*, 36(17–18):1665–1697, November/December 2013.

[AE10] H. Alemdar and C. Ersoy. Wireless sensor networks for healthcare: A survey. *Computer Networks*, 54(15):2688–2710, October 28, 2010.

[AIM10] L. Atzori, A. Iera, and G. Morabito. The Internet of things: A survey. *Computer Networks*, 54(15):2787–2805, October 28, 2010.

[ALRL04] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on dependable and secure computing*, 1(1):11–33, January/March 2004.

[Ama13] Amazon Web Services. Amacon EC2 service level agreement. `http://aws.amazon.com/ec2/sla/`, June 2013.

[AN91] E. Arjas and I. Norros. Stochastic order and martingale dynamics in multivariate life length models: a review. In K. Mosler and M. Scarsini, editors, *Stochastic Orders and Decision under Risk. IMS Lecture Notes—Monograph Series*, volume 19, pages 7–24. Institute of Mathematical Statistics, Hayward, CA, 1991.

[AR02] C. W. Ahn and R. Ramakrishna. A genetic algorithm for shortest path routing problem and the sizing of populations. *Evolutionary Computation, IEEE Transactions on*, 6(6):566–579, December 2002.

[AS08] A. Andreas and J. Smith. Mathematical programming algorithms for two-path routing problems with reliability considerations. *INFORMS Journal on Computing*, 20(4):553–564, 2008.

[ASS03] I. Aydin, W. Seok, and C. C. Shen. Cellular SCTP: a transport-layer approach to Internet mobility. In *Proc. 12th International Conference on Computer Communications and Networks ICCCN 2003*, pages 285–290, Dallas,USA, October 20–22 2003.

[Ave10a] T. Aven. *Misconceptions of Risk*. Statistics in Practice. John Wiley & Sons, Inc., Chichester, UK, 2010.

[Ave10b] T. Aven. On how to define, understand and describe risk. *Reliability Engineering and System Safety*, 95(6):623–631, June 2010.

[Ave11] T. Aven. *Quantitative Risk Assessment. The Scientific Platform.* Cambridge University Press, Cambridge, UK, 2011.

[Bai10] S. R. Bailey. Disaster preparadness and resiliency. In C. R. Kalmanek, S. Misra, and Y. R. Yang, editors, *Guide to Reliable Internet Services and Applications*, chapter 14, pages 517–543. Springer-Verlag Ltd., London, UK, 2010.

[BB98] P. Bishop and R. Bloomfield. A methodology for safety case development. In F. Redmill and T. Anderson, editors, *Industrial Perspectives of Safety-critical Systems: Proc. 6th Safety-critical Systems Symposium, Birmingham 1998*, pages 194–203. Springer-Verlag, 1998.

[BBC+10] A. Bobbio, G. Bonanni, E. Ciancamerla, R. Clemente, A. Iacomini, M. Minichino, A. Scarlatti, R. Terruggia, and E. Zendri. Unavailability of critical SCADA communication links interconnecting a power grid and a telco network. 95(12):1345–1357, 2010. 19th European Safety and Reliability Conference on reliability.

[BCCS00] K. Brady, J. Chandra, Y. Cui, and N. D. Singpurwalla. Hazard potentials and dependent network failures. In *Proc. 33rd Hawaii International Conference on System Sciences HICSS-33*, Wailea Maui, HI, January 4-7 2000.

[BD12] W. Bold and W. Davidson. Mobile broadband: redefining Internet access and empowering individuals. *The Global Information Technology Report 2012: Living in a Hyperconnected World*, pages 68–77, 2012.

[BDS+10] R. Bauer, D. Delling, P. Sanders, D. Schieferdecker, D. Schultes, and D. Wagner. Combining hierarchical and goal-directed speed-up techniques for Dijkstra's algorithm. *J. Exp. Algorithmics*, 15:2.3:2.1–2.3:2.31, March 2010.

[BDW11] R. Bauer, D. Delling, and D. Wagner. Experimental study of speed up techniques for timetable information systems. *Networks*, 57(1):38–52, March 24 2011.

[Bel56] R. Bellman. On a routing problem. *NOTES*, 16(1), 1956.

[BGBF12] L. Budzisz, J. Garcia, A. Brunstrom, and R. Ferrús. A taxonomy and survey of SCTP research. *ACM Computing Surveys*, 44(4):18:1–18:36, August 2012.

[BGC12] H. Blodget, P. Gobry, and A. Cocotas. The future of mobile. *Business Insider*, March 22, 2012.

[BGM+00] Y. Breitbart, M. Garofalakis, C. Martin, R. Rastogi, S. Seshadri, and A. Silberschatz. Topology discovery in heterogeneous IP networks. In *Proc. IEEE Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2000*, volume 1, pages 265–274, Tel Aviv, Israel, March 26–30 2000.

[Bha94] R. Bhandari. Optimal diverse routing in telecommunication fiber networks. In *Proc.13th IEEE Networking for Global Communications INFOCOM '94*, volume 3, pages 1498–1508, Toronto, Ont., June 1994.

[Bha99] R. Bhandari. *Survivable networks: algorithms for diverse routing.* Kluwer Academic Pub, 1999.

[BHK+04] L.-O. Burchard, M. Hovestadt, O. Kao, A. Keller, and B. Linnert. The virtual resource manager: an architecture for SLA-aware resource management. In *IEEE International Symposium on Cluster Computing and the Grid, CCGrid 2004*, pages 126–133, April 19-22 2004.

[BL08] J.-C. Bolot and M. Lelarge. A new perspective on Internet security using insurance. In *Proc. 27th IEEE Conference on Computer Communications INFOCOM 2008*, Phoenix, AZ, April 15-17 2008.

[BM90] G. Brush and N. Marlow. Assuring the dependability of telecommunications networks and services. *IEEE Network*, 4(1):29–34, January 1990.

[BP75] R. Barlow and F. Proschan. *Statistical theory of reliability and life testing: probability models*. Holt, Rinehart and Winston New York, 1975.

[BP05] S. Bryant and P. Pate. RFC 3985: Pseudo wire emulation edge-to-edge (PWE3) architecture. IETF, Internet Engineering Task Force, 2005.

[BS05] C. Beckman and G. Smith. Shared networks: making wireless communication affordable. *IEEE Transactions on Wireless Communications*, 12(2):78–85, 2005.

[BSC01] P. Bhoj, S. Singhal, and S. Chutani. SLA management in federated environments. *Computer Networks*, 35(1):5–24, January 2001.

[BZ14] O. Bello and S. Zeadally. Intelligent Device-to-Device communication in the Internet of Things. *IEEE Systems Journal*, PP(99):1–11, 2014.

[CAI11] The cooperative association for Internet data analysis CAIDA: Macroscopic Internet topology data kit (ITDK). `http://www.caida.org/data/active/internet-topology-data-kit/`, 2011.

[CBB+05] R. Clemente, M. Bartoli, M. Bossi, G. D'Orazio, and G. Cosmo. Risk management in availability SLA. In *Proc. 5th International Workshop on the Design of Reliable Communication Networks DRCN 2005*, pages 411–418, Lacco Ameno, Island of Ischia, Italy, October 16–19 2005.

[Cen13] CenturyLink. Savvis SLA attachment. `http://www.centurylinktechnology.com/legal/sla`, 2013.

[Che99] P. Checkland. *Systems Thinking, Systems Practice: Includes a 30-Year Retrospective*. John Wiley & Sons, Inc., New York, NY, 1999.

[CIRG09] C. Christakos, A. Izquierdo, R. Rouil, and N. Golmie. Using the media independent information service to support mobile authentication in fast mobile IPv6. In *IEEE Wireless Communications and Networking Conference WCNC 2009*, pages 1–6, Budapest, Hungary, April 2009.

[Cis15] Cisco. Cisco visual networking index: Global mobile data traffic forecast update, 2014-2019. `http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html`, February 3, 2015.

[CJ10] P. Chołda and A. Jajszczyk. Recovery and its quality in multilayer networks. *IEEE/OSA Journal of Lightwave Technology*, 28(4):372–389, February 15, 2010.

[CM07] I. Cascos and I. Molchanov. Multivariate Risks and Depth-trimmed Regions. *Finance and Stochastics*, 11(3):373–397, July 2007.

[CMH+07] P. Chołda, A. Mykkeltveit, B. E. Helvik, O. J. Wittner, and A. Jajszczyk. A survey of resilience differentiation frameworks in communication networks. *IEEE Communications Surveys & Tutorials*, 9(4):32–55, 2007.

[CMHJ09] P. Chołda, A. Mykkeltveit, B. E. Helvik, and A. Jajszczyk. Continuity-based resilient communication. In *Proc. 7th International Workshop on the Design of Reliable Communication Networks DRCN 2009*, Washington, D.C., October 25-28 2009.

[CP10] A. Clark and C. J. Pavlovski. Wireless networks for the smart energy grid: application aware networks. In *Proceedings of the International MultiConference of Engineers and Computer Scientists*, volume 2, Hong Kong, March 17–19 2010.

[CPRW06] C.-H. K. Chu, H. Pant, S. H. Richman, and P. Wu. Enterprise VoIP reliability. In *Proc. 12th International Telecommunications Network Strategy and Planning Symposium NETWORKS 2006*, pages 1–6, New Delhi, India, November 2006.

[CSK02] W. Cui, I. Stoica, and R. Katz. Backup path allocation based on a correlated link failure probability model in overlay networks. In *Proc. 10th IEEE International Conference on Network Protocols*, pages 236–245, Paris, France, November 12–15 2002.

[CSKM07] B.-Y. Choi, S. Song, G. Koffler, and D. Medhi. Outage analysis of a university campus network. In *Proc. 16th International Conference on Computer Communications and Networks ICCCN 2007*, Honolulu, HI, August 13-16 2007.

[CTC+09] P. Chołda, J. Tapolcai, T. Cinkler, K. Wajda, and A. Jajszczyk. Quality of resilience as a network reliability characterization tool. *IEEE Network*, 23(2):11–19, March/April 2009.

[DAS97a] B. Dengiz, F. Altiparmak, and A. Smith. Efficient optimization of all-terminal reliable networks, using an evolutionary approach. *IEEE Transactions on Reliability*, 46(1):18–26, March 1997.

[DAS97b] B. Dengiz, F. Altiparmak, and A. Smith. Local search genetic algorithm for optimal design of reliable networks. *IEEE Transactions on Evolutionary Computation*, 1(3):179–188, September 1997.

[DC04] M. Denuit and A. Charpentier, editors. *Mathématiques de l'Assurance Non-Vie*, volume 1, Principes Fondamentaux de Théorie du Risque. Economica, Paris, France, 2004.

[DDF+07] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardo, R. Lopez, T. Kodama, and H. Schulzrinne. Seamless proactive handover across heterogeneous access networks. *Wireless Personal Communications*, 43(3):837–855, June 28, 2007.

[DF07] B. Donnet and T. Friedman. Internet topology discovery: a survey. *Communications Surveys Tutorials, IEEE*, 9(4):56–69, 2007.

[Dij59] E. W. Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1:269–271, 1959. 10.1007/BF01386390.

[DK04] G. Despotou and T. Kelly. Extending the safety case concept to address dependability. In *Proc. 22nd International System Safety Conference ISSC 2004*, Providence, RI, August 2-6 2004.

[DSSW09] D. Delling, P. Sanders, D. Schultes, and D. Wagner. Engineering route planning algorithms. In J. Lerner, D. Wagner, and K. Zweig, editors, *Algorithmics of Large and Complex Networks*, volume 5515 of *Lecture Notes in Computer Science*, pages 117–139. Springer Berlin Heidelberg, 2009.

[DYSH11] F. Demers, H. Yanikomeroglu, and M. St-Hilaire. A survey of opportunities for free space optics in next generation cellular networks. In *Communication Networks and Services Research Conference (CNSR), 2011 Ninth Annual*, pages 210–216, Ottawa, ON, May 2–5 2011.

[E-806] ITU-T E.860; Framework of a service level agreement, February 2006.

[E.808] ITU-T E.800; Terms and definitions related to quality of service and network performance including dependability, September 2008.

[Emm10] B. Emmerson. M2M: the Internet of 50 billion devices. *WinWin Magazine*, pages 19–22, January 2010.

[EN09] M. B. E. Nordmark. Shim6: Level 3 multihoming shim protocol for IPv6. IETF network working group, 2009.

[EUu02] The European Parliament Council: Directive on universal service and users' rights relating to electronic communications networks and services, March 7, 2002.

[FCC05] Federal Communications Comission: Internet policy statement, September 23, 2005.

[FCC10] Federal Communications Commission: Connecting America: The national broadband plan. Directive 2002/22/EC, March 16, 2010.

[FFK+11] Z. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki. Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine*, 49(4):60–65, April 2011.

[FH09] E. L. Følstad and B. E. Helvik. Managing availability in wireless inter domain access. In *Proc. International Conference on Ultra Modern Telecommunications Workshops ICUMT '09*, pages 1–6, October 12–14 2009.

[FH10] E. L. Følstad and B. E. Helvik. Determining dependencies in multi technology inter domain wireless access; a case study. In *IEEE GLOBECOM workshops (GC Wkshps) 2010*, pages 1146–1150, Miami, FL, December 6–10 2010.

[FH11] E. L. Følstad and B. E. Helvik. Failures and changes in cellular access networks; a study of field data. In *Proc. 8th International Workshop on the Design of Reliable Communication Networks DRCN 2011*, pages 132–139, Krakow, Poland, October 10–12 2011.

[FH13a] E. L. Følstad and B. E. Helvik. Optimizing service continuity in a multi operator multi technology wireless environment. In *Proc. 9th International*

Conference on the Design of Reliable Communication Networks DRCN 2013, pages 111–118, Budapest, Hungary, March 4–7 2013.

[FH13b] E. L. Følstad and B. E. Helvik. Reliability modelling of access point selection and handovers in heterogeneous wireless environment. In *Proc. 9th International Conference on the Design of Reliable Communication Networks DRCN 2013*, pages 103–110, Budapest, Hungary, March 4–7 2013.

[Fic12] 54 A/2012 M; Regulation on communications networks and services, May 2012.

[FL09] A. Freedman and M. Levin. Virtual drive test: an in-situ method for network measurements and optimization. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, IWCMC '09, pages 1433–1437, New York, NY, USA, June 21–24 2009. ACM.

[FMXY12] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid; the new and improved power grid: A survey. *CIEEE Communications Surveys & Tutorials*, 14(4):944–980, October 28, 2012.

[Fra12] U. Franke. Optimal IT service availability: Shorter outages, or fewer? *IEEE Transactions on Network and Service Management*, 9(1):22–33, March 2012.

[G8106] ITU-T G.8110.1; Architecture of transport MPLS (T-MPLS) layer networks, November 2006.

[GH10] A. J. González and B. E. Helvik. Guaranteeing service availability in SLAs; a study of the risk associated with contract period and failure process. *IEEE (Revista IEEE America Latina) Latin America Transactions*, 8(4):410–416, August 2010.

[GH12a] A. J. Gonzalez and B. E. Helvik. Analysis of failures characteristics in the UNINETT IP backbone network. *International Journal of Space-Based and Situated Computing*, 2(1):3–11, 2012.

[GH12b] A. J. Gonzalez and B. E. Helvik. System management to comply with SLA availability guarantees in cloud computing. In *Proc. 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom) 2012*, pages 325–332, Tapei, China, December 3–6 2012.

[GHHK10] A. J. Gonzalez, B. E. Helvik, J. K. Hellan, and P. Kuusela. Analysis of dependencies between failures in the UNINETT IP backbone network. In *Proc. 16th Pacific Rim International Symposium on Dependable Computing PRDC 2010*, Tokyo, Japan, December 13-15 2010.

[GHW06] Q. Gan, B. E. Helvik, and O. Wittner. Refined classification of service unavailability for comparison: Shared path protection vs. rerouting. In *Proc. 2006 International Conference on Communication Technology ICCT 2006*, Guilin, China, November 27-30, 2006.

[GJ03] E. Gustafsson and A. Jonsson. Always best connected. *IEEE Wireless Communications*, 10(1):49–55, February 2003.

[GM13] B. S. Ghahfarokhi and N. Movahhedinia. A survey on applications of IEEE 802.21 media independent handover framework in next generation wireless networks. *Computer Communications*, 36(10–11):1101–1119, June 2013.

[GMWD06] A. V. Gheorghe, M. Masera, M. Weijnen, and L. J. De Vries. *Critical Infrastructures at Risk. Securing the Eutopian Electric Power System*, volume 9 of *Topics in Safety, Risk, Reliability and Quality*. Springer, Dordrecht, The Netherlands, 2006.

[Gre86] J. J. Grefenstette. Optimization of control parameters for genetic algorithms. *IEEE Transactions on Systems, Man and Cybernetics*, 16(1):122–128, January 1986.

[GSA11] T. O. Grøtan, F. Størseth, and E. Albrechtsen. Scientific foundations of addressing risk in complex and dynamic environments. *Reliability Engineering and System Safety*, 96(6):706–712, June 2011.

[GSK+11] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke. Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4):529–539, November 2011.

[GT88] A. Goyal and A. Tantawi. A measure of guaranteed availability and its numerical evaluation. *IEEE Transactions on Computers*, 37(1):25–32, January 1988.

[Hai09] Y. Y. Haimes. *Risk Modeling, Assessment, and Management*. Wiley Series in Systems Engineering and Management. John Wiley & Sons, Inc., Hoboken, NJ, 2009.

[Har05] K. L. Hartley. Defining effective service level agreements for network operation and maintenance. *Bell labs technical journal*, 9(4):139–143, 2005.

[Hel04] B. E. Helvik. Perspectives on the dependability of networks and services. *Telektronikk*, 100(3):27–44, 2004.

[HLC10] C.-M. Huang, M.-S. Lin, and L.-H. Chang. The design of mobile concurrent multipath transfer in multihomed wireless mobile networks. *The Computer Journal*, 53(10):1704–1718, 2010.

[Hol92] J. Holland. Adaptation in natural and artificial systems. 1975. *Ann Arbor, MI: University of Michigan Press and*, 1992.

[HSWW05] M. Holzer, F. Schulz, D. Wagner, and T. Willhalm. Combining speed-up techniques for shortest-path computations. *J. Exp. Algorithmics*, 10:2.5:1–2.5:18, December 2005.

[HT09] P. E. Heegaard and K. S. Trivedi. Network survivability modeling. *Computer Networks*, 53(8):1215–1234, June 2009.

[HTHB97] M. Hecht, D. Tang, H. Hecht, and R. W. Brill. Quantitative reliability and availability assessment for critical systems including software. In *Proc. 12th Annual Conference on Computer Assurance COMPASS'97*, Gaithersburg, MD, June 16-19 1997.

[HUI+12] W. Hapsari, A. Umesh, M. Iwamura, M. Tomala, B. Gyula, and B. Sebire. Minimization of drive tests solution in 3GPP. *IEEE Communications Magazine*, 50(6):28–36, June 2012.

[HWJ06] J. Han, D. Watson, and F. Jahanian. An experimental study of Internet path diversity. *IEEE Transactions on Dependable and Secure Computing*, 3(4):273–288, October/December 2006.

[IAS06] J. Iyengar, P. Amer, and R. Stewart. Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths. *IEEE/ACM Transactions on Networking*, 14(5):951–964, October 2006.

[IEE08] IEEE 802.21,D11; Draft standard for local and metropolitan area networks: Media indepenedent handover services, 2008.

[IEE09] IEEE standard for local and metropolitan area networks - part 21: Media independent handover services, 2009.

[INSZ09] P. Iovanna, M. Naldi, R. Sabella, and C. Zema. Economics-driven short-term traffic management in MPLS-based self-adaptive networks. In *Proc. IFIP 4^{th} International Workshop on Self-Organizing Systems IWSOS 2009*, Zurich, Switzerland, December 9-11 2009.

[Int13] International Telecommunication Union. Trends in telecommunication reform 2013. transnational aspects on regulation in a networked society. Technical report, May 2013.

[IRR11] Merit Nnetwork, inc.: Internet routing registry, 2011.

[iso05] ISO/IEC 20000-1 Information technology service management part 1: Specification, and part 2: Code of practice, December 2005.

[IY02] M. Iskander and Z. Yun. Propagation prediction models for wireless communication systems. *IEEE Transactions on Microwave Theory and Techniques*, 50(3):662–673, March 2002.

[Jap08] Japan Internet Provers Aassociation (JAIPA), Telecommunications Carrears Association (TCA), Telecom Services Association (TELESA) and Japan Cable and Telecommunications Association (JCTA): Guideline for packet shaping, May 2008.

[Joh05] D. M. Johnson. QoS control versus generous dimensioning. *BT Technology Journal*, 23(2):81–96, April 2005.

[JT03] B. Jæger and D. Tipper. Prioritized traffic restoration in connection oriented QoS based networks. *Computer Communications*, 26(18):2025–2036, December 2003.

[KAB+14] A. Kvalbein, S. E. Arge, D. Baltrūnas, A. Elmokashfi, and O. Lysne. Robusthet i norske mobilnett. tilstandsrapport 2013. Technical Report ISBN 978-82-92593-13-4, CRNA, Center of Resilient Networks & Applications, February 2014.

[KAK11] A. Khan, M. Adda, and T. Khan. LRPF: an RF coverage reporting protocol for LTE systems. *IEEE Wireless Communications*, 18(6):64–72, 2011.

[Kel98] T. P. Kelly. *Arguing Safety. A Systematic Approach to Safety Case Management.* PhD thesis, Department of Computer Science, University of York, York, UK, September 1998.

[Ker11] T. Kernen. Public route server and looking glass list. `http://www.traceroute.org/`, 2011.

[KG81] S. Kaplan and B. J. Garrick. On the quantitative definition of risk. *Risk Analysis*, 1(1):11–28, March 1981.

[KHMS11] J. H. Kietzmann, K. Hermkens, I. P. McCarthy, and B. S. Silvestre. Social media? get serious! understanding the functional building blocks of social media. *Business Horizons*, 54(3):241–251, May/June 2011.

[KIK+04] S. Kashihara, K. Iida, H. Koga, Y. Kadobayashi, and S. Yamaguchi. Multipath transmission algorithm for end-to-end seamless handover across heterogeneous wireless access networks. *EICE Transactions on Communications*, E87-B(3):400–496, March 1, 2004.

[KKKY11] A. Khan, W. Kellerer, K. Kozu, and M. Yabusaki. Network sharing in the next mobile network: TCO reduction, management flexibility, and operational independence. *IEEE Communications Magazine*, 49(10):134–142, October 2011.

[KKP08] M. Kassar, B. Kervella, and G. Pujolle. An overview of vertical handover decision strategies in heterogeneous wireless networks. *Computer Communications*, 31(10):2607–2620, June 25, 2008.

[KMH05] K. Kim, S. Min, and Y. Han. Fast handover method for mSCTP using FMIPv6. *Lecture notes in computer science*, 3794:846–855, December 13–15 2005.

[KN10] P. Kuusela and I. Norros. On/off process modeling of IP network failures. In *Proc. 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2010*, pages 585–594, Chicago, IL, June 28 – July 1 2010.

[Kuh97] D. R. Kuhn. Sources of failure in the public switched telephone network. *IEEE Computer*, 30(4):31–36, April 1997.

[Kun02] H. Kunreuther. The role of insurance in managing extreme events: Implications for terrorism coverage. *Business Economics*, 37(2):6–16, April 2002.

[LAJ99] C. Labovitz, A. Ahuja, and F. Jahanian. Experimental study of Internet stability and backbone failures. In *Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing, 1999. Digest of Papers*, pages 278–285, June 15–18 1999.

[LHD13] P. Leitner, W. Hummer, and S. Dustdar. Cost-based optimization of service compositions. *IEEE Transactions on Services Computing*, 6(2):239–251, 2013.

[LHTC12] G. Levitin, K. Hausken, H. A. Taboada, and D. W. Coit. Data survivability vs. security in information systems. *Reliability Engineering and System Safety*, 100:19–27, April 2012.

[LL06] J. Lepropre and G. Leduc. Inferring groups of correlated failures. In *Proc. 2nd Conference on Future Networking Technologies CoNEXT'06*, Lisbon, Portugal, December 4-7 2006.

[LMB+02] W. Lai, D. McDysan, J. Boyle, M. Carlzon, R. Coltun, T. Griffin, E. Kern, and T. Reddington. Network hierarchy and multilayer survivability, November 2002.

[LMK08] H. Liu, C. Maciocco, and V. Kesavan. Using predictive triggers to improve handover performance in mixed networks. *Lecture Notes in Computer Science*, 4982:877–888, May 5–9 2008.

[LML10] H.-W. Lee, E. Modiano, and K. Lee. Diverse routing in networks with probabilistic failures. *IEEE/ACM Transactions on Networking*, 18(6):1895–1907, December 2010.

[Low76] W. W. Lowrance. *Of Acceptable Risk: Science and the Determination of Safety*. William Kaufmann, Inc., Los Altos, CA, 1976.

[LSGTG08] X. Li, R. Schelb, C. Görg, and A. Timm-Giel. UMTS HSPA and R99 traffic separation. *Wireless and Mobile Networking*, 284:213–224, 2008.

[LW02] F. Li and J. Whalley. Deconstruction of the telecommunications industry: from value chains to value networks. *Telecommunications Policy*, 26(9–10):451–472, October/November 2002.

[LWZ08] J. Liao, J. Wang, and X. Zhu. cmpSCTP: An extension of SCTP to support concurrent multi-path transfer. In *Proc. IEEE International Conference on Communications ICC '08*, pages 5762–5766, May 19–23 2008.

[LY15] C. Liang and F. Yu. Wireless network virtualization: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, 17(1):358–380, Firstquarter 2015.

[MBCCM11] J. Márquez-Barja, C. T. Calafate, J.-C. Cano, and P. Manzoni. An overview of vertical handover techniques: Algorithms, protocols and tools. *Computer Communications*, 34(8):985–997, June 1 2011.

[MC08] H. Maciejewski and D. Caban. Estimation of repairable system availability within fixed time horizon. *Reliability Engineering & System Safety*, 93(1):100–106, January 2008.

[MFE05] A. J. McNeil, R. Frey, and P. Embrechts. *Quantitative Risk Management: Concepts, Techniques and Tools*. Princeton University Press, Princeton, NJ, 2005.

[MH09] A. Mykkeltveit and B. E. Helvik. Adaptive management of connections to meet availability guarantees in SLAs. In *Proc. IFIP/IEEE 11th International Symposium on Integrated Network Management IM 2009*, Long Island, NY, June 1-5 2009.

[MIB+08] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot. Characterization of failures in an operational IP backbone network. *IEEE/ACM Transactions on Networking*, 16(4):749–762, August 2008.

[Mic13] Microsoft. Windows azure cloud services, virtual machines, and virtual network service level agreement (SLA). `http://www.microsoft.com/en-us/download/details.aspx?id=38427`, 2013.

[MM10] A. Mateus and R. Marinheiro. A media independent information service integration architecture for media independent handover. In *Proc. 9th International Conference on Networks (ICN), 2010*, pages 173–178, April 11–16 2010.

[MN11a] L. Mastroeni and M. Naldi. Network protection through insurance: Premium computation for the on-off service model. In *Proc. 8th International Workshop on the Design of Reliable Communication Networks DRCN 2011*, pages 46–53. IEEE, October 2011.

[MN11b] L. Mastroeni and M. Naldi. Options and overbooking strategy in the management of wireless spectrum. *Telecommunication Systems*, 48(1-2):31–42, October 2011.

[MVM02] S. M. Matz, L. G. Votta, and M. Malkawi. Analysis of failure and recovery rates in a wireless telecommunications system. In *Proc. International Conference on Dependable Systems and Networks DSN 2002*, pages 687–693, June 23–26 2002.

[MyS10] MySQL Team. MySQL reference manuals. `http://dev.mysql.com/doc/`, 2010.

[MYY07] C. Moon, S. Yang, and I. Yeom. Performance analysis of decentralized RAN (radio access network) discovery schemes for IEEE 802.21. In *Proc.66th IEEE Vehicular Technology Conference VTC-2007 Fall*, pages 41–45, Baltimore, MD, September 30 – October 3 2007.

[MZB+13] D. S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, and D. Cvetkovic. Smart power grid and cloud computing. *Renewable and Sustainable Energy*, 24:566–577, 2013.

[NBW06] M. Newman, A.-L. Barabási, and D. J. Watts. *The Structure and Dynamics of Networks*. Princeton University Press, Princeton, NJ, 2006.

[ND08] M. Naldi and G. D'Acquisto. A normal copula model for the economic risk analysis of correlated failures in communications networks. *Journal of Universal Computer Science*, 14(5):786–799, March 2008.

[Nex13] Nextgen group. Service level agreement (SLA). `http://www.nextgennetworks.com.au/about/service-management-centre/service-level-agreement/`, 2013.

[NFS+09] P. Neves, F. Fontes, S. Sargento, M. Melo, and K. Pentikousis. Enhanced media independent handover framework. In *Proc. 69th IEEE Vehicular Technology Conference VTC Spring 2009*, pages 1–5, Barcelona, Spain, April 26–29 2009. IEEE.

[NGAM07] N. Nasser, S. Guizani, and E. Al-Masri. Middleware vertical handoff manager: A neural network-based solution. In *Proc. IEEE International Conference on Communications ICC '07*, pages 5671–5676, Glasgow, Scotland, June 26–28 2007.

[NKS08] I. Norros, P. Kuusela, and P. Savola. A dependability case approach to the assessment of IP networks. In *Proc. 2nd International Conference on Emerging Security Information, Systems and Technologies SECUWARE 2008*, Cap Esterel, France, August 25-31 2008.

[NNLS13] L. Norros, I. Norros, M. Liinasuo, and K. Seppnen. Impact of human operators on communication network dependability. *Cognition, Technology & Work*, 15:363–372, November 2013.

[Nor04] L. Norros. *Acting under Uncertainty. The Core-Task Analysis in Ecological Study of Work*. VTT Technical Research Centre of Finland, Espoo, Finland, 2004. VTT Publications: 546.

[NR08] I. Norros and H. Reittu. Network models with a 'soft hierarchy': A random graph construction with loglog scalability. *IEEE Network*, 22(2):40–46, March/April 2008.

[NSG15] S. Ntalampiras, Y. Soupionis, and G. Giannopoulos. A fault diagnosis system for interdependent critical infrastructures based on HMMs. *Reliability Engineering & System Safety*, 138:73–81, 2015.

[NSTW06] H. Ng, M. Sim, C. Tan, and C. Wong. Wireless technologies for telemedicine. *BT Technology Journal*, 24(2):130–137, April 2006.

[O'B09] K. J. O'Brien. Ericsson and Nokia Siemens are managing just fine. *The New York Times*, April 12, 2009.

[Off07a] Office of Government Commerce (OGC). *ITIL Core Books, Service Operation*. The Stationery Office (TSO), May 2007.

[Off07b] Office of Government Commerce (OGC). *ITIL Core Books, Service Transition*. The Stationery Office (TSO), May 2007.

[ON11] N. Ogino and H. Nakamura. Telecommunications network planning method based on probabilistic risk assessment. *IEICE Transactions on Communications*, E94-B(12):3459–3470, December 2011.

[OS07] A. Oliner and J. Stearley. What supercomputers say: A study of five system logs. In *Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN 2007*, pages 575–584, Edinburgh, UK, June 25–28 2007.

[Ouy14] M. Ouyang. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 121:43–60, 2014.

[PCR+08] H. Pant, C. Chu, S. Richman, A. Jrad, and G. O'Reilly. Reliability of next-generation networks with a focus on IMS architecture. *Bell Labs Technical Journal*, 12(4):109–126, 2008.

[PDGB+03] S. Porcarelli, F. Di Giandomenico, A. Bondavalli, M. Barbera, and I. Mura. Service-level availability estimation of GPRS. *IEEE Transactions on Mobile Computing*, 2(3):233–247, July/September 2003.

[PJA10] C. Perkins, D. Johnson, and J. Arkko. Mobility support in IPv6. IETF mobile IP working group Internet-draft obsoletes: 3775 (if approved), 2010.

[PKH+00] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J. Makela, R. Pichna, and J. Vallstron. Handoff in hybrid mobile data networks. *IEEE Personal Communications*, 7(2):34–47, 2000.

[PKV+02] C. Pattichis, E. Kyriacou, S. Voskarides, M. Pattichis, R. Istepanian, and C. Schizas. Wireless telemedicine systems: an overview. *IEEE Antennas and Propagation Magazine*, 44(2):143–153, April 2002.

[pot11] M. R. potentialsnd. *Risk Assessment. Theory, Methods, and Applications.* John Wiley & Sons, Inc., Hoboken, NJ, 2011.

[Ree10] C. R. Reeves. Genetic algorithms. In M. Gendreau, J.-Y. Potvin, and F. S. Hillier, editors, *Handbook of Metaheuristics*, volume 146 of *International Series in Operations Research & Management Science*, pages 109–139. Springer US, 2010.

[Rin04] S. M. Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *Proc. 37th Annual Hawaii International Conference on System Sciences*, page 8pp., Big Island, HI, January 5–8 2004.

[RS95] G. Rubino and B. Sericola. Interval availability analysis using denumerable markov processes: application to multiprocessor subject to breakdowns and repair. *IEEE Transactions on Computers*, 44(2):286–291, February 1995.

[RT88] A. Reibman and K. Trivedi. Numerical transient analysis of markov models. *Computers & Operations Research*, 15(1):19–36, 1988.

[RT07] M. Riegel and M. Tuexen. Mobile SCTP. (09), November 2007.

[SAU12] N. Saputro, K. Akkaya, and S. Uludag. A survey of routing protocols for smart grid communications. *Computer Networks*, 56(11):2742–2771, July 31 2012.

[SBM09] J. Sauvé, C. Bartolini, and A. Moura. Looking at business through a keyhole. In *Proc. IFIP/IEEE International symposium on integrated network management-workshops IM*, pages 48–51, New York, NY, June 1–5 2009.

[Sch11] F. Schulz. Decision support for business-related design of service level agreements. In *Proc.2nd IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pages 35–38, Beijing, China, July 15–17 2011.

[SCK04] D. P. Siewiorek, R. Chillarege, and Z. T. Kalbarczyk. Reflections on industry trends and experimental research in dependability. *IEEE Transacions on Dependable and Secure Computing*, 1(2):109–127, April/June 2004.

[Sco13] J. Scott, J. M.and Burns. Study on impact of traffic off-loading and related technological trends on the demand for wireless broadband spectrum. Technical report, European Commission, Directorate-General for Communications Networks, Content and Technology, 2013.

[SG10] B. Schroeder and G. Gibson. A large-scale study of failures in high-performance computing systems. *IEEE Transactions on Dependable and Secure Computing*, 7(4):337–351, October/December 2010.

[SK01] C. Simache and M. Kaaniche. Measurement-based availability analysis of Unix systems in a distributed environment. In *Proc.12th International Symposium on Software Reliability Engineering ISSRE 2001*, pages 346–355, Hong Kong, November 27–30 2001.

[SNLW08] E. Stevens-Navarro, Y. Lin, and V. Wong. An MDP-based vertical handoff decision algorithm for heterogeneous wireless networks. *IEEE Transactions on Vehicular Technology*, 57(2):1243–1254, 2008.

[SPC11] B. M. Sousa, K. Pentikousis, and M. Curado. Multihoming management for future networks. *Mob. Netw. Appl.*, 16(4):505–517, August 2011.

[Spr77] J. Spragins. Dependent failures in data communication systems. *IEEE Transactions on Communications*, COM-25(12):1494–1499, December 1977.

[SR93] S. Soh and S. Rai. Experimental results on preprocessing of path/cut terms in sim of disjoint products technique. *IEEE Transactions on Reliability*, 42(1):24–33, 1993.

[SRM+12] B. Sayrac, J. Riihijärvi, P. Mähönen, S. Ben Jemaa, E. Moulines, and S. Grimoud. Improving coverage estimation for cellular networks with spatial bayesian prediction based on measurements. In *Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design*, CellNet '12, pages 43–48, New York, NY, USA, 2012. ACM.

[SSNW08] C. Sun, E. Stevens-Navarro, and V. Wong. A constrained MDP-based vertical handoff decision algorithm for 4G wireless networks. In *Proc. IEEE International Conference on Communications ICC '08*, pages 2169–2174, Bejing, China, May 19–23 2008.

[SSY12] Y. K. Salih, O. H. See, and S. Yussof. MIH: State of art and a proposed future direction in the heterogeneous wireless networks. *Journal of Applied Sciences(Faisalabad)*, 12(13):1318–1331, 2012.

[Suu74] J. W. Suurballe. Disjoint paths in a network. *Networks*, 4(2):125–145, 1974.

[SW07] N. Svendsen and S. Wolthusen. Graph models of critical infrastructure interdependencies. *Lecture Notes in Computer Science*, 4543:208–211, 2007.

[SWG10] A. Snow, G. Weckman, and V. Gupta. Meeting SLA availability guarantees through engineering margin. In *Proc. 9th International Conference on Networks (ICN)*, pages 331–336, Menuires, France, April 11–16 2010.

[SXM+00] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. RFC2960: Stream control transmission protocol, 2000.

[SZ06] F. Siddiqui and S. Zeadally. Mobility management across hybrid wireless networks: Trends and challenges. *Computer Communications*, 29(9):1363–1385, 2006.

[Sze05] G. Szegö. Measures of risk. *European Journal of Operational Research*, 163(1):5–19, May 2005.

[TA11] J. Tømmerås and T. Aven. A framework for reliability and risk centered maintenance. *Reliability Engineering and System Safety*, 96(2):324–331, February 2011.

[Tak57] L. Takács. On certain sojourn time problems in the theory of stochastic processes. *Acta Mathematica Hungarica*, 8(1):169–191, 1957.

[TBvdZ04] J. Trienekens, J. Bouman, and M. van der Zwan. Specification of service level agreements: Problems, principles and practices. *Software Quality Journal*, 12(1):43–57, 2004.

[TC07] N. Taesombut and A. A. Chien. Evaluating network information models on resource efficiency and application performance in lambda-grids. In *Proc.ACM/IEEE conference on Supercomputing SC '07*, pages 1–12, New York, NY, USA, 2007. ACM.

[TCv10] R. Tafazolli, L. M. Correia, and various. eMobility mobile and wireless communications technology platform. 2010.

[Tel14a] Telenor. Prisliste for kapasitetsprodukt. `https://www.jara.no/produkter/kapasitet/priserogavtaler/`, June 2014.

[Tel14b] Telstra. Standard restoration and SLA premium. `http://www.telstra.com.au/customer-terms/business-government/other-services/restoration-sla-premium/`, June 2014.

[TFC11] H. Tabrizi, G. Farhadi, and J. Cioffi. A learning-based network selection method in heterogeneous wireless systems. In *Proc. IEEE Global Telecommunications Conference (GLOBECOM 2011)*, pages 1–5, Huston, TX, December 5–9 2011.

[Tit11] Text of code of federal regulations/e-CFR: Title 47 telecommunication, 2011.

[Tod06] M. T. Todinov. Reliability analysis based on the losses from failures. *Risk Analysis*, 26(2):311–335, April 2006.

[TRDA11] J. Turkka, T. Ristaniemi, G. David, and A. Averbuch. Anomaly detection framework for tracing problems in radio networks. In *Proc.10th International Conference on Networks ICN*, pages 317–321, St Maarten, The Netherlands Antilles, January 23–28 2011.

[TS210a] 3GPP TS 23.002; Network architecture, December 2010.

[TS210b] 3GPP TS 25.331; Mobile radio interface layer 3 specification; radio resource control (rrc) protocol, February 2010.

[TS313a] 3GPP TS 32.421; Subscriber and equipment trace; trace concepts and requirements, April 2013.

[TS313b] 3GPP TS 36.300; Overall description; stage 2, September 2013.

[TS313c] 3GPP TS 37.320; Radio measurement collection for minimization of drive tests (MDT), April 2013.

[TS410] 3GPP TS 44.018; Mobile radio interface layer 3 specification; radio resource control (rrc) protocol, March 2010.

[TT05] R. Taylor and C. Tofts. Death by a thousand SLAs: a short study of commercial suicide pacts. *Forschungsbericht, Hewlett-Packard Labs*, 2005.

[UHV11] I. B. Utne, P. Hokstad, and J. Vatn. A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering and System Safety*, 96(6):671–678, June 2011.

[UNI11] The norwegian research network UNINETT: Downtime statistics. `http://drift.uninett.no/downs/`, 2011.

[Var07] U. Varshney. Pervasive healthcare and wireless health monitoring. *Mob. Netw. Appl.*, 12(2-3):113–127, March 2007.

[VCD+05] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M. Jaeger. General availability model for multilayer transport networks. In *Proc. 5th International Workshop on Design of Reliable Communication Networks (DRCN 2005)*, pages 85–92, Lacco Ameno, Island of Ischia, Italy, October 16–19 2005.

[Ver13] Verizon. European service level agreement for: Verizon Internet dedicated, Internet DSL office and Internet DSL solo. `http://www.verizonenterprise.com/terms/emea/at/sla/`, 2013.

[VTA13] K. Vajanapoom, D. Tipper, and S. Akavipat. Risk based resilient network design. *Telecommunication Systems*, 52(2):799–811, 2013.

[WAD09] W. Willinger, D. Alderson, and J. C. Doyle. *Mathematics and the Internet: A source of enormous confusion and great potential.* Defense Technical Information Center, 2009.

[Wat67] L. J. Watters. Reduction of integer polynomial programming problems to zero-one linear programming problems. *Operations Research*, 15(6):1171–1174, 1967.

[WB10] L. Wu and R. Buyya. Service level agreement (SLA) in utility computing systems. *Arxiv preprint arXiv:1010.2881*, 2010.

[Whe11] E. Wheeler. *Security Risk Management.* Syngress, Waltham, MA, 2011.

[WK13] L. Wang and G.-S. Kuo. Mathematical modeling for network selection in heterogeneous wireless networks; a tutorial. *IEEE Communications Surveys & Tutorials*, 15(1):271–292, 2013.

[Wol10] Wolfram Research, Inc. Documentation centre. `http://reference.wolfram.com/mathematica/guide/Mathematica.html`, 2010.

[Wol11] Wolfram Research, Inc. Documentation centre. `http://reference.wolfram.com/mathematica/guide/Mathematica.html`, 2011.

[WTJ+11] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson. M2M: From mobile to embedded Internet. *IEEE Communications Magazine*, 49(4):36–43, 2011.

[X.792] CCITT X.720; Information technology open systems interconnection structure of management information: Management information model, January 1992.

[XTMM11] M. Xia, M. Tornatore, C. U. Martel, and B. Mukherjee. Risk-aware provisioning for optical WDM mesh networks. *IEEE/ACM Transactions on Networking*, 19(3):921–931, June 2011.

[YCG07] S.-J. Yoo, D. Cypher, and N. Golmie. LMS predictive link triggering for seamless handovers in heterogeneous wireless networks. In *Proc. IEEE*

Military Communications Conference MILCOM 2007, pages 1–7, October 29–31 2007.

[YGB14] M. Yigit, V. C. Gungor, and S. Baktir. Cloud computing for smart grid applications. *Computer Networks*, 70:312–329, 2014.

[YMBB05] M. Yannuzzi, X. Masip-Bruin, and O. Bonaventure. Open issues in interdomain routing: a survey. *IEEE Network*, 19(6):49–56, 2005.

[YSN10] X. Yan, Y. A. Sekercioglu, and S. Narayanan. A survey of vertical handover decision algorithms in fourth generation heterogeneous wireless networks. *Computer Networks*, 54(11):1848–1863, 2010.

[ZG05] L. Zhou and W. Grover. A theory for setting the "safety margin" on availability guarantees in an SLA. In *Proc. 5th International Workshop on the Design of Reliable Communication Networks DRCN 2005*, pages 403–409, Lacco Ameno, Island of Ischia, Italy, October 16-19 2005.

[ZJZ12] M. Zekri, B. Jouaber, and D. Zeghlache. A review on mobility management and vertical handover solutions over heterogeneous wireless networks. *Computer Communications*, 35(17):2055–2068, 2012.