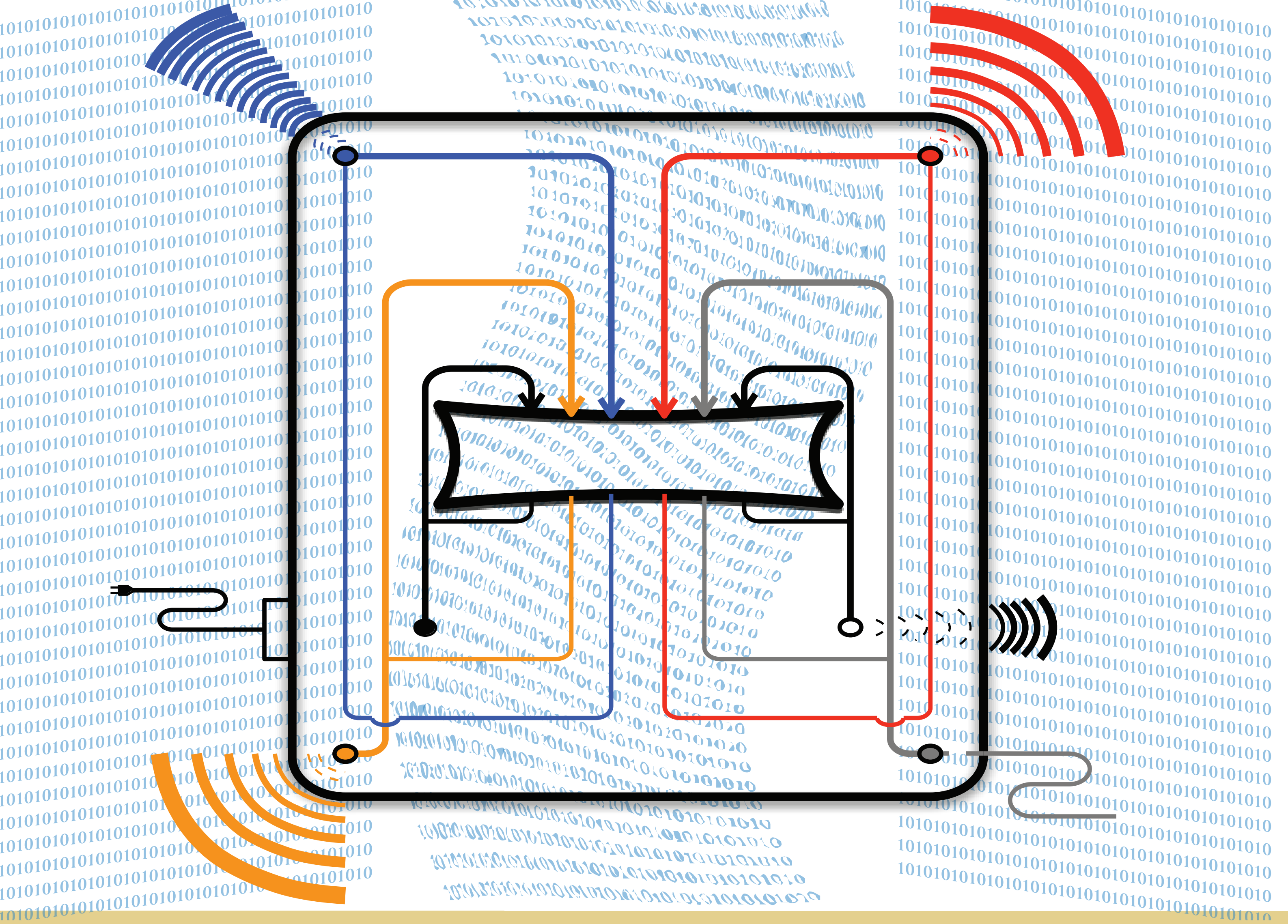


Bruno Miguel de Oliveira Sousa

Multihoming Aware Optimization Mechanism

Tese de Doutoramento em Engenharia Informática (pré Bolonha)
orientada por Marilia Pascoal Curado e Konstantinos Pentikousis

Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia
da Universidade de Coimbra
Julho de 2013

Multihoming Aware Optimization Mechanism

Mecanismo de Optimização com Suporte de Múltiplos Caminhos

Bruno Miguel de Oliveira Sousa

Department of Informatics Engineering

Faculty of Sciences and Technology
University of Coimbra

A thesis submitted for the degree of

Doctor of Philosophy

2013

Multihoming Aware Optimization Mechanism

Bruno Miguel de Oliveira Sousa

Department of Informatics Engineering

Faculty of Sciences and Technology
University of Coimbra

Thesis submitted as partial fulfillment of the requirements of Doctor of Philosophy on Informatics Engineering (before Bologna) in the University of Coimbra, for the award of Doctor in the domain of Telematics Networking and Communications under the care of advisor Professor Marilia Pascoal Curado and co-advisor Dr. Konstantinos Pentikousis.

Grant from Fundação para a Ciência e a Tecnologia (FCT) SFRH/BD/61256/2009.

2013

To my mother Alzira and to my brother Pedro,
whose sacrifice and love, have tailored
the person I am today.

Acknowledgements

A thesis is a work of a high magnitude, requiring the best of us. Believing in every moment, probably is the first step to arrive here. To my supervisor, It's unfair to acknowledge the support throughout the thesis within a few words, my sincere excuses for this. You made me believe that it was possible, that the best of me could reach it with success. The remarkable guidance lead me to work with the feeling that I was performing a 'big and important mission' - research. I was paving the way, to a better world tomorrow, with efficient multihoming mechanisms. Dear Marilia Curado, my eternal thanks.

To my co-supervisor, Konstantinos Pentikousis, for pushing me to high limits, to overcome my limitations with success. Thanks for your courage to demonstrate that, in some moments, I could have done better, perfection is, indeed, your *Lemma*. Thanks for sharing and teaching me that the perfection *Lemma* lead us to horizons never thought before.

Life gives us friends that share knowledge life moments, that some way grow up with us. Vitor Bernardo thanks for the fruitful discussions, and I must confess that I admire your courage and dedication when you read my article with almost twenty pages, with plenty of mathematical formulas. David thank you for sharing things you just learned in the moment and for the active comments. I do remember that I've shared with you some LaTeX tips, but afterall you became the master.

Probably, there is always someone in every project that must do the hard work. Ricardo Santos you were this one, without afraid of the job. Without you I could not have tested MeTHODICAL in the cloud, in a real testbed. Alexandre thanks for programming on the implementation of mCoA++.

Love can inspire us to move mountains. To my wife, Célia I express my deep gratitude, for being there in the 'optimized' moments and for keeping my perseverance in high levels to overcome the moments when there was no light. To my two daughters, the oldest, Susana for asking me what was the thesis about, It made me believe in it with other perspective. To the youngest, Luana whose premise is enjoying life by playing, but smart enough to understand that thesis was very important to Daddy. To you, Luana, I ask my excuses for the time stolen by the thesis.

Abstract

THE always best connected paradigm has gain a lot of interest in the research and scientific community. The availability of different wireless technologies and the proliferation of devices supporting multiple connections are opening new possibilities for users to share information everywhere and everytime. The multihoming support is being enriched to levels never before established. Indeed, users can configure devices to meet their own requirements, decrease communication costs by choosing links with no expenses associated, or opting for links that provide extended coverage. Such kind of configuration is often limited to static policies that aim the maximization of a single requirement, such as monetary cost or coverage. This approach is not efficient. For instance, if the optimization aims to decrease cost, extend coverage and increase security support simultaneously, static policies do not scale and have narrow support for multihoming goals, namely resilience, ubiquity and load sharing.

Multihoming is an important aspect in computer networks. To enable higher levels of availability or optimize recovery processes in the presence of failures are goals that mechanisms improving resilience aim to support. Other goals, in a ubiquity aspect, can include networks providing extended coverage but with minimized costs. To successfully achieve such goals and others, multihoming must be considered from the early phases of Internet architectures development. The choice of protocols and technologies with the best multihoming support is an important step to conceive network architectures that are multihoming efficient. With this concern in mind, this thesis introduces the specification of resilience and ubiquity frameworks that assess the support of resilience and ubiquity goals in protocols. These evaluation frameworks provide a taxonomy that fully characterize multihoming goals.

Efficient multihoming support requires the optimization of multiple criteria comprising diverse goals. This *NP-hard* problem considers benefits criteria providing profit and costs criteria introducing some kind of overhead. Techniques like Multiple Attribute Decision Mechanism (MADM) provide ideal solutions for such kind of optimization problems, as they are not tied to a specific number of criteria. Even though, previously defined MADM techniques include criteria preferences, they do

not specify how these preferences can be expressed in objective and consistent ways. In addition, they can introduce side-effects, such as unnecessary handovers. Bearing with these issues in mind, this work introduces MeTHODICAL, an optimization technique that provides a complete solution for optimization within the multihoming context.

By introducing a complete optimization technique that determines optimal paths according to multihoming support, in this thesis, paths providing a better benefit/-cost ratio are selected. The introduced optimization technique includes a weighting algorithm that allows users to specify criteria preferences objectively and coherently. Moreover, MeTHODICAL addresses the *NP-hard* problem by specifying a technique that includes a decision stability factor to avoid side-effects and can be deployed in any scenario irrespective of the number of possible connections. The optimization technique organizes hierarchically the different multihoming criteria according to their type (e.g. benefits or costs) and for each communication path. Standard measurement mechanisms are applied to determine values of the diverse multihoming criteria, as specified in the proposed resilience and ubiquity evaluation frameworks. As values of diverse criteria are collected, they are normalized and combined with the respective preferences. Ideal solutions are determined based on maximum benefits and minimum costs values. The distance of benefits and costs criteria of each path establishes how far a path is to the ideal solution. The path with lower benefits and costs distance is the one providing a better multihoming experience.

The performance of MeTHODICAL has been extensively analysed in different evaluation scenarios with multiple types of applications and employing diverse evaluation metrics. Results demonstrate that MeTHODICAL improves multihoming support, by choosing paths with the best benefit/cost ratio. The evaluation results also demonstrate an increase in path selection stability, and for VoIP applications, an increase in VoIP quality, outperforming related approaches. These results highlight that multihoming experience on end-devices can meet user expectations by employing MeTHODICAL, an efficient optimization mechanism with low computational complexity.

Resumo

O paradigma de estar sempre ligado começa a atingir níveis nunca antes alcançados. A proliferação de múltiplas tecnologias e de dispositivos com suporte para diversas ligações está a enriquecer o suporte de *multihoming*. Os utilizadores podem agora partilhar informação em qualquer lugar e em qualquer altura. Em certa medida, os utilizadores podem configurar os dispositivos para ir ao encontro das suas expetativas, para reduzir os custos de comunicação ao escolher ligações sem custos associados ou optar por ligações com melhores coberturas. No entanto, este tipo de configuração asssenta em políticas estáticas que têm por fim maximizar apenas um dos requisitos, por exemplo, o custo monetário ou a cobertura. Neste sentido, o suporte de *multihoming* associado aos objetivos de resiliência, ubiquidade e partilha de carga, é bastante débil.

Quer a resiliência quer a ubiquidade foram objeto de pesquisa nos últimos anos. Contudo os diversos trabalhos apresentados até agora, apresentam falhas na definição de uma *framework* genérica que permita caraterizar de forma eficiente o suporte de resiliência e ubiquidade por parte de um protocolo. Tendo este aspeto em consideração, esta dissertação especifica *frameworks* para avaliar o suporte de resiliência e ubiquidade de uma forma objetiva, em qualquer fase da conceção de uma arquitetura com suporte para *multihoming* e com a vantagem de não requerer a intervenção de peritos.

Um suporte eficiente de *multihoming* requer mecanismos de optimização com suporte para múltiplos critérios. Este tipo de problema é considerado *NP-hard* - complexidade não polinomial e inclui benefícios e custos como critérios. As técnicas de optimização, denominadas de *Multiple Attribute Decision Mechanism (MADM)* conseguem identificar soluções ótimas e têm a flexibilidade de incluir diversos critérios. Contudo a especificação de técnicas *MADM* encontra-se incompleta visto que mecanimos coerentes para a atribuição de pesos dos múltiplos critérios não se encontram definidos, levando à existência de pesos inconsistentes e ilógicos. Tendo isto presente, MeTHODICAL é uma especificação completa, dado que engloba esta componente.

Com a introdução de uma técnica completa para otimização de diferentes caminhos num cenário de *multihoming*, esta tese propõe uma solução com a melhor relação custo/benefício. O MeTHODICAL inclui um algoritmo para definir os pesos de uma forma consistente e objetiva. Acresce ainda o algoritmo de seleção de caminhos otimizados que pode ser utilizado em qualquer cenário, independentemente do número de alternativas/caminhos. Os múltiplos critérios são organizados de uma forma hierárquica e tendo em conta o tipo de critério, ou seja, benefícios ou custos. Mecanismos padrão de medição são utilizados para medir os valores dos múltiplos critérios. A distância de cada alternativa/caminho à solução ideal permite definir o caminho que suporta *multihoming* de uma forma mais eficiente.

Os resultados obtidos em diferentes cenários de avaliação, com diversos tipos de aplicações, demonstram uma melhoria no suporte de *multihoming* com o MeTHODICAL quando comparado com técnicas semelhantes. Os resultados evidenciam estabilidade na escolha dos caminhos e, para aplicações *Voice over IP (VoIP)*, uma melhoria substancial da qualidade. Deve-se ainda referir que a complexidade associada aos mecanismos do MeTHODICAL é bastante reduzida, não ultrapassando a complexidade de mecanismos do estado da arte.

Foreword

THE work described in this thesis was conducted at the Laboratory of Communication and Telematics (LCT) of the Centre for Informatics and Systems of the University of Coimbra (CISUC) within the context of the following projects:

Project CoFiMOM – Project Combating Fire with Multihoming and Mobility (CoFIMOM), PTDC/EIA-EIA/116173/2009. The candidate has been the responsible for the project proposal concept definitions and for architecture definition and implementation.

Project TRONE – Project Trustworthy and Resilient Operations in a Network Environment (TRONE), CMU-PT /RNQ/0015/2009. The candidate was responsible for the multihoming aspects in the TRONE architecture. Moreover, the candidate also managed the team performing the design and implementation of advanced reconfiguration Stream Control Transport Protocol (SCTP) algorithms.

The performed work resulted in the following publications:

- Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**EVA: Enhancing VoIP Applications**", in proceedings of the 11th IEEE Global Communications Conference Exhibition & Industry Forum (GLOBECOM), December, 2013, Atlanta, USA.

- Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Enhancing Path Selection in Multihomed Nodes**", in proceedings of the 5th International Conference on Mobile Networks and Management (MONAMI), September, Cork, Ireland, 2013.

- Bruno Sousa, Ricardo Santos, Marilia Curado, Soila Pertet, Rajeev Gandhi, Carlos Silva, Kostas Pentikousis, "**Expedient Reconfiguration in the Cloud**", in proceedings of the 18th IEEE International Workshop on Computer-Aided

Modeling Analysis and Design of Communication Links and Networks (CAMAD), September, 2013, Berlin, Germany.

➤ Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Multihoming: A Comprehensive Review**", Advances in Computers, Volume 90, First Edition, July, 2013 - Elsevier, Impact Factor 0.384 [Sousa et al., 2013].

➤ Antonio Casimiro, Paulo Verisimo, Diego Kreutz, Filipe Araujo, Raul Barbosa, Samuel Neves, Bruno Sousa, Marilia Curado, Carlos Silva, Rajeev Gandhi, Priya Narasimhan, "**TRONE: Trustworthy and Resilient Operations in a Network Environment**", in the proceedings of IEEE/IFIP 42nd International Conference on Dependable Systems and Networks Workshops (DSN-W), 25-28 June 2012, Boston [Casimiro et al., 2012].

➤ Bruno Sousa, Kostas Pentikousis, Marilia Curado,"**MeTHODICAL: Multihoming for Urban Networks**", poster of SAIL summer school, Spain, 2012.

➤ Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Multihoming Management for Future Networks**", Mobile Networks and Applications, MONET, August, 2011 - Springer, Volume 16, Impact Factor 1.109 [Sousa et al., 2011a].

➤ Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**A Multiple Care of Addresses Model**", in proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC'11, June 28 2011-July 1 2011, Kerkyra, Greece, 2011 [Sousa et al., 2011d].

➤ Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**A Study of Multimedia Application Performance over Multiple Care-of Addresses in Mobile IPv6**", in proceedings of the 16th IEEE Symposium on Computers and Communications, MediaWin'11, June 28 2011-July 1 2011, Kerkyra, Greece, 2011 [Sousa et al., 2011c].

➤ Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Ubiquity Evaluation Framework (UEF)**", in proceedings of the 9th IFIP TC 6 international conference on Wired/Wireless Internet Communications, WWIC'11, Catalonia, Spain, on June 15-17, 2011 [Sousa et al., 2011b].

➤ Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Resilience Evaluation Framework (REF)**", in proceedings of the 4th IEEE Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), October 2010, Moscow, Russia, [Sousa et al., 2010].

The candidate has also released to the scientific community software implementations:

- **mCoA++**, a protocol implementing multihoming features, in the OMNeT++, namely Multiple Care of Address (MCoA), which is publicly available to the community [Sousa, 2013a].
- **MADM Evaluation Methodology**, a implementation of MADM evaluation framework [Sousa, 2013b] in the R-project [Team, 2010].

In addition, the following papers are under review:

- Bruno Sousa, Kostas Pentikousis, Marilia Curado, " **MeTHODICAL: Towards the Next Generation of Multihomed Applications**", Computer Networks, 2013.
- Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Evaluation of Ubiquity Support in Mobile Computing Systems**", in Springer Handbook "Resource Management in Mobile Computing Environments", 2013.

Contents

List of Figures

List of Tables

List of Algorithms

List of Theorems

Acronyms

ABC Always Best Connected.

AHP Analytic Hierarchy Process.

AIS Aggregation with Increasing Scopes.

ALOC Core address space.

AMR Association Max Retrans.

API Application Programming Interface.

APT A Practical Transit Mapping Service.

AS Autonomous System.

BA Binding Acknowledgment.

BE Binding Error.

BGP Border Gateway Protocol.

BRR Binding Refresh Request.

BU Binding Update.

CCID Congestion Control IDentifier.

CCN Content-Centric Network.

CCoA Collocated Care of Address.

CMT Concurrent Multipath Transfer.

CN Correspondent Node.

CoT Care of Test.

CoTI Care of Test Init.

CR Consistency Ratio.

CRIO Core Router-Integrated Overlay.

CRR Correct Rankings Ratio.

DAD Duplicate Address Detection.

DCCP Datagram Congestion Control Protocol.

DHCP Dynamic Host Configuration Protocol.

DiA Distance to Ideal Alternative.

DNS Domain Name System.

DOA Delegation Oriented Approach.

DONA Data Oriented Network Architecture.

DRUID Dynamic Recursive Unified Internet Design.

ECI Ephemeral Correspondent Identifier.

ECMP Equal Cost Multipath.

eFIT Enabling Future Internet Transit.

EID Endpoint IDentifier.

ELOC Edge address space.

ESP Encapsulating Security Payload.

FARA Forwarding directive, Association, and Rendezvous Architecture.

FMIPv6 Fast Mobile IPv6.

FPP Fuzzy Programming Preference.

FQDN Fully Qualified Domain Name.

FTP File Transfer Protocol.

GA Global Authority.

GLI-Split Global locator and Identifier Split.

HA Home Agent.

HAIR Hierarchical Architecture for Internet Routing.

HI HIP Initiator.

HIDRA Hierarchical Inter-Domain Routing Architecture.

HIP Host Identity Protocol.

hiPv4 Hierarchical IPv4.

HIT Host Identification Tag.

HMIPv6 Hierarchical Mobile IPv6.

HoT Home of Test.

HoTI Home of Test Init.

HR HIP Responder.

HRA Hierarchical Routing Architecture.

I3 Internet Indirection Infrastruture.

IANA Internet Assigned Numbers Authority.

ICMP Internet Control Message Protocol.

IDA Intra-domain Address.

IETF Internet Engineering Task Force.

ILNP Identifier Locator Network Protocol.

IP Internet Protocol.

IPDV IP Delay Variation.

IPMIP IP network multi-pathing.

IPNL IP Next Layer.

IPsec IP Security.

IPvLX IP with Virtual Link Extension.

ISP Internet Service Provider.

IvIP Internet Vastly Improved Plumbing.

LIMA Less-Is-More Architecture.

LISP Locator Identifier Separation Protocol.

LNA Layered Naming Architecture.

Loc/ID Locator-Identifier.

MADM Multiple Attribute Decision Mechanism.

MDT Mean Down Time.

MEF Multihoming Evaluation Framework.

MeTHODICAL MulTiHOming-aware Decision-makIng meChanism for AppLications.

MILSA Mobility and Multihoming support Identifier Locator Split Architecture.

MIP Mobile IP.

MIPv6 Mobile IPv6.

MN Mobile Node.

MPLS Multi Protocol Label Switching.

MPTCP Multipath Transport Control Protocol.

mSCTP Mobile SCTP.

MUT Mean Up Time.

NA Neighbour Acknowlegment.

NAROS Name Address and Route System.

NAT Network Address Translation.

NBS Name Based Sockets.

NDN Name Data Networking.

NetInf Network Information.

NIIA Node ID Internetworking Architecture.

NIRA New Internet Routing Architecture.

NMMD Novel Method based on Mahalanobis Distance.

NNC Networking Named Content.

NRLS Name-to-Route Lookup Service.

NS Neighbour Solicitation.

NTP Network Time Protocol.

NUD Neighbour Unreachability Detection.

OS Operating System.

OWAMP One-way Active Measurement Protocol.

OWD One Way Delay.

PERM Practical End-host Multihoming.

PRISM Proxy-based Inverse Multiplexer.

QoR Quality of Resilience.

QoS Quality of Service.

RA Router Advertisement.

RANGI Routing Architecture for the Next Generation Internet.

RD-QoS Resilience-Differentiated Quality of Service.

REAP Reachability Protocol.

REF Resilience Evaluation Framework.

RHR Required Handover Ratio.

RS Router Solicitation.

RTT Round Trip Time.

RVS RendezVous Server.

RZBS Realm-Zone Bridging Server.

SACKs Selective Acknowledgements.

SCTP Stream Control Transport Protocol.

SHIM6 Site Multihoming by IPv6 Intermediation.

SIA Switched Internet Architecture.

SILMS Scalable and Secure Identifier-to-Locator Mapping Service.

SILOS Architecture for Services Integration, controL, and Optimization for the Future Internet.

SIP Session Initiation Protocol.

SMR Solicit-Map-Request.

SNF Split Naming/Forwarding.

SST Structure Stream Transport.

TCP Transport Connection Protocol.

TFN Triangular Fuzzy Number.

TOPSIS Technique for Order Preference by Similarly to Ideal Solution.

TP Traffic Performance.

TRIAD Translating Relaying Internet Architecture integrating Active Directories.

TRRP Tunneling Route Reduction Protocol.

UCAN Ubiquitous Computing Application Development and Evaluation Process Model.

UEF Ubiquity Evaluation Framework.

UIA Unmanaged Internet Architecture.

UID Unique Identifier.

URI Universal Resource Identifier.

v6DH IPv6 Dual Homing.

ViAggre Virtual Aggregation.

XIA eXpressive Internet Architecture.

XIP eXpressive Internet Protocol.

—Nothing in life is to be feared,
it is only to be understood. Now
is the time to understand more,
so that we may fear less.
Marie Curie

1 Introduction

THIS thesis is focused on the multihoming research topic. Contributions on this topic include the specification of a framework to assess multihoming support in protocols. Multihoming is also optimized with the specification of an optimization algorithm that enhances the way multiple available interfaces/-paths can be used. The research scope and the motivation of the thesis are further discussed together with the thesis objectives and respective contributions.

1.1 Motivation and Problem Statement

Multihoming is a term, often associated (and confused) with multiaccess, multiaddressing, overlapping networks and multi-interface nodes terms [Bagnulo et al., 2006]. The availability of multiple interfaces and diverse addresses opens a window of opportunities to increase resilience, improve coverage, reduce costs and optimize energy consumption. In short, multihoming aims to accomplish different goals [Espi et al., 2009]. First, resilience, as the diversity of multiple interfaces/paths can improve resilience since upon the failure of one interface/path, another one can be employed to provide connectivity. Second, ubiquity, since multiple network interfaces, in particular when used in a mobile and wireless network environment, enable ubiquitous access to the Internet over different media. Third, load sharing, as multiple interfaces/paths can be used simultaneously to improve throughput. Finally, flow distribution, as flows can be stripped in a dynamic way to meet user policies.

Multihoming is classified into three categories: end-host, end-site and hybrid multihoming [Paul et al., 2009]. The first considers the support of multihoming on end-nodes. The second includes multihoming support enabled at the network side. The third requires the participation of end-nodes and network to enable multihoming. When evaluating such multihoming support, researchers analyse multihoming support restricted to a single metric, such as cost [Richard, 2010], or focus their analysis in a small subset of multihoming protocols [Shinta et al., 2006; de Launois and Bagnulo, 2006; Fekete and Hämälänen, 2009], therefore, being restricted to a certain type of multihoming (e.g. end-host multihoming).

Diverse approaches evaluating multihoming support only address one goal. For instance, resilience is evaluated for the Multi Protocol Label Switching (MPLS) [Cholda et al., 2008, 2009]. Such kind of evaluation considers resilience specific metrics, such as steady-state availability or mean downtime. Nonetheless, the evaluation methodology is tied to MPLS, lacking a broader applicability to other protocols. Other evaluations include recovery efficiency and the supported protection model (e.g. 1+1 or 1:N) [Pioro and Medhi, 2004]. Nevertheless, evaluations rely on the application requirements. Instead of considering the resilience goal, other approaches focus on the performance of Ubiquitous Computing (UbiComp) systems. The ubiquity goal can be evaluated in terms of quality, which assesses the level of capabilities (i.e. technical characteristics) and the level of extensions [Kwon and Kim, 2006; Scholtz and Consolvo, 2004]. This evaluation is based on interviews with experts in the field (e.g. with ubiquitous computing experience). Therefore this approach requires the involvement of experts to characterize the system regarding its technical capabilities (e.g. how efficient it is, how is mobility managed and what security mechanisms are included). Other approaches evaluate the performance of a UbiComp system through prototyping [Kwon and Kim, 2006; Resatsch, 2010]. Nonetheless, this approach has the drawback of requiring a working system, which has high complexity.

Multihoming is leading to enhancements in well-known protocols. Mobile IPv6 (MIPv6) [Johnson et al., 2011] is, to a large degree, the archetypical mobility management protocol for IPv6 networks. Maintaining established communications while moving is similar to preserving established communications through outages in the multihoming context. MIPv6 maintains established communications while a mobile node moves across networks. However, current MIPv6 does not fully support multihoming, as it assumes that the home address does not change during the mobility management process. With such assumption, whenever there is a change in the home address, e.g. a node with multiple prefixes in the home network, MIPv6 does not support new addresses acting as the home address. Even if binding update messages convey information in advance about alternative prefixes [de Launois and Bagnulo, 2006], this may not be enough to enable session survivability, as MIPv6 procedures fail, since they rely on a single address. Considering the decreased multihoming support, several extensions have been specified to enhance the MIPv6 protocol. Multiple Care of Address (MCoA) [Pan et al., 2008a] extends MIPv6 to allow the registration of multiple addresses. The mobile node is always reachable at a unique permanent IPv6 address (employed as an identifier) while several temporary addresses (Care of Addresses) are used as locators to reveal the current network location of the node. The specification of flow bindings [Tsirtsis et al., 2011a; Toseef et al., 2008] extends MIPv6 and MCoA specifications defining how multiple flows can be exchanged between two nodes, in a multihoming context. This enables to bind a particular flow to a Care of Address and use another address to receive information from other flows.

Mobile IPv6 (MIPv6) implementations are now available in operating systems and network simulators. For instance, xMIPv6 [Yousaf and Bauer, 2013] is a simulation model that implements MIPv6 in OMNeT++ and provides an accurate implementation of MIPv6 and related protocols, such as the Fast Mobile IPv6 (FMIPv6) [Koodli, 2008] or the Hierarchical Mobile IPv6 (HMIPv6) [Soliman et al., 2008]. Nonetheless, xMIPv6 does not have support for MCoA or Flow Bindings. Implementation of Mobile IPv6 and NEMO for Linux (UMIP) [Kuntz, 2013a] enable MIPv6 and MCoA protocols in Linux operating system [Kuntz, 2013b]. Moreover, there are others implementations of MCoA and Flow Bindings but they are not open to the research community [de la Oliva et al., 2011]. Indeed, there is a gap of MCoA implementations in network simulators, that enable experiments with multihomed configurations. This thesis introduces mCoA++, an implementation of MCoA, in the OMNeT++ simulator, which is publicly available to the community.

Multihomed nodes have different ways of using the multiple interfaces. Optimization techniques determine which paths are optimal considering multiple criteria, for instance throughput, cost and energy. The *NP-hard* problem [Muscariello et al., 2009; Xue et al., 2007] can be solved using network- or user-centric approaches. The former protects the network from high loads (i.e. high number of users), as selection is controlled by the network. Nonetheless, it requires the involvement of all the access networks, introducing communications overhead and requiring cooperation between users and networks. On the other hand, the user-centric approach is distributed as selection is controlled by the user. This enables to include user preferences, decreasing the complexity and avoiding communication overheads. Nonetheless, as users can have 'selfish' behaviour, there is the risk of overloading the network [Charilas and Panagopoulous, 2010].

Linear Programming (LP) [Hillier and Lieberman, 1995] and Multiple Objective Programming (MOP) [Marler and Arora, 2004] techniques provide optimal solutions, but increase complexity in terms of deployment. Moreover, for each problem or scenario, a specific formulation needs to be derived, as optimization goals may be different. The optimal solution corresponds to the one with the best partial evaluations. Other kinds of optimization mechanisms are efficient for network selection. For instance, Markov based decision algorithms model optimization problems under the assumption that the decision can follow a certain probability distribution [Zekri et al., 2012]. Despite having accurate results, they have associated implementation issues.

Outranking Multiple Attribute Decision Mechanism (MADM) techniques [Figueira et al., 2005] are considered techniques flexible enough to accommodate quantitative and qualitative data, as the case of Analytic Hierarchy Process (AHP). MADM techniques have been employed in distinct areas (e.g. logistics, computer science, safety, health management) [Behzadian et al., 2012] and have low complexity. Moreover, MADM are able to accommodate several criteria no matter the research problem associated [Zekri et al., 2012; Charilas and Panagopoulous, 2010]. In particular, the outranking MADM techniques formulate optimization by scoring the multiple path alternatives. Indeed, the efficiency with the simplicity of such methods lead to a plethora of MADM techniques.

Simple Additive Weighting (SAW) and Multiplicative Exponent Weighting (MEW) are simple MADM techniques that combine multiple criteria and weights using sum and product functions, respectively [Kaleem, 2012]. Nonetheless, they have issues, such as weight inconsistency, as they do not consider properly the configuration of weights. More robust MADM techniques include Technique for Order Preference by Similarly to Ideal Solution (TOPSIS), Distance to Ideal Alternative (DiA) [Tran and Boukhatem, 2008] and Novel Method based on Mahalanobis Distance (NMMD) [Lahby et al., 2012], as they consider the distance to ideal solutions according to the criteria type, if costs or benefits.

Multihoming cannot be analysed solely based on one metric, such as cost, and cannot be attached to the specificities of a protocol, as well. Such kind of analysis does not provide a full evaluation of multihoming and may lack a general applicability if based on a specific protocol.

Optimization techniques dealing with *NP-hard* problems cannot impose deployment concerns or introduce more complexity on networks that are getting each day more complex to accommodate new services. Optimization can be formulated through distinct techniques, such as LP and MADM. Flexible techniques like MADM that do not require any adaptation between different scenarios are more interesting to future networks. Nonetheless, several issues are pointed to these techniques such as the ranking identification and ranking abnormality that compromise their accuracy and efficiency.

The main goal of this thesis is the proposal of an efficient and flexible optimization algorithm for multihoming that does not have the issues of MADM techniques. Moreover, such algorithm relies on the different goals, above-mentioned, that multihoming solutions must pursue, namely resilience, ubiquity and load sharing. In addition, this thesis has also been motivated by a framework to evaluate multihoming support in different protocols, through the assessment of multihoming goals achievement.

1.2 Objectives and Contributions

The main goals of this thesis are to propose a mechanism to evaluate multihoming support and a mechanism to optimize the multihoming experience of a node with multiple interfaces or paths. The specific goals of the thesis include:

G.1 Enable objective evaluation of multihoming support, promoting the comparison between protocols, regarding the efficiency of the multihoming mechanisms.

G.2 Propose a mechanism that can optimize the multihoming experience of a multi-interface or multi-path node. The optimization mechanism must include the criteria that is employed in the multihoming evaluation mechanism and must be efficient and without introducing *hard-to-meet* requirements.

Several contributions are associated with this thesis, as summarized in the following subsections.

Multihoming Taxonomy

The multihoming concept has been objectively defined to avoid misunderstandings with related terms, such as multi-access. In addition, a state of the art has characterized multihoming support in terms of goals and distinguished the diverse multihoming types, namely end-host, end-site and hybrid.

Multihoming evaluation framework

This contribution meets the **G.1** goal, as a framework to assess multihoming support is proposed. This framework considers multihoming goals, more specifically resilience and ubiquity to determine how efficient a protocol is regarding its multihoming support.

The Resilience Evaluation Framework (REF) and the Ubiquity Evaluation Framework (UEF) are frameworks that allow to assess resilience and ubiquity multihoming goals.

Performance assessment of multihoming evaluation framework

The performance assessment of Resilience Evaluation Framework (REF) and Ubiquity Evaluation Framework (UEF) was performed analytically. Diverse protocols have been employed as study cases. For instance, the Stream Control Transport Protocol (SCTP) [Eklund et al., 2009] has been studied regarding its resilience support with the primary-backup protection model included in the native specification of SCTP.

In a comparative approach, MIPv6 and HIP protocols have been assessed regarding their ubiquity support.

Multihoming aware optimization mechanism

MeTHODICAL is the optimization mechanism introduced in this thesis, to enhance the multihoming experience of nodes with multiple interfaces/paths. MeTHODICAL is a flexible optimization technique that enables optimal path selection by considering multiple criteria and with a low computational complexity. Moreover, MeTHODICAL follows a MADM approach, allowing users to specify weights for the diverse criteria in an objective way.

MeTHODICAL has been integrated in the architectures of Combating Fire with Multihoming and Mobility (CoFIMOM) and Trustworthy and Resilient Operations in a Network Environment (TRONE) projects to enhance communications in fire-fighting scenarios and cloud environments, respectively.

Multiple Attribute Decision Mechanism accuracy evaluation framework

Outranking MADM techniques, such as DiA [Tran and Boukhatem, 2008] are often evaluated subjectively or using methodologies that cannot be applied generically. This thesis includes a MADM accuracy evaluation framework that is based on Design of Experiments (DoE) [Sandanayake et al., 2008] to allow the objective comparison between different MADM techniques, relying on statistical properties, such as F-statistic or coefficient of determination, R^2.

Performance assessment of multihoming aware optimization mechanism

MeTHODICAL has been evaluated analytically using data collected in real scenarios and has been assessed in a cloud testbed within the context of high-volume data transfers.

The performance assessment of MeTHODICAL was based on objective metrics that establish the correct ranking of paths and determine the required handover ratios. Moreover, MeTHODICAL has been compared objectively with similar techniques such as TOPSIS [Figueira et al., 2005] and DiA using the proposed MADM accuracy evaluation framework.

Implementation to enhance multihoming support

One final contribution that is associated to this thesis is a set of implementations to enhance multihoming support. In the TRONE project, an implementation of the optimization algorithm has been incorporated in the TRONE architecture. Indeed, the optimization algorithm has been employed to reconfigure SCTP regarding the path to use, when multiple addresses are available in a cloud context. The mCoA++ is an implementation of the MCoA protocol, which extends the multihoming support of MIPv6. This contribution has not been left on a closed community, but instead it has been made public and available to the global research community.

1.3 Thesis Outline

The following paragraphs, briefly introduce the outline of the thesis.

Chapter 2 is the foundation chapter for multihoming and related terminology. A in-depth state of the art is provided in this chapter, where multihoming support in diverse protocols of different network layers is analysed regarding multihoming goals fulfilment.

Chapter 3, inspired on the previous chapter, introduces two evaluation frameworks, to assess the multihoming support of a protocol. Specifically, REF establishes the required formulation to assess the resilience support of a protocol. Moreover, UEF evaluates to what extent a protocol supports ubiquity and thus, can be tailored for Ubiquitous Computing (UbiComp) systems.

Chapter 4 addresses the optimization problem in multihoming contexts. A Multihoming aware optimization technique is specified in two distinct algorithms. First, a criteria weighting algorithm is provided to allow user preferences mapping through objective and consistent weights. Second, a path optimization algorithm is specified to enable optimal path selection. Indeed, path optimization, following a MADM approach, is a flexible scheme that can be adapted easily to multihoming scenarios, accommodate more multihoming and traffic performance criteria, without requiring modifications in the optimization process.

Chapter 5 introduces a case of improving the multihoming support of the MIPv6 protocol. Such improvement, relies on a software implementation of the MCoA protocol, in the OMNeT++ simulator. Experimental results are also discussed, namely the gain in VoIP quality regarding the multihoming support that MCoA includes.

The conclusions that emerged from the research work described in this thesis, are outlined in Chapter 6.

*—In 1972, Tinker Air Force Base joined the Net and [..] wanted redundant network connections. Upon hearing this news, I distinctly remember thinking "Ah, great idea!" and a second later, thinking, "O *#@* that isn't going to work!"*

John Day, *Patterns in Network Architecture*

2 Multihoming in IP Networks

THIS chapter presents the state of the art on Multihoming and Multiaccess in Internet Protocol (IP) networks. A comprehensive survey of protocols acting at different layers of the Transport Connection Protocol (TCP)/IP model is presented. Furthermore, protocols with some kind of support for multihoming, namely, end-host, end-site and hybrid multihoming are also analysed. An overview of multihoming support in operating systems is also included, as well as implementation details in Operating Systems (OSes).

Multihoming support in the diverse protocols is analysed through a candidate's proposed taxonomy. This taxonomy considers multihoming goals fulfillment (i.e. resilience, ubiquity, load sharing, and flow distribution). This approach of analysing multihoming support is more objective than other approaches that use only one metric, such as cost [Richard, 2010], or which focus only on a subset of multihoming protocols, such as [Shinta et al., 2006; de Launois and Bagnulo, 2006; Fekete and Hämälänen, 2009]. The following paragraphs, present the outline of each section, in the chapter.

Section 2.1 introduces terms used in the multihoming taxonomy. Concepts related to multihoming are defined and end-host, end-site and hybrid multihoming types are characterized.

Section 2.2 presents design considerations for multihoming solutions and identifies the goals that characterize multihoming. In addition, multihoming open issues are also presented.

Section 2.3 highlights protocols supporting multihoming at the application layer and discusses multihoming support in operating systems.

Section 2.4 overviews multihoming support of protocols acting at the transport layer of the Internet protocol suite.

Section 2.5 depicts IPv6 mobility management protocols and their extensions to enhance multihoming support. IPv4 mobility management procotols are excluded, as they have limitations for future mobile networks.

Section 2.6 introduces protocols supporting end-host multihoming. Such kind of protocols operate on end-nodes (i.e. user devices) and implement mechanisms to support multihoming on their own.

Section 2.7 introduces protocols supporting end-site multihoming. With this type of protocols, multihoming is enabled with network assistance.

Section 2.8 provides an overview of hybrid multihoming protocols. These protocols merge functionalities from end-host and end-site multihoming approaches, to enable multihoming by allowing end-nodes to take decisions with the assistance of network. The chapter concludes with Section 2.9.

2.1 Multihoming Types and Concepts

This section introduces concepts related with multihoming, such as multiaddressing, multiaccess and overlapping networks. In addition, three different types of multihoming are characterized, namely end-host, end-site and hybrid multihoming.

2.1.1 Concepts

Multihoming is associated with other concepts, including multiaddressing, overlapping networks, multiple interfaces and overlay routing. Multiaddressing, for example, corresponds to a configuration in which multiple addresses are assigned to a given host based on prefixes advertised in different connections [Bagnulo et al., 2006]. Overlapping networks correspond to networks that are configured in a way that there is a common area of coverage. Typically, mobile end-nodes connecting to these (overlapping) networks must have multiple interfaces, each one specific to the technology

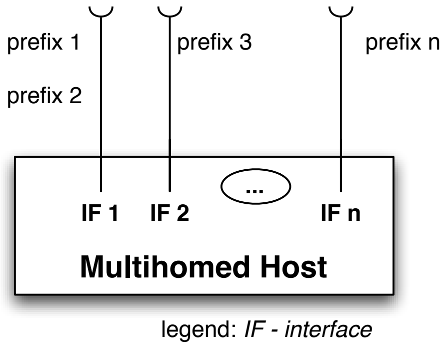


Figure 2.1: Multihomed host

sustaining the respective network [Blanchet and Seite, 2011]. Overlay routing is associated with inter-domain routing techniques that improve fault-tolerance, and is only applied in an end-site context. Throught this thesis Multihoming is used as per Definition 2.1.

Definition 2.1 (*Multihoming*)

> *Multihoming is an entity (host or network) configuration that has several first-hop connections to a given destination. Such connections can be accommodated through single or multiple (physical or logical) network interfaces.*

Alternative definitions consider multihoming as the availability of two or more connectivity providers to offer fault tolerance and traffic engineering capabilities [Bagnulo et al., 2006]. Or simply, a host is considered multihomed if it has multiple IP addresses [Braden, 1989].

2.1.2 End-host Multihoming

End-host multihoming is defined according to Definition 2.2.

Definition 2.2 (*End-host multihoming*)

> *End-host Multihoming is an host entity configuration that has several first-hop connections to a given destination and employs its own mechanisms to select connection(s).*

A multihomed host with different interfaces (logical or physical) is depicted in Figure 2.1. In addition, each interface can have different network prefixes configured.

For instance, interface *IF 1* has been assigned two prefixes, namely *prefix 1* and *prefix 2*. Moreover, the host can have multiple physical interfaces which have been associated with a single prefix, as is the case of *IF 2* and *IF n* with *prefix 3* and *prefix n*, respectively. This configuration is possible when virtual interfaces are assigned to a physical interface, as depicted in Listing 2.1. Prefix and address terms are used here interchangeably. From an *end-host* perspective, a multihomed host has multiple prefixes configured on the links it connects to, thus having the possibility to explore several paths to reach a peer, as each prefix is normally advertised by different access routers.

List 2.1: Example of IPv6 aliases configuration for FreeBSD

```
ifconfig if1 inet6 2001:db8:1::1/48 alias
ifconfig if1 inet6 2001:db8:1::2/48 alias
```

2.1.3 End-site Multihoming

End-site multihoming is defined according to Definition 2.3.

Definition 2.3 (*End-site multihoming*)

> *End-site Multihoming is an network entity configuration that has several first-hop connections to a given destination.*

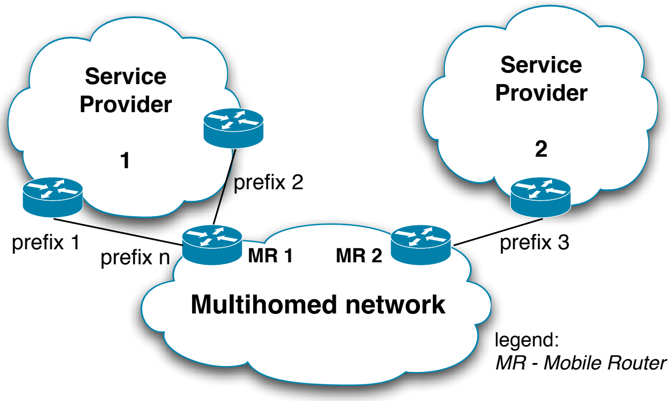


Figure 2.2: Multihomed network

End-site multihoming is defined in Definition 2.3, and corresponds to a site using multiple connections to the Internet to increase network reliability or improve performance [Abley et al., 2003; Dhraief and Montavont, 2008]. *End-site* multihoming first came up in the context of ARPANet back in 1972 due to the desire to have redundant network connections, thus allowing for more robust network operation [Day, 2008].

Figure 2.2 illustrates a multihomed site, which has connections to two service providers. A multihomed network can have multiple routers, such as, for example, *MR 1* connecting to Service Provider 1 and *MR 2* connecting to Service Provider 2. Moreover, a single router can have several external interfaces that connect to the same or different service providers, as the example of *MR 1*.

Different perspectives can be followed to consider a mobile network as multihomed [Ng et al., 2007a; Ernst and Charbon, 2004; Choi et al., 2006]. The First approach, the **ownership-oriented** approach that takes into account the ownership of the Home Agent (HA) and Mobile Routers. A mobile router is defined as an entity providing Internet access to the multihomed network, as mentioned above. If these network elements are controlled by a single entity, this is called the Internet Service Provider (ISP) model, otherwise it is referred to as the Subscriber/Provider model. Second, the **problem-oriented** approach considers the number of home agents and network prefixes advertised. Finally, the **configuration-oriented** approach considers different parameters such as the number of home agents, the number of prefixes available and the number of Collocated Care of Addresses (CCoAs).

2.1.4 Hybrid Multihoming

Hybrid multihoming is considered throughout the thesis according to Definition 2.4.

Definition 2.4 (*Hybrid multihoming*)

> *Hybrid Multihoming is an entity configuration that has several first-hop connections to a given destination, which require cooperation between nodes and network for an efficient operation.*

Hybrid Multihoming mixes both end-host and end-site characteristics, but requires the participation of end-host and network entities (e.g. servers) for full multihoming support. Most current proposals are hybrid multihoming solutions that target issues on networks, such as routing scalability, but at the same time also address drawbacks of the current TCP/IP architecture, such as the dual role of IP address (identifier and locator). According to Figure 2.3, MH1 is a multihomed host, but multihoming management requires support from the network (server) to maintain the location information, so that other end-hosts in the Internet can communicate with MH1.

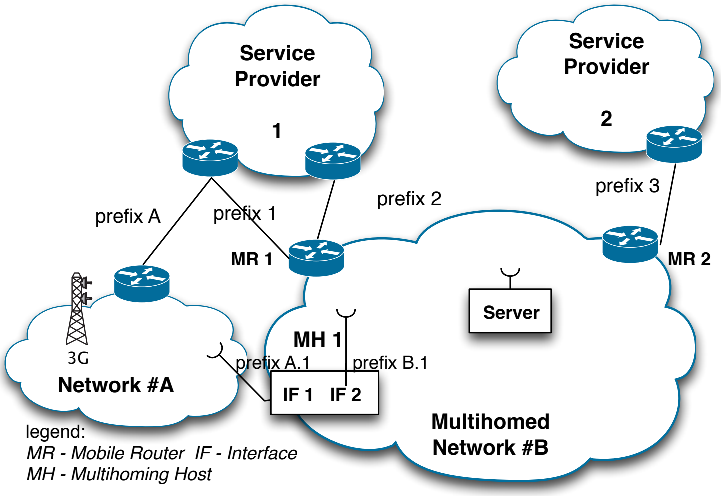


Figure 2.3: Hybrid multihoming scenario

2.2 Designing for Multihoming

This section introduces the overall goals that current and future multihoming solutions ought to pursue. Open problems and current solution space in this research area are also presented.

2.2.1 Goals

Multihoming has gained attention over the last few years [Espi et al., 2009], due to the potential benefits it can provide. In particular, multihoming solutions aim to achieve the following goals: **R**-Resilience, **U**-Ubiquity, **L**-Load balancing/sharing and **F**-Flow distribution.

The diversity of multiple interfaces/paths can improve **resilience** as upon a failure of one interface/path, another one can be employed to provide connectivity. For instance, as mentioned above, a *primary-backup* model is adopted by Stream Control Transport Protocol (SCTP) [Budzisz et al., 2008]. That is, if the primary path fails, the backup path can be used seamlessly without causing any application-layer service interruption. Multiple network interfaces, in particular when used in a mobile and wireless network environment, enable **ubiquitous access** to the Internet over different media.

Load sharing goes one step further than the primary-backup model, as multiple interfaces/paths can be used simultaneously to improve throughput, as for instance to enable concurrent multiple transfers in SCTP [Iyengar et al., 2006].

Flow distribution, or flow stripping, offers even finer granularity than load sharing. Flow distribution is the ultimate goal to achieve, as it implicitly means that all previous goals are also attained. Flows are stripped, perhaps even dynamically, according to policies and preferences aiming to reduce cost, optimize bandwidth use, and minimize the effect of bottlenecks to delay-sensitive applications, among others.

2.2.2 Open Issues

As multihoming aspects are introduced in current specifications of the IP architecture, there are still several issues that need to be addressed [Montavont et al., 2008; Blanchet and Seite, 2011].

The first problem relates to **default gateway mechanisms**. Current specifications use a default gateway to assure connectivity to the network. Such a mechanism introduces limitations in the exploration of multiple connections, as flows cannot be forwarded across different connections to meet user requirements (e.g. load balancing). A simple solution is to use static routes, on a flow or destination granularity, but this type of approach is not scalable and it is difficult to manage in practice.

A second issue is related with **configuration parameters**. Network nodes, running IPv4 or IPv6, receive specific configurations for each active connection via the Dynamic Host Configuration Protocol (DHCP) [Droms, 1997], Router Advertisement (RA) [Hagen, 2006] or other mechanisms. In these scenarios, issues such as split Domain Name System (DNS) might occur since there is no binding mechanism between the resolution name and the destination. Split DNS refers to the case of getting different name resolution results depending on which of the available network interfaces is used to issue the DNS lookup. Solutions to overcome these issues rely on merging interface-specific to node configurations to avoid conflicting result sets, as is the case with name resolution in private networks.

Failure detection also poses restrictions on multihoming support. Current failure detection mechanisms do not perform well as they mainly rely on timers. For instance, existing RAs do not detect failed links on the failure event, but only on the failure of an event advertisement, which relies on timers. A solution to mitigate such problem is to use cross-layer information, such as link layer events to detect network attachment [Krishnan et al., 2007] and loss of connectivity.

Path exploration mechanisms introduce performance constraints limiting multihoming support. Reachability between pairs of addresses must be reactive, and reduce the overhead of signalling procedures. For instance, one strives to reduce the number of messages (and payload size) necessary to detect that a path is congested or is not reachable at all [Fitzpatrick et al., 2009].

Another problem with multihoming is related with **path selection**. As available and working paths are identified, upper-layers (e.g. applications) should become aware of such path diversity. The introduction of multiple addresses raises source address selection issues, as upper layers need to select the right source address to deliver data to the corresponding path. A standard solution to perform source address selection is still missing. **Ingress filtering** requires compatibility with other mechanisms, such as source-address selection. If the source address is not properly assigned to the respective link, existing filtering processes will discard these packets. Solutions to overcome this limitation include source-based routing mechanisms, or routing based on interface-scoped sets, instead of node-scoped. In the former, routing is based on the source address and not on the traditional destination address. In the latter, routing is performed based on the interface characteristics to meet the application requirements.

Rehoming corresponds to the process of diverting existing sessions from one path to another. Existing flows need to be redirected to a new path or, if such flow redirection is not supported, new sessions must be established. Protocols like Site Multihoming by IPv6 Intermediation (SHIM6) [Nordmark and Bagnulo, 2009] or SCTP [Stewart, 2007] provide mechanisms that introduce support for rehoming.

Locator-identifier split approaches extend multihoming support by separating the roles of an IP address. Nevertheless, such approaches are not devoid from multihoming issues. Mechanisms to efficiently select a locator can be hard to implement or even introduce incompatibility in the fulfillment of multihoming goals (e.g. resilience and load balancing). If these approaches do not support dynamic capabilities negotiation they may not adapt to mobile environments or end up with scalability issues.

Security is another important issue in multihoming architectures, as they can introduce new security threats, like "time-shifting" attacks, which affect proposals that adopt the locator-identifier split approach [Bagnulo et al., 2006]. As locators change during communications, an attacker does not need to be always present in the path between a source and a destination host. This kind of attack is similar to the man-in-the-middle one, as the attacker can inform a destination host that the real source can be found at a location different than the legitimate one and controlled by the attacker.

2.2.3 Multihoming Design Considerations

Architecture proposals for multihoming addressing issues such as failure detection, security, path selection and default gateway choice [Rathnayake et al., 2010; Blanchet and Seite, 2011], should consider different design guidelines to meet multihoming goals. Briefly, design considerations include adopting a locator-identifier split approach for end-host, end-site and hybrid multihoming. Moreover, support at the network level, by modifying site exit routers, is required for end-site and hybrid multihoming approaches.

The first guideline that should be considered relates to **locator-identifier split**. Conventional IP architectures assume that transport layer endpoints are the same entities as those used by the network layer. Thus, multihoming support based on a locator-identifier split requires that the transport layer identity is decoupled from the network layer locator in order to allow multiple forwarding paths to be used by a single transport session. Different approaches can be considered [de Launois and Bagnulo, 2006], either by modifying an existing protocol or by introducing a new layer. With the latter approach, upper layer protocols (e.g. applications) use endpoint identifiers to uniquely identify a session while the lower layer protocols (e.g. network) employ locators. If this approach is used, a mapping between an identifier and a locator is necessary. In principle, this mapping can be maintained at any layer of the protocol stack. One reasonable choice is to place this functionality between the transport and the application layers, so that applications would interface with the endpoint identity protocol stack element through an Application Programming Interface (API). A second approach is to place a new layer between the transport and the network layers. With the modified layer approach, an existing layer can be adapted to perform the mapping between identifiers and locators. For instance, if the transport layer functionalities are modified, a set of locators can be bound to a session, and the locator is communicated to a remote entity. On the other hand, if the network layer is modified, there are two ways to achieve the desired functionalities. The first is by rewriting the packet header and the second is by using encapsulation to perform packet header transformation.

Another consideration for end-site and hybrid multihoming includes the **modification of a site exit-router**. End-site multihoming can be assured by a network element. For instance, an exit-router can perform packet rewriting for a given locator of a correspondent node. Nevertheless, this type of approach raises security concerns, which might be difficult to overcome. Redirection attacks are such an example, which may compromise routing, since packets for a destination can be redirected to any location [de Launois and Bagnulo, 2006; Fekete and Hämäläinen, 2009].

Scalability is of essence in any network architecture and multihoming is not an exception. Multihoming architectures should be scalable and need to strive to minimize the impact on routers and end hosts. Basic connectivity must be always provided. If any modification is required it should be in the form of logically separating added functions from existing ones [Espi et al., 2009].

Security is also paramount for future architectures. Multihoming proposals should not introduce new security threats. For instance, multihoming solutions should be resilient to redirection attacks that compromise routing, new packet injection attacks (malicious senders can inject bogus packets into the packet stream between two communicating peers) and flooding attacks, which are normally associated with Denial of Service attacks [Fekete and Hämäläinen, 2009].

2.3 Operating Systems and Applications

This section is devoted to the support of multihoming in proposals acting at the application layer and in operating systems. For instance, Name Based Sockets (NBS) [Ubillos et al., 2010] represents a change of paradigm on how applications see the information of layers bellow. Moreover, as presented in subsection 2.3.2, server applications incorporate mechanisms to support multiple interfaces or multiple paths.

2.3.1 Protocols at Application layer

This subsection discusses two application-layer protocols, namely Session Initiation Protocol (SIP) and NBS.

2.3.1.1 Session Initiation Protocol

SIP [Rosenberg et al., 2002] is a session protocol that enables mobility at the application layer. SIP employs a Universal Resource Identifier (URI) to represent the user identity connected to a SIP domain. Sessions, therefore, are bound to the URI and not to an IP address. On mobility events, the user sends a binding update message that renews the mapping in the SIP server (URI to IP address). In this case, communication proceeds, as the URI is used to identify the user during the entire session. One drawback of SIP is that it is intended for User Datagram Protocol (UDP) applications. Thus, TCP applications cannot have the support of SIP in mobility events [Jain et al., 2012], as the change of IP address leads to the termination of connections. Some proposals mitigate this issue by combining SIP with Mobile IP [Seta et al., 2007].

Another drawback of SIP relates to the privacy of user IDs. PrivaSIP [Karopoulos et al., 2010] enables the protection of caller and caller's IDs by the use of cryptography. Further, the media multihoming proposal [Verma, 2012] combines SIP with SCTP, enhancing multihoming support, to improve resilience. Nonetheless, in this last proposal the information provided is not sufficient to enable its implementation.

2.3.1.2 Name Based Sockets (NBS)

The NBS proposal [Ubillos et al., 2010] introduces a novelty that in a sense facilitates multihoming. Applications only use domain names, while IP addresses (e.g. selection, discovery) are managed by the operating system. Such functionality is proposed as an extension to the socket API. Nodes communicating with each other, initially exchange names, in a piggyback scheme. The first packets convey the name on an IP-Option/IPv6 extension header. A receiver node, upon detecting such option, adds its name in the reply packets. The name can be based on a Fully Qualified Domain Name (FQDN), on ip6.arpa (host interface address) or nonces (session identifiers). The ports rely on service keywords attributed by the Internet Assigned Numbers Authority (IANA) (e.g. http for port 80).

The Name Based Sockets proposal can be combined with other protocols, such as SHIM6 to enable mobility [Xu et al., 2010]. Nevertheless, it requires node modifications and removes the possibility of applications to use multiple addresses according to their own requirements. This proposal did not attain enough support in Internet Engineering Task Force (IETF) standardization. Nonetheless, it has the advantage of not requiring new infrastructure to be deployed [Ming et al., 2012].

Table 2.1: Multihoming support in application-layer protocols.
MH-Multihoming, OS-Operating System.

Protocol	MH Goals				Strengths	Flaws	Implementation	
	R	U	L	F			Simulators	OS
SIP	X	√	X	X	Widely available. Resilience can be supported.	No flow distribution capabilities.	Yes	Yes
NBS	X	√	X	X	Resilience can be supported.	Not standardized.	–	Linux[a]

[a] [Ming et al., 2012]

■ Table 2.1 summarizes multihoming support in application-layer protocols. SIP enjoys widespread implementation, efficient mobility support, and can be extended to also support resilience. Such extension relies on the combination of SIP and SCTP. The same logic applies to NBS, that can support resilience if combined with SHIM6. But, in contrast to SIP, NBS represents a new concept and introduces modifications that may hinder its widespread implementation. ■

2.3.2 Operating Systems and Server Applications

Although most mobile devices have very rudimentary mechanisms for heterogeneous network access selection and management, modern operating systems have connection managers to select the best path for applications based on preference sets (e.g. cost, bandwidth) [Wasserman and Seite, 2011]. Others explore techniques similar to *IP aliasing* to support multiple IP addresses due to the different (physical/virtual) network connections [IBM, 2001]. IP network multi-pathing (IPMIP) [SUN, 2009] extends the functionality of IP aliasing techniques by providing interface failure detection and by offering load sharing in systems with multiple interfaces.

Linux supports multipath routing by allowing the specification of multiple next hops for a given destination. The motivation for multipath routing can include tolerance to failures (using a backup route) or load sharing to increase throughput [Benvenutti, 2005]. While simple reliability can be based on the specification of several routes with different weights, load balancing requires more advanced mechanisms that can be based on identical weights such as the implemented Equal Cost Multipath (ECMP) algorithm [Hopps, 2000]. The distribution of traffic, under multipath configuration, is based on routing cache entries to distribute traffic according to different algorithms, such as *Weighted Round Robin*. In FreeBSD 8.0, the routing infrastructure was modified to split layer2 (L2) and L3 information [Li and Macy, 2009]. This split introduces benefits that facilitate the utilization of parallel computing and introduce support for ECMP.

Server applications such as DHCP and File Transfer Protocol (FTP) can be configured according to the sets of each subnet a host can connect to. For instance, *vsftpd*, an FTP daemon, can be configured for multiple FTP domains [RedHat, 2013b]. Both approaches have drawbacks, since this kind of configuration requires IP addresses for each FTP domain and a multihomed DHCP server can perform differently for each network [RedHat, 2013a]. Apache, a web server, provides support for multihoming via *virtual hosts* [Foundation, 2013] that give the possibility of hosting several domains on a single physical machine. Domains can be identified on a name or IP configuration basis. In the last approach, a virtual host is configured based on a server IP address.

A clear distinction between Apache and *vsftpd* is that in the former configuration is centralized and not split on a domain basis.

2.4 Multihoming and Transport Protocols

An overview on multihoming support at the transport layer is presented in this section. This overview includes proposals standardized by IETF, and non-standardized proposals. Proposals like TCP Multi-Home Options [Matsumoto et al., 2003], Multiple TCP Fairness [Tse, 2006], among others, are grouped in a subsection and is included in this overview primarily for historical reasons, as many of these proposals have been pioneers in the introduction of multihoming support in transport protocols. Other proposals like Proxy-based Inverse Multiplexer (PRISM) [Kim and Shin, 2007] include a complete architecture to support multihoming, but changes act at the transport layer. Standardized solutions include Multipath Transport Control Protocol (MPTCP) [Ford et al., 2011, 2013], SCTP [Stewart, 2007] with respective extensions and Datagram Congestion Control Protocol (DCCP) [Kohler et al., 2006].

2.4.1 Non-Standard TCP-based Proposals

With **TCP Multi-Home Options** [Matsumoto et al., 2003], TCP peers first negotiate the multihoming permitted option. During connection establishment, the path based on the current address is marked as the primary path. As soon as the primary path is established, the multihoming *Add* and *Delete* options may be used to convey local address information from the sender to the destination. Then, on the reception of a multihoming option, all paths that can be created are registered. If the option corresponds to *Delete*, paths are unregistered after a certain amount of time. Although the proposed scheme attempts to enhance TCP with multihoming support, it mainly focuses on increasing resiliency to path failures, by capitalizing on the availability of different network interfaces. The scheme does not enable bandwidth sharing between different paths or applications [Qureshi and Saleem, 2007].

With **Multiple TCP Fairness** [Tse, 2006] an application may employ multiple TCP instances to stripe packets across all available paths. The issue with this approach resides on the independency of each path. For instance, it is hard to guarantee that the multiple TCP instances do not displace more bandwidth on a single link as a single TCP instance over the path would take. In other words, a “fairness” issue arises as greedy applications employing more than one TCP connection in parallel receive a larger portion of what is their fair share of network resources. The Multiple TCP

Fairness proposal allows multiple TCP instances but ensures that an application does not take a disproportionate share of the available bandwidth. As such, the proposal introduces bi-level congestion control mechanisms which feature a single "master" congestion control mechanism to determine the overall sending rate and appropriate it to different number of subflows, which run their own congestion control procedures. "TCP fairness" introduces overhead in TCP operation.

FAST TCP [Wei et al., 2006] is a TCP variant that significantly improves the protocol's performance especially over high-speed long-distance connections. FAST TCP employs a delay-based congestion algorithm. An extension to FAST TCP [Arshad and Mian, 2008] is proposed to support multihoming and improve end-to-end throughput. Multihoming support is based on different functionalities, which include sender and receiver mechanisms and Selective Acknowledgements (SACKs). At the sender, for each available path, there is a window control mechanism to estimate Round Trip Time (RTT) and keep track of sent and acknowledged packets. The window control mechanisms are required on a per interface basis, since different bandwidth and delay conditions may exist. A drawback with the FAST TCP multihoming mechanism is its susceptibility to throughput problems, namely, network congestion situations on the path from destination to source. One-way congestion measurement is proposed to avoid erroneous RTT estimates [Arshad and Mian, 2008]. Moreover, different paths can have diverse RTT values leading to unfair share of resources [Belhaj and Tagina, 2008].

TCP Extension for Using Multiple Network Interfaces Simultaneously (TCP EUMNIS) [Valdovinos and Diaz, 2009] extends TCP to support simultaneous connections on heterogeneous interfaces. This extension modifies the TCP connection setup to allow multiple addresses. In addition, it introduces a new TCP option to maintain compatibility with existing TCP proposals.

■ Table 2.2 compares non standard tranport protocols with TCP and UDP. TCP Multi-Home Options [Matsumoto et al., 2003] introduces new TCP options in messages to add and remove addresses, that can be used to reach a particular destination, employing a primary-backup model. TCP Fairness [Tse, 2006] introduces support for multi-priority flows and specific congestion control mechanisms using a bi-level congestion control framework under the management of a master process. Different control mechanisms enable the support of multiple paths, nevertheless with a considerable delay in the probing of the different paths (e.g. in terms of RTT). The FAST TCP multihoming approach [Wei et al., 2006] introduces sender and receiver mecha-

Table 2.2: Multihoming support in non standard transport protocols.
MH-Multihoming, OS-Operating System, Sim.-Simulators.

Protocol	MH Goals				Strengths	Flaws	Implementation	
	R	U	L	F			Sim.	OS
UDP	X	X	X	X	Fast and widely available.	No Multihoming support.	Yes	Yes
TCP	X	X	X	X	Reliable and widely available.	No Multihoming Support.	Yes	Yes
TCP Multihome Options	√	X	X	X	Simple implementation.	Not standardized.	OMNeT++[a]	–
TCP Fairness	√	X	√	X	Support multiple paths independently	Overhead in the probing process. No public implementation	In ns2[b]	–
FAST TCP Multihoming	√	X	X	X	Available implementation.	Issues with heterogeneous paths.	In ns2[c]	–
TCP EUMNIS	√	X	X	X	Simultaneous Paths.	No Mobility support.	–	–

[a] [Qureshi and Saleem, 2007] [b] [Tse, 2006] [c] [CUBINLab, 2007]

nisms (specific congestion control) and SACKs. The concentration of mechanisms at the sender and receiver sides poses some issues with heterogeneous links. TCP EUMNIS [Valdovinos and Diaz, 2009] is an extension that enables the concurrent usage of paths in TCP, but has not entered in the standardization track. ■

2.4.2 PRISM

Proxy-based Inverse Multiplexer (PRISM) [Kim and Shin, 2007] is a proposal to improve TCP performance over wireless networks by capitalizing on collaborative multihomed mobile nodes. In such an environment, TCP performance can often be dramatically degraded due to packet reordering and heterogeneity of wireless links.

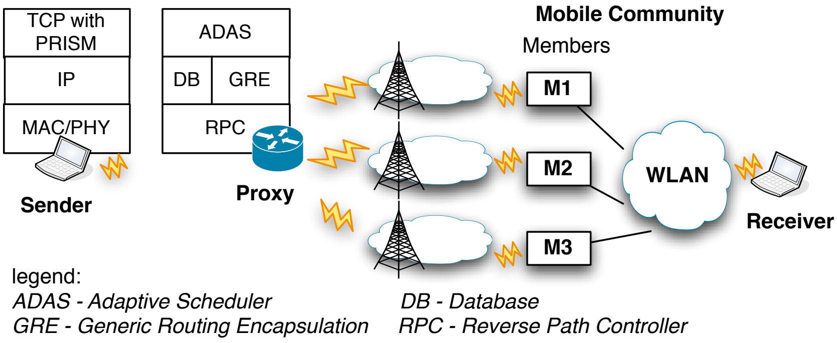


Figure 2.4: PRISM architecture

PRISM, illustrated in Figure 2.4, uses a proxy for routing, and is responsible to stripe each TCP flow over multiple links. In addition, the server (proxy) includes congestion control mechanisms to avoid packet loss. Besides the TCP mechanisms, mobile nodes can be organized in a community-like network in order to share connections. Although PRISM may have great potential, the reliance on a gateway/proxy node can be a concern. For example, despite providing support for simultaneous use of different paths, PRISM requires nodes to trust on the proxy server, which rises security issues. Moreover, upon a proxy failure, nodes cannot employ the advanced mechanisms provided by PRISM. Also as resources are shared between nodes in a community, mechanisms to guard against malicious or abusive users must be put in place, but this is not addressed [Kim and Shin, 2007].

2.4.3 MultiPath TCP

Multipath Transport Control Protocol (MPTCP) [Ford et al., 2011, 2013] allows the simultaneous use of diverse paths that can exist between a sender and a receiver. MPTCP represents the most recent efforts that the IETF has promoted to enhance the TCP capabilities to handle multiple addresses. The goals of MPTCP include throughput and resilience improvement by performing resource pooling, on which multiple addresses can be joined transparently to applications. MPTCP divides the transport layer into two sublayers, the MPTCP sublayer providing ordering of application data and reliability, congestion control and path management (detect multiple paths), and the subflow sublayer that assures reliable delivery of data, working as standard TCP. Initially MPTCP, establishes a connection setup and if multiple addresses exist, additional subflows are added to the initial established connection. When establishing a connection, peers exchange their capabilities in terms of MPTCP support and, in addition, specific options are introduced to allow the creation of subflows or to inform about new configured addresses.

The Multipath TCP API [Scharf and Ford, 2013] allows MPTCP-aware applications to control MPTCP. Through the API, applications can activate or deactivate MPTCP for certain data transfers, can query MPTCP regarding the addresses used on the MPTCP subflows, obtain the connection identifier and restrict MPTCP binding to a set of addresses. Nevertheless, the proposed API does not allow management of paths or scheduling of data.

2.4.4 Stream Control Transport Protocol and Extensions

The Stream Control Transport Protocol (SCTP) is a connection-oriented protocol designed to assure reliable signalling and transport [Stewart, 2007]. SCTP distinguishes itself from earlier proposed transport protocols due to its native support for multihoming, which allows, for instance, hosts to use all available IP addresses.

The multihoming support of SCTP is based on several mechanisms [Siddiqui and Zeadally, 2006]. First, address management at association setup, during which a node informs its peers about its IP addresses .Associations include information from the verification tag field of the SCTP common header and a checksum field, which allows the verification of the association a packet belongs to. Second, path and peer monitoring so-called *HEARTBEAT* chunks are employed to monitor peers and path status (active or inactive). Finally, for path selection, as the association setup proceeds, an active path is chosen as the primary path. SCTP uses Selective *ACKs* (SACKs) mechanisms to improve RTT estimation. The detection of a path failure is based on timeout and retransmission approaches [Charoenpanyasak and Paillassa, 2007].

The SCTP API [Stewart et al., 2011] allows associating an SCTP endpoint with multiple addresses. The SCTP API includes support for connection-less features (e.g. as UDP) to allow the control of multiple associations (*a one-to-many* mode), and support for connection-oriented features (e.g. as TCP). Applications can get information from the SCTP data, such as used addresses and status of each association. Another option, is that applications can subscribe to events and notifications. For instance, they can be notified when an association is established, or when there is a modification in the addresses of an association.

Mobile SCTP (mSCTP) [Stewart et al., 2007] extends SCTP to support mobile environments. mSCTP allows dynamic address reconfiguration by modifying IP addresses that were negotiated during the SCTP association setup. Such support is specified with new message types that contain the IP address and parameters to indicate the operation to perform, namely add, remove or modify the primary address. mSCTP can be employed by fault-intolerant applications, which require fast recovery. Different proposals extend mSCTP to allow different metrics for network selection [Fitzpatrick et al., 2009].

Concurrent Multipath Transfer (CMT) [Iyengar et al., 2006] adds simultaneous data transfer capabilities across multiple paths to SCTP. CMT addresses some performance issues of SCTP, such as unnecessary fast retransmission at the sender and increased ACK traffic due to fewer delayed ACKs. If the available paths have unbalanced delay or bandwidth, an SCTP receiver can experience packet reordering, which will consequently lead to fast retransmission at the sender. CMT mitigates these issues by introducing modifications in the SCTP specification. A receiver delays the ACKs, instead of immediately acknowledging out-of-order packets. Packet loss measurement, besides considering SACKs, also employs historical information. Moreover, the connection window, *cwnd*, is updated according to the path conditions. CMT still needs to mitigate RTT issues due to the different paths characteristics.

2.4.5 Datagram Congestion Control Protocol

Datagram Congestion Control Protocol (DCCP) [Kohler et al., 2006] is an unreliable transport protocol that can employ different profiles to control data congestion, also known as Congestion Control IDentifier (CCID) profiles. For instance, CCID2 is a profile that exhibits a TCP-like behaviour [Floyd and Kohler, 2006], while CCID4 [Floyd and Kohler, 2009] can be used by applications that want to follow a TCP-friendly rate control but are bound to use small packets.

DCCP does not support multihoming natively. A multihoming extension to DCCP has been proposed [Kohler, 2006], but it did not advance within the IETF standardization track. The extension introduces multihoming and mobility support by grouping multiple transport connections into a single application level entity (also called generalized connection). While applications only see one socket, transport connections can be transferred from one address to another. This requires extra information during the handshake. First the generalized connection identifiers are set between the peers and, on a second stage, transport connections are added to the generalized connection, via the DCCP request message. Nonetheless, multihoming and mobility support is limited, since there is no support for simultaneous movements or load sharing between the different connections [de Launois and Bagnulo, 2006].

Table 2.3: Multihoming support in transport protocols.
MH-Multihoming, OS-Operating System, Sim-Simulators.

Protocol	MH Goals				Strengths	Flaws	Implementation	
	R	U	L	F			Sim	OS
MPTCP	√	X	√	X	Compatible with TCP.	Security concerns.	ns2[a], htsim[b]	Linux[c]
PRISM	√	X	√	√	Flow distribution according to links.	Security Issues.	ns2[d]	Linux[d]
SCTP	√	X	X	X	Supports multiple paths natively.	No mobility support.	ns2, OMNeT++[e]	multiple[f]
mSCTP	√	√	X	X	Advanced mobility support.	No simultaneous use of paths.	–	FreeBSD[f]
CMT	√	X	√	X	Load sharing support.	Issues with heterogeneous paths.	ns2[f]	FreeBSD[f]
DCCP extension	√	√	X	X	Supports multiple addresses.	Limited mobility support.	ns2[g]	Only DCCP

[a] [Nishida, 2010] [b] [UCL, 2012] [c] [networking Lab, 2012] [d] [Kim and Shin, 2007] [e] [INET, 2012] [f] [Franken, 2013] [g] [Dedu, 2013]

■ Table 2.3 summarizes the main characteristics of the aforementioned transport protocols support for multihoming, listing the respective strong and weak aspects and evaluates the attainment of the multihoming goals of TCP, SCTP and DCCP derived proposals. DCCP and UDP, due to their unreliable nature, do not support multihoming efficiently or have limited support.

Standard TCP is being extended by Multipath TCP (MPTCP) to support multiple paths using centralized congestion control mechanisms. Despite the plurality of proposals to enhance TCP features for better multihoming support, only MPTCP advanced in the IETF standardization track. PRISM [Kim and Shin, 2007] introduces a network element, acting as a proxy, that stripes flows over multiple links. Such an approach, however, does not work if the proxy experiences a failure, introduces security issues, and does not support mobility.

Another transport protocol with native multihoming is SCTP [Stewart, 2007] that supports multiple IP addresses which are negotiated during the association phase, establishing primary and secondary paths. Notwithstanding, SCTP does not support dynamic update of addresses that occur on mobility events. Mobile SCTP [Stewart et al., 2007] addresses such limitation. Others, such as CMT [Iyengar et al., 2006], enhance SCTP to support the simultaneous use of different paths. ■

2.5 Multihoming and Mobility Management

This section overviews multihoming support in IPv6-based protocols, namely Mobile IPv6 [Kong et al., 2008], Proxy Mobile IPv6 (PMIPv6) [Kong et al., 2008] and respective extensions. IPv4-related protocols are left out of scope as their solutions for multihoming are less scalable and not forward-looking (e.g. future support for mobility with IPv4 is limited).

2.5.1 Mobile IPv6

MIPv6 [Kong et al., 2008] is, to a large degree, the archetypical mobility management protocol for IPv6 networks. Maintaining established communications while moving is similar to preserving established communications through outages in the multihoming context. MIPv6 maintains established communications while a mobile node moves across networks. However, current MIPv6 does not fully support multihoming, as it assumes that the home address does not change during the mobility management process. With such an assumption, whenever there is a change in the home address, e.g. a node with multiple prefixes in the home network, MIPv6 does not support new addresses acting as the home address. Even if binding update messages convey information in advance about alternative prefixes [de Launois and Bagnulo, 2006], this may not be enough to enable session survivability, as MIPv6 procedures fail, since they rely on a single address.

2.5.2 Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) [Kong et al., 2008] is a network mobility management protocol designed to assist IPv6 mobile nodes that do not have functionality to support mobility management. PMIPv6 introduces two entities, namely the Local Mobility Anchor (LMA), which acts as the home agent of the Mobile Node; and the Mobile Access Gateway (MAG) which is an access router capable of managing the signalling for a mobile node attached to its link.

PMIPv6 supports multihoming according to the configuration of prefixes and addresses. The configuration scenarios can include a unique prefix per interface, a unique address or a shared address across interfaces [Devarapalli et al., 2009; Kim and Choi, 2010]. The most efficient configurations are the dedicated prefixes/addresses per interfaces, as they allow the mobile node to use simultaneously both connections, nevertheless they have associated issues, such as multi-link subnet issues. The shared address configuration has limited multihoming support, as only one IP address is visible to applications.

The logical interface specification [Melia and Gundavelli, 2012], allows handovers between heterogenous technologies, by hiding physical details from IP layer. Thus, improving multihoming support of PMIPv6.

2.5.3 Multiple Care of Addresses and Flow Bindings

Multiple Care of Address (MCoA) [Pan et al., 2008a] extends MIPv6 to allow the registration of multiple Care of Addresses. With several Care of Addresses the mobile node can maintain concurrent paths with its correspondent nodes [Mitsuya et al., 2007]. The mobile node is always reachable at a unique permanent IPv6 address (employed as an identifier) while several temporary addresses (Care of Addresses) are used as locators to reveal the current network location of the node. Since locators change over time, each path is identified with a Binding Unique Identification (BID) number. Moreover, multiple registrations can be conveyed in a single message to reduce overhead. The enhanced multihoming support of MIPv6, empowered by MCoA registration, lacks a specification on how multiple registered addresses can be used. For instance, if the addresses can be used simultaneously, or if an address is chosen based on the link characteristics.

The specification of flow bindings [Tsirtsis et al., 2011a; Toseef et al., 2008] extends MCoA specification defining how multiple flows can be exchanged between two nodes, in a multihoming context. This enables to bind a particular flow to a Care of Address and use another address to receive information from other flows. The flow bindings specification conveys policies between the mobile node and other mobility agents (e.g. home agents) [Toseef et al., 2008]. Whilst the flow bindings specification deals with the transfer of policies, the way they can be generated or mapped to user preferences (e.g. link with higher bandwidth) is left out of scope. Due to its specificity, PMIPv6 is being extended to support flow bindings on a distinct proposal [Bernardos, 2013].

2.5.4 Network Mobility

Network Mobility (NEMO) is a protocol [Kuntz, 2007] that manages the mobility of a network of nodes typically moving in tandem. NEMO Basic Support extends MIPv6 procedures, through the addition of the Mobile Router (MR) entity. Each Mobile Network Node is connected to the MR, and all together form the mobile network. A mobile network is considered multihomed when a MR has multiple egress interfaces connecting to the Internet, or when there are multiple MRs or multiple global prefixes on the network [Wang et al., 2008]. Each of the multihoming goals has different requirements for NEMO multihoming support [Wang et al., 2008]. In order to achieve permanent and ubiquitous access, at least one bi-directional tunnel must be available. For reliability, both inbound and outbound traffic must be transmitted over another bi-directional tunnel once the active one fails. Moreover, multiple simultaneous tunnels must be maintained to assure load sharing and load balancing. Multihoming support in NEMO can also be classified based on the number of Mobile Routers, number of prefixes and the number of Collocated Care of Address (CCoA)-prefixes, instead of resorting to the number of Home Agents [Choi et al., 2006]. Multihoming models are based on a packet flow classification, which is divided into three segments. First, the segment between CN and HA, which is affected by the number of prefixes available. Second, the segment between HA and MR, which depends on the number of CCoAs, and finally the segment between MR and the MNNs.

NEMO Extended Support (NEMO-ES) [Deleplace et al., 2007] enables route optimization and policy based routing. Multihoming support is improved, as care is taken with the choice of the router that will route packets in a nested mobile network [Ng et al., 2007b].

■ Table 2.4 compares the protocols presented in this section. With respect to MIPv6, the main restrictions for multihoming include the assumption that the home address does not change during the mobility management process and the use of a

Table 2.4: Multihoming support in mobility management protocols.
MH-Multihoming, OS-Operating System.

Protocol	MH Goals				Strengths	Flaws	Implementation	
	R	U	L	F			Simulator	OS
MIPv6	X	√	X	X	Supports global mobility.	Limited multihoming support.	In ns2[a]and OMNeT++[b].	BSD, Linux[c].
MCoA	X	√	√	X	Supports multiple bindings.	No load sharing.	MCoA for OMNeT++[d].	Draft version[c].
Flow Bindings	X	√	√	√	Enables distribution of policies.	No definition of local policies.	–	In Linux[e].
PMIPv6	X	√	X	X	Easy deployment.	No specificity of physical interfaces.	In ns2[f]	In Linux[f].
NEMO	X	√	X	X	Supports network mobility.	Limited multihoming support.	In OMNeT++[b]. No public extensions for ns-2[h].	BSD, Linux[c].

[a] [Ernst, 2002] [b] [Yousaf and Bauer, 2013] [c] [Nautilus, 2009] [d] Candidate contribution [Sousa, 2013a]
[e] [Boutet et al., 2008] [f] [Choi, 2010] [g] [OpenAir3, 2013] [h] [Kong, 2008]

single binding between a care of address and the home address [Johnson et al., 2011]. MCoA [Wakikawa et al., 2009] and flow bindings [Tsirtsis et al., 2011a] proposals overcome the last restriction of MIPv6. Protocols like Fast Mobile IPv6 (FMIPv6) [Koodli, 2008] and Hierarchical Mobile IPv6 (HMIPv6) [Soliman et al., 2008], despite their improved mobility support when compared with MIPV6, have not been discussed as they share the same limitations of MIPv6 regarding multihoming support.

PMIPv6 [Gundavelli et al., 2008] is a protocol that provides mobility-assistance to nodes which are not Mobile IP (MIP)-aware. Different configurations are possible within multihomed nodes: a unique prefix per interface, a unique address per interface and a shared address across interfaces. Nonetheless support from the network (e.g. context transfer capabilities between access routers) and configuration-tuning on nodes (logical interfaces) may be required.

The multihoming support analysis in NEMO [Devarapalli et al., 2005] can follow the configuration approach, depending on the number of mobile routers, advertised mobile network prefixes and home agents. Moreover, NEMO can be associated with other protocols, such as HIP [Nováczki et al., 2008] to overcome the non-optimized routing performance in NEMO and to enhance security and multihoming support.

On the implementation front, the Nautilus6 project [Nautilus, 2009] enhances and maintains the main implementations of MIPv6 and NEMO protocols in GNU/Linux and BSD systems. ■

2.6 End-host Multihoming

This section overviews protocols and architectures tailored for end-host multihoming support. Proposals like SHIM6 [Garcia-Martinez et al., 2010], Host Identity Protocol (HIP) [Gurtov, 2008] constitute the standardized ones, while others, such as Name Address and Route System (NAROS) [Launois et al., 2003], or Practical End-host Multihoming (PERM) [Thompson et al., 2006] have not reached standardization.

2.6.1 Site Multihoming by IPv6 Intermediation

SHIM6 [Garcia-Martinez et al., 2010] is a multihoming protocol that adds a shim layer in the IP stack of end hosts. SHIM6 brings the advantage of assuring transport layer communication survivability, as the identity and location functions are split. For instance, the switch between address pairs is transparent to applications, since the identifier is only used to identify endpoints, while the locator is used to perform routing. In this split, SHIM6 provides the mapping function between upper layer identifier and locator at the receiver and sender end-hosts.

SHIM6 uses failure detection and recovery mechanisms described in the Reachability Protocol (REAP) [de la Oliva et al., 2010], which work independently from upper layer protocols. Failure detection can be based on keep-alive mechanisms or using information from upper layers (e.g. TCP control features). Recovery mechanisms rely on the exploration of available addresses, so that in the end an operational pair can be found and used.

Despite providing fault tolerance, SHIM6 breaks the functionality of some protocols, such as Internet Control Message Protocol (ICMP), since routers on the path cannot see the host identifier. Notwithstanding, SHIM6, when compared to other multihoming solutions, for instance HIP, has the advantage of an easier deployment in the Internet [Dhraief and Montavont, 2008], since SHIM6-compatible hosts can communicate with other nodes that are not SHIM6-aware.

SHIM6 is accompanied by a socket API [Komu et al., 2011; Fekete, 2010] that allows applications to access information about failure detection and path exploration. Moreover, through this API, applications can turn on/off shim layer functionality, and obtain or set preferred source and destination locator(s). Applications can also employ the API to inform the shim layer about the status of the communication or even control the frequency on which the REAP mechanism is executed.

2.6.2 Host Identify Protocol and Extensions

HIP [Gurtov, 2008] is a protocol that adopts a locator-identifier split approach and supports multihoming natively. HIP introduces a new host identity namespace and a new host identity layer between the network and the transport layers. In addition, HIP decouples identifiers (used by transport layer protocols) from locators (used for routing purposes). In short, the transport layer sockets and the IP security associations are bound to host identifiers, which in the end are tied to IP addresses.

Multihoming support in HIP is based on two approaches: *LOCATOR* parameter and *RendezVous* service [Gurtov et al., 2009]. Using the *LOCATOR* parameter approach, a HIP host can notify a correspondent peer about alternate addresses through which it is reachable. With the HIP *RendezVous* service, each HIP host publishes its host identifier with a *RendezVous* Server. The *RendezVous* Server maintains the mapping between the host identifiers and the locators, with limited support for mobility. HIP may raise issues with firewalls and middleboxes that need to inspect packet contents. Also, multihoming support does not include traffic engineering or policy address selection schemes.

HIP Application Programming Interface (API) [Komu and Henderson, 2011] relies on the SHIM6 API for different functionalities. HIP API introduces a new socket family and allows applications to open sockets based on Host Identification Tags (HITs) solely, to start communications with unknown peer identifiers and to perform explicit locator-identifier mapping.

HIP-based Simultaneous Access [Pierrel et al., 2007; Camarillo et al., 2010] introduces a policy system based on HIP to allow simultaneous multiaccess. The proposal extends HIP by allowing flows to use different paths independently of each other, since HIP does not support load sharing. To enable flow distribution support, flows are identified by source and destination ports and by HIT. The *RendezVous* Server, specified in [Laganier and Eggert, 2008], is extended to include the storage of flow policies. Then, *POLICY UPDATE* messages are employed to negotiate policies between peers during the HIP association lifetime. Whilst these policies define the usage rules of the available interfaces, the proposal does not detail policy specification (e.g. rules actions, interface priority, and cost).

2.6.3 End-Host Non-Standard Proposals

NAROS [Launois et al., 2003] is a mechanism that supports traffic engineering for unequal load balancing distribution, without impacting the routing system. Thre drawback of NAROS is that it requires modifications of end-hosts and does not preserve traffic flows across address changes [Launois et al., 2003; Savola and Chown, 2005; Dunmore et al., 2005].

Practical End-host Multihoming (PERM) [Thompson et al., 2006] enables flow scheduling in multihomed hosts, by extending the Linux socket API. PERM also introduces the concept of collaborative multihoming, in which users share their Internet connection with others. Flows are distributed using a scheduling algorithm that considers flow volume, load of a link and the respective RTT. Nonetheless, such metrics are not measured and are based on estimation techniques.

Strawman architecture [Habib et al., 2007] also modifies the Linux socket API to perform flow distribution at the session layer. Flows are stripped over multiple connections to maximize throughput and minimize delay, jitter and loss. Multimedia applications are also supported, by allowing in-order delivery but without transport guarantees. The drawback of this architecture is the fact of using IP addresses for location and identification simultaneously.

Forwarding directive, Association, and Rendezvous Architecture (FARA) [Clark et al., 2003] follows a location/identifier split approach that optimizes end-host mobility support by using rendezvous mechanisms. In FARA, no global namespace exists, instead the association IDs, the entity names and the end system address are used to establish communication between entities. FARA requires modifications in the network (i.e. for mapping) and on end-hosts, which does not facilitate its deployment [Ahlgren et al., 2005].

Layered Naming Architecture (LNA) [Balakrishnan et al., 2004] is a proposal that modifies end-hosts and the naming resolution system. LNA introduces a delegation system, where middleboxes stand-up on behalf of other entities, for instance, NAT routers or firewalls. Nonetheless, LNA introduces overhead with mappings, as they are performed twice.

Table 2.5: End-host multihoming proposals.
MH-Multihoming, OS-Operating System, Sim-Simulators.

Protocol	MH Goals				Strengths	Flaws	Implementation	
	R	U	L	F			Sim	OS
HIP[1]	√	X	X	X	IP family agnostic	Deployment issues	HIPSim++[a]	InfraHIP[b]
HIP SIMA[1]	√	√	√	√	Security	Limited policy specification	–	–
SHIM6[1]	√	X	X	X	Easier deployment than HIP	Mobility and security issues	REAP in OPnet[c]	LinShim6[d]
NAROS[2]	√	X	√	X	Load sharing for unequal paths	No LoC/ID split.	–	–
PERM[3]	√	X	√	√	Security	No LoC/ID split.	–	–
Strawman[3]	√	X	√	√	Security	No LoC/ID split.	–	–
LNA[1]	√	X	X	X	Delegation	Overhead in updates	–	–
FARA[1]	√	√	X	X	Supports mobility		–	–

[a] [Bokor, 2013] [b] [Gurtov, 2013] [c] [Khan, 2013] [d] [INL, 2013] [1] Loc/ID split [2] Routing/TE decouple [3] Flow Strip [h]

■ The pros and cons of the reviewed proposals for end-host multihoming support are summarized in Table 2.5, according to the multihoming goals fulfillment.

End-host multihoming proposals can follow different approaches. The Locator-

Identifier (Loc/ID) split is one of the approaches aiming to break the dual role of IP addresses. SHIM6 [Nordmark and Bagnulo, 2009] is a locator-identifier multihoming approach that adds a shim layer between the network and transport layers. SHIM6 uses REAP [Arkko and van Beijnum, 2009] to perform the detection of invalid locators and recover in an application-independent fashion. SHIM6 also includes security mechanisms to enable the protection of nodes identity. Nevertheless, SHIM6 must be combined with other protocols, such as MIPv6, to provide mobility support.

HIP [Gurtov, 2008] is an identity protocol that also decouples identifiers from locators. Its multihoming support relies on two approaches, one that resorts to the inclusion of new options in the HIP messages, that is, the *LOCATOR* parameter, and another that employs a *RendezVous* Server that maintains the mapping between identifiers and locators. Extensions to HIP [Pierrel et al., 2007] introduce load sharing and flow distribution support. The *RendezVous* servers are modified to store flow policies and HIP messages are updated to convey policies. This proposal extends the HIP4BSD implementation [Pekka Nikander, 2008], but is not publicly available.

NAROS [Launois et al., 2003] explores a routing/TE decoupling approach by implementing a server that holds the information of the appropriate source address a multihomed host must use when communicating with a certain peer. This approach alleviates the changes on routing systems (network part) but stresses the modification on the host part, as each node must query the server for each new communicating peer. With a different approach, LNA [Balakrishnan et al., 2004] introduces modification at the network side to accommodate mappings.

The strawman architecture [Habib et al., 2007] and PERM [Thompson et al., 2006] explore flow stripping mechanisms. Whilst such approaches have fine-grained capabilities (e.g. support of flow distribution according to policies), they require applications to be modified to support multihoming. These proposals are implemented by extending the functionalities of the Linux sockets API. ■

2.7 End-site Multihoming

This section overviews end-site multihoming proposals that are tailored for networks. Such proposals are defined according to Definition. 2.3, introduced in subsection 2.1.3. End-site multihoming has gained more attention than end-host multihoming, mainly due to the routing scalability problems that the Internet is facing (e.g. high growth in the core routing). End-site multihoming approaches can be classified in three major types: First, **address rewriting** approaches, which change addresses in packets; Second, **hierarchical** approaches, which structure networks to address scalability; Third, **mapping and encapsulation** approaches, which implement locator/identifier (Loc/ID) split paradigm, and as such, require mapping facilities to retrieve locator from identifiers, or vice-versa. Current IP routing architectures in Internet, such as Border Gateway Protocol (BGP) [van Beijnum, 2002], are not overviewed as these do not support Loc/ID paradigm.

2.7.1 Address Rewriting Approaches

In the *address rewriting* approach, the 128 bits of an IPv6 address are split, where the 64 most significant bits are used as the routing locator and the 64 least significant bits are used as the endpoint identifier. Figure 2.5 illustrates the process of address rewriting. The routing locator information is not known by the end nodes. Whilst this approach supports IPv6 only, it allows for consistency between prefix assignment and physical network topology.

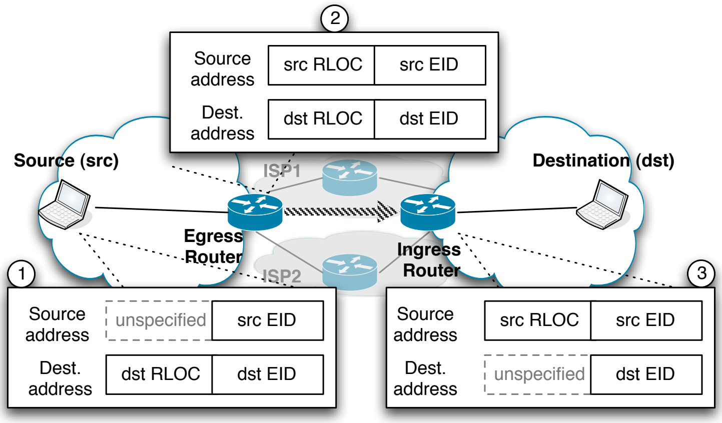


Figure 2.5: *Address rewriting* approach

2.7.1.1 Global locator and Identifier Split

Global locator and Identifier Split (GLI-Split) [Menth et al., 2010] is a locator-identifier addressing and routing architecture. GLI-Split implements a global locator for global routing, local locator inside domains and identifier split. Locators and identifiers are coded as IPv6 addresses to allow compatibility with IPv6 protocols.

GLI-gateway is in charge of performing address rewriting, with the assistance of the mapping systems. GLI-split supports mobility, but requires modifications to protocols like Dynamic Host Configuration Protocol (DHCP) to support multihoming.

2.7.1.2 4+4

The 4+4 proposal [Paul et al., 2009; Turányi et al., 2003] extends the Network Address Translation (NAT) architecture [Srisuresh and Egevang, 2001] to enable end-to-end host transparency. 4+4 uses two name spaces in DNS: one corresponds to the private IP addresses of the end-host and the other one is the public IP address of the NAT router responsible for the end-host. Thus, 4+4 address is formed by concatenating two IPv4 addresses, the public and the private one. As routing occurs, 4+4 routers (NAT gateways) perform swapping of addresses to assure that private IPv4 addresses are never used outside the network they belong to. The proposal allows end-hosts to have more than one address, and allows incremental deployments. Nevertheless, 4+4 only applies to IPv4 networks.

2.7.1.3 IP Next Layer

IP Next Layer (IPNL) [Francis and Gummadi, 2001] also extends NAT by adding a new layer between IP and TCP. It is different from 4+4 as it introduces new paradigms regarding the identification of a host. The end-host is identified by its FQDN, and the IPNL address, which is the locator. The IPNL address corresponds to the gateway address, the realm number and the host address triplet. Thus, for each communication, peers must use the FQDN, obtaining the IPNL address in the initial packet exchange. The host itself does not know all the possible addresses it has (when behind several routers) since it is only aware of its name. This type of design introduces overhead in packet processing; for instance, NAT routers need to maintain FQDN records per host [Turányi et al., 2003].

2.7.1.4 Translating Relaying Internet Architecture integrating Active Directories

Translating Relaying Internet Architecture integrating Active Directories (TRIAD) [Gritter and Cheriton, 2001] is a proposal that also uses names as identifiers and introduces a new paradigm for routing that is based on content, with the goal of reducing the access time to content. A content layer and content routers holding mapping information are introduced to allow the access to specific information identified in the form of an Universal Resource Locator. A host contacts a content router that answers to a request with the next available content router. At the end, the router close to the destination content server replies with the preferred address of the server. With such approach, a client gets the best path to the content server. TRIAD has some implementation issues, since modifications are required in the end-hosts and routers with NAT or gateway functionalities.

2.7.1.5 Pluralistic Network Architecture

Pluralistic Network Architecture (Plutarch) [Crowcroft et al., 2003] is a proposal that introduces contexts to suppress the need of global names to identify hosts. Moreover, Plutarch argues that naming and addressing should be handled by end-to-end systems and not hierarchical, domain-based system, such as DNS. The dedicated functions are assured by context borders (e.g. NAT routers) to assure end-to-end service. Despite including some implementation primitives, Plutarch specification is not ready for a global adoption in the Internet as important aspects, such as failure notification are not specified.

Table 2.6: End-Site multihoming proposals with address rewriting approach. MH-Multihoming, OS-Operating System.

Protocol	MH Goals				Strengths	Flaws	Implementation*
	R	U	L	F			OS
GLI-Split[2]	√	√	√	X	Security	Requires nodes changes	–
4+4[3]	X	X	X	X	Facilitates deployment	Only for IPv4.	In Linux[b]
IPNL[3]	√	√	X	X	Supports mobility	Hosts are not aware of their multihoming condition	In Linux[c]
TRIAD[3]	X	X	X	X	Optimized access to content	Weak multihoming approach	–
Plutarch[3]	X	X	X	X	Routing based on context	Weak multihoming approach	–

[a] [OpenLisp, 2013] [b] [Turányi and Valkó, 2003] [c] [Francis and Gummadi, 2001] [2] Address rewrite [3] NAT extension [*] Implementations in network simulators are not available.

■ Some proposals build upon current practices in the Internet architecture and implement extensions to NAT, to allow the support of multihoming and enable end-to-end communication, as summarized in Table 2.6. For instance, 4+4 [Turányi et al., 2003] supports multiaddressing, but raises security concerns since it exposes private addresses in packets. Others, such as IP Next Layer (IPNL) [Francis and Gummadi, 2001] address security but disable the multihoming information on end-hosts (e.g. hosts do not know if they have multiple addresses). Translating Relaying Internet Architecture integrating Active Directories (TRIAD) [Gritter and Cheriton, 2001] introduces the concept of routing by content, but requires many modifications to the actual Internet architecture. Also Plutarch [Crowcroft et al., 2003] uses context to enable identification and puts emphasis on end-hosts functionalities. Nonetheless, Plutarch does not include failure detection mechanisms. GLI-Split [Menth et al., 2010] maintains compatibility with IPv6, but requires changes to protocols like DHCP. ■

2.7.2 Hierarchical Approaches

Hierarchical approaches organize the network in a logical way, in order to overcome limitations (scalability) and overhead of flat networks. For instance, alternatives to BGP routing are proposed where convergence is enhanced, and the support of policies is improved. This subsection details proposals that include multihoming support through a hierarchical architecture [Subramanian et al., 2005].

2.7.2.1 Hierarchical IPv4

Hierarchical IPv4 (hiPv4) [Li, 2011] is a framework that splits the core address space from the edge address space. The first address space is globally unique, while the last is only used for routing and forwarding purposes inside local domains. With core and edge address spaces there is a hierarchical organization of addresses, in the sense that the core address space can correspond to the Autonomous System (AS). hiPv4 introduces a Locator Swap router to perform the change between prefixes and locators. Additionally a host identifier scheme is introduced to avoid locator renumbering at security nodes (e.g. firewalls). hiPv4 requires modifications to DNS, nodes, routers and security elements, which does not facilitate its implementation. In addition, hiPv4 may break the functionality of other protocols, such as Mobile IP, since the IPv4 header is changed.

2.7.2.2 Aggregation with Increasing Scopes

Aggregation with Increasing Scopes (AIS) [Khare et al., 2010] is a locator identifier split approach in which prefixes are aggregated in different steps and according to their scope. The first step aggregates prefixes with the same next hop. A second step configures a router as an aggregation point router that aggregates prefixes as a virtual prefix. Other routers, not acting as aggregation points, store only routes announced on the virtual prefixes. Aggregation leads to reduction in the mapping sizes, nevertheless may also lead to route traffic through non-optimal paths since they must traverse the routers acting as aggregation points. AIS has no support for mobility and does not include failure notification mechanisms to enable multihoming.

2.7.2.3 IRON-RANGER

IRON-RANGER [Templin, 2011] implements an overlay network, where specific routers manage virtual prefixes, from which provider independent prefixes are leased to end-nodes (e.g. customer sites). This proposal introduces serving routers, clients in end-user networks, and relay routers. Serving routers perform forwarding and mapping services, while the clients connect end user networks to the overlay network, via tunnels. The relay routers connect the IRON network to the rest of the Internet, and also advertise virtual prefixes. IRON-RANGER supports mobility and also enables end-hosts to register multiple locators. Nonetheless, there are no public implementations.

2.7.2.4 Enabling Future Internet Transit

Enabling Future Internet Transit (eFIT) [Massey et al., 2009] divides the network into user networks and transit wire. To accommodate heterogenous user networks, eFIT introduces a mapping service to translate user network addresses into transit wire addresses. Transit wire addresses are structured with the provider ID (globally unique); location ID containing the continent ID, country ID and metropolitan area ID; and the subnet ID and interface ID (current IP address). This structure of the transit wire addresses allows organizing the network in a hierarchical fashion. eFIT requires changes to protocols, such as BGP to include support for the new address structure. In addition, the specification lacks details regarding the mapping service (e.g. implemented via DNS or distributed hash tables). eFIT includes resilience and mobility support.

2.7.2.5 IPv6 Dual Homing

IPv6 Dual Homing (v6DH) [Brian Dickson, 2008] introduces an addressing convention where all addresses are routable and are specified in a primary secondary form. When a failure occurs on a certain address, another one can be used. For such, non working addresses are identified based on ICMP. Moreover, V6DH keeps information of unreachable links instead of maintaining all the links in the routing table. While scalability can be assured with this approach (less routes), it requires a change in the behaviour of BGP to enable resilience [Clevenger, 2010].

Table 2.7: Hierarchical End-Site multihoming proposals,
MH-Multihoming.

Protocol [*]	Multihoming Goals				Strengths	Flaws
	R	U	L	F		
hiPv4	√	√	√	X	Hierarchical organization	Impacts other protocols
AIS	X	X	X	X	Address aggregation done by scope	Unclear multihoming support
IRON-RANGER	√	√	√	√	Follows a business model.	Relies on an overlay network
eFIT	√	√	X	X	Supports mobility.	Requires changes to BGP
V6DH	√	X	X	X	Requires changes in DNS.	Facilitates deployment

[*] No public implementations are available in simulators and Operating Systems

■ Table 2.7 summarizes hierarchical approaches. hiPv4 [Li, 2011] is a hierarchical proposal that requires changes to protocols like DHCP to enable multihoming support. Similarly, eFIT [Massey et al., 2009] requires changes to BGP. Aggregation with Increasing Scopes (AIS) [Khare et al., 2010] is another hierarchical proposal that has routing scalability concern. As such, AIS avoids non-optimal paths. IRON-RANGER [Templin, 2011] introduce parallel networks to introduce benefits on a first one. v6DH [Brian Dickson, 2008] introduces a primary-backup protection model by requiring the specification of a primary and a backup address. This proposal enhances resilience support at the cost of requiring changes in current protocols (e.g. BGP). ■

2.7.3 Map and Encapsulation Approaches

The *map-and-encap* approach, as depicted in Figure 2.6, is based on the mapping and encapsulation processes as follows. A source host, on a domain sending a packet to a destination, inserts the source Endpoint Identifier (EID) and the destination EID in the packet header (Figure 2.6:1). When the packet arrives at the border router of the same domain, the Ingress Tunnel Router (ITR) performs the mapping between the destination EID and the Routing Locator (RLOC) (Figure 2.6:2-mapping phase). After, ITR encapsulates the packet and sets the destination address to the RLOC retrieved in the mapping phase (Figure 2.6:3-encapsulation phase). Finally, the packet arrives at the destination domain, on which a border router, the Egress Tunnel Router (ETR), performs the decapsulation and the delivery to the destination EID (Figure 2.6:4). This approach supports both IPv4 and IPv6, leaving end hosts unchanged, and minimizes modifications in the routing system.

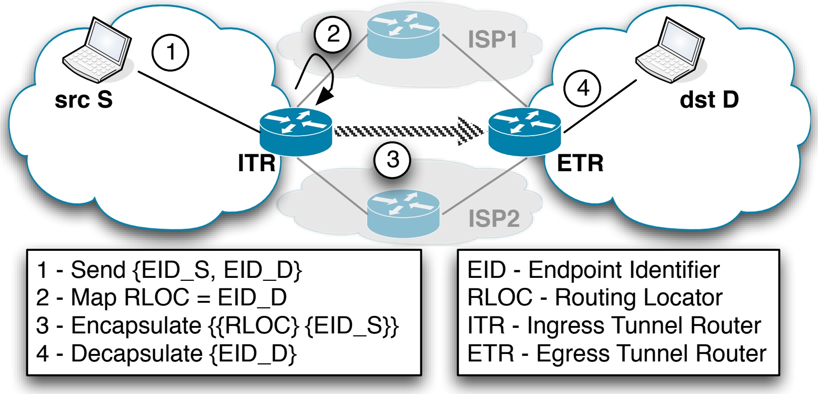


Figure 2.6: *Map and encap* approach

2.7.3.1 Locator Identifier Separation Protocol

Locator Identifier Separation Protocol (LISP) is a map-and-encap protocol [Dave, 2008] aiming to improve site multihoming. LISP decouples site addressing from provider addressing, and reduces the overhead associated with routing tables (e.g. size and latency lookup operations). To implement such goals, LISP specifies the data plane on which the mapping and encapsulation processes take place, and the control plane to manage the EID-RLOC mapping system. Since LISP only defines the messages for querying data and receiving information from the mapping system, it adopts a flexible design that allows different solutions for a mapping system. The proposals to perform EID-RLOC mapping under standardization include LISP Alternative Topology (LISP-ALT) [Dave, 2008] and LISP Map Server (LISP-MS). LISP-ALT uses existing protocols to build an alternative topology in order to manage the mapping. LISP-MS includes MAP-Servers that accept map-requests from ITRs and resolve the EID-to-RLOC mapping using a database, which is filled with the authoritative EID-to-RLOC mappings provided by ETRs.

2.7.3.2 Internet Vastly Improved Plumbing

Internet Vastly Improved Plumbing (IvIP) architecture [Zhang et al., 2010b] is a core-edge split proposal implementing a map-and-encap approach. IvIP uses a fast-push mapping scheme, where all mapping information is kept on query database servers. Ingress tunnel routers query database servers to determine the correct egress tunnel router to which traffic must be routed. IvIP works for IPv4 and IPv6 and supports mobility through extensions. Nevertheless, the mapping requires real-time reachability monitoring.

2.7.3.3 A Practical Transit Mapping Service

A Practical Transit Mapping Service (APT) [Jen et al., 2007] is a proposal that aims to reduce the number of nodes that must be modified. APT introduces the encapsulation/decapsulation routers that maintain a reduced cache of mappings. Only the default mappers, new elements, have all the maps, and are used by the encapsulation routers when no match is found in their cache. The full mapping is obtained from a specific BGP instance, which introduces more overhead. In addition, as no reachability is preserved on the mapping, APT relies on external protocols (e.g. BGP) to detect failures on mappings. In comparison to LISP, APT has some advantages since no modifications are performed at the edge sites [Clevenger, 2010]. Nonetheless, the proposal has not been standardized and no specifications for incremental deployment have been produced.

2.7.3.4 Core Router-Integrated Overlay

Core Router-Integrated Overlay (CRIO) [Zhang et al., 2006] aims at mitigating the trade-off between path length and routing table size. CRIO decouples address hierarchy from physical topology and is suitable for global and VPN routing, as it relies on tunnels to forward data and on virtual prefixes to reduce routing tables size. CRIO supports mapping weights that establish the preference of entries over another in a multihoming context. CRIO in some cases does not provide the shortest path in the mapping. Mapping distribution relies on BGP and it has not reached standardization despite not requiring new hardware and supporting non continuous networks due to the aggregation of virtual prefixes [Clevenger, 2010].

2.7.3.5 IP with Virtual Link Extension

IP with Virtual Link Extension (IPvLX) [Templin, 2007; Clevenger, 2010] aims to allow IPv6 and IPv4 coexistence. IPvLX recommends to employ IPv6 addressees as identifiers and IPv4 addresses as locators, although this is not a rigid rule. IPvLX uses DNS for mapping, thus requiring changes on DNS systems, and implements a 'site-local' resolution system to hold records of nodes that are more dynamic. IPvLX has not reached standardization and is more suitable to be employed with IPv4 to IPv6 transition solutions.

2.7.3.6 Tunneling Route Reduction Protocol

Tunneling Route Reduction Protocol (TRRP) [Clevenger, 2010; Herrin, 2007] relies on GRE tunnels to forward traffic. It uses DNS for mapping and introduces new records that establish how traffic is forwarded on IPv4 or IPv6 tunnels. As such, by having multiple entries in DNS with the respective preference, multihoming is supported, since a destination can be reached through several addresses. Nevertheless, routers must be modified to accommodate several records in the lookup operation. The TRRP specification describes an implementation plan that includes different phases; nevertheless, no mobility support is stated.

2.7.3.7 Virtual Aggregation

Virtual Aggregation (ViAggre) [Ballani et al., 2009] is a proposal that also aims to reduce the routing table size by aggregating routes into virtual prefixes and using such virtual networks inside the ISP. Virtual prefixes have no topological meaning and can be obtained by aggregating IPv4 addresses into 128 bit addresses. A router acting as an aggregation point only maintains routes for the virtual prefixes that it is aggregating. When there is need to send packets to external routers, then MPLS tunnels are employed to avoid loops inside the ISP network. One advantage of ViAggre includes the possibility of incremental deployments as no changes are required in the routers or network protocols, and it is transparent between ISPs [Clevenger, 2010]. Nevertheless, ViAggre requires ISPs to use MPLS to enable encapsulation between aggregation points and introduces management overhead inside the ISP network, as configuration of aggregation points is needed. ViAggre has no public implementation available, although the authors published evaluation results from a real testbed.

Table 2.8: End-Site multihoming proposals with map and encapsulation, MH-Multihoming, OS-Operating System, Imp-Implementation.

Protocol	MH Goals				Strengths	Flaws	Imp[*]
	R	U	L	F			OS
LISP	√	X	√	X	Flexible mapping	Encapsulation overhead	FreeBSD[a]
IvIP	√	X	√	√	Mobility support	Scalability issues	–
APT	√	X	√	√	Mobility support	Scalability issues.	–
CRIO	√	X	√	√	Policies support	No Mobility Support.	–
IPvLX	√	√	X	X	For IPv4 to IPv6 transition	Not Standardized.	–
TRRP	√	X	X	X	Works with existent protocols	Requires changes in routers.	–
ViAggre	√	√	X	X	Incremental deployments	Requires MPLS.	–

[a] [OpenLisp, 2013] [*] Public implementation in network simulators are not available

■ Mapping and encapsulation approaches, summarized in Table 2.8, have the advantage of facilitating deployment. LISP [Dave, 2008] is expected to decrease the size of routing tables in the core network when deployed. Others, such as IvIP [Zhang et al., 2010b] do not address mobility natively. APT [Jen et al., 2007] has deployment concerns, since it aims to reduce the number of nodes that require modification. In the same line of deployment concern, Core Router-Integrated Overlay (CRIO) [Zhang et al., 2006] does not require new hardware, as aggregation of prefixes is employed, but it does not provide the shortest path. Some proposals, like IPvLX [Templin, 2007] are tailored for IPv4-to-IPv6 transition, and as such, have limited multihoming support. Tunneling Route Reduction Protocol (TRRP) [Clevenger, 2010] requires changes on DNS to allow the retrievement of multiple records, corresponding to the multiple addresses of an end-host. ViAggre [Ballani et al., 2009] is one of the proposals that enable ViAggre-compliant nodes to communicate with standard nodes (deployment concerns), but relies on MPLS to avoid loops. ■

2.8 Hybrid Multihoming

This section describes hybrid multihoming approaches in three distinct categories: First, **content/service-centric** approaches, which include solutions that focus on information; Second, **locator-identifier** split approaches enable the separation of the dual-role (location and identification) in IP addresses; Third, **new architectures and routing-centric** approaches that enable multihoming by providing scalable and efficient routing mechanisms.

2.8.1 Content-Centric and Service-Centric Approaches

This subsection includes proposals with architectures that rely on data/information and not on IP addresses, such as Content-Centric Networks (CCNs). For instance, Name Data Networking (NDN) [Zhang et al., 2010a] performs routing based on the interest that a node has on certain (named) data. Another proposal is the Architecture for Services Integration, controL, and Optimization for the Future Internet (SILOS) [Dutta et al., 2007] that has multihoming support but lacks failure-tolerance mechanisms. SILOS, in comparison to NDN, has the disadvantage of not supporting mobility, while it incorporates cross-layer schemes that facilitate adding new functionalities. The Service-Centric End-to-End Abstractions for Network Architecture [Wolf, 2006] approach specifies the data service to forward information. To enable such transfer, functionalities are added on routers or other nodes closest to end-hosts. Nonetheless, no support for flow distribution or mobility is provided. With limited multihoming support NetServ [Schulzrinne et al., 2013] is an architecture that virtualizes services to facilitate adding new functionalities. Services have also associated resilience mechanisms that allow efficient failure detection. Nonetheless advanced features, such as mobility or flow distribution, are not supported.

2.8.1.1 Networking Named Content

Networking Named Content (NNC) [Jacobson et al., 2009] introduces an architecture where all operations focus on data. Nodes request content by using interest packet types and NNC nodes (e.g. ISP routers) use distinct tables to inspect the Interest packets. For instance, if the requested content is found on their cache, the nodes reply immediately with data packets, otherwise they forward packets. These packet types do not carry any information regarding location, but rather the content name with a hierarchical structure. Mobility is supported, since bindings are not performed to IP addresses. Also, NNC supports resilience and flow distribution [Paul et al., 2011]. Implementation of this proposal is publicly available in [CCNx, 2013].

2.8.1.2 Data Oriented Network Architecture

Data Oriented Network Architecture (DONA) [Chawla et al., 2007] proposes a new clean-state architecture, where names are generated based on public key mechanisms, routing is based on names and name resolution relies on specific handlers that reply to clients in the presence of "find" packets. The transport layer binds to names and not to IP information. DONA also assures that the shortest path is found for certain data, as packets are forwarded to the data servers closest to the node requesting the data. In addition, DONA includes failure detection mechanisms and supports concurrent use of multiple connections. Unfortunately, no public code is available.

2.8.1.3 Multiaccess Network Information

Multiaccess Network Information (NetInf) [Pentikousis and Rautio, 2010] is an information -centric proposal that allows the creation, distribution and retrieval of information using different components. The name resolution service enables the resolution of local and global (e.g. outside local domain) resources. The notification service informs applications about the domains they are connected to. One of the advantages of NetInf includes mobility and multihoming support, as objects are decoupled from their storage location. NetInf has already a public implementation [Christian Dannewitz, 2013], where well-known applications, such as Firefox and Thunderbird have been adapted to work in the NetInf architecture.

■ Table 2.9 summarizes information-centric proposals where routing/forwarding is based on names and not on current IP addresses. With such characteristics, there is

Table 2.9: Hybrid Multihoming proposals with content-centric approaches. MH-Multihoming, OS-Operating Systems.

Protocol	MH Goals				Strengths	Flaws	Implementation	
	R	U	L	F			Simulator	OS
NDN[1]	√	√	√	√	Routing by names.	Issues with security	OMNeT++[a]	Linux[b]
NNC[1]	√	√	√	√	Routing by names.	No public implementation	–	–
DONA[1]	√	√	√	√	Routing by names.	No public implementation	–	Linux[c]
NetInf[2]	√	√	√	√	Routing by Information.	Issues in security.	OpenNetInf[e]	Linux[d]
Service-Centric[1]	√	X	X	X	Routing by Information	Specification with open issues	–	–
SILOS[3]	X	X	X	X	Cross-layer mechanisms	Incompatible with Internet model	–	–
NetServ[3]	√	X	X	X	Mobility and Flow Distribution can be added.	Incompatible with Internet model	–	–

[a] [Rossini et al., 2013a] [b] [Rossini et al., 2013b] [c] [Chawla et al., 2007] [d] [Pentikousis and Rautio, 2010] [e] [Christian Dannewitz, 2013] [1] Content Network [2] Information Network [3] Functional blocks

no compatibility with current TCP/IP architectures, which constitutes a disadvantage regarding near-term deployment. For instance, SILOS [Dutta et al., 2007] focuses on services and their interaction with other layers and nodes and moreover it does not support multihoming. Data Oriented Network Architecture (DONA) [Chawla et al., 2007] and Networking Named Content (NNC) [Jacobson et al., 2009] support all multihoming goals. Other proposals, like Service-Centric End-to-End Abstractions [Wolf, 2006] and NDN [Zhang et al., 2010a] are not mature as they miss details in their specifications. NetServ virtualizes services per application request [Schulzrinne et al., 2013]. However all these proposals fail to provide a mature implementation that can practically demonstrate the advantages of routing by data/information on a large scale. ■

2.8.2 Address Rewriting Approaches

Hybrid multihoming proposals support the Locator/Identifier split paradigm through address rewriting, such as the example of Identifier Locator Network Protocol [Atkinson et al., 2010] and Routing Architecture for the Next Generation Internet (RANGI) [Li, 2011].

2.8.2.1 Identifier Locator Network Protocol

Identifier Locator Network Protocol (ILNP) [Atkinson et al., 2010] is a proposal that implements a locator-identifier split by employing address rewriting. The locator is used to route traffic, while the identifier is employed as a node identifier without topological significance. The identifier is obtained in a IEEE EUI-64 bit format, while locators correspond to the 64 bit prefix of an IPv6 address. Applications bind their sessions to the identifier and not to the locator. If the identifier is globally unique, procedures like Duplicate Address Detection (DAD) are not necessary, which improves mobility support. ILNP requires modifications to DNS in order to allow nodes to update their locator records.

2.8.2.2 Routing Architecture for the Next Generation Internet

Routing Architecture for the Next Generation Internet (RANGI) [Li, 2011] introduces a host identifier layer between the network and transport layers. The host identifier has an organizational structure to allow easier mappings between identifiers and locators, which are based on IPv4 addresses embedded in IPv6 addresses. The mapping between domain name and host identifiers is done via DNS, while the mapping between identifiers and locators is performed on a distributed mapping system. RANGI allows incremental deployment and facilitates the migration from IPv4 to IPv6 networks. Although no procedures are specified for handling mobility updates and the lack of a publicly available implementation, RANGI, through the use of proxies, allows its interoperation with standard IPv4 and IPv6 nodes.

Table 2.10: Hybrid multihoming proposals with address rewriting approaches.

Protocol	Multihoming Goals				Strengths	Flaws
	R	U	L	F		
ILNP	√	√	√	√	Supports end-host multihoming	Requires changes to DNS
RANGI	√	√	X	X	Facilitates IPv4 to IPv6 migration.	Requires changes to hosts

■ Both ILNP and RANGI require changes to DNS or to hosts, as summarized in Table 2.10, which can limit their adoption. Nonetheless ILNP offers better multihoming support, as all multihoming goals are supported. RANGI has also the advantage of facilitating the migration from IPv4 to IPv6 networks. ■

2.8.3 Hierarchical Approaches

Other hybrid proposals implement the Loc/ID paradigm by organizing the network into hierarchies. The motivation for hierarchal approaches can be diverse and proposals like the Hierarchical Routing Architecture (HRA) [Xu and Guo, 2008] aim to mitigate routing scalability issues. Other proposals likeNode ID Internetworking Architecture (NIIA) [Schütz et al., 2010] organizes the network as a tree, where routing inside domains uses locators and between domains employs Node ID or default routes to parent nodes in the tree. NIIA also supports multiple registration on the tree, to accommodate nodes with multiple interfaces.

2.8.3.1 Less-Is-More Architecture

Less-Is-More Architecture (LIMA) [Li et al., 2012] is a locator-identifier split approach that enables inter-domain routing. LIMA proposes a hierarchical scheme, on which addresses are composed by a globally unique provider AS number, a provider local stub AS number and deploys a stub-local intra domain address. LIMA borders routers implement two routing tables, one for provider numbers and another for stub networks. With this, routers no longer need to perform longest prefix match or have information about stubs. The operation of LIMA requires changes to multiple protocols, such as DHCP and DNS. For instance, DNS must maintain intra-domain mappings. LIMA supports multiaddressing with the aid of transport protocols such as

SCTP or MPTCP. LIMA also includes Name Based Sockets to perform translation between names and addresses at the end-nodes. Finally, LIMA supports policies and mobility via dynamic DNS mechanisms.

2.8.3.2 iMark

iMark [Chowdhury et al., 2009] uses global identifiers to enable end-to-end communication. iMark employs virtual networks to distinguish between infrastructure providers and service providers (i.e. providing virtual resources). Virtual networks are organized hierarchically, where controllers are the elements that provide name resolution and address location inside a network, while adapters are responsible for protocol/address translation between virtual networks. iMark supports simultaneous connections, even on heterogeneous networks, by using distinct global identifiers. iMark also distinguishes the type of mobility in order to manage the respective updates; at the micro-level updates occur inside a virtual network, while at the macro-level end-users connect to a different virtual network. iMark specification lacks details, namely how identifiers are generated and in what form they are provided (e.g. FQDN). The evaluation in a testbed demonstrates the proposal scalability, but the respective code is not publicly available.

2.8.3.3 HiiMap

HiiMap [Hanka et al., 2009] is a locator-identifier split approach that uses DHT to perform mapping between identifiers and locators. HiiMap introduces a region prefix in the unique identifier to organize networks hierarchically and deploy trust relations between the global authority and local authorities of the different regions (e.g. countries). Addresses in HiiMap include the unique identifier that is a flat, and randomized worldwide unique 128 bit address and is attributed by the global authority. The region prefix identifies the region where mapping the unique identifier to the corresponding locator is performed (can be compared to the home network in Mobile IP). HiiMap has an implementation in a testbed but no public code is available. HiiMap supports mobility between networks and between regions, since locators are updated in the home region. It also includes security mechanisms to provide authentication.

2.8.3.4 Scalable and Secure Identifier-to-Locator Mapping Service

Scalable and Secure Identifier-to-Locator Mapping Service (SILMS) [Hou et al., 2009] is a hybrid approach that introduces modifications in end-hosts and networks. SILMS is a locator-identifier split approach that optimizes lookups on the mapping services by caching the most frequent maps in all service nodes. The most important maps are determined via Bloom filters (probabilistic data structures) and with management servers that collect statistics about mapping data. The identifier in SILMS follows the same logic of HIP (see subsection 2.6.2), and the locator corresponds to an IPv6 address. SILMS supports flow distribution by introducing a hierarchical architecture, with policy and management servers and with border routers that manage local mappings. However, there is no efficient mobility support and no public implementation is available.

2.8.3.5 Mobility and Multihoming support Identifier Locator Split Architecture

Mobility and Multihoming support Identifier Locator Split Architecture (MILSA) [Pan et al., 2008b] is a locator-identifier split proposal that introduces different hierarchies in the network, namely the realm-zone bridging zone hierarchy and the realm hierarchy, as depicted in Figure 2.7.

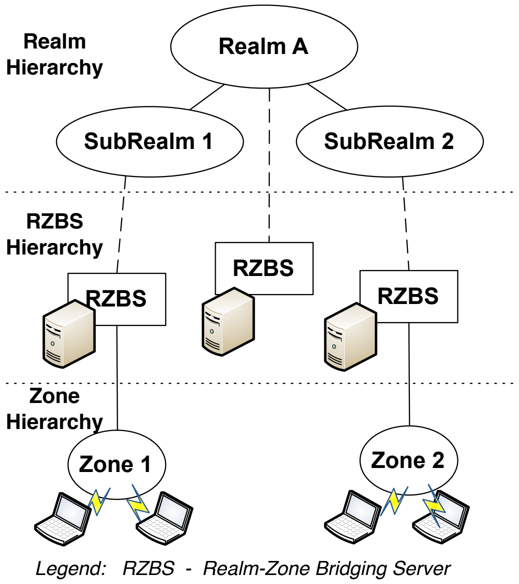


Figure 2.7: MILSA

The realm hierarchy corresponds to a logical concept, in which the trust relationships between different groups of objects are maintained. The realm-zone bridging zone hierarchy contains an overlay network of servers that map identifiers to locators. MILSA does not affect DNS and includes support for mobility. Enhanced MILSA

(EMILSA) [Pan et al., 2009] avoids global routing and improves the mobility and multihoming support of MILSA. In addition, a specific sublayer is added in the network layer to perform the separation between identifiers and locators.

2.8.3.6 TurfNet

TurfNet [Schmid et al., 2005] is a locator-identifier split approach and aims to enable the communication between autonomous and heterogeneous networks that may use different addressing schemes. A new host identity namespace is introduced, and the network is composed vertically (relation between ISP and customer) and/or horizontally (between peer networks), denominating the composed networks by turfs. Registration and lookup services enable inter-turf communication and announce the reachability of end-nodes outside their local turfs. Gateways keep soft-state of the communications of the local turfnodes and inter-turf gateways perform locator and protocol translation for packets traversing different turfs. The TurfNet proposal supports mobility, even when end-nodes move between heterogenous domains, since nodes are required to register with the lookup service. The proposal is evaluated empirically [Pujol et al., 2005] to demonstrate its scalability performance. Nonetheless, no public implementation is available.

2.8.3.7 Hierarchical Architecture for Internet Routing

Hierarchical Architecture for Internet Routing (HAIR) [Feldmann et al., 2009] introduces different levels of hierarchy with the goals of supporting mobility, traffic engineering and reducing the size of routing tables. End-nodes have the function of translating identifiers and locators, while functions to assure scalability are placed in the network. The mapping service is distributed at the authorities owning such mapping. The hierarchical organization introduced in the proposal, includes edges, where hosts are attached, intermediate routers to allow routing between edges and core, and finally the core. Intermediate routers are responsible to manage locators and mappings in the intermediate network mapping. When a node needs to communicate with another, it first retrieves the identification of the destination (e.g. via DNS) and after the respective location. One of the drawbacks of HAIR is that it does not include specification on the format of identifiers [Clevenger, 2010]. Nevertheless, HAIR has an implementation for demonstration purposes [Feldmann et al., 2012].

2.8.3.8 Hierarchical Inter-Domain Routing Architecture

Hierarchical Inter-Domain Routing Architecture (HIDRA) [Clevenger, 2010] is a proposal with two concerns, the first one is to reduce the size of routing tables at core networks and the second is related with deployment concerns. HIDRA is a hierarchical network architecture that uses mapping and encapsulation, and also employs IPv4 addresses for location and identification purposes, to maximize the compatibility with existent approaches. HIDRA uses BGP as a proactive mapping system (with the overhead of transmitting routes that may not be necessary), nevertheless the mapping devices are placed at the edges, near end-nodes. As one of the concerns in HIDRA is deployment, detailed steps are provided to enable migration from existing architectures to HIDRA. For instance, a default route must be installed to send all traffic to an encapsulation point. An implementation in a Linux testbed is used to test HIDRA. Nevertheless, reactive mapping optimizations are not specified.

■ Hybrid proposals rely on the locator-identifier split paradigm, nonetheless, some organize the network in an hierarchical way to facilitate deployment and management. The NIIA [Schütz et al., 2010] organizes the network as a tree, and employs default routes to parent nodes to enable inter-domain routing. In addition, NIIA supports multiple registration of nodes in the tree (useful when there are multiple interfaces). Less-Is-More Architecture (LIMA) [Li et al., 2012] uses a hierarchical structure to enable efficient inter-domain routing and relies on transport protocols such as SCTP and MPTCP to enable multiaddressing configurations. iMark [Chowdhury et al., 2009] includes support for simultaneous connections between heterogeneous networks. Nonetheless, details to enable its implementation are missing, such as the mechanism to generate identifiers. HiiMap [Hanka et al., 2009] organizes the network according to a region prefix, allowing trust relationships with authorities. MILSA [Pan et al., 2008b] has the advantage of not introducing changes on DNS, or even relying on this service to support mobility. Hierarchical Architecture for Internet Routing (HAIR) [Feldmann et al., 2009] is a hierarchical proposal that aims to enable traffic engineering and puts emphasis on the role of end-hosts by moving core functionalities to end-hosts, but lacks details regarding identifiers. Hierarchical Inter-Domain Routing Architecture (HIDRA) [Clevenger, 2010] is also a proposal that aims to foster deployment. For instance, it relies on existing routing protocols such as BGP to allow a proactive mapping system. Proposals like HRA [Xu and Guo, 2008] support mobility by extending HIP and BGP protocols. SILMS [Hou et al., 2009] has the limitation of only supporting IPv6. Instead of aiming compatibility, other proposals pursue a

Table 2.11: Hybrid multihoming proposals with hierarchical approaches. MH-Multihoming, Imp-Implementation, OS-Operating Systems.

Protocol	MH Goals				Strengths	Flaws	Imp
	R	U	L	F			OS
LIMA[1]	√	√	√	√	Supports multihoming.	Changes on DHCP and DNS	–
iMark[1]	√	√	√	√	Concurrent connections.	Specification incomplete	–
HiiMap[1]	√	√	X	X	Support Security	No public implementation available	–
HRA[1]	√	√	X	X	Scalable	No flow distribution	–
SILMS[1]	√	X	X	√	Flow distribution	Only for IPv6	–
MILSA[1]	√	√	√	√	Flow distribution	No public implementation	–
TurfNet[1]	√	√	X	X	Mobility	No public implementation	–
NIAA[1]	√	√	X	X	Security	No public implementation	–
HAIR[2]	√	√	√	√	Hierarchical networking	No implementation details	Linux[a]
HIDRA[2]	√	√	√	√	deployment details	Optimize mode not specified	Linux[b]

[a] [Feldmann et al., 2012] [b] [Clevenger, 2010] [1] Loc/ID split [2] Routing Architecture

security-oriented paradigm. NIIA [Schütz et al., 2010] includes native security mechanisms, aiming to protect the identity of nodes. ■

2.8.4 Map and Encapsulation

This subsection details proposals that implement the locator-identifier split paradigm through mapping and encapsulation mechanisms.

2.8.4.1 LISP Mobile Node

LISP-Mobile Node [Farinacci et al., 2012] is a version of LISP that targets mobile nodes. Some of the functionalities of Ingress and Egress Tunnel routers of LISP are placed on the mobile node. As such, the node has capabilities of handling mobility without the assistance of servers in the network. LISP Mobile nodes behave as a LISP site, updating locators in the associated mapping system when performing handovers. The identifiers (EID), also employed in LISP, do not change and are used in all the connections of the LISP Mobile Node.

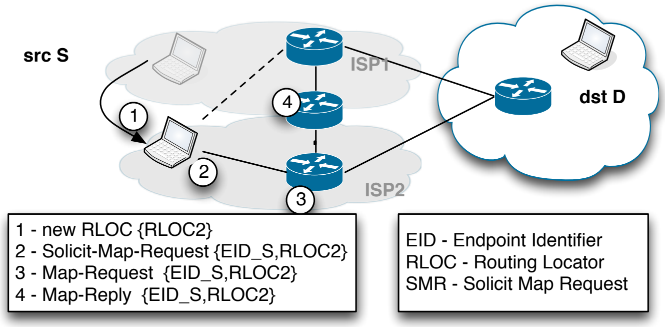

src S
ISP1
dst D
4
1
2
3
ISP2
1 - new RLOC {RLOC2}
2 - Solicit-Map-Request {EID_S,RLOC2}
3 - Map-Request {EID_S,RLOC2}
4 - Map-Reply {EID_S,RLOC2}
EID - Endpoint Identifier
RLOC - Routing Locator
SMR - Solicit Map Request

Figure 2.8: LISP Mobile Node handover

As pictured in Figure 2.8, LISP Mobile Node (node S), receives a new Routing Locator (RLOC), when connecting to ISP2. Afterwards, the respective mappings need to be updated. For such, the MN sends a solicit-map-request message, which is intercepted by next-hop LISP routers which, in turn, forward the message as map-request to the mapping server, which replies with a map-reply message. Nodes must be compliant with the LISP Mobile node specification, nevertheless, a mapping server can be employed to allow the communication with non LISP nodes. Moreover, the proposal has an implementation available [Farinacci et al., 2013].

2.8.4.2 Unmanaged Internet Architecture

Unmanaged Internet Architecture (UIA) [Ford, 2008] is compatible with current IP architecture and can be incrementally deployed. UIA targets personal devices and specifies a transport protocol - the structure stream transport to enable efficient transport of streams. This transport protocol has the advantage of supportting transactions like HTTP, nevertheless it does not have multihoming features like SCTP does (e.g. primary-backup model). UIA integrates a routing architecture that enables peer devices to communicate in an ad-hoc way. Moreover, security and privacy are included natively. Distributed hash tables are employed to hold the mappings of locators and identifiers.

2.8.4.3 Delegation Oriented Approach

Delegation Oriented Approach (DOA) [Walfish et al., 2004] focuses on the specification on middleboxes (e.g. NAT, firewalls) to eliminate their side-effects (e.g. alter or hinder end-to-end communication between peers) and to facilitate implementation. DOA provides identifiers to hosts and means to end-nodes to perform delegation (if packets should be/or not sent off-path boxes). The Endpoint IDentifier (EID) identifies the end-node, while the IP address is employed as a locator. EIDs, acting as global identifiers, are generated with public keys and are placed into each packet. Mappings can be in the tuple EID, IP address or EID to a list of EIDs. The latter one reflects the nodes on which the packet goes through the delegated nodes before reaching destination. DOA implements security mechanisms, since EIDs can only be modified by the respective end-nodes. Nevertheless, it does not include mechanisms to update locators in mobility events [Paul et al., 2009].

2.8.4.4 Six/One Router

Six/One router [Vogt, 2008] introduces the translation between provider-independent and provider-dependent addresses. Six/One router has some similarities with SHIM6 as it uses one of the locators for the node identity during the session and only targets IPv6 networks. The translation of addresses is assured by specific hardware that performs translation of network source and destination addresses. If the mapping holds records for source and destination addresses, Six/One can support multihoming and mobility, nevertheless mapping must be assured by an external specification such as DNS. One major advantage of Six/One is communicating with non Six/One routers [Clevenger, 2010] and the reduced size of the routing table and the update frequency. Flow diversity is enabled in Six/One with the extended proposal [Paul et al., 2010a] that adds monitoring features and inform upper layers (e.g. TCP) on the best performant paths.

2.8.4.5 Old and non-standard proposals

The Internet Indirection Infrastruture (I3) [Stoica et al., 2004] is among the first Loc/ID split approaches, where packets contain data and identifiers. A server holds the role of mapping identifiers to locators. The namespace is based on DHTs, and I3 employs the concept of triggers to announce services (e.g. web-service). Nonetheless, I3 is prone to security issues, namely, denial-of-service attacks. With this in mind, secure-I3 [Adkins et al., 2003] has been proposed, with the principle of hiding end-node addresses. Host identity indirection infrastructure (Hi3) [Gurtov et al., 2008] combines secure-I3 and HIP and introduces better multihoming support by introducing identifier layers for service and hosts. Dynamic Recursive Unified Internet Design (DRUID) [Touch et al., 2011] is an architecture where the data, control, management and security planes are unified, so that different planes can act coordinated in the presence of events (attacks, failures, etc). Another proposal with enhanced security support but with limited multihoming capabilities is the Split Naming/Forwarding (SNF) architecture [Jonsson et al., 2003] that includes three namespaces: the FQDN acting as identifiers, locators based on IP addresses, and Ephemeral Correspondent Identifier (ECI) used to identify packets, which avoid sending identifiers. SNF, in comparison to DRUID, supports mobility but has no resilience built-in mechanism. Some proposals, like the HIP Mobile Router (HIP-MR) [Ylitalo et al., 2008] extend protocols to enable hybrid multihoming support. For instance, in HIP-MR the mobile router maintains bindings of the mobile nodes, so that on mobility events peers can be updated with the location of mobile nodes. Nonetheless, this type of solution is limited to nodes supporting the extended protocol, in the case of HIP-MR, HIP nodes. General Internet Signaling Transport (GIST) Overlay Networking Extension, or GONE [Fu and Crowcroft, 2006], also combines multiple protocols such as GIST, SCTP and HIP to enable support for multihoming and resilience against failures and DoS attacks. GONE, in comparison to HIP-MR, supports all multihoming goals, but has the disadvantage of introducing signalling overhead. Some proposals focus on supporting multiple technologies. For instance, Spontaneous Virtual Networks (SpotVNet) [Roland Bless and Waldhorst, 2011] supports Bluetooth and others by employing cross-layer mechanisms. However, such characteristic does not enhance multihoming support.

■ Hybrid multihoming proposals can follow a map and encapsulation approach as summarized in Table 2.12. LISP-MN [Farinacci et al., 2012] extends LISP [Dave, 2008] to enhance mobile nodes capabilities, regarding mobility and multihoming support. HIP Mobile Router [Ylitalo et al., 2008] extends HIP to support end-site multihoming. Proposals like Six/One router [Vogt, 2008] are limited as they only apply to IPv6. DRUID [Touch et al., 2011] presents a unified coordination in the presence of events. Despite following Loc/ID split paradigm, DRUID fails to be a complete specification (e.g. mapping system details). Tailored for events, I3 [Stoica et al., 2004]

Table 2.12: Hybrid multihoming proposals with map and encapsulation approach. MH-Multihoming, OS-Operating Systems.

Protocol	MH Goals				Strengths	Flaws	Implementation
	R	U	L	F			OS
LISP-MN	√	√	X	X	Mobility	No Load sharing	LISPMob[a]
HIP MR	√	√	X	X	Security	Only HIP-aware nodes	Linux[b]
DRUID	√	X	X	X	Includes trustiness.	No mobility support	–
I3	√	√	X	X	Multicast/ anycast services.	Security issues	Linux[c]
DOA	√	X	X	X	Security	No mobility	–
Six/One Router	√	√	√	√	Flow distribution support	Only for IPv6	–
SNF	X	√	X	X	Security	Limited resilience support	–
SpotVNet	√	√	X	X	Incremental deployment	Limited multihoming.	–
GONE	√	√	√	√	Multihoming support	Signaling overhead	Linux[d]

[a] [Farinacci et al., 2013] [b] [OpenHIP, 2012] [c] [Adkins, 2006] [d] [Demter and Fu, 2006]

introduces the concept of triggers, which end-hosts must use to indicate their interest in certain data (e.g. web-service). I3 but has been extended by secure-I3 [Adkins et al., 2003] and Hi3 [Gurtov et al., 2008] to improve security. SNF [Jonsson et al., 2003] introduces translation gateways to enable communication between domains, and supports security but, similarly to Delegation Oriented Approach (DOA) [Walfish et al., 2004], it does not support mobility. Some proposals aim to allow incremental deployments, as such, for example, SpotVNet [Roland Bless and Waldhorst, 2011]. Unfortunately, multihoming support for current architectures is not very advanced. For instance, resilience and flow distribution are not supported. Other proposals, like GONE [Fu and Crowcroft, 2006], combine several protocols for an efficient multihoming support , which however may introduce significant signalling overhead. ■

2.8.5 New and Routing-Centric Architectures

New routing architectures try to combine the positive aspects of standards that enable services used worldwide. For instance, the Switched Internet Architecture (SIA) [Shenoy, 2013] combines aspects of the IP architecture and the telephone architecture, where addresses are organized hierarchically including a network ID and a host ID. The network ID is formed based on the geographical information (e.g. country) and organization code. The host ID corresponds to a numeric identifier, similar to a cellular number. But such kind of architecture needs to be evaluated in order to assess its benefits [Paul et al., 2011].

Other proposals for new architectures stand by a hierarchical organization of the network. For instance, Internet 3.0 [Paul et al., 2010b] divides the network into multiple tiers, where the first tier corresponds to the infrastructure, the second to resources or hosts and the final tier to data and users. Internet 3.0 supports mobility, flow distribution mechanisms and resilience mechanisms. Once again, such approach needs to be evaluated in order to determine if all the tenets support security and enable scalability.

2.8.5.1 New Internet Routing Architecture

New Internet Routing Architecture (NIRA) [Yang et al., 2007] is a policy based network architecture that allows user-specified routes, and mitigates the routing problems in different components, such as route discovery, route availability discovery, route representation and packet forwarding, and provider compensation. Route discovery is performed via a dedicated protocol that divides the task of discovery between source and destination, sharing information between them to optimize routes. One drawback of the route discovery mechanism is the initial delay to establish connections. NIRA employs source routing as the route representation and packet forwarding mechanism. The main concern with NIRA is that it introduces too many modifications that do not facilitate deployment [Clevenger, 2010].

2.8.5.2 User-Controlled Routes

User-Controlled Routes [Yang, 2006] is a proposal to enable source routing. Users or end-hosts can select routes according to their preferences. The architecture is modular, and each module has different functionalities. For instance, one can detect the routes that are available, while another implements controls to detect failures. The detection of routes requires their advertisement from operators, which advertise routes according the service level agreements. The name-to-route lookup service Name-to-Route Lookup Service (NRLS) is a service that performs mapping of hosts into route maps, and is assured by the network. Source routing is a mechanism that enables multihoming support in terms of flow distribution, but has issues, such as ingress filtering. Moreover, this proposal does not have mechanisms for mobility management.

2.8.5.3 eXpressive Internet Architecture

eXpressive Internet Architecture (XIA) [Anand et al., 2011] introduces the eXpressive Internet Protocol (XIP) to enable interaction between different elements, such as users, content and services. Elements are identified by the respective identifiers. It is up to XIP communication between components placed on different hosts. XIP replaces IP, and consequently includes all the procedures to allow communication and packet structure. For instance, a XIP packet may contain information of multiple paths to a destination. XIA supports mobility, resilience and flow distribution but no public implementation is available. XIA is not compatible with current Internet architectures, which do not facilitates its deployment.

■ The current Internet architecture has evolved, despite the associated drawbacks (recall the dual-role of the IP address). New architectures require bootstrapping (e.g. start from zero), as they are not compatible with current model of Internet. Table 2.13 summarizes proposals introducing new architectures or modifying existent ones to accommodate new functionalities. In a future vision of services, successor of Web 2.0, Internet 3.0 [Paul et al., 2010b] introduces multiple tiers to support security and policies between the different entities. As such, multihoming support is high in the research agenda but implementations are not available to assess such enhancement regarding multihoming and support for future services. The Switched Internet Architecture [Shenoy, 2013] merges aspects of the IP architecture and telephone systems to improve location and identification in the Internet. Nonetheless, the benefits of such merge are not clear [Paul et al., 2011]. eXpressive Internet Architecture (XIA) [Anand

Table 2.13: Hybrid multihoming proposals with new and routing-centric approach. MH-Multihoming.

Protocol[*]	MH Goals				Strengths	Flaws
	R	U	L	F		
NIRA[1]	√	X	√	√	Supports policies	Initial round trip time to establish connections
Internet 3.0[2]	√	√	√	√	Strong security support	Not implemented
User-Controlled[1]	√	X	√	√	Supports flow distribution	No implementation
Switched Internet[1]	√	√	X	X	Security support	No implementation
XIA[1]	√	√	√	√	Security support	No implementation

[1] Routing Architecture [2] New Architecture [*] No implementations available

et al., 2011] is also a proposal that includes an architecture where the components are the users, content and services. With such concepts, a packet may contain information of multiple paths to a destination, but a public implementation is not available. Proposals, such as New Internet Routing Architecture (NIRA) [Yang et al., 2007], and User-Controlled Routes [Yang, 2006], have the drawback of introducing high delay in address configuration, or have a limited mobility support, but enable the support of flow distribution. ■

2.8.5.4 Hybrid multihoming remarks

The best approach for an efficient hybrid multihoming support is not clear, as each one has its own advantages and disadvantages. Content-centric proposals focus their specification on content/information, which is nowadays the main usage of current architectures (e.g. access, update, share information). Solutions that consider the goal of information transfer might be a good paradigm to follow. The address of a packet is not relevant, what really matters is its content. Questions arise regarding the representation of such content, how to disseminate it and how to assure privacy [Paul et al., 2011].

Locator-identifier split approaches break the dual-role of current IP addresses. This is an advance regarding multihoming support. But this characteristic by its own is not enough to meet multihoming and mobility challenges. The way the locator-identifier split paradigm can be explored includes hierarchical organization of networks, efficient and scalable mapping systems (e.g. map identifier to locator), or new architectures that break the compatibility with the current IP architecture. Current solutions do extend, or include HIP functionalities, to enable identification of nodes. For instance, HIP Mobile Router [Ylitalo et al., 2008] and GONE [Fu and Crowcroft, 2006] incorporate HIP to allow unique and secure identities. Another aspect to consider is the placement and type of mapping systems. If centrally organized, they can represent a point-of-failure or have scalability issues. When distributed, they can scale better, but lookups might not be efficient [Hou et al., 2009].

Proposals, where implementation must be done from scratch, must have their benefits validated, as the price to pay for deployment is high. New architectures fall into this type of proposals. The native security support is an attractive point, others can also be pointed as the bleeding edge, such as the ability to coordinate path selection between users and service operators.

2.9 Summary

Multihoming may require support from all layers in the Internet protocol stack, including applications. Of course, the decision to place the bulk of multihoming support at any particular layer comes with its own advantages and drawbacks. Typically, one resorts to the utilization of different paths according to preference sets, for instance, based on bandwidth and delay estimates. An application which supports multihoming may be better suited to control its flows with much finer granularity than what is possible, say, for example, with HIP and a set of static policies. On the other hand, in the absence of scalable source routing mechanisms, applications cannot be assured that their preferences will always be attended to with the current crop of transport protocols. Furthermore, presently there is no standard mechanism for sharing network path information with the applications. As such, advanced applications usually employ active and passive measurement mechanisms and/or participate in overlay networks in order to obtain a better view of network performance across different paths.

Throughout the analysis of the state of the art, the evaluation of multihoming support can be subjective or incomplete. In this chapter, diverse protocols, architectures, proposals regarding their multihoming goals fulfillment have been compared. Such approach, is more accurate than comparisons based solely on a single criterion, such as cost.

The performed comparison, also demonstrates that there is a need for a framework that allows to evaluate multihoming support of a protocol in a objective way. For instance, to establish objectively the difference regarding resilience or ubiquity support between protocols. Moreover, techniques to optimize multihoming support are also required.

This chapter has culminated in the following journal publications:

1. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Multihoming Management for Future Networks**", Mobile Networks and Applications, 2011, Springer [Sousa et al., 2011a].

2. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Multihoming: A Comprehensive Review**", Advances in Computers, volume 90, 2013, Elsevier [Sousa et al., 2013].

—The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

Mark Weiser

3 Multihoming Evaluation Framework

THIS chapter presents a framework to assess the multihoming support - Multihoming Evaluation Framework (MEF). MEF comprises the Resilience Evaluation Framework (REF), which determines resilience support and the Ubiquity Evaluation Framework (UEF) that evaluates how ubiquitous a protocol is. Such frameworks, proposed in this thesis, can be used in the design phase of a network architecture to allow the selection of protocols with improved multihoming support.

This chapter is composed by several sections. Section 3.1 introduces terms and overviews the state of the art regarding resilience and ubiquity support evaluation. Section 3.2 specifies REF to assess the resilience support of a protocol and Section 3.3 introduces UEF specification to evaluate the ubiquity support of a protocol. Finally, Section 3.4 concludes the chapter with an overview of the achievements herein described, underlying the outcomes performed by the candidate.

3.1 Introduction

This section introduces concepts and related work towards multihoming evaluation. Goals and requirements of evaluation frameworks are described. Definition of terms used along the chapter are introduced. An overview of the related work and open issues is also presented.

3.1.1 Objectives and Requirements

The objectives within this chapter include:

1. Establish a framework to assess resilience support of a protocol.
2. Establish a framework to assess ubiquity support of a protocol.

Each of these frameworks needs to meet a set of requirements, which are described as follows:

Generic Support any protocol, without being tied to the specificities of a given protocol (e.g., Multi Protocol Label Switching (MPLS) [Rosen et al., 2001]).

Objective Allow the objective comparison between protocols. For instance, to determine which protocols supports resilience or ubiquity more efficiently.

Thorough Evaluation metrics must be objective and fully representative to determine the support of resilience or ubiquity.

Autonomous Evaluation must be autonomous, in such a way that there is no need for an expert or a specific tool.

Flexible Do not need any working system or particular scenario. For instance, evaluation can be performed at any phase of the system design. Initially, it can be employed to allow the selection of a protocol based on its specificities.

3.1.2 Definitions

This subsection introduces definitions of terms that are employed through the chapter, namely Resilience and Ubiquity, as per Definition 3.1, Definition 3.2 and Definition 3.3.

Definition 3.1 (*Resilience*)

> *Resilience is a mechanism to assure service robustness, by ensuring that resources are re-established in case of failures. This re-establishment is possible due to protection (actions before failure) and/or restoration schemes (actions after failure) that aim to maximize availability.*

This definition is proposed in this thesis and is based on [Pioro and Medhi, 2004].

Definition 3.2 (*Ubiquity*)

> *Ubiquity is the ability to support secure and optimized mobility to enable access to services anywhere and anytime, with acceptable quality levels.*

The term *path* is defined in this thesis, according to Definition 3.3 to avoid misunderstanding with related terms such as interfaces, or routes.

Definition 3.3 (*Path*)

> *Path is a logical communication facility identified by source and destination end-hosts, which is linked to a physical interface.*

3.1.3 State of the Art

This subsection presents the state of the art on resilience evaluation and ubiquity support assessment in Ubiquitous Computing (UbiComp) Systems.

Resilience has been evaluated in different ways and for various protocols. Both the Resilience-Differentiated Quality of Service (RD-QoS) framework [Autenrieth, 2003a] and Quality of Resilience (QoR) [Cholda et al., 2008, 2009] assess the resilience support of MPLS. However RD-QoS does not assess the recovery cost and only includes a time analysis based on the ITU-T M.495 model [ITU-T, 1993]. QoR combines Quality of Service (QoS) metrics (e.g., packet loss, delay) with resilience metrics (e.g., steady-state availability, mean downtime). Moreover, QoR employs histograms that can be mapped to user satisfaction. Nonetheless, the evaluation methodology is tied to MPLS, lacking a broader applicability to other kind of protocols.

Other kind of evaluation includes recovery efficiency and the protection model supported (e.g., 1+1 or 1:N) [Pioro and Medhi, 2004]. Nevertheless, the evaluation relies on non deterministic methods, which depends on the application requirements. Evaluation methodologies fail to provide a complete evaluation of resilience support, as the example of proposals that only assess availability [Autenrieth, 2003a; Akella et al., 2003; Huang et al., 2007].

Other evaluation frameworks consider qualitative (e.g., risk) and quantitative characteristics of resilience and related-terms (i.e. dependability, fault-tolerance) in systems [Al-Kuwaiti et al., 2009]. Nonetheless, they consider physical aspects of architectures, which limits their applicability to protocols in other layers of the OSI model.

With a different perspective, other proposals only address the optimal configurations of failover mechanisms for protocols supporting resilience, such as Stream Control Transport Protocol (SCTP) [Eklund et al., 2009; Budzisz et al., 2008], operating at the transport layer.

Table 3.1: Resilience evaluation summary.

Proposal	Generic	Objective	Thorough
RD-QoS[a]	X only MPLS	X	X only time analysis
QoR[b]	X only MPLS	X	√
Pioro[c]	X depends on application	X	√
Akella[e]	X only physical aspects	X	√
Huang[f]	X	X	X only availability
Al-Kuwaiti[g]	X	X	X only protection
Eklund[h]	X only SCTP	X	X
Budzsisz[i]	X only SCTP	X	X

[a] [Autenrieth, 2003a] [b] [Cholda et al., 2009] [c] [Pioro and Medhi, 2004] [d] [Akella et al., 2003] [e] [Huang et al., 2007] [f] [Al-Kuwaiti et al., 2009] [g] [Eklund et al., 2009] [h] [Budzisz et al., 2008]

Table 3.1 summarizes the proposals analysed by the candidated, regarding requirements fullfillment, namely Generic, Objective, and Thorough, previously, introduced in subsection 3.1.1. Other requirements, such as Flexible were not meet by the related proposals.

Ubiquitous computing (UbiComp) is a model where computers live in the world of people, aware of their location, but in a transparent form to the user [Symonds, 2009]. Modern devices and networks to some degree implement this vision for ubiquitous computing as they enable users to access online services 24-hours a day at "any time" and from "any place". In principle, the choice of technologies, system architecture and protocols must be considered in the design phase of UbiComp systems. However, the evaluation approaches taken for UbiComp Systems so far [Resatsch, 2010; Stevenson et al., 2009] typically consider user-perspective ratings only, or assess a limited set of functionalities. For example, some assessments follow a prototype-based approach and thus have high development costs while not always being fully representative of the final system [Resatsch, 2010]. Others rely on user surveys requiring at least a partially complete and functional system [Stevenson et al., 2009]. Moreover, when multiple choices for the software components are available, said approaches do not provide insights for the selection of the best ones during the design phase.

UbiComp systems can be evaluated in terms of quality, which assesses the level of capabilities (i.e. technical characteristics) and the level of extensions [Kwon and Kim, 2006; Scholtz and Consolvo, 2004]. The assignment for each capability/item usually relies on interviews with experts in the field (e.g., with ubiquitous computing experience), giving a classification in the range $\{1, 2, ..., 7\}$. These solutions require the involvement of experts.

Ubiquitous Computing Application Development and Evaluation Process Model (UCAN) is a ubiquitous computing application development and evaluation process model [Resatsch, 2010], which evaluation includes different stages and methods, for instance, the original idea can be evaluated using interviews, while the prototype is assessed through user acceptance methods. Whilst UCAN requires prototypes and is tailored for applications relying on user satisfaction metrics, other proposals allow the evaluation of the overall system [Kwon and Kim, 2006].

Ontonym [Stevenson et al., 2009] is a framework that allows the evaluation of pervasive systems. The framework models context based on ontologies. For instance, people are modeled by using classes with different attributes such as *Name* and *ReligiousName*. The evaluation considers three aspects: design principles, (e.g., extensibility and documentation); content (e.g., clarity and consistency); and purpose (in which domain the evaluation is performed). Despite using established standards, Ontonym focuses on the context representation problem, and therefore does not provide objective and comparable metrics to evaluate UbiComp systems.

In a UbiComp system, the mobility management is a key factor to enable the always connected paradigm. As such, considering the software component of UbiComp systems, there is a need to establish the degree of mobility supported by IP mobility management protocols. For instance, how a certain protocol manages mobility. This evaluation may consider different performance metrics. Usually, metrics include packet delivery cost, handover delay, location update cost, signalling cost, multiple interfaces and simultaneous mobility support. The packet delivery cost metric, for instance, determines the cost (e.g., processing or transmission) of the different packet delivery mechanisms (e.g., tunnel, direct) [Wang and Abu-Rgheff, 2006]. The handover delay metric includes movement detection, address configuration, security operations and location registration [Kong et al., 2008; Liu et al., 2007]. The signalling cost is a compound metric that combines the packet delivery cost and the handover cost, commonly designated by location update cost [Wang and Abu-Rgheff, 2006]. The location update cost is determined according to the network model (e.g., number of hops, number of domains, wired and wireless links), message rate and respective message length. The difference between these proposals resides on the fact that some of them include the functions of each involved entity (e.g., home agent, correspondent node), while others only include the mobile node or the cost of specific operations (e.g., tunnelling) [Makaya and Pierre, 2008]. The support of simultaneous mobility metrics is often neglected in evaluations, assuming fixed correspondent nodes [Wang and Abu-Rgheff, 2006; Makaya and Pierre, 2008], although some consider the probability of simultaneous movement [Wong et al., 2007]. Paging efficiency is another metric to consider when evaluating mobility management protocols in a ubiquitous environment, specially due to energy efficiency. Paging support evaluations assess the power consumption cost, the paging delay cost, but in a technology-dependent or application-dependent way [Lee et al., 2008; Do and Onozato, 2007; Tang et al., 2007].

Table 3.2: Ubiquity evaluation summary.

Proposal	Generic	Objective	Thorough
UCAN[a]	√	√	X only user perspective
Ontonym[b]	√	√	X only user perspective
Kwon[c]	√	√	X only characteristics and extensions
Scholtz[d]	√	√	X only characteristics and extensions
Wang[e]	X only Mobile IP	X	X only mobility's degree
Kong[f]	X only Mobile IP	X	X only mobility's degree
Liu[g]	X only Mobile IP	X	X only mobility's degree
Makaya[h]	X only Mobile IP	X	X only mobility's degree
Lee[i]	√	√	X only paging
Lo Onozato[j]	√	√	X only paging
Tang[k]	√	√	X only paging

[a] [Resatsch, 2010] [b] [Stevenson et al., 2009] [c] [Kwon and Kim, 2006] [d] [Scholtz and Consolvo, 2004] [e] [Wang and Abu-Rgheff, 2006] [f] [Kong et al., 2008] [g] [Liu et al., 2007] [h] [Makaya and Pierre, 2008] [i] [Lee et al., 2008] [j] [Do and Onozato, 2007] [k] [Tang et al., 2007]

Table 3.2 summarizes the proposals evaluating UbiComp performance or a specific function in UbiComp systems, regarding the requirements fulfillment. Only the first three requirements (Generic, Objective, Thorough) were considered.

3.1.4 Open Issues

From the analysis of the state of the art on resilience evaluation, summarized in Table 3.1, the following open issues were identified:

- Existent evaluation frameworks fail to provide a solution that allows the evaluation of resilience in a standardized form for any protocol.
- Evaluation frameworks do not include a complete set of metrics or methods that allow to fully evaluate resilience support on a protocol.
- Existent evaluation frameworks do not establish methods to make an objetive comparison regarding resilience support.

From the analysis of the state of the art on UbiComp evaluation, summarized in Table 3.2, the following open issues were identified:

- Ubiquity evaluation needs to be characterized regarding technical aspects, extensions and the degree of mobility supported. These items were not supported simultaneously by any of the frameworks.
- Ubiquity evaluation must be autonomous without requiring interviews or intervention from experts.

To cope with the identified issues, Resilience Evaluation Framework (REF) was proposed as the baseline to evaluate resilience support in a protocol and Ubiquity Evaluation Framework (UEF) was specified to evaluate ubiquity support.

3.2 Resilience Evaluation Framework

This section starts by presenting the objectives of the Resilience Evaluation Framework (REF) and the formulation for availability and recovery components. The evaluation of resilience support in SCTP and respective results conclude this section.

3.2.1 Objectives & General aspects

The main objective of REF is to evaluate resilience support of a protocol. REF is a framework to assess resilience support in a protocol. REF is not tied to a specific protocol or technology and promotes objective comparison between protocols.

Resilience is considered according to Definition 3.1, where R_{MH}- Resilience is a function of Av- Availability and Rc- Recovery, as per Equation 3.1.

$$R_{MH} = Av \times Rc \tag{3.1}$$

Recovery has associated distinct protection models, which provide different levels of protection [Cholda et al., 2009]:

- **M:N** model is a model, on which *N* backup paths protect *M* primary paths.
- **1:N** model, where N backup paths protect one primary path.
- **1:1** or primary-backup model. A backup path is employed only when the primary fails. This is the default protection model of SCTP and represents a subcase of the **M:N** model [Fekete, 2010].
- **1+1** or concurrent model. Paths are used simultaneously to increase resilience. An example is the Concurrent Multipath Transfer (CMT) [Iyengar et al., 2006] extension of SCTP.
- **1+N** model, which represents the case when there are at least three paths that can be used all simultaneously.

Different considerations are assumed in the formulation of REF, as summarized in Table 3.3.

Table 3.3: REF Considerations

Type	**Description**	**Units**	**Values**
$\delta(t)$	time variables	*milliseconds* (ms)	
$S(x)$	size variables	*bytes*	
$C(x)$	capacity variables	*byte/s*	constant
$P(x)$	Percentage		$[0, 1]$
$f(n)$	Failures		*min* $\{0\}$ *max* $\{n\}$
z	Paths in node		*min* $\{2\}$ *max* $\{z\}$
bk	Backups paths in node		*min* $\{1\}$ *max* $\{bk\}$

The most common protection models are the primary-backup model and the concurrent model [Cholda et al., 2009; Pioro and Medhi, 2004].

3.2.2 Availability

This subsection defines how availability is determined in REF.

Figure 3.1 depicts an availability model on which the service has two states, available ($state = 1$) or unavailable ($state = 0$), according to ITU-T E.800 [ITU-T, 2008]. After a failure instant, $tFail_n$, the procedures for failure processing are undertaken

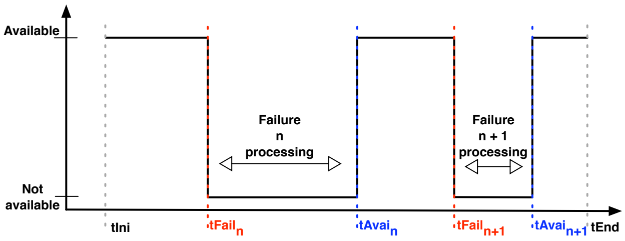


Figure 3.1: ITU-T E.800 availability model [ITU-T, 2008].

[Pioro and Medhi, 2004]. Whilst failure processing mechanisms can be handled at different layers, REF only considers the processes taken at the layer of the evaluated protocol. For instance, if the envisioned protocol acts at the transport layer, failure processing mechanisms operating at the physical layer are ignored[1].

Availability - Av - in REF is the ratio of Mean Up Time (MUT) over the total time, which is MUT+ Mean Down Time (MDT) [Cholda et al., 2009; Pioro and Medhi, 2004], as per Equation 3.2.

$$Av = \frac{MUT}{MUT + MDT} \tag{3.2}$$

Considering the E.800 model, depicted in Figure. 3.1, MUT corresponds to the moments where *available* $= 1$ and can be formulated for generic cases with n failures according to Equation 3.3. On a non failure situation, $MUT = tEnd - tIni$, since $tFail_n = 0$ and $tAvai_n = 1$.

$$MUT = (tFail_1 - tIni) + \sum_{i=2}^{n}(tFail_i - tAvai_{i-1}) + (tEnd - tAvai_n) \tag{3.3}$$

Mean Down Time considers the moments where *available* $= 0$, that is when the service is down, therefore for n failures, it is determined according to Equation 3.4.

$$MDT = \sum_{i=1}^{n}(tAvai_i - tFail_i) \tag{3.4}$$

A key aspect in REF is the evaluation of availability in the context of end-host multihoming, which can have multiple interfaces. Previous availability approaches only take into account the availability of the overall service [Cholda et al., 2009] or of interfaces/paths in isolation [Akella et al., 2003; Huang et al., 2007], without taking into consideration the role of each path. The role of a path dictates whether it acts as a pri-

[1] The Open Systems Interconnection (OSI) model was applied in this comparison.

mary path or as a backup path. This role is associated with the protection model, with the *1:1* and *1+1* models being the most generic from a multihoming perspective [Pioro and Medhi, 2004]. Having this in mind, the following subsections formulate availability for the primary-backup and concurrent models.

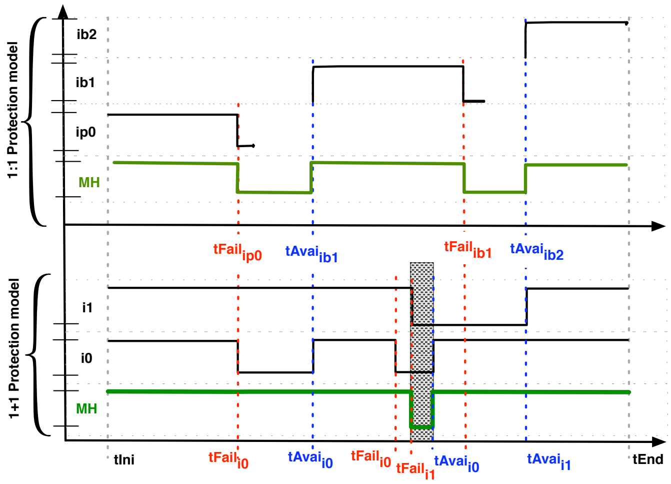


Figure 3.2: Availability with **1:1** and **1+1** protection models.

3.2.2.1 Availability in the primary-backup protection model

Availability in the primary-backup model also follows the E.800 availability model, pictured in Figure 3.2 for 1:1 and 1+1 protection models. In this case, MUT is determined according to Equation 3.5, where bk corresponds to the backup path and failures occur at the primary path.

$$MUT_{1:1} = (tFail_0 - tIni) + \sum_{t=1}^{bk-1} (tFail_t - tAvai_t) + (tEnd - tAvai_{bk}) \tag{3.5}$$

$MUT_{1:1}$ considers the availability of all paths in a sequential mode, starting with the primary and following the respective backup paths.

3.2.2.2 Availability in the concurrent protection model

In the 1+1 or concurrent protection model, *i0* - the primary path is used simultaneously with *i1* - the backup path, as illustrated in Figure 3.2. The Mean Up Time corresponds to the union of the MUTs for each path, which are determined according to

Equation 3.3. An *OR* boolean logic can be employed to determine MUT, by including all the moments on which, at least, one path is available. The probability of downtime is lower, as if one path fails, another assures the service delivery. Thus, the downtime corresponds to the intersection of Mean Down Time on both interfaces, which is calculated based on the difference between the minimum m available time and the maximum M failure time, as given in Equation 3.6.

$$MDT_{1+1} = MDTit_{1+1}\text{with, } it_{1+1} = m\{tAvai_0, tAvai_1\} - M\{tFail_0, tFail_1\} \quad (3.6)$$

3.2.3 Recovery

This subsection specifies recovery in REF for generic models and also for the primary-backup and concurrent protection models. Recovery performance in REF is determined according to the ITU-T M.495 [ITU-T, 1993] model that defines the terminology and principles related with restoration and diversity. This model has been enhanced to include the determination of Fault-detection (FD), Fault Notification (FN) and recovery switching (RS) events [Autenrieth, 2003b]. Recovery encompasses the actions necessary to return to a normal state after the identification of a failure. For such different processes may occur within a recovery scheme, which can go from fault detection to a final step that corresponds to the restoration of the initial service levels. As per ITU-T M.495 model, recovery performance can rely on the recovery time-tRc, which is determined according to Equation 3.7.

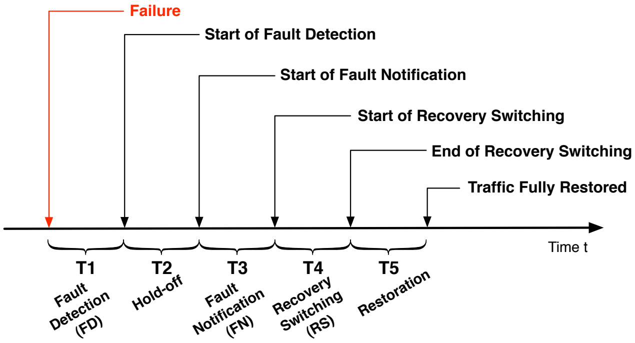


Figure 3.3: ITU-T M.495 Enhanced recovery model [Autenrieth, 2003b].

$$tRc = \sum_{i=1}^{5} T_i \quad (3.7)$$

In a simplistic approach, the recovery time can be determined based on the end time of recovery ($teRS$) and the start time of Failure Detection ($tsFD$), as depicted in Equation 3.8.

$$tRc = teRS - tsFD \tag{3.8}$$

Considering all the processes of a recovery scheme, defined in the ITU-T M.495 model, the recovery time is formulated as per Equation 3.9.

$$tRc = tFD + tFN + tRS \tag{3.9}$$

Recovery performance cannot simply rely on the recovery time metric. For instance, two protocols can recover at the same time, but the restoration to the initial conditions (i.e. before failure) can be different. As such different metrics/factors must be evaluated, as follows:

- **ERc** - recovery time efficiency.
- **LRc** - the recovery impact, which corresponds to the affected traffic.
- **ORc** - the recovery overhead, i.e. the cost of recovery in terms of signalling.
- **QRc** - the quality provided by recovery, which measures whether operation returns to the same conditions as before failures.

Recovery, Rc, is determined according to Equation 3.10, where the interest is, on one hand, to minimize the affected traffic and the overhead of recovery procedures, and on the other, to maximize the quality provided by recovery and the recovery efficiency. The following paragraphs detail how the different metrics are determined.

$$Rc = \beta_R(LRc \times ORc) + (1 - \beta_R)(ERc \times QRc) \tag{3.10}$$

The recovery efficiency ERc corresponds to the ratio between the time to recover from all failures $\{i \cdots n\}$ and the mean downtime, as given in Equation 3.11. With this metric it is possible to differentiate protocols that have optimized mechanisms providing fast recovery.

$$ERc = \left(1 + \frac{\sum_{i=1}^{n} tRc_i}{MDT}\right)^{-1} \tag{3.11}$$

The recovery impact, LRc, is determined based on the affected traffic (considered lost or prone to restransmission) during the recovery process, as depicted in Equation 3.12. REF considers the relation of capacity between the current path, C_c and the primary path C_p, as opposed to other works that consider only the capacity of the primary path [Cholda et al., 2009]. By considering the C_c/C_p ratio it is possible to determine the affected traffic based on the recovery time and capacities of paths.

$$LRc = \frac{C_c \sum_{i=1}^{n}(teRS_{c,i} - tsFD_{c,i})}{C_p(tEnd - tStart)} \tag{3.12}$$

The recovery overhead, ORc, represents the signalling cost of the recovery operations, as per Equation 3.13. This compound metric establishes the difference between the recovery models, as protection models have backup links pre-established, while restoration models need to establish them based on signalling. ORc expresses a cost function, where the interest is, on one hand, to minimize signalling ratio (e.g. signalling distributed along the service lifetime) and on the other hand, to maximize signalling ratio diversity (e.g. improve load sharing).

$$ORc = \beta_O sigRt + (1 - \beta_O)sigDv \tag{3.13}$$

In REF, the determination of signalling considers the approaches that are based on message signalling and approaches that employ timers to trigger recovery actions. REF considers average values for MSi - message size and TDu - timeout durations, as these can vary in the measurement intervals. The recovery overhead is determined with the overall signalling - $allSig$, the signalling ratio - $sigRt$ and the signalling ratio diversity - $sigDv$ metrics. The overall signalling includes all the signalling in the interval ($tEnd - tStart$) and is calculated according to Equation 3.14.

$$allSig = nM \cdot \overline{MSi} + nT \cdot \overline{TDu} \tag{3.14}$$

The overall signalling includes the MSi with nM- total number of messages transmitted, and nT- number of timeouts, with different durations TDu. The signalling performed during recovery ($sigRc_i$) from failure i is calculated by the signalling overhead during tRc_i - the time of recovery, employing the same logic for the overall signalling, but only for the instant tRc_i. The signalling ratio, $sigRt_{(t)}$, for path t, establishes the relation between the signalling during recovery from possible n failures and the overall signalling, as depicted in Equation 3.15. Higher values indicate that the signalling overhead is concentrated in the recovery processes.

$$sigRt_{(t)} = \frac{\sum_{i=1}^{n} sigRc_{t,i}}{allSig_t} \tag{3.15}$$

The signalling ratio diversity, $sigDv$, assesses how signalling is balanced among all paths and can be calculated based on the relation of the minimum ratio and the maximum ratio for all paths, as demonstrated in Equation 3.16.

$$sigDv = min\{sigRt_{(t)}\}/max\{sigRt_{(t)}\} \tag{3.16}$$

If $sigDv \to 1$ the signalling load is distributed more evenly between the paths. The recovery overhead metric in REF is clearly distinct from previous proposals [Calle et al., 2004; Cholda et al., 2009], which do not consider the signalling overhead, or consider it in a simplistic manner without any diversity analysis.

QRc is determined by restorability and backup link quality [Calle et al., 2004; Cholda et al., 2009]. Restorability indicates the percentage of failed paths that can be recovered [Griffith et al., 2003]. As with availability, the operation of the recovery scheme depends on the adopted protection and/or restoration model. While protection models have one of more backup paths pre-established before failures, restoration models establish the backup path on failure events. The former can attain better performance in terms of recovery time (no need of signalling to establish a path), but with the drawback of having a higher cost in terms of resources, since a path is dedicated for recovery [Cholda et al., 2009; Autenrieth, 2003a]. The quality provided by recovery, QRc, is a relation between Xb - the quality of backup paths and $R(n)$ - the restorability. The Xb factor is determined based on C_c and C_p the capacity of current and primary path, respectively, as given in Equation 3.17 [Cholda et al., 2009].

$$Xb_c = \begin{cases} 1 & \text{if } C_c/C_p \geq 1 \text{ or } C_p = 0, \\ C_c/C_p & \text{otherwise.} \end{cases} \tag{3.17}$$

The restorability - $R(n)$ accounts the ratio of failed connections n, successfully recovered $r(n)$, as depicted in Equation 3.18. Restorability in REF allows to assess to what extent the recovery is performed. QRc is based on the average quality of backup paths, as each path has its own quality factor and on the restorability ratio, $QRc = \overline{Xb} \times R(n)$.

$$R(n) = \frac{r(n)}{n} \tag{3.18}$$

3.2.3.1 Recovery in the primary-backup protection model

Recovery efficiency, $ERc_{1:1}$, considers the time of recovery of all paths (primary and backups) and their respective Mean Down Time, as demonstrated in Equation 3.19.

$$ERc_{1:1} = \left(1 + \frac{tRc_0 + \sum_{t=1}^{bk}(tRc_t)}{MDT_0 + \sum_{t=1}^{bk} MDT_t}\right)^{-1} \tag{3.19}$$

Recovery impact, $LRc_{1:1}$, assesses the affected traffic during recovery of the primary path and the restoration of the respective backup paths, considering the theoretical traffic that could be transmitted, if no failures had occurred, during the time service, as illustrated in Equation 3.20.

$$LRc_{1:1} = \frac{C_0 \cdot tRc_0 + \sum_{t=1}^{bk}(C_t \cdot tRc_t)}{C_0(tEnd - tStart)} \tag{3.20}$$

Finally, recovery overhead, $ORc_{1:1}$, is determined according to Equation 3.13. Nevertheless, the signalling during recovery is determined for the instant of recovery and includes the messages or timers that are associated with the primary path and backup paths, as given in Equation 3.21.

$$sigRc_{1:1} = nM_0 \cdot \overline{MSi_0} + nT_0 \cdot \overline{TDu_0} + \sum_{t=1}^{bk}\left(nM_t \cdot \overline{MSi_t} + nT_t \cdot \overline{TDu_t}\right) \tag{3.21}$$

3.2.3.2 Recovery in the concurrent protection model

In the *1+1* protection model, the recovery processes only occur when both interfaces are down simultaneously, as shown in Figure 3.2. The time for a path to recover from failure i ($tRc_{i_{1+1}}$) depends on the minimum time of recovery and on the maximum time of failure detection from one of the paths {*i0*,*i1*}, following the logic depicted in Equation 3.6.

The recovery efficiency, ERc_{1+1}, is determined based on the recovery time from n possible failures and on the respective simultaneous downtime as per Equation 3.22.

$$ERc_{1+1} = \left(1 + \frac{\sum_{i=1}^{n} tRc_{i_{1+1}}}{\sum_{i=1}^{n} MDTit_i}\right)^{-1} \tag{3.22}$$

The affected traffic, LRc_{1+1}, must consider the affected traffic in two distinct cases:

1. *Simultaneous*, $_{sim}LRc_{1+1}$ - on which there is no service since both paths are

down simultaneously.

2. *Partial* - on which failures only affect one path.

The affected traffic, LRc_{1+1}, corresponds to the relation between the affected traffic in the simultaneous case and the sum of the affected traffic in the partial cases, see Equation 3.23. Within z paths, the simultaneous cases assume that traffic is forwarded simultaneously on different paths, thus the capacity is considered the sum of all affected paths. In the partial cases, the traffic impact is considered in isolation for each failed path.

$$LRc_{1+1} = \frac{simRc_{1+1}}{\sum_{j=1}^{z} parLRc_j} = \frac{\frac{(C_0+C_1)\sum_{i=1}^{n}\left(tRc_{i_{1+1}}\right)}{(C_0+C_1)(tEnd-tStart)}}{\sum_{j=1}^{z}\frac{(C_c)\sum_{j=1}^{n_c}(tRS_j-tFD_j)}{C_c\ (tEnd-tStart)}} \tag{3.23}$$

Although, partial failures can affect the traffic, the service is only disrupted on simultaneous failures, therefore the signalling performed during recovery - $sigRc_{1+1}$, in the recovery overhead determination, only considers the recovery performed for n_s simultaneous failures, as depicted in Equation 3.24. The overall signalling includes all the signalling performed during the time service in all paths.

$$sigRc_{1+1} = \sum_{j=1}^{n_s}\left(nM_{i0(j)}\cdot\overline{MSi_{i0(j)}}+nT_{i0(i)}\cdot\overline{TDu_{i0(j)}}+nM_{i1(j)}\cdot\overline{MSi_{i1(j)}}nT_{i1(j)}\cdot\overline{TDu_{i1(j)}}\right) \tag{3.24}$$

In the *1+1* cases, the primary and backup path are used simultaneously, therefore there is no real notion for backup path. In this context, the backup link quality corresponds to the minimum quality level that is achieved on a failure event, as per Equation 3.25.

$$Xb_{1+1} = \begin{cases} 1 & \text{if } \frac{C_{afterFailure}}{C_{befFailure}} \geq 1 \text{ or } C_{befFailure} = 0, \\ \frac{C_{afterFailure}}{C_{befFailure}} & \text{otherwise.} \end{cases} \tag{3.25}$$

The restorability metric $R(n)_{1+1}$ considers the number of successful recoveries are performed for each path considering the number of failures in the respective path, as given in Equation 3.26.

$$R(n)_{1+1} = \frac{r(n)_{i0} + r(n)_{i1}}{n_{i0} + n_{i1}} \tag{3.26}$$

The quality provided by recovery, QRc_{1+1}, in the *1+1* protection model is calculated based on the possible n failures and on the path where failures occur.

$$QRc_{1+1} = \begin{cases} 1 \cdot R(n)_{1+1} & \text{if n = 0,} \\ Xb_{i0} \cdot R(n)_{1+1} & \text{if } C_0 > C_1 \text{ and } n_{i0} \geq 1, \\ Xb_{i1} \cdot R(n)_{1+1} & \text{if } C_1 \geq C_0 \text{ and } n_{i1} \geq 1. \end{cases} \tag{3.27}$$

REF can be employed to assess the resilience of any given protocol as long as the protection model (i.e. primary-backup or concurrent) is taken into consideration. For instance, the Stream Control Transport Protocol (SCTP) is under the 1:1, while the Multi Protocol Label Switching (MPLS) can be under the 1+1, if considering load balancing characteristics.

3.2.4 Evaluation

This subsection provides details regarding the resilience support evaluation of SCTP using REF.

3.2.4.1 Objectives

The goals of this evaluation are:

- Compare the resilience support of SCTP with standard (Std) and optimized (Opt) fault-tolerance configurations.
- Assess the impact that SCTP failover mechanisms have on VoIP and data applications.
- Assess the accuracy of REF through a comparison with QoR.

3.2.4.2 Scenario

This subsection provides details regarding the simulation scenario to evaluate resilience performance of SCTP in multihomed nodes.

Figure 3.4 illustrates the simulation scenario, which includes multihomed nodes with a primary path and two backup paths. The scenario includes nodes that introduce "background" traffic that causes congestion (based on bursts) in the respective paths. This scenario allows to evaluate SCTP resilience in the presence of failures occurring in the primary and backup paths and considers different types of data traffic. Different networks are configured on the source and destination sides. Moreover, the

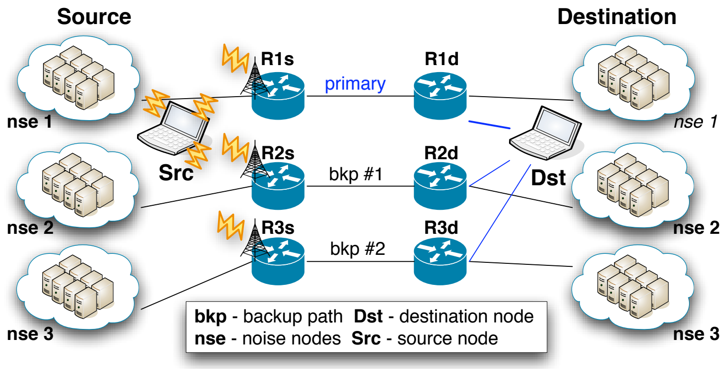

Source
Destination
nse 1
nse 2
nse 3
Src
R1s
R2s
R3s
R1d
R2d
R3d
primary
bkp #1
bkp #2
Dst
nse 1
nse 2
nse 3
bkp - backup path **Dst** - destination node
nse - noise nodes **Src** - source node

Figure 3.4: Evaluation Scenario implemented on OMNeT++ [OMNeT++, 2009] simulator.

source node moves linearly and starts connected to all wireless access routers (in order to include all the configured addresses during the association phase of SCTP). The scenario is modeled in OMNeT++ simulator [OMNeT++, 2009] using the SCTP extension [Rungeler et al., 2008], that is included in the most recent versions of INET[1].

The source node performs two handovers, from primary to bkp #01 and from bkp #01 to bkp #02 paths, respectively. In addition, $\beta_O = \beta_R = 0.05$, an empirical value based on experiences with the simulation scenario.

3.2.4.3 Methodology

The evaluation considers both SCTP failover parameters and the application in use (both include the sets for data and VoIP applications). The SCTP failover parameters are configured according to RFC 4960 [Stewart, 2007] while the optimized configurations are derived from SCTP optimization studies [Eklund et al., 2009; Budzisz et al., 2008].

SCTP failover parameters are configured as detailed in Table 3.4. Other configurable parameters of SCTP, such as Association Max Retrans (AMR) and RTOinit follow the values recommended in RFC 4960, 10 and 3s, respectively.

Evaluation includes both VoIP and data applications, due to the diversity in their requirements. VoIP traffic is based on the G.723.1 [ITU-T, 1996] codec employing a bit rate of 6.3kbps. In addition, SCTP is configured to deliver all DATA chunks received immediately to the upper layer (i.e. unordered). FTP is chosen to represent

[1] INET is a framework with protocols for communication networks (wired, wireless) for OMNeT++ simulator. INET includes, among others, UDP, TCP, SCTP and IPv6 protocols.

data applications. Each test comprises 20 runs and a simulation time of 300s.

3.2.4.4 Results and discussion

This subsection presents the achieved results with the evaluation performed in the simulation scenario. Comparison regarding availability of REF and QoR is discussed in first place. The recovery performance of SCTP is also analysed and resilience support is presented afterwards.

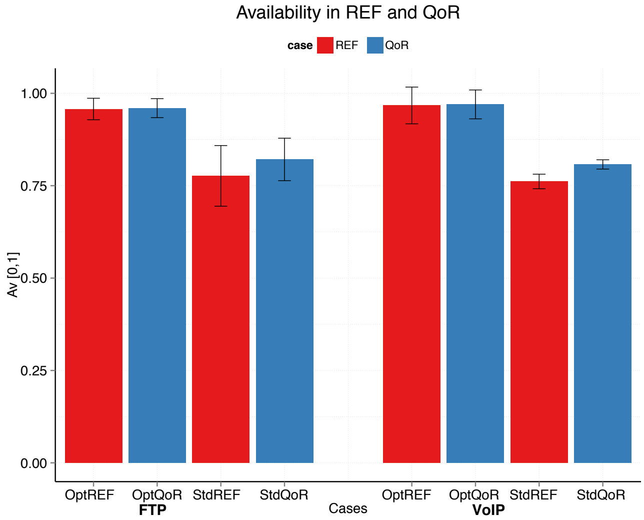


Figure 3.5: SCTP availability measured by REF (Av) and QoR (Q_A).

The Av- Availability parameter of REF can be compared with QA- Quality of Availability of QoR. REF is similar to QoR, as it determines a higher degree of availability of SCTP for optimized cases (with decreased SACK interval), as shown in Figure 3.5. Moreover, REF and QoR point out the fact that the availability in SCTP relies solely on its failover parameters and not on the sets of applications.

Table 3.4: Configuration of SCTP failover parameters

Parameter	**RFC4960 (*Std*)**	**Optimized (*Opt*)**
PMR	5	3
RTOmin	1000 (ms)	20 (ms)
RTOmax	60000 (ms)	60000 (ms)
SACK delay	200 (ms)	20 (ms)

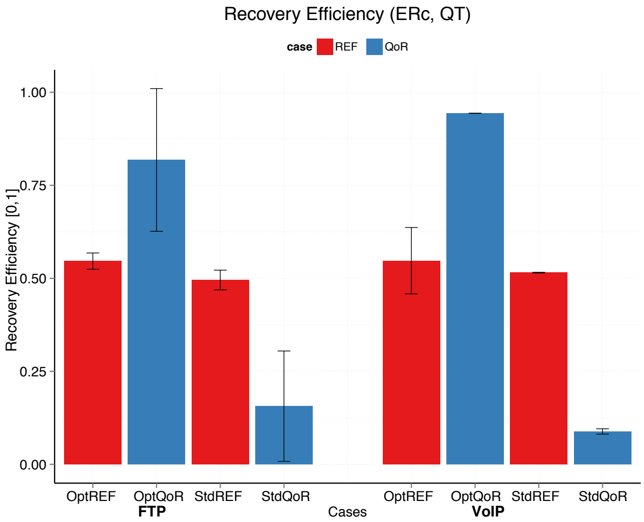


Figure 3.6: SCTP recovery efficiency as measured by REF and QoR.

Recovery is depicted in Figure 3.6. Both REF and QoR point out SCTP to recover more efficiently with optimized configurations. Nonetheless, the difference between standard and optimized configurations is higher in QoR. An explanation for such behaviour is presented when analysing resilience results.

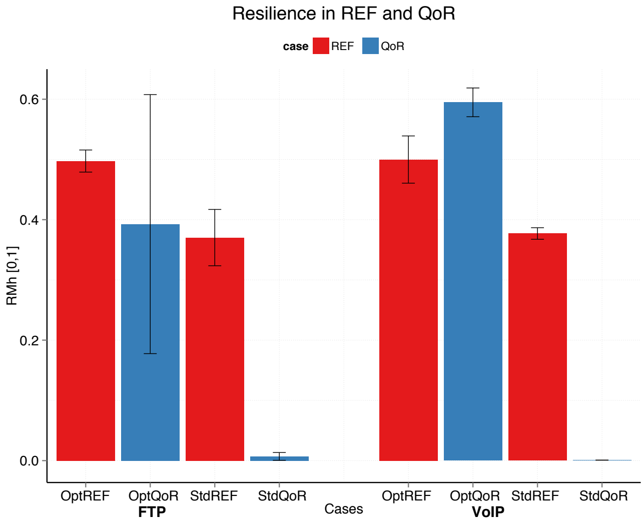


Figure 3.7: SCTP resilience as measured by REF and QoR.

Figure 3.7 illustrates the resilience of SCTP as measured by REF and QoR. In contrast with the results on availability, it is observable a divergence between REF and

QoR measured resilience values. QoR reports that SCTP with standard configuration as per RFC 4960 has virtually no resilience. REF, due to the protection model, reports a resilience value of 0.37 for both data and VoIP applications. Both QoR and REF show that SCTP resilience improves with optimized configurations. In particular, REF reports a resilience value ≈ 0.50. QoR, on the other hand, reports a resilience value ≈ 0.37 for FTP traffic and ≈ 0.6 for VoIP traffic. The spread of the QoR resilience values is considerably larger than for REF.

3.3 Ubiquity Evaluation Framework

This section formulates Ubiquity Evaluation Framework (UEF) to evaluate ubiquity support in a protocol. Goals and general aspects introduce UEF specification. A study case where UEF is applied to determine the ubiquity support of Mobile IPv6 (MIPv6) [Johnson et al., 2011] and Host Identity Protocol (HIP) [Gurtov, 2008] is also presented.

3.3.1 Objectives & General aspects

UEF is proposed to provide an objective evaluation methodology, that can be used at any stage of the UbiComp system development, without requiring experts on the field (i.e. not using interview methods). UEF establishes the base for protocol comparison regarding ubiquity support, without requiring any prototype or working system to assess the ubiquity support.

Table 3.5: UEF Consideration

Type	**Description**	**Units**	**Values**	**Examples**
$\Delta(t)$	time variables	*milliseconds* (ms)		Handover, processing delay, idle intervals
$S(x)$	size variables	*bytes*		size of data structures,
$C(x)$	capacity variables	*byte/s*	constant	
$P(x)$	Ratio		$[0, 1]$	procedure finalization and preparation rates

UEF addresses ubiquity as stated in Definition 3.2. This definition combines aspects of UbiComp systems with the functionalities of a protocol. UbiComp aspects are divided into two major groups: technical features and supported extensions. The protocol functionality is related with the degree of mobility support in the multihoming context. This mobility support enables Always Best Connected (ABC) paradigm, which is important in UbiComp systems [Louta et al., 2011].

The considerations to formulate UEF are summarized in Table 3.5. The next section formulates ubiquity.

3.3.2 Ubiquity U_{MH}

Ubiquity, as per Definition 3.2, combines lC-technical capabilities and lU-extensions of UbiComp systems, according to the Ψ-degree of mobility supported by a protocol. Equation 3.30 formulates Ubiquity - U_{MH}, where w_{lC} and w_{lU} are the weights for technical characteristics and extensions aspects, respectively. Weights assignment satisfy the following constraint: $w_{lC} + w_{lU} \leq 1$. A simple rule to assign weights can be based on the number of technical or extension items and the overall number of items (technical + extensions), as Equation 3.28 and Equation 3.29 show for technical and extensions items respectively. Other kind of weights assignment can be performed, such as $w_{lC} = 0.5$ and $w_{lU} = 0.5$.

$$W_{lC} = \frac{nLC}{nLC + nLU} = 0.65 \tag{3.28}$$

$$W_{lU} = \frac{nLU}{nLC + nLU} = 0.35 \tag{3.29}$$

$$U_{MH} = (W_{lC} \times lC + W_{lU} \times lU) \times \Psi \tag{3.30}$$

Technical capabilities and extensions are determined for each component of a UbiComp system, namely user (U), software (S) and hardware or computing platform (H), as shown in Table 3.6 and Table 3.7, respectively. MIPv6 and HIP, as protocols enabling mobility management, fall in the software component (S). Thus, their capabilities and extensions are evaluated by considering only the capabilities and extensions of the software component. A Table entry marked with "$\surd$" means that the respective capability is supported; "0" means that it is not supported; and "$-$" means that the capability is not applicable.

Capabilities and extensions are evaluated using a Boolean scale (0-not supported and 1-fully/partially supported). Moreover, to avoid ambiguity in the evaluation, UEF employs the meaning of each capability/extension according to standard dictionaries IEEE [1990]; Union [2013]; International Electrotechnical Commission [2013b,a];

Table 3.6: Technical capabilities of UbiComp systems in UEF for (S) - Software, (U) - User and (H) - Hardware components (in a total of 39)

Technical Capability	**(H)ardware**	**(U)ser**	**(S)oftware**	**MIPv6**	**HIP**
Accessibility	√	–	√	√	√
Accuracy	√	√	√	√	√
Adaptability	√	–	√	√	√
Adjustability	√	√	√	√	√
Adoptability	–	√	–	–	–
Analyzability	√	√	√	√	√
Compatibility	√	√	√	√	√
Configurability	√	–	√	√	√
Connectivity	√	–	√	√	√
Credibility	–	√	–	–	–
Customizability	√	–	√	√	√
Decomposability	√	–	√	0	0
Downloadable	–	–	√	√	√
Embeddedness	√	–	√	√	√
Effectiveness	√	–	√	√	√
Efficiency	√	–	√	√	√
Extensibility	√	–	√	√	√
Integrability	√	–	√	√	√
Interoperability	√	–	√	√	√
Interpretability	–	√	–	–	–
Invisibility	√	–	–	–	–
Learnability	–	–	√	0	0
Maintainability	√	–	√	√	√
Mobility	√	√	√	√	√
Portability	√	–	√	0	0
Predictability	√	–	√	√	√
Proactiveness	–	–	√	0	0
Reconfigurability	√	–	√	0	0
Reliability	√	–	√	√	√
Reusability	√	–	√	√	√
Scalability	√	–	√	√	√
Security	√	–	√	√	√
Sensibility	√	√	√	√	√
Shareability	√	–	√	0	0
Stability	√	–	√	√	√
Testability	–	–	√	√	√
Understandability	–	√	–	–	–
Usability	–	√	–	–	–
Wearability	√	–	–	–	–
Total:	**30**	**11**	**32**	**26**	**26**

Table 3.7: Extensions of UbiComp systems in UEF for (S) - Software, (U) - User and (H) - Hardware components (in a total of 22)

Extensions	**(H)ardware**	**(U)ser**	**(S)oftware**	**MIPv6**	**HIP**
Authentication	–	–	√	–	√
Authorization	–	–	√	–	√
Automation	√	–	√	√	√
Autonomy	√	–	√	√	√
Context Reusability	–	–	√	–	–
Durability	√	–	–	–	–
Entity Tracking	–	–	√	–	√
Identity Tracking	–	–	√	–	√
Inferred Context	–	–	√	–	–
Location Tracking	–	–	√	–	√
Negotiation	–	–	√	–	–
Response Time	√	–	√	√	√
Seamlessness	√	–	√	√	–
Self-Control	–	√	–	–	–
Service Coverage	√	–	√	√	–
Standardization	√	–	√	√	√
Trust	–	√	–	–	–
User Context	–	–	√	–	–
User preference	–	–	√	–	–
User profile	–	–	√	–	–
User Satisfaction	–	√	–	–	–
Utility	–	√	–	–	–
Total:	**7**	**4**	**17**	**6**	**9**

Oxford University Press [2013]. The definitions of all the terms employed in UEF can be found in appendix A. Finally, UEF considers non-overlapping capabilities and extensions as opposed to Kwon and Kim [2006]; Scholtz and Consolvo [2004] that evaluates an item twice, namely as a capability and as an extension, which increases complexity in the evaluation process. Each capability/extension is determined according to Equation 3.31, as specified by Kwon and Kim Kwon and Kim [2006], where n is the number of supported capacities/extensions, C_i is the value of the capacity (0 or 1) with $MaxScale = 1$, and n_ξ is the number of capacities/extensions that apply to the component.

$$C_\xi = \frac{\sum_{i=1}^{n} C_i}{n_\xi \cdot MaxScale}, with\ \xi \in \{u, s, h\} \tag{3.31}$$

This simplistic evaluation of technical capabilities and extensions in UEF promotes comparison between different proposals for UbiComp systems. Besides including all the components of such systems, UEF only requires a general knowledge of a specific solution. For instance, between the choice of WiFi or Bluetooth technologies, the general knowledge includes coverage, transmission power, data transfer ratios characteristics, among others.

UEF assesses mobility support through the degree of mobility Ψ, which is a compound metric of performance and cost aspects of the mobility management process, as per Equation 3.32. Costs represent processes that introduce overhead, such as signalling. Common approaches [Wang and Abu-Rgheff, 2006; Makaya and Pierre, 2008] consider cost aspects only. Performance aspects include the level of energy efficiency Ef and handover procedure preparation rate λ_{prep}. Cost aspects include handover Hc and signalling Sc costs, as well as the handover procedure finalization rate λ_{fina}. The term $N \cdot maxS$ corresponds to the number of cost aspects and the maximum cost value, respectively, with $maxS = 1$, and $N = 3$. β_m is used to distinguish performance and cost aspects, as employed in additive von Neumann Morgenstern utility functions [von Neumann et al., 2007].

$$\Psi = N \cdot maxS + \beta_m(Ef + \lambda_{prep}) - (1 - \beta_m) \cdot (Hc + Sc + \lambda_{fina}) \tag{3.32}$$

In IP mobility management evaluation, UEF includes metrics for energy efficiency and the procedure preparation rate, an improvement over previous work that only evaluates mobility management performance by assessing costs. UEF explores the end-host mobility approach, when all procedures are triggered by the mobile node, and includes support for simultaneous mobility events. In the latter case, the correspondent node plays a dual role as it is also a mobile node. The procedure rates include λ_{prep}-procedure preparation rate before the handover and λ_{fina}-procedure finalization rate after handover. Considering a total of n_{proc} procedures and $n_{proc} = n_{prep} + n_{fina}$, Equation 3.33 and Equation 3.34 formulate λ_{prep} and λ_{fina}, respectively.

$$\lambda_{prep} = \frac{n_{prep}}{n_{proc}} \tag{3.33}$$

$$\lambda_{fina} = \frac{n_{fina}}{n_{proc}} \tag{3.34}$$

Hc, the handover cost, quantifies cost in terms of handover delay, d, measuring the sum of procedure delays in the n_e entities. Handover delay is determined according to Equation 3.35, with n_{je} procedures executed at entity e with Δt_{proc} processing time.

$$d = \sum_{e=1}^{n_e} \sum_{j=0}^{n_{je}} \Delta t_{proc_{j,e}} \tag{3.35}$$

The handover cost, as per Equation 3.36, includes the cost of procedures invoked only after handover. A sigmoid function normalizes delay values that have increased granularity by a factor of d_g (=1000 by default). Handover cost could consider other metrics, such as handover delay at Layer 2 Liu et al. [2007], but this would tie UEF to a specific radio access technology and prevent the framework from apportioning the performance of the assessed protocol. Moreover, this does not restrict the evaluation on a specific phase of UbiComp systems.

$$Hc = \frac{1}{1 + e^{-\frac{\sqrt{d+1}}{d_g}}} \tag{3.36}$$

The signalling cost, as per Equation 3.37, determines the procedure overhead of the protocol, for all the procedures that are employed for signalling Qi Wang and Mosa Ali Abu-Rgheff [2006]. Signaling cost is considered for the mechanisms of a protocol, which correspond to a set/group of procedures *Gp*. For instance, in MIPv6, registration of addresses includes several messages, such as Binding Update (BU), Binding Acknowledgment (BA) and Binding Refresh Request (BRR).

$$Sc = \left[1 + e^{-\sqrt{\frac{\sum C_p}{max(C_p})}} \right]^{-1} \quad \forall_p \in Gp \tag{3.37}$$

The relation between the sum of all procedures $\sum C_p$ and the maximum cost of all the procedures $max(C_p)$ is the base for the signalling cost formulation. In UEF, the cost of a procedure C_p is formulated according to the message size, the message transmission frequency or the number of transmissions, and the processing cost Φ of each entity. Most approaches rely only on the message size Qi Wang and Mosa Ali Abu-Rgheff [2006]. Equation 3.38 determines the cost of a procedure invoked nI times, with message size L_i and transmitted nTx times or at a frequency Q_i.

$$C_p = \sum_{n=0}^{nI} \left[\sum_{t=1}^{nTx} \sum_{i=1}^{nM} \left(L_{n,t,i} \times Q_{n,t,i} \times \sum_{e \in \{\times\}} \Phi_{n,t,i,e} \right) \right] \tag{3.38}$$

For the number nTx and frequency Q_i of transmissions, the following assumptions are made:

- $Q_i = 1$, if $nTx > 1$, i.e. when there are retransmissions.
- $nTx = 1$, if $Q_i > 1$, for instance, messages that do not require any reliability but are sent frequently (e.g. router advertisements).

Equation 3.38, by including the nTx number of transmissions or Q_i frequency, aims to have a broader applicability, since protocols can perform signalling based on the number of transmissions or simply by sending messages after a certain interval (e.g. heartbeat messages of SCTP Fu and Atiquzzaman [2004]).

$P\Phi_e$- processing cost of an entity e is the relation between the Pc_e-operation cost of a procedure and Nif_e-number of interfaces of entity, as depicted in Equation 3.39.

$$P\Phi_e = Nif_e \times Pc_e \tag{3.39}$$

UEF considers multihomed nodes and does not rely on upper-layer parameters (e.g. session rate) to determine the processing cost. Instead, Pc corresponds to the relation between the processing delay $pDelay$ and the operation complexity, as per Equation 3.40. Complexity is modeled by the number of operations $nOper$, and the size of data structures $sizeData$. Whilst the size of the data structures can be dynamic, UEF only considers the size of a single record, for simplicity. When procedures do not involve data structures, $sizeData = 0$. $sizeData$ differs from message length, since it accounts for the size of data structures necessary to perform the operations in procedures (e.g. record in a routing table).

$$Pc = [nOper \times (1 + sizeData)] \times pDelay \tag{3.40}$$

Energy efficiency, Ef, considers the rates of reducing the active area $\lambda_{rdActArea}$ and the paging cost λ_{rdPagC}, as per Equation 3.41. Paging cost includes all the signalling mechanisms to enable paging. N is the number of cost aspects and $maxS$ the maximum value of these costs, with $N = 1$ and $maxS = 1$. Power saving mechanisms at the physical layer are not included in order to meet the technology independence requirement, as well as the possibility to perform evaluation isolatedly, this is without requiring a specific technology to evaluate a protocol.

$$Ef = N \times maxS + \beta_e \times \lambda_{rdPagC} - (1 - \beta_e) \times \lambda_{rdActArea} \tag{3.41}$$

The rate of active area reduction, $\lambda_{rdActArea}$, is the relation between the domain

$dArea$ and the paging area $pArea$, as formulated in Equation 3.42.

$$\lambda_{rdActArea} = \frac{dArea - pArea}{dArea} \tag{3.42}$$

The paging area is determined by considering the node that initiates paging till the endpoint (e.g. mobile node). Additionally, the area can consider the radius coverage (in meters), or simply the number of hops between the paging initiator and the endpoint Lee et al. [2008]. The domain area is limited by the prefix management entity, for instance an IPv6 router, and the endpoints. Values close to 1 indicate that the paging area is too small, with reduced costs, but with few optimizations. The paging cost, $PagC$ is given in Equation 3.43, where L represents the message size, transmitted nTx times. Each entity e participating in the paging group Ga has Nif interfaces in idle state during Δt interval, and for each paging message the processing cost is Pc. The paging group Ga includes all entities involved in paging signalling.

$$PagC = \sum_{t=1}^{nTx} L_t \times \sum_{\forall_e \in Ga} (Nif_{e,t} \times Pc_{e,t} \times \Delta t_{e,t}) \tag{3.43}$$

The processing cost, Pc, is determined according to Equation 3.40 with $sizeData = 0$. The ratio of paging cost reduction, λ_{rdPagC}, depicted in Equation 3.44 , is the relation between paging cost at effective idle intervals, Δt_idle, and theoretical intervals, Δt_Tidle, during which the a mobile end-node could remain in idle state (e.g. no data transfer and no mobility management signalling exchanges).

$$\lambda_{rdPagC} = \frac{PagC_{\Delta t\_idle}}{PagC_{\Delta t\_Tidle}} \tag{3.44}$$

The following subsection formulates ubiquity support using UEF for MIPv6 and HIP protocols.

3.3.3 UEF Use Case: Ubiquity in MIPv6 and HIP

In order to clarify the usability of UEF, this section specifies MIPv6 Johnson et al. [2011] and HIP Gurtov [2008] ubiquity support. These protocols have been chosen as MIPv6 is the main management mobility protocol for IPv6 networks, and HIP is a protocol that supports Locator/Identifier split paradigm, an important aspect in multihoming support and future Internet architectures Sousa et al. [2011a]. HIP supports mobility management with the RendezVous extension. The ubiquity support is determined according to its technical capabilities and extensions.

The analysis, herein performed is based solely on MIPv6 Johnson et al. [2011] and HIP Gurtov [2008] specifications. No expert on mobility management or in UbiComp systems was required. Technical capabilities of MIPv6 and HIP are similar as presented in Table 3.6, $lC_{MIP} = lC_{HIP} = 26/32 = 0.81$. Extensions are different between MIPv6 and HIP, as summarized in Table 3.7 where $lU_{MIP} = 6/17 = 0.35$, and $lU_{HIP} = 9/17 = 0.53$. According to UEF, HIP seems to be better suited for UbiComp systems regarding the technical and extensions capabilities. Nonetheless, the mobility management functionality cannot be ignored. Therefore, the assessment on how the degree of mobility is supported in MIPv6 and HIP needs to be determined. The following paragraphs illustrate the study case for MIPv6 and HIP to assess degree of mobility support and consequently, ubiquity.

The formulation of the degree of mobility includes diverse procedures:

- **Registration** (RG) - register new location information.
- **Security** (AA) - protect and secure identity of mobile node.
- **Address Configuration** (AD) - configure addresses in new networks.
- **Movement Detection** (MD) - detect availability of new networks.

The different procedures employ specific messages to convey signalling for the operations being supported, as summarized in Table 3.8, for MIPv6 and HIP protocols.

Table 3.8: Messages and procedures of mobility management

Procedure	**MIPv6**	**HIP**
Registration	BU[a],BA[b],BRR[c]	I1,R1, I2,R2
Security	HoTI[d],HoT[e], CoTI[f],CoT[g]	included in Registration
Address Configuration	unsolicited NS[l], unsolicited NA[m], RS[h], RA[i], DAD[j] mechanism	
Movement Detection	solicited NS, solicited NA, RS, RA, NUD[k] mechanism	
Tunnelling	Header information in IPv6 packets	

[a] Binding Update (BU) [b] Binding Acknowledgment (BA) [c] Binding Refresh Request (BRR) [d] Home of Test Init (HoTI) [e] Home of Test (HoT) [f] Care of Test Init (CoTI) [g] Care of Test (CoT) [h] Router Solicitation (RS) [i] Router Advertisement (RA) [j] Duplicate Address Detection (DAD) [k] Neighbour Unreachability Detection (NUD) [l] Neighbour Solicitation (NS) [m] Neighbour Acknowlegment (NA)

Each procedure is specified according to Equation 3.31. Mobility management in MIPv6 includes the Mobile Node (MN), Home Agent (HA) and Correspondent Node

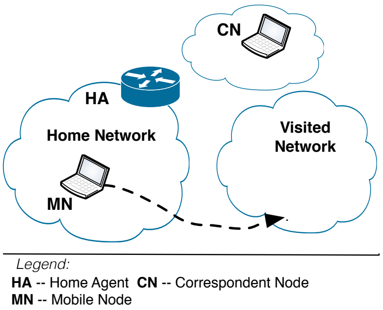


Figure 3.8: MIPv6 mobility scenario.

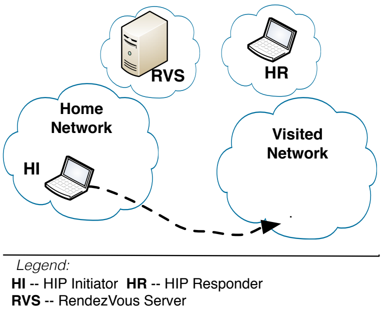


Figure 3.9: HIP mobility scenario.

(CN) entities, as illustrated in Figure 3.8. In HIP, the HIP Initiator (HI), the RendezVous Server (RVS) and the HIP Responder (HR) manage mobility, as depicted in Figure 3.9. As some procedures rely on IPv6 mechanisms, $E1$ denotes the MN or the HI, while $E2$ stands for the HA or the RVS. Finally the $E3$ represents CN or HR entities.

3.3.3.1 Registration

Mobile IPv6 (MIPv6) registration is based on binding messages. MN sends BUs to the HA and CN when new addresses are available to trigger the registration process. Binding Acknowledgment is transmitted to acknowledge the reception of a BU and the status of treatment initiated by the BU. Moreover, binding can be refreshed using BRR, or the CN can inform the MN about errors using Binding Error (BE) message. The cost is determined in the same fashion as HIP, Equation 3.45, but with Binding Update, Binding Acknowledgment, Binding Error and Binding Refresh Request messages.

HIP registration is performed in three steps (*s1*, *s2*, *s3*) according to the handover phase. In the *s1* step, HI and HR register with RVS using *I1, R1, I2* and *R2* messages. The cost of this step is determined by Equation 3.45. Such messages are exchanged between HI and RVS nodes and between HI and HR nodes, to perform registration in RendezVous Server and HIP Responder nodes. The base exchange (step *s2*) corresponds to a four-way handshake between HIP Initiator and HIP Responder and only involves the RendezVous Server to forward I1 messages.

$$C_{RG-HIP_{s1,s2}} = \sum_{t=1}^{nTx} L_{I1,t} \cdot \sum_{e \in \{HI,RVS,HR\}} (Nif_{e,t} \cdot Pc_{e,t}) + L_{R1} \cdot \sum_{e \in \{HI,RVS,HR\}} (Nif_e \cdot Pc_e)$$
$$+ L_{I2} \cdot \sum_{e \in \{HI,RVS,HR\}} (Nif_e \cdot Pc_e) + L_{R2} \cdot \sum_{e \in \{HI,RVS,HR\}} (Nif_e \cdot Pc_e) \qquad (3.45)$$

After the handover (step *s3*), HI needs to update the locator information on $dest$ nodes, which include RVS and HR. For such purpose, it employs the update message with locator information, and issues an *echo_request*, which status of update is reported in the *echo_response* message. The registration cost of the update is determined according to Equation 3.46.

$$C_{RG-HIP_{s3}} = \sum_{t=1}^{nTx} L_{UPD(locator),t} \cdot \sum_{e \in \{HI,dest\}} (Nif_{e,t} \cdot Pc_{e,t}) \qquad (3.46)$$
$$+ L_{UPD(echo\_req)} \cdot \sum_{e \in \{dest,HI\}} (Nif_e \cdot Pc_e) + L_{UPD(echo\_resp)} \cdot \sum_{e \in \{HI,dest\}} (Nif_e \cdot Pc_e)$$

3.3.3.2 Security

MIPv6 can rely on external mechanisms, such as IP Security [Kent and Atkinson, 1998], to enable higher levels of security. Nevertheless, this study focuses on the return routability, since it is an internal procedure of MIPv6 that allows the verification of addresses when the MN is at visited networks. Equation 3.47 formulates the cost of this procedure relying on the Home of Test Init (HoTI), Care of Test Init (CoTI) and respective reply messages, namely Home of Test (HoT) and Care of Test (CoT).

$$C_{AA-MIP} = \sum_{t=1}^{nTx} L_{HoTi,t} \cdot \sum_{e \in \{MN,HA,CN\}} (Nif_{e,t} \cdot Pc_{e,t}) \qquad (3.47)$$
$$+ \sum_{t=1}^{nTx} L_{CoTi,t} \cdot (Nif_{MN,t} Pc_{MN,t} + Nif_{CN,t} Pc_{CN,t})$$
$$+ L_{HoT} \cdot \sum_{e \in \{MN,HA,CN\}} (Nif_e \cdot Pc_e) + L_{CoT} \cdot (Nif_{MN} \cdot Pc_{MN} + Nif_{CN} \cdot Pc_{CN})$$

Integrity protection and encryption is performed in HIP by employing the Encapsulating Security Payload (ESP). The registration cost already includes the security cost C_{AA-HIP}, as ESP security association is part of the base exchange. Regarding security, HIP establishes a distinction comparatively with MIPv6, as security is included in the registration process.

3.3.3.3 Address Configuration

Address configuration in MIPv6 and HIP nodes relies on IPv6 schemes that include Router Solicitation (RS), Router Advertisement (RA) and the messages in the Duplicate Address Detection (DAD) mechanism. Neighbour Solicitation (NS) messages are sent to multicast addresses with the reply of Neighbour Acknowlegment (NA) messages. In addition, IPv6 routers (at home and foreign networks, Rtr_h and Rtr_f, respectively) advertise prefixes using Router Advertisement messages, while Router Solicitation messages are retransmitted on error events. Equation 3.48 defines the cost of address configuration.

$$\begin{aligned}C_{AD} &= \sum_{t=1}^{nTx} L_{NS,t} \cdot \sum_{e\in\{E1,E2,E3\}} (Nif_{e,t} \cdot Pc_{e,t}) + L_{NA} \cdot \sum_{e\in\{E1,E2,E3\}} (Nif_e \cdot Pc_e) \\ &+ \sum_{t=1}^{nTx} L_{RS,t} \cdot \sum_{e\in\{E1,E2,E3\}} (Nif_{e,t} \cdot Pc_{e,t}) + Q_{RA_{home}} \cdot L_{RA_{home}} \cdot \sum_{e\in\{E1,Rtr_h,E2,E3\}} (Nif_e \cdot Pc_e) \\ &+ Q_{RA_{foreign}} \cdot L_{RA_{foreign}} \cdot \sum_{e\in\{E1,Rtr_f,E2,E3\}} (Nif_e \cdot Pc_e) \qquad (3.48)\end{aligned}$$

The DAD mechanism is employed to assure the uniqueness of a configured address, since, on IPv6 networks these can be configured based on the advertised prefixes in RA messages.

3.3.3.4 Movement Detection

Movement detection also relies in IPv6 schemes, namely the Neighbour Unreachability Detection (NUD) mechanism. NUD uses solicited Neighbour Solicitation and Neighbour Acknowlegment messages and the respective cost is formulated according to Equation 3.49.

$$C_{MD} = \sum_{t=1}^{nTx} L_{NS,t} \cdot \sum_{e\in\{E1,E2,E3\}} (Nif_{e,t} \cdot Pc_{e,t}) + L_{NA} \cdot \sum_{e\in\{E1,E2,E3\}} (Nif_e \cdot Pc_e) \qquad (3.49)$$

The NUD mechanism enables a node to determine the reachability of a router. For instance, when a router does not respond to Neighbour Solicitation, it means that the node is moving to another network.

3.3.3.5 Tunneling

Finally, MIPv6 includes the tunnel cost, since packets can be forwarded to MNs at visited networks via tunnels. The cost of tunnel establishment is determined in an application independent fashion, as tunnelling relies on IPv6 encapsulation mechanisms. The tunnel establishment cost, as per Equation 3.50, considers only the size of message headers and respective processing cost in MN, HA and CN.

$$\begin{aligned} C_{TU} = & \sum_{t=1}^{nTx} HdrT_{MN,t} \cdot (Nif_{MN,t} \cdot Pc_{MN,t}) \\ & + \sum_{t=1}^{nTx} HdrT_{HA,t} \cdot (Nif_{HA,t} \cdot Pc_{HA,t}) + \sum_{t=1}^{nTx} HdrT_{CN,t} \cdot (Nif_{CN,t} \cdot Pc_{CN,t}) \end{aligned} \tag{3.50}$$

3.3.4 Evaluation

This section details the methodology used when applying UEF in an evaluation study. After deriving all the formulation for MIPv6 and HIP protocols, an evaluation is performed to assess the impact that the number of handovers and communication nodes can have on such protocols, and consequently on the performance of UbiComp systems employing these protocols.

3.3.4.1 Objectives

The goals for this evaluation are two-fold:

1. Determine the ubiquity support of MIPv6 and HIP, assessing which protocol is best suited for UbiComp systems, considering the same underlying technologies and applications.

2. Determine the impact that different configurations, such as number of handovers and correspondent nodes have on ubiquity.

The second evaluation goal is associated with scalability, in terms of the velocities achieved and the number of simultaneous communications that can be supported.

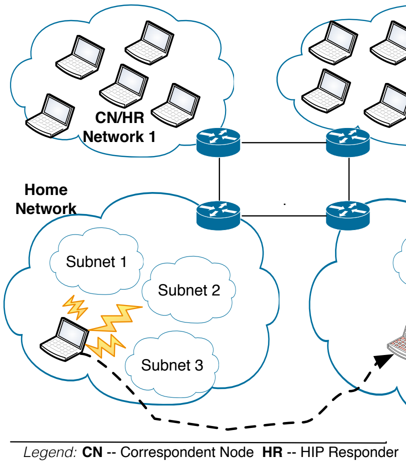


Figure 3.10: Evaluation scenario.

3.3.5 Evaluation Scenario

The evaluation scenario used in the case study is illustrated in Figure 3.10. The different nodes (e.g. MN, HI, CN, HR) are configured with three interfaces, a common configuration in mobile terminals, if considering the example of a laptop with WiFi, Bluetooth and 3G capable interfaces. Moreover, Mobile Node/HIP Initiator can communicate simultaneously with several correspondent nodes or HIP responders, which can be located in different networks.

3.3.5.1 Evaluation Parameters

UEF is applied in a study where the choice of a protocol to manage mobility in UbiComp system is considered at the design phase. MIPv6 and HIP protocols are assumed to be operating with the maximum message size (e.g. with all options filled). In addition, only the mandatory messages are considered; optional messages, such as *HIP - NOTIFY*, are not included.

The nodes with three interfaces, $nif = \{3\}$ can communicate with $ncns = \{1, 5, 10\}$ other nodes. In addition, nodes move with different speeds, thus having to handle a number of handovers $nho = \{10, 50, 100, 200\}$. All sessions last for 300s. Assuming, that evaluation is in the design phase of a UbiComp system, values of processing delay cannot be measured (as no prototype is available). Thus for this study case, all the processing times follow normal and exponential distributions, with different means $x = \{1s, 10s\}$ and rate $\lambda = 1$. Different distributions are used to accommodate different modeling mechanisms for processing times.

The analytical evaluation has been performed using the R framework Team [2010] and considering that both MIPv6 and HIP do not include energy efficiency mechanisms $Ef = 0$, as no paging schemes are incorporated. We stress that such kind of evaluation enables ubiquity support determination, promoting the choice of most performant protocols regarding ubiquity support.

Ubiquity weights $w_{lC} = 0.65$ and $w_{lU} = 0.35$ are used according to the number of items in technical and extensions categories, as summarized in Table 3.6 and Table 3.7. The degree of mobility weight is equal to $w_m = 0.5$, as no energy efficiency mechanisms are considered and thus the degree of mobility relies mainly on the cost. Values higher than 0.5 tend to neglect the impact of cost in mobility support.

3.3.5.2 Results

The results reported in this section are based on 100 runs to improve statistical significance, and are reported considering the number of handovers, for MIPv6 and HIP protocols. Ubiquity, as a compound metric is discussed in first place. The remaining metrics, such as the degree of mobility supported, handover cost and signalling overhead are also discussed.

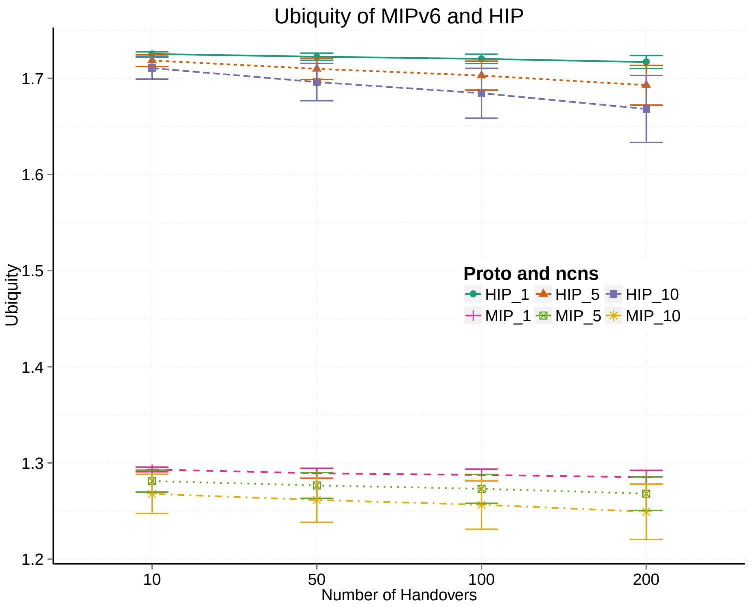


Figure 3.11: Ubiquity support in MIPv6 and HIP protocols

UEF can assess ubiquity taking into consideration protocol functionalities in different conditions that UbiComp systems can face. Under mobile scenarios, the number of handovers impacts the performance of mobility management protocols, as more signalling is required.

Figure 3.11 depicts the ubiquity support of MIPv6 and HIP protocols for different number of handovers. HIP supports ubiquity to a greater extent, as values rely ≈ 1.7 when compared to MIPv6 that has values ≈ 1.3. Ubiquity results consider technical capabilities and extensions, as well as the degree of mobility supported (recall Equation 3.30). As previously determined, the technical capabilities of MIPv6 and HIP are equal, $lC_{MIP} = lC_{HIP} = 26/32 = 0.81$, but the number of supported extensions is different, with HIP as a protocol more prone to be employed in UbiComp systems, $lU_{MIP} = 6/17 = 0.35$, and $lU_{HIP} = 9/17 = 0.53$.

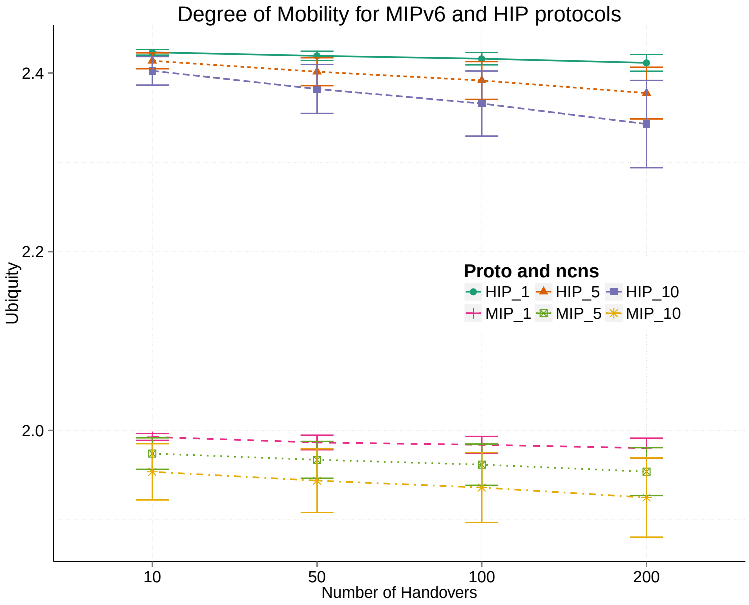


Figure 3.12: Degree of Mobility support in MIPv6 and HIP protocols

The number of handovers and the number of correspondent nodes have an impact in the ubiquity support as explained bellow. Figure 3.12 depicts the degree of mobility for both protocols. With higher number of handovers, all procedures required to handle mobility are triggered often, introducing degradation in the performance, as signalling overhead increases. With the increased number of correspondent nodes, ubiquity support and the degree of mobility support are lower since updates need to be forwarded to more nodes.

The handover cost, depicted in Figure 3.13, is determined according to Equation 3.35 and accounts the processing delay in both protocols. As per the evaluation method-

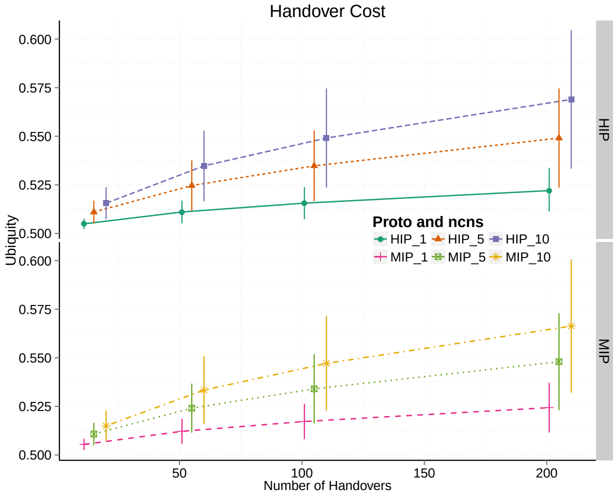


Figure 3.13: Handover cost of MIPv6 and HIP for different correspondent nodes

ology, this time has not been measured, but was assumed to follow an exponential distribution, which means that the processing delay is the same in both protocols. Nonetheless, it can be observed that the handover cost increases linearly with the number of handovers and with the number of correspondent nodes.

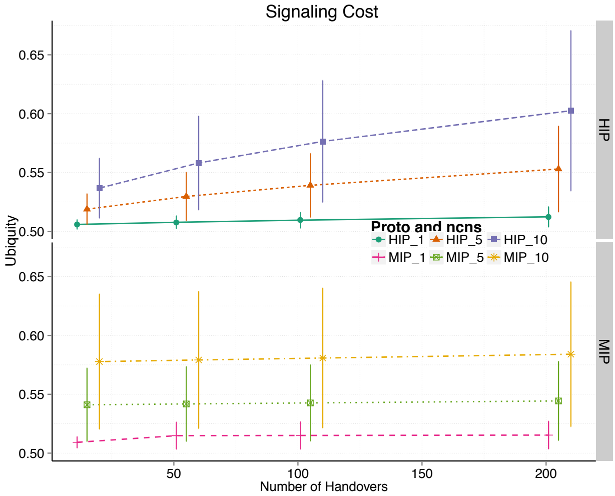


Figure 3.14: Signalling cost of MIPv6 and HIP for different correspondent nodes

The signalling cost, depicted in Figure 3.14, is determined according to Equation 3.38 and accounts for the overhead of a protocol. HIP is more impacted with the number of handovers, since signalling cost of HIP increases linearly. For instance, with 200 handovers it is above 0.60 while MIPv6 is ≈ 0.58. In contrast, MIPv6 is more impacted with the number of correspondent nodes than with the number of handovers. For instance, signalling cost does not increase as in HIP with the number of handovers.

The difference between MIPv6 and HIP relies on the registration and security procedures, as movement detection and address configuration share the same DAD and NUD mechanisms. First, the four-way handshake nature of HIP leads to more message exchange. Finally the messages exchanged have higher sizes, when compared to MIPv6. HIP signalling overhead results UEF are inline with similar approaches dedicated to the evaluation of HIP and MIPv6 protocols Toledo et al. [2011].

Such results allow to determine that HIP supports ubiquity to a greater extent in comparison to MIPv6. For a UbiComp system, HIP is preferable in comparison to MIPv6, mainly due to the locator/identifier split paradigm. Moreover, such results are inline with related evaluations, that point HIP as a protocol with stronger security mechanisms Faigl et al. [2011].

3.4 Summary

This chapter presented, Multihoming Evaluation Framework (MEF) which comprises two evaluation frameworks that establish the ground-base towards multihoming evaluation. Such evaluation is performed considering resilience and ubiquity multihoming goals fulfillment.

The Resilience Evaluation Framework (REF) and the Ubiquity Evaluation Framework (UEF) have also been applied to analyse different protocols, regarding their resilience and ubiquity support. Stream Control Transport Protocol (SCTP) was analysed regarding the resilience support, since it incorporates failure-tolerance mechanisms to enable primary-backup protection model. Mobile IPv6 (MIPv6) and Host Identity Protocol (HIP) protocols were analysed regarding their ubiquity support, as these protocols enable mobility management for nodes in UbiComp systems. With REF it was concluded that SCTP with optimized failover configurations supports resilience more efficiently than with standard configurations.

UEF, comparing MIPv6 and HIP protocols, highlights HIP as providing an extended ubiquity support. Notwithstanding, such enhanced ubiquity support is associated with deployment issues in existent IP networks, as it implements a locator-identifier split paradigm.

The results achieved, demonstrate that the path towards an enhanced multihoming support must include support for the locator-identifier split paradigm, as introduced a previous chapter (i.e Section 2.2 of Chapter 2). HIP is a protocol that follows such paradigm.

The outcomes of this chapter include the following publications:

1. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Resilience Evaluation Framework (REF)**", WMNCT , 2010 [Sousa et al., 2010].

2. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Ubiquity Evaluation Framework (UEF)**", WWIC, 2011 [Sousa et al., 2011b].

The following submission was performed as well:

1. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Evaluation of Ubiquity Support in Mobile Computing Systems**", in Springer Handbook "Resource Management in Mobile Computing Environments", 2013.

—Try to turn as many soft, aspirational goals as possible into success criteria, and make them specific enough that you can actually tell whether or not you've met them.

Erin Kissan *The Elements of Content Strategy*

4 Multihoming Aware Optimization Mechanism

THIS chapter presents a multihoming aware optimization mechanism for path selection. MulTiHOming-aware Decision-makIng meChanism for AppLications (MeTHODICAL), proposed in this thesis, comprises an algorithm for criteria weighting and a Multiple Attribute Decision Mechanism (MADM) that optimizes path selection by including multihoming benefits and costs criteria. This chapter includes different sections, as summarized in the next paragraphs. Section 4.1 overviews related work and introduces the motivation for MeTHODICAL algorithms. Section 4.2 introduces the taxonomy and assumptions to formulate MeTHODICAL. Section 4.3 specifies the criteria weighting algorithm, that can serve as input for MADM techniques that use preferences for the different criteria. Section 4.4 formulates a path optimization algorithm, which relies on MADM, but with improved distance and scoring functions that are tailored for multihoming optimization. Section 4.5 introduces an evaluation methodology for MADM techniques that allows to assess the accuracy of a Multiple Attribute Decision Mechanism. Section 4.6 establishes the methodology employed to evaluate MeTHODICAL. The performed evaluation includes different scenarios with specific and heterogeneous requirements. Section 4.7 discusses and presents results of the different evaluations and Section 4.8 summarizes the chapter.

4.1 Introduction

This section introduces the goals and requirements of the optimization algorithms. An overview of the state of the art and open issues is also presented.

4.1.1 Objectives and Requirements

Nodes that are multihomed-aware have a plethora of forms to optimize traffic in multiple links. For instance, optimization may aim to maximize battery life or simply application performance. Moreover, optimization can consider N criteria in the determination of optimal solutions (i.e the ones that provide better performance), such as bandwidth and loss.

The following goals drive the specification of the different proposed algorithms in this chapter:

Goal 1 Specify a technique that allows an user to map her preferences in terms of criteria weighting. A scheme that allows to choose the importance of criterion over another objectively. For instance, to state bandwidth as the more important criterion, followed by packet loss and Round Trip Time (RTT).

Goal 2 Specify an optimization technique that is flexible enough to accommodate multiple criteria and is tailored to multihoming optimization.

Goal 3 Specify a mechanism to assess the accuracy of the proposed optimization technique, for multihoming.

As with Resilience Evaluation Framework (REF) and Ubiquity Evaluation Framework (UEF) proposals, the following requirements for the specification of the algorithms were established:

Generic Not tied to a specific problem or particular scenarios.

Objective Allow the unbiased comparison between similar techniques.

Thorough Evaluation metrics must be objective and include standard measurement mechanisms.

Autonomous No need for an expert in the area to be deployed.

Implementable Can be easily implemented without requiring other kind of programs or libraries, for instance GNU Linear Programming Kit (GLPK) [GNU, 2013].

Deployable To have low computation overhead, allowing it to be deployed in diverse types of nodes and for real-time problems.

Flexible Can easily accommodate more criteria.

The following subsections introduce the state of the art.

4.1.2 State of the Art

This subsection overviews the state of the art regarding techniques providing optimized path selection, algorithms formulating criteria weighting for optimization techniques, and evaluation methodologies to compare optimization mechanisms.

4.1.2.1 Techniques for optimized path selection

This subsection overviews the most relevant techniques for optimized path selection.

Path optimization or network selection can be performed in network- and user-centric approaches. The former protects the network from high loads (i.e. high number of users), as selection is controlled by the network. Nonetheless, it requires the involvement of all the access networks, having communication overhead and requiring cooperation between users and networks. On the other hand, the user-centric approach is a distributed approach as selection is controlled by the user. Such characteristic allows to include user preferences, decreasing the complexity and avoiding communication overheads. Nonetheless, as users can have 'selfish' behaviour, there is the risk of overloading a network [Charilas and Panagopoulous, 2010].

Efficient multihoming and multiaccess support in heterogeneous networks is still inhibited by mechanisms that perform path selection based on presets and static policies, as presented in Chapter 2. Optimized path selection mechanisms need to consider multiple criteria, such as availability, available capacity, monetary cost, packet loss, delay, and IP delay variation, so that the overall performance is improved. Indeed, profit is assured if benefits are maximized and costs are minimized. In such context, optimal path selection becomes a *NP-hard* problem [Muscariello et al., 2009; Xue et al., 2007]. Efficient optimal path selection can be provided by optimization

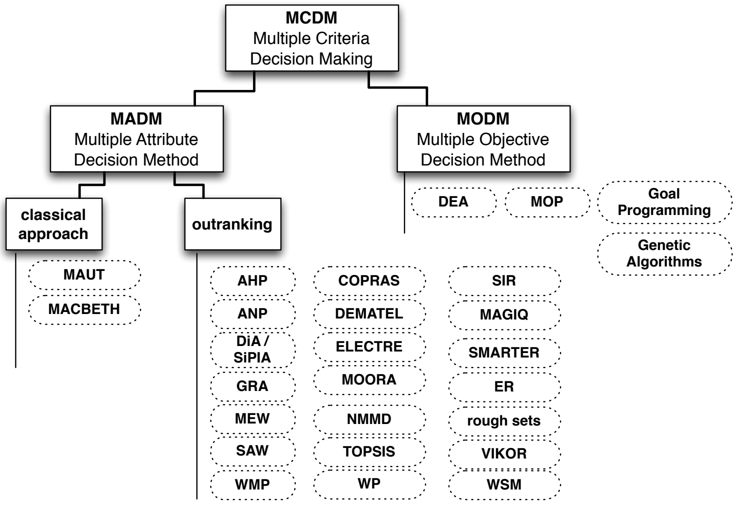


Figure 4.1: Multiple Criteria Decision Making methods

techniques that enable solutions with low computation complexity that foster deployment, as discussed in the next paragraphs, for user-centric approaches.

When dealing with a *NP-hard* problem several approaches can be followed to perform optimization. A Multiple Attribute Decision Making (MCDM) analysis can be performed, and different methods can be pursued to select optimal paths, as illustrated in Figure 4.1. More specifically, two approaches can be followed, namely Multiple Attribute Decision Mechanism (MADM) or Multiple Objective Decision Making (MODM). The former employs utility functions or pairwise comparisons to rank the available paths and determine the optimal path with the best score. The latter establishes objectives, such as minimizing delay, and employs optimization methods to determine the optimal solution, according to the initial optimization goals.

One of the mathematical optimization methods commonly employed is Linear Programming (LP) [Hillier and Lieberman, 1995]. LP techniques provide optimal solutions, but have deployment issues associated, since for each problem or scenario, a specific formulation needs to be derived, as optimization goals may be different. For instance, path selection for heterogeneous networks can be optimized by maximizing an utility function that considers connectivity, preferred operator, handovers and link quality criteria [Choque et al., 2011]. With the same optimization problem scope, flow management for heterogeneous networks is modelled as an optimization problem aiming to maximize application quality and, at the same time, to minimize power consumption and access prices [Mehani et al., 2011]. Multipath routing can also be optimized via LP considering buffer sizes and jitter effects [Anjali et al., 2010]. Concurrent transmission in heterogeneous networks is optimized by throughput and fairness [Yang et al., 2010; Dionysiou et al., 2010]. Each of these approaches addresses the *NP-hard* optimization problem with different optimization criteria and specific optimization functions. Despite providing optimal solutions, such kind of approaches, by the fact of being tied to the problem, require reformulation when introducing new criteria (i.e, Mean Opinion Score, RTT). Moreover, such approaches [Choque et al., 2011; Mehani et al., 2011] require specific solvers such as the GLPK [GNU, 2013] or MiniZinc [NICTA, 2013], respectively.

With Multiple Objective Programming (MOP) [Marler and Arora, 2004], optimization is formulated with objective functions that can be evaluated partially. The optimal solution corresponds to the one with the best partial evaluations. Despite not considering the criteria preferences, this kind of technique can be extended to include the degree of consideration for objectives [Kim et al., 2012]. MOP techniques, by expressing the objectives in functions where criteria are correlated, share the same issues as linear and integer programming approaches.

Other techniques do not incur in the complexity of Linear Programming and employ utility functions. Such kind of functions combine multiple criteria in a linear form. For instance, a generic selection algorithm, mCASE, is proposed to allow the network selection in heterogeneous networks [Choque et al., 2012]. mCASE considers as criteria the preferred operator, handovers, link quality and load. Mission Cognition Score (MCS) [Eswaran et al., 2010] employs an utility function to assess how accurately a network fulfills its mission. MCS considers a desired accuracy (i.e. a mission requires at least 80%) and the latency in the mission accomplishment. As with LP, utility functions are tied to the optimization problem and require reformulation to support more criteria, despite being simple to apply [Charilas and Panagopoulous, 2010].

Accuracy in optimization can be achieved through statistical techniques. For instance, Bayesian learning is a statistical approach that allows to make decisions in the presence of uncertainties, based on Bayes theorem. Using such theorem, it is possible to determine the network quality probability of being inside some thresholds [Ong and Khan, 2008]. Nonetheless, the issue with such kind of approach is the associated complexity and the high computational overhead [Charilas and Panagopoulous, 2010].

Techniques like Multi-Armed Bandits approaches [Yi Gai and Jain, 2012] have deployment issues, as both problem formulation and corresponding policies have some limitations when exploring different combinations. The polynomial time approximation schemes [Xue et al., 2007] are mainly tailored for delay-constrained least cost problems, where the minimum cost is subject to a given delay constraint. Moreover, these approaches require considerable modification for each optimization problem, even if the change between problems is only the addition of a criterion.

Other kinds of optimization mechanisms are efficient for network selection [Zekri et al., 2012]. Markov based decision algorithms model optimization problems under the assumption that the decision can follow a certain probability distribution. Despite having accurate results, they have the same implementation issues of LP techniques. Fuzzy based mechanisms have the advantage of dealing with imprecise data but are complex and have, therefore, implementation issues. Moreover, they need to be combined with other techniques to determine optimal solutions. Other mechanisms model the network selection problem under game theory approaches. For instance, cooperative games have the issues associated with network-centric approaches, since cooperation between user and network is required. Other approaches employ evolutionary games to formulate network selection. For instance, different users groups compete to share available network bandwidth, optimization is formulated in an evolutionary equilibrium to guarantee access to the maximum number of users groups. Once again, these approaches have high complexity associated, and as the remaining approaches herein referred (i.e. Markov, fuzzy based), are not flexible since they are tied to the optimization problem.

Outranking Multiple Attribute Decision Mechanism (MADM) techniques [Figueira et al., 2005] are pointed as techniques being flexible enough to accommodate quantitative and qualitative data, as the case of Analytic Hierarchy Process (AHP). MADM techniques have been employed in distinct areas (e.g, Logistics, computer science, safety, health management) [Behzadian et al., 2012] and have low complexity associated. Moreover, MADM can accommodate several criteria no matter the research problem [Zekri et al., 2012; Charilas and Panagopoulous, 2010]. In particular, the outranking MADM techniques formulate optimization by scoring the multiple path alternatives, through mathematical operations. Indeed, the efficiency, allied to the simplicity of such methods lead to a plethora of MADM techniques, as pictured in Figure 4.1.

Multiple Attribute Utility Theory (MAUT) is also a MADM technique that aims to determine the best alternative among a set. As opposed to outranking MADM techniques, MAUT establishes a utility function to determine one single optimal alternative, which has the disadvantage of being tied to the optimization problem [Charilas and Panagopoulous, 2010]

Table 4.1 summarizes the requirements fulfilment in the most relevant schemes, where $\surd$ stands for applicable and X is the opposite. For instance, LP is not generic and neither flexible.

Table 4.1: Optimization techniques

Technique	Generic	Autonomous	Flexible	Thorough	Objective	Implementable	Deployable
Linear Programming and **MOP**	X	X	X	√	X	X	√[a]
Utility Functions and **MAUT**	X	X	X	√	X	√	√
Bayesian learning	X	X	X	√	X	X	X
Multi-Armed Bandits and **Polynomial Approximation**	X	X	X	√	X	X	√[a]
Outranking MADM	√	√	√	√	X	√	√
Markov-based	X	X	X	X	X	√[b]	√
Fuzzy-Based	X	X	X[c]	X	X	X	X
Game Theory	X	X	X	X	X	X	X

[a] By requiring an external solver it may limit its deployment. [b] With associated complexity. [c] Can deal with unprecise data.

4.1.2.2 Outranking MADM techniques

Diverse outranking MADM exist, as pictured in Figure 4.1. This section overviews outranking MADM techniques that can be employed in path optimization problems.

Simple Additive Weighting (SAW) is a MADM technique that scores path alternatives using a weighted sum of all criteria, in the form of $\sum_{j=1}^{N} w_j \cdot r_{ij}$, for N criteria and M alternative paths, where $i \in M$. Multiplicative Exponent Weighting (MEW) is also a MADM technique that applies a weighted product to score path alternatives, in the form of $\prod_{j=1}^{N} r_{ij}^{w_j}$. Both of these techniques set as optimal paths the ones with the highest score [Kaleem, 2012]. Despite their simplicity, these MADM techniques have issues associated. For instance, weights are not considered appropriately, as when the weight for a criterion is set to a high value, scoring does not reflect the importance of such weight. SAW has a ranking identification problem, as no accuracy exists in identifying the alternative ranks [Tran and Boukhatem, 2009].

The Technique for Order Preference by Similarly to Ideal Solution (TOPSIS) [Tong et al., 2004] is a technique that scores path alternatives based on the distance from each alternative to ideal solutions. Such ideal solutions are determined by considering the ones that have higher values for benefits, denominated as positive ideal solution and lower values for costs criteria, considered as negative ideal solution. Optimal paths are those with the highest closeness index that combines the benefits similarity and costs similarity distances. The similarity distance is based on the Euclidean distance, as illustrated in Equation 4.1, for benefits criteria.

$$S_j^+ = \sqrt{\sum_{j=1}^{N}(x_j^+ - x_{ij})} \tag{4.1}$$

Technique for Order Preference by Similarly to Ideal Solution (TOPSIS) is considered as a classical MADM that has been employed in distinct areas [Behzadian et al., 2012]. As such, different proposals have been specified to assess issues that are characteristic to TOPSIS. For instance, TOPSIS is pointed to have ranking abnormality, which corresponds to inconsistent optimal solutions when the least performant path alternative is removed from the alternatives. Distance to Ideal Alternative (DiA) [Tran and Boukhatem, 2008] was developed to select dynamically the best path. DiA is based on TOPSIS but employs the Manhattan distance to assess how far path alternatives are from the ideal solutions, as depicted in Equation 4.2, for benefits criteria.

$$S_j^+ = |x_j^+ - x_{ij}|, \text{with } j = 1, \cdots, n \tag{4.2}$$

The Novel Method based on Mahalanobis Distance (NMMD) [Lahby et al., 2012] has been proposed to mitigate ranking abnormality. The main innovation in this proposal is the employment of the Mahalanobis distance to assess how far path alternatives are from ideal solutions, as depicted in Equation 4.3. Nonetheless, the covariance determination, besides introducing complexity, requires high volume data to be statistically significant.

$$D_M(x) = (x-u)^T \times S^{-1} \times (x-u), \tag{4.3}$$
$$\text{where } S^{-1} \text{ is the inverse covariance matrix}$$

TOPSIS, DiA and NMMD techniques are compared in a heterogenous scenario with

WiFi, UMTS and WiMAX networks. Results demonstrate that NMMD and DiA are able to reduce ranking abnormality when compared to TOPSIS.

Gray Relational Analysis (GRA) [Huszak and Imre, 2010] establishes a gray relational coefficient of each path alternative, which describes the similarity with each path and the ideal values. The optimal path is the one that has a higher degree of similarity. Nonetheless, issues are pointed to this type of approach, such as the high number of path alternatives to be statistically efficient. Moreover, criteria must follow linear or log probability distributions [Tzeng and Huang, 2011].

Multi-Criteria Optimization and Compromise Solution (VIKOR) [Mehbod et al., 2013] is a MADM technique that can work with conflicting criteria.VIKOR establishes a compromise-ranking list of path alternatives. The ranking is also based on the distance that a path has to the ideal solution. VIKOR has the advantage of being employed when weights are not known in the beginning [Mehbod et al., 2013]. Issues are pointed to this technique regarding the score consistency. In a comparison between TOPSIS and VIKOR, TOPSIS is presented as the technique providing the most significant results in a spearman correlation coefficient evaluation [Antucheviciene et al., 2011].

Complex Proportional Assessments (COPRAS) [Antucheviciene et al., 2011] is a MADM technique that determines the complex efficiency of the project, which is proportional to the relative effect of values and weights of the considered criteria. COPRAS performs normalization and combination of weights in a single step, as opposed to TOPSIS and similar techniques that have distinct steps for such operations. Optimal paths in COPRAS can be selected based on their relative significance, where the most significant correspond to the best paths. Indeed, by a spearman correlation evaluation it is demonstrated that COPRAS has the same performance of TOPSIS.

The Elimination and Choice Translating Priority (ELECTRE) [Figueira et al., 2005] is a MADM technique that requires a reference vector to be specified by a decision maker to work as ideal alternative. From the reference vector, concordance and discordance matrices are determined for each path alternative. Different versions of ELECTRE exist [Munier, 2011]. ELECTRE-I corresponds to the first specification of ELECTRE and works with the concordance and discordance matrices. Optimal solutions are selected from the outranking matrix. ELECTRE-II is based on ELECTRE-I but employs thresholds to the ordering of alternatives. ELECTRE-III completes ELECTRE-II specification by adding preference and indifference thresholds for the diverse criteria. ELECTRE-IV does not require weights for the different criteria, which is a form of avoiding subjectivity.

Table 4.2: Multiple Attribute Decision Mechanisms (MADM)

Technique	Advantages	Disadvantages
SAW	Simple to employ	Issues with weights, ranking identification
MEW	Simple to employ	Issues with weights, ranking identification
GRA	Can include qualitative criteria	Complexity and criteria requirements associated
TOPSIS	Simple to employ	Ranking abnormality, optimal solution depends on the vector position of alternatives
DiA/SiPiA	Simple to employ	Ranking abnormality, optimal solution depends on the vector position of alternatives
AHP	Can include qualitative criteria	With subjectivity
ELECTRE	Simple to employ	Requires a reference vector
NMMD	Reduces ranking abnormality	Complexity associated, optimal solution depends on the vector position of alternatives
VIKOR	Can be used even if weights are not known	No consistent results
PROMETHEE	Can include stability analysis	Requires too much input, choice of transfer functions, and choice of alternatives

Another MADM mechanism is the Preference Ranking Organization Method for Enrichment Evaluations (PROMETHEE), which works by making comparisons between alternatives and computing the difference, and afterwards applies a transfer function. To establish weights it is necessary to use an evaluation table. Moreover, the transfer function can be based on data characteristics. For instance, if a criterion has uncertainty, then a gaussian function can be employed. PROMETHEE requires more information than ELECTRE [Munier, 2011]. For instance, a decision maker must choose the transfer function and how alternatives are chosen, if based on minimum or maximum values. In addition, several versions of PROMETHEE are specified.

PROMETHEE-I does not compare conflicting alternatives, and only it considers those where a strong preference exists. PROMETHEE-II, as opposed to PROMETHEE-I, performs a complete ranking of alternatives. Moreover, PROMETHEE-II uses a sensitivity analysis to determine if solutions are stable. PROMETHEE-III uses integer linear programming and fuzzy logic to avoid subjectivity. PROMETHEE-IV is a version that is optimized for a large number of path alternatives. PROMETHEE-V uses integer linear programming to select alternatives previously identified by PROMETHEE II and subject to a set of restrictions.

Table 4.2 summarizes the different MADM approaches regarding their advantages and respective issues.

Different methodologies have been followed to evaluate and compare MADM techniques. Numerical analysis is commonly employed to compare techniques. For instance, GRA, TOPSIS, VIKOR, SAW and MEW were compared in 4G networks to improve the performance of VoIP and data applications [Stevens-Navarro and Wong, 2006]. Authors argue that GRA and MEW are tailored for data applications, while the remaining techniques improve the performance of VoIP applications. Following the same approach and envisioning the same techniques, an evaluation in IEEE 802.11 and 3G networks is conducted, considering bandwidth, delay, jitter and bit error rate criteria [Chakraborty and Yeh, 2012]. Results demonstrate that MEW, SAW and TOPSIS have similar performance for conversational, streaming, interactive, and background classes. Nonetheless, GRA is able to provide higher bandwidth and lower delay for interactive and background classes. Researchers point out that SAW has a better performance when compared to TOPSIS. Such type of evaluations formulate conclusions from very narrow evaluations that cannot be extrapolated for most of the path optimization scenarios. Moreover, the effect of weights is also often neglected.

Other kinds of evaluation consider the spearman rank correlation coefficient, which determines the relations between the ranks of variables [Antucheviciene et al., 2011; Chakraborty and Yeh, 2012]. Such kind of evaluation does not formulate any assumption regarding the distribution of data and allows the comparison between two ranks, as expressed in Equation 4.4. Nonetheless, this type of evaluation only considers rank results, and does not asses the effect of weights in the final ranking.

$$\rho = 1 - \frac{6 \times \sum_{i=1}^{I} d_i^2}{I^3 - 1}, \text{with, } i = 1, 2, \cdots, I \tag{4.4}$$

d_i is the difference between the ranks for the decision alternatives

Design of Experiments (DoE) [Montgomery, 2008] is another method to assess efficiency of MADM techniques. For instance, TOPSIS efficiency is assessed in computer-integrated manufacturing technologies [İç, 2012; Sandanayake et al., 2008]. DoE, in comparison to spearman ranking correlation coefficient, considers the effects of weights in MADM evaluation, as different experiments are performed, where each one is configured with the respective weight set.

4.1.2.3 Criteria Weighting

MADM techniques can also be used for criteria weighting, namely Analytic Hierarchy Process (AHP) [Figueira et al., 2005] that does not introduce restrictions on the number of criteria which can include both qualitative and quantitative aspects [Figueira et al., 2005; Mahmoodzadeh et al., 2007]. AHP uses matrices for its operations, where n-criteria are represented in columns and the m-alternatives (the available paths in the path selection problem) correspond to rows. As such, the complexity of AHP is $O\big(m \cdot n\big)$. Nevertheless, the AHP scale is often associated with subjectivity and unbalanced judgments, that is, the importance of the diverse criteria is based on the $\{1, \cdots, 9\}$ scale, which lacks objectivity. Fuzzy AHP combines fuzzy logic with AHP [Sun, 2010], to determine the weights of the different elements objectively. For such, Fuzzy AHP simplifies the AHP scale and maps numbers into linguistic terms, which are easily understood by humans, and avoid the need for experts in the field. Nonetheless, like AHP, Fuzzy AHP does not support consistent judgments [Wang et al., 2010; Mikhailov and Singh, 2003]. Fuzzy Programming Preference (FPP) [Mikhailov, 2003] overcomes this issue, by implementing an alpha-cut technique that enables to test consistency in judgments. The alpha-cut introduces small variations in the fuzzy intervals, allowing to test consistency in a large number space.

Linear Programming Technique for Multidimensional Analysis of Preference (LINMAP) [Srinivasan and Shocker, 1973; Xia et al., 2006] can be used to establish weights for diverse criteria by performing pairwise comparisons. Nonetheless, as a linear technique, it requires adaptation to each path optimization problem. For instance, if a new weight needs to be added, the respective modifications are required.

Decision-Making Trial and Evaluation Laboratory (DEMATEL) [Tseng, 2010] is a MADM technique that also performs pairwise comparisons to generate a direct-relation matrix. The direct-relation matrix corresponds to a causal diagram, that provides a visual representation of the relations between criteria. Nonetheless, this technique does not seem to be as efficient as AHP [Tzeng and Huang, 2011].

4.1.3 Open Issues

Considering the initial goals and requirements, the following issues are identified in the state of the art:

1. Outranking MADM techniques are able to accomplish all the goals established initially. However the outranking schemes have several issues that do not allow to preemptively state that a certain technique performs better than others.
2. Evaluation of MADM techniques is subjective, incomplete or based on metrics that do not enable an objective comparison between different techniques. Moreover, some evaluations do not consider the effect of weights.
3. Subjectivity is often pointed out as a drawback of MADM techniques, namely in the weights determination. Fuzzy logic with Fuzzy Programming Preference (FPP) mitigates such issue, but does not address consistency of weights.

This thesis proposes algorithms to mitigate these issues. First, a criteria weighting algorithm is specified to determine consistent weights; second, an algorithm to perform optimal path selection considering multihoming and Traffic Performance (TP) is introduced. Finally, a methodology to evaluate outranking MADM techniques is specified.

4.2 Taxonomy and Assumptions

This subsection introduces definitions used along this chapter. MeTHODICAL corresponds to the set of algorithms specified in this chapter to perform criteria weighting and path selection optimization.

The term path is considered according to Definition 3.3, previously presented in Chapter 2.

Definition 4.1 (*Relevant Range*)

> *Relevant Range - is an interval where performance of a path criterion is known to be above the average or close to ideal values.*

The relevant range is employed in the path selection optimization algorithm to determine the distance of each path to ideal values (i.e. most performant path).

Different assumptions are assumed in the specification of MeTHODICAL, these include:

- Each node performing path optimization is able to collect the different criteria used in MeTHODICAL.

- For finer and accurate measurement process, nodes and networks need to have synchronization of clocks. For such mechanisms such as Network Time Protocol (NTP) can be employed.

- All the specification of MeTHODICAL is tailored for end-nodes, thus MeTHODICAL is able to improve end-host multihoming.

MeTHODICAL includes a flexible address-interface mapping as it does not assume a *one-to-one* mapping, commonly found on earlier work in this area [Nacef and Montavont, 2008; Dionysiou et al., 2010; Lahde et al., 2010]. The *one-to-one* mapping considers that a physical interface has only a single address. However, the use of virtual interfaces by an operating system breaks this rule. As such, MeTHODICAL formulates optimal path selection according to Definition 3.3, where end-hosts can be identified by IPv6 and IPv4 addresses or other types of identifiers, such as Host Identity Tags [Moskowitz and Nikander, 2006], and can thus support *N-to-one* mappings.

4.3 Weighting Criteria Algorithm

The MeTHODICAL criteria weighting algorithm is described in this section. The respective block diagram is given in Figure 4.2 and all the steps are described in the following subsections.

4.3.1 Hierarchical Structure of Benefits and Costs

MeTHODICAL considers multihoming and Traffic Performance (TP) criteria, organized hierarchically into two types: Benefits – corresponding to all criteria that must be maximized (Figure 4.3) as they provide profit, and Costs – representing all the criteria that must be minimized (Figure 4.4), as they have associated overheads. Such classification complies naturally with optimization problems, as each path has associated its own advantages-benefits and disadvantages-costs.

The top-down approach of organizing criteria hierarchically includes, at the top of the tree, the generic goals that must be achieved (common part of both trees) and, at the bottom layers, the criteria that characterize the generic goals, according to their type. Generic goals include resilience, ubiquity and traffic performance goals. The criteria are derived from two goals that multihoming solutions should support, namely

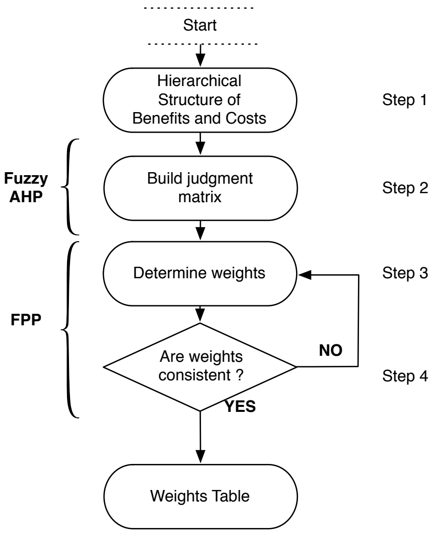


Figure 4.2: MeTHODICAL criteria weighting algorithm

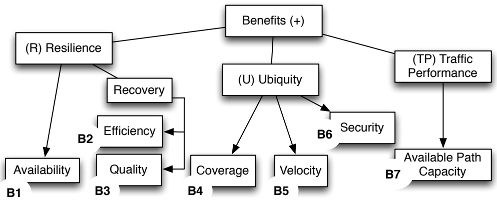


Figure 4.3: Benefits criteria tree

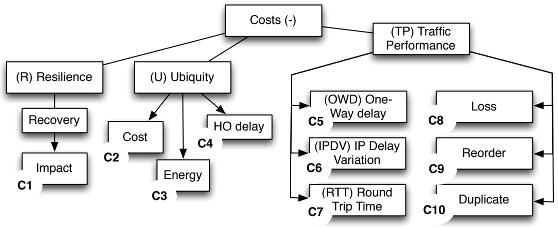


Figure 4.4: Costs criteria tree

resilience and ubiquity, as described in Chapter 2. Higher availability levels and more efficient recovery mechanisms are preferred. Recovery mechanisms that are efficient can recover quickly and maximize quality, establishing the same conditions as before failure. Nonetheless, when recovering, the impact on applications should be minimized (e.g. reduce packet loss). From an ubiquity perspective, extended coverage, stronger and efficient security mechanisms are more interesting. But, as with resilience criteria, ubiquity has also associated costs (e.g. monetary or other, such as power consumption) that should be minimized.

Traffic Performance (TP) criteria include available path capacity, one-way delay, IP delay variation, round trip time, IP packet loss, IP packet reordering and IP packet duplications. TP criteria follow the IP Performance Metrics (IPPM) Internet Engineering Task Force (IETF) working group [Wei and Ansari, 2001] definitions. This way, ambiguity in metric definition is avoided as, for instance, jitter can be interpreted as delay variation or as the variation of signal. Second, standard measurement schemes are specified, which promote deployment and comparison between different mechanisms. For instance, the One-way Active Measurement Protocol (OWAMP) [Shalunov et al., 2006] specifies a full framework to collect and measure TP metrics. Finally, objective criteria units are also specified, which avoids misinterpretation. For instance, available path capacity [Chimento and Ishac, 2008] could be considered in bytes/s or bits/s, but with its specification no doubt exists regarding the bits/s unit. In the benefits type criteria, TP criteria include available path capacity [Chimento and Ishac, 2008]. TP costs criteria type include One Way Delay (OWD) [Guy Almes and Zekauskas, 1999a], IP Delay Variation (IPDV) [Demichelis and Chimento, 2002] and Round Trip Time (RTT) [Guy Almes and Zekauskas, 1999c], Packet Loss [Guy Almes and Zekauskas, 1999b], packet reordering [Morton et al., 2006] and packet duplication [Uijterwaal, 2009]. Some applications, such as Voice over IP (VoIP) can consider also Packet Loss pattern (loss distance) [Koodli and Ravikanth, 2002] to determine Mean Opinion Score (MOS) from the E-model [ITU-T, 2011].

4.3.2 Building the Judgment Matrix

Weights represent the importance of a criterion over another. For instance, resilience can be preferred over ubiquity with 70% or 60% of preference ratio in comparison to 30% and 40% of ubiquity, respectively.

Table 4.3: Used evaluation scale [Wang et al., 2010]

Categories	TFN
Identity (I)	(1,1,1)
Equal (E)	(1,1,2)
Equal+ (E+)	(1,2,3)
Weak (W)	(2,3,4)
Weak+ (W+)	(3,4,5)
Fairly Strong (FS)	(4,5,6)
Fairly Strong+ (FS+)	(5,6,7)
Very Strong (VS)	(6,7,8)
Very Strong+ (VS+)	(7,8,9)
Absolute (A)	(8,9,9)

To express such criteria preferences Analytic Hierarchy Process (AHP) [Figueira et al., 2005] is employed and enhanced by fuzzy logic (Fuzzy AHP [Sun, 2010]) to determine the weights of the different elements objectively, simplifying the AHP scale, that is often associated to subjectivity and unbalanced judgments. With Fuzzy AHP numbers are mapped into linguistic terms, which are easily understood by humans, and thus avoiding the need for experts in the field, as depicted in Table 4.3. In the example considered, resilience can be fairly strong (FS) preferred than ubiquity.

$$\mu(\tilde{x}) = \begin{cases} (x-l)/(m-l), & l \leq x \leq m \\ (u-x)/(u-m), & m \leq x \leq u \\ 0, & \text{otherwise} \end{cases} \tag{4.5}$$

In Fuzzy AHP, criteria weights are obtained through Triangular Fuzzy Numbers (TFNs) that define sets according to the membership function $\mu(\tilde{x})$, defined in Equation 4.5, which is based on l-lower, m-medium and u-upper bounds. The weighting criteria algorithm in MeTHODICAL employs fuzzy sets corresponding to the association of subjective categories and TFN, as specified in Table 4.3. Moreover, reciprocal TFN are determined as follows: $\mu^{-1} = (l, m, u)^{-1} = (1/u, 1/m, 1/l)$ and additional operations with fuzzy numbers are performed according to the fuzzy logic [Sun, 2010]. In the resilience preference example, the reciprocal would be $FS^{-1} = (1/6, 1/5, 1/4)$.

$$\tilde{A} = \begin{bmatrix} 1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n} \\ \tilde{a}_{21} & 1 & \cdots & \tilde{a}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{a}_{n1} & \tilde{a}_{n2} & \cdots & 1 \end{bmatrix} = \begin{bmatrix} 1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n} \\ 1/\tilde{a}_{12} & 1 & \cdots & \tilde{a}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/\tilde{a}_{1n} & 1/\tilde{a}_{2n} & \cdots & 1 \end{bmatrix} \tag{4.6}$$

The judgment matrix corresponds to a fuzzy judgment matrix, $\tilde{A}$, as per Equation 4.6, where a_{ij} is a fuzzy comparison value of dimension *i* to criterion *j*, according to the categories and respective TFN detailed in Table 4.3. The judgment matrix corresponds to the mapping of user preferences and application requirements into multihoming and TP criteria.

$$\begin{array}{c|ccc|} & \textit{Resilience} & \textit{Ubiquity} & \textit{TP} \\ \textit{Resilience} & (I) & (E+) & (FS+) \\ \textit{Ubiquity} & (E+)^{-1} & (I) & (W) \\ \textit{TP} & (FS+)^{-1} & (W)^{-1} & (I) \end{array} \tag{4.7}$$

Equation 4.7 extends the resilience preference example, by also adding a comparison for Traffic Performance (TP) criterion. As such, preference is indicated as follows:

resilience is preferred in comparison to ubiquity and Traffic Performance.

4.3.3 Weights Determination

Fuzzy AHP outputs a vector representing weights of the diverse criteria, but by itself does not assure consistent judgments [Wang et al., 2010; Mikhailov and Singh, 2003], that is no guarantee on the preference of one criterion over others is assured.

$$l_{ij}\tilde{\leq}\frac{w_i}{w_j}\tilde{\leq}u_{ij}\ i=1,\cdots,n-1,j=2,\cdots,n,j>i \tag{4.8}$$

The Fuzzy Programming Preference (FPP) method [Mikhailov, 2003] enables consistent judgments using an alpha-cut technique that introduces small variations in lower and upper TFN limits of each criterion, since $0 \leq \alpha \leq 1$. Consistency and weights are determined according to Equation 4.8, where $l_{ij}(\alpha) = \alpha(m_{ij} - l_{ij}) + l_{ij}$ and $u_{ij}(\alpha) = \alpha(m_{ij} - u_{ij}) + u_{ij}$, with $0 \leq \alpha \leq 1$. Equation 4.8 can be rewritten in another form to establish constraints for lower and upper TFN limits, as depicted in Equation 4.9. Judgments are fully consistent if and only if all alpha-cuts are also consistent.

$$\begin{aligned} w_i - w_j u_{ij}&\tilde{\leq}0, \\ -w_i + w_j l_{ij}&\tilde{\leq}0, \quad i=1,\cdots,n-1,j=2,\cdots,n,j>i \end{aligned} \tag{4.9}$$

Considering Equation 4.9, the lower and upper TFN limits, in a total of $m = n*(n-1)$ constraints can be arranged in a matrix form $Rw\tilde{\leq}0$, where matrix $R \in \Re^{m\times n}$. With such formulation, the m constraints can be combined with d_k - the degree of satisfaction, which establishes thresholds to accept judgments as consistent. For instance, if judgments must be 100% consistent ($d_k = 1$) or only 80% ($d_k = 0,8$). With the several constraints and with the degree of satisfaction an optimization problem can be formulated, in order to maximize the degree of membership λ. FPP solves such optimization via a linear problem, as depicted in Equation 4.10.

$$\begin{aligned} \text{maximize} \quad & \lambda \\ \text{s.t.} \quad & d_k\lambda + R_k w \leq d_k, \\ & \sum_{i=1}^{n} w_i = 1, w_i > 0, i=1,2,\cdots,n \\ & k=1,2,\cdots,2m \end{aligned} \tag{4.10}$$

The solution of this linear problem is a vector (w^*, λ^*), where the first element is the priority vector (corresponding to criteria weights) and the second is the consistency value, which in ideal situations can be equal to d_k - the degree of satisfaction. Considering the resilience preference example, using the procedure described so far and with a degree of satisfaction of 100%, weights are respectively 60%, 30% and 10% for resilience, ubiquity and TP, respectively. Alpha cut can be performed with $\alpha = 0.1$ to accommodate a representative variation of consistency values, λ^*.

4.3.4 Weights Consistency

As stated before, weights are consistent if and only if all alpha-cuts n_{alpha_cut} are also consistent, therefore consistency must also consider the interval judgments of alpha-cuts. As such, interval judgments are consistent when $\lambda^* \geq 1$ leading to $n_{\lambda^* \geq 1}$.

$$CR = \frac{n_{\lambda^* \geq 1}}{n_{alpha\_cut}} \tag{4.11}$$

Algorithm 4.1 - MeTHODICAL Criteria Weighting

```
$\mathbf{b}_B, \mathbf{k}_K \leftarrow 0$ #Initialize weight vectors
$\mathbf{B}_{n,B}, \mathbf{K}_{i,K} \leftarrow 0$ #Hierarchization of criteria
repeat
    $\tilde{A} = \begin{bmatrix} 1 & \tilde{a}_{12} & \cdots & \tilde{a}_{1n} \\ 1/\tilde{a}_{12} & 1 & \cdots & \tilde{a}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/\tilde{a}_{1n} & 1/\tilde{a}_{2n} & \cdots & 1 \end{bmatrix}$
    $\begin{cases} l_{ij}(\alpha) = \alpha(m_{ij} - l_{ij}) + l_{ij} \\ u_{ij}(\alpha) = \alpha(m_{ij} - u_{ij}) + u_{ij}, \; 0 \leq \alpha \leq 1 \end{cases}$ #Alpha-cuts
    $\begin{cases} w_i - w_j u_{ij} \tilde{\leq} 0, \; -w_i + w_j l_{ij} \tilde{\leq} 0, \\ i = 1, \cdots, n-1, j = 2, \cdots, n, j > i \end{cases}$ #Constraints $R \in \Re^{m \cdot n}$
    $\begin{cases} \text{maximize} & \lambda \\ \text{s.t.} & d_k \lambda + R_k w \leq d_k, \\ & \sum_{i=1}^{n} w_i = 1, w_i > 0, i = 1, 2, \cdots, n \\ & k = 1, 2, \cdots, 2m \end{cases}$
    $CR = \frac{n_{\lambda^* \geq 1}}{n_{alpha\_cut}}$ #Consistency Ratio (CR)
until CR=$d$ #Where $d$ is the desired consistency ratio
```

The criteria weighting algorithm in MeTHODICAL introduces the *Consistency Ratio (CR)* metric, which measures the level of consistency from all alpha cuts of the respective judgment. The *CR* is determined according to the Equation 4.11, and allows to assess if the degree of satisfaction is accomplished in all alpha cuts. A judgment is fully consistent when $CR = 1$, which means that the preference of a certain criterion over others is unquestionable and understandable.

The criteria weighting algorithm, summarized in Algorithm 4.1, is executed until the desired consistency ratio has been reached (e.g. 100%). CR is expressed in the range of $[0, 1]$, where 0 means it is accepted any value for consistency, and 1 indicates full consistency of weights.

The criteria weighting algorithm in MeTHODICAL has a complexity in the order of $O\big(mc^{nv}\big)$, considering mc-constraints and nv-variables. This complexity, is mainly associated with the simplex method employed in the linear programming problem [Matouek and Gärtner, 2006].

4.3.5 Criteria Weights for Classes of Service

This subsection describes the applicability of the criteria weighting algorithm to derive weights from ITU-T Y.1541 [ITU-T, 2006] Classes of Service (CoS).

Diverse options could be pursued, when considering classes of service [Stankiewicz et al., 2011]. The IETF model in RFC 4594 [Babiarz et al., 2006] specifies 12 classes, which have been aggregated, later in RFC 5127 [Chan et al., 2008]. Nonetheless, all these classes appear associated with Diffserv mechanisms and do not provide any values (or bounds) regarding TP criteria. Other models, such as IEEE 802.1p [Choi et al., 2007] are associated with specific technologies and also fail to establish limits for TP criteria. The ITU-T Y.1541 [ITU-T, 2006] recommendation specifies 7 classes of service, summarized in Table 4.4, in two types: mandatory, where all parameters should be within bounds; and provisional, where values do not pose stringent requirements. As applicability is envisioned for a full range of applications, MeTHODICAL considers the ITU-T Y.1541 classes of service, because bounds for TP criteria are well defined, and are not tied to any particular technology or architecture.

The preferences for different classes regarding TP criteria are established by considering the purpose of the class (e.g. the service associated with the class), the bounds established for the diverse criteria, and by comparing the different classes. Comparing Class 0 and Class 1, for example, it is noticed that the latter supports higher values of OWD, thus the IPDV criterion is more important, as packet loss is similar. Moreover, between Class 3 and Class 4, delay is restricted with higher bounds, therefore Class 4 gives preference to packet loss. In Class 5, all parameters are unspecified, as such traditional Internet applications are more affected by RTT, and mechanisms to react

Table 4.4: Classes of Service in ITU-T Y.1541, values are based on ITU-T Y.1541 [ITU-T, 2006] and ITU-T G.1050 [ITU-T, 2007].

CoS type	CoS	OWD	IPDV	Packet Loss	Reorder	Description	Services/Applications
Mandatory	**0**	100ms	50ms	10^{-3}	U.[a]	Real-Time, jitter sensitive, high interaction	High quality VoIP and video, Video Teleconference. Multiplayer Interactive Gaming.
	1	400ms	50ms	10^{-3}	U.	Real-Time, jitter sensitive, interaction	VoIP, Video Teleconference.
	2	100ms	U.	10^{-3}	U.	Transaction data, highly interactive	Signalling, lower quality video and VoIP.
	3	400ms	U.	10^{-3}	U.	Transaction data, interactive	Signalling.
	4	1s	U.	10^{-3}	U.	Low loss, short transactions, bulk data	Video streaming.
	5	U.	U.	U.	U.	Traditional Internet Applications	Web Browsing (HTTP), Instant Messaging, Media content downloads.
Provisional	**6**	100ms	50ms	10^{-5}	10^{-6}	Loss sensitive Applications	Television transport, high-capacity TCP transfers, time-division multiplexing.
	7	400ms	50ms	10^{-5}	10^{-6}		Television transport, high-capacity TCP transfers.

[a] U.-Unspecified

to packet losses are widely implemented for this type of applications. Classes 6 and 7 can be related to Classes 0 and 1, as jitter and delay have the same values, respectively. Nonetheless, in Classes 6 and 7 packet loss tolerance is lower, therefore these two classes give preference to jitter and packet loss criteria. The difference relies on the reordering importance for Class 7 applications.

Multihoming and TP criteria are configured by considering two representative configurations: *prefMH*- giving preference to Multihoming goals, with priority for Resilience, Ubiquity and then to TP criteria (i.e. in the same line of the resilience preference example). *prefTP*- gives preference to Traffic Performance criteria and then to

Table 4.5: Weights of Benefits criteria with Multihoming (prefMH) and Traffic Performance (prefTP) preferences.

Pref	Class	Availability	Efficiency	Quality	Coverage	Velocity	Security	Path capacity
prefMH	AP[a]	0.48	0.024	0.096	0.09	0.03	0.18	0.1
prefMH	AC[b]	0.48	0.096	0.024	0.09	0.03	0.18	0.1
prefTP	AP	0.08	0.004	0.016	0.09	0.03	0.18	0.6
prefTP	AC	0.08	0.016	0.004	0.09	0.03	0.18	0.6

[a] AP applies to all classes with 1:1 protection model. [b] AC applies to all classes with 1+1 protection model.

multihoming goals with preference for ubiquity and then to resilience. In both cases, level one benefits criteria are configured identically to level one costs (e.g. resilience, ubiquity and TP).

Moreover, a distinction between the desired protection model is also performed. The (P)-primary backup and (C)-concurrent protection models can lead to different criteria preferences. For instance, it is assumed that the concurrent protection model has preference for recovery efficiency than to recovery quality. Table 4.5 summarizes weights of benefits criteria for (A)-all the classes with (P)-primary backup and (C)-concurrent protection models, for *prefMH* and *prefTP* configuration cases. Weights of TP costs criteria type are depicted in Table 4.6 for *prefMH* and *prefTP* configuration cases. Costs are specific to each class but do not have any difference between the diverse protection models. The following paragraphs present the reasoning to determine such values.

For a judgment matrix $\tilde{A}$ (see Equation 4.6) of 2×2, judgments in extreme positions are not considered, i.e. those that reduce the importance of one criterion over the others (e.g. 90%, 10%). As such, values lying in the middle are chosen. For instance, taking the example of the judgment matrix for resilience sub-criteria, preference is given to (Av)-Availability and then to (Rc)-Recovery. Matrix 4.12 illustrates the logic that is applied to all the criteria in a 2×2 matrix.

$$\begin{array}{c} \\ \textit{Availability} \\ \textit{Recovery} \end{array} \begin{array}{c} \begin{array}{cc} \textit{Availability} & \textit{Recovery} \end{array} \\ \left[\begin{array}{cc} (I) & (W+) \\ (W+)^{-1} & (I) \end{array} \right] \end{array} \tag{4.12}$$

$$w_{Av} = 0.8 \; w_{Rc} = 0.2$$

Table 4.6: Weights of Costs criteria with Multihoming (prefMH) and Traffic Performance (prefTP) preferences.

Pref	**Class**	**Impact**	**Cost**	**Energy**	**HO delay**	**OWD**	**IPDV**	**RTT**	**Loss**	**Reorder**	**Duplicate**
prefMH	0A[a]	0.6	0.048	0.192	0.06	0.020	0.019	0.016	0.018	0.017	0.009
	1A	0.6	0.048	0.192	0.06	0.019	0.020	0.016	0.018	0.017	0.009
	2A	0.6	0.048	0.192	0.06	0.020	0.009	0.018	0.019	0.017	0.016
	3A	0.6	0.048	0.192	0.06	0.020	0.009	0.018	0.019	0.016	0.017
	4A	0.6	0.048	0.192	0.06	0.019	0.009	0.018	0.020	0.017	0.016
	5A	0.6	0.048	0.192	0.06	0.018	0.017	0.020	0.019	0.016	0.009
	6A	0.6	0.048	0.192	0.06	0.018	0.020	0.009	0.019	0.017	0.016
	7A	0.6	0.048	0.192	0.06	0.017	0.020	0.016	0.019	0.018	0.009
prefTP	0A	0.1	0.048	0.192	0.06	0.120	0.114	0.099	0.109	0.104	0.054
	1A	0.1	0.048	0.192	0.06	0.114	0.120	0.099	0.109	0.104	0.054
	2A	0.1	0.048	0.192	0.06	0.120	0.054	0.109	0.114	0.104	0.099
	3A	0.1	0.048	0.192	0.06	0.120	0.054	0.109	0.114	0.099	0.104
	4A	0.1	0.048	0.192	0.06	0.114	0.054	0.109	0.120	0.104	0.099
	5A	0.1	0.048	0.192	0.06	0.109	0.104	0.120	0.114	0.099	0.054
	6A	0.1	0.048	0.192	0.06	0.109	0.120	0.054	0.114	0.104	0.099
	7A	0.1	0.048	0.192	0.06	0.104	0.120	0.099	0.114	0.109	0.054

[a] 0A applies to all protection models for CoS0.

For judgment $\tilde{A}$ with 3×3, it is considered that the importance of each criterion over another should be clearly distinct, that is no marginal importance differences between criteria should be given (e.g. one with 10% and other with 5%). The logic applied in the general case of 2×2 matrices is also employed here, thus the values employed in judgments do not rely on extremes, but rather on the middle. Matrix 4.13 demonstrates judgments for sub-criteria of benefits ubiquity type, where preferences occur in the following order: First (Cov)-coverage; Second (Vel)-Velocity; and finally (Sec)-Security.

$$\begin{array}{c|ccc} & Coverage & Velocity & Security \\ \hline Coverage & I & E & E+^{-1} \\ Velocity & E^{-1} & I & FS+^{-1} \\ Security & E+ & FS+ & I \end{array} \tag{4.13}$$

$$w_{Cov} = 0.6 \; w_{Vel} = 0.3 \; w_{Sec} = 0.1$$

The most complex judgments are depicted in Matrix 4.14. The 6×6 matrix compares TP cost criteria, namely One Way Delay (OWD), IP Delay Variation (IPDV), RTT, Loss, Reorder and (Dup)-Duplicate.

$$\begin{array}{c} \\ OWD \\ IPDV \\ RTT \\ Loss \\ Reorder \\ Duplicate \end{array} \begin{array}{c} \begin{array}{cccccc} OWD & IPDV & RTT & Loss & Reorder & Duplicate \end{array} \\ \begin{bmatrix} I & E & E & E & E & E+ \\ E^{-1} & I & E & E & E & E+ \\ E^{-1} & E^{-1} & I & E & E & E+ \\ E+^{-1} & E^{-1} & E^{-1} & I & E & E+ \\ E^{-1} & E^{-1} & E^{-1} & E^{-1} & I & E+ \\ E+^{-1} & E+^{-1} & E+^{-1} & E+^{-1} & E+^{-1} & I \end{bmatrix} \end{array} \tag{4.14}$$

$$w_{OWD} = 0.20 \; w_{IPDV} = 0.19 \; w_{RTT} = 0.18$$

$$w_{Loss} = 0.17 \; w_{Reord} = 0.16 \; w_{Dup} = 0.1$$

To enable a fair judgment between criteria, weights are set according to Matrix 4.14. It is considered that a single criterion should not be disregarded due to the weak importance.

As MeTHODICAL organizes criteria in a hierarchical form, the final weights of criteria must consider all the levels. For instance, the weight for security must consider the weight of ubiquity. Considering the *prefMH* case, the security weight is $w_{Sec} = w_{ubiquity} \times w_{levelSec} = 0.3 \times 0.1 = 0.03$.

4.4 Path Optimization Algorithm

This subsection details the different steps of MeTHODICAL path optimization algorithm, which is summarized in Figure 4.5. The path optimization algorithm corresponds to an enhanced Multiple Attribute Decision Mechanism (MADM) technique.

4.4.1 Measurements

Measurements can be collected in proactive and reactive modes. In a reactive mode, measurements are performed when certain events occur, for instance, a new path is detected or a path is removed. In the proactive mode, measurements are performed at a given frequency. While the former does not introduce overhead in the network or the end-host, which needs to send and process measurement data, it has the disadvantage that it may not provide an up-to-date view of path performance. The second approach introduces signalling overhead, as measurement traffic is generated with

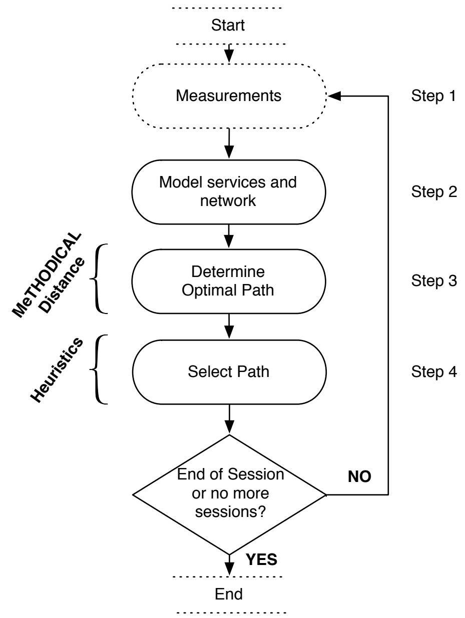


Figure 4.5: MeTHODICAL path optimization algorithm

more frequency, when compared to the reactive approach. Nonetheless, this approach is more accurate, as it provides a complete view of path performance across time.

As stated, the OWAMP framework is proposed to collect TP criteria values. In this framework, measurements follow a proactive approach, where intervals of measurements can be configured to avoid excessive overhead.

4.4.2 Network Modelling

The second step of MeTHODICAL corresponds to the modeling of the network and services. MeTHODICAL models the network as a graph.

The MeTHODICAL network graph is depicted in Figure 4.6, where the source node (S) has multiple applications/services (App1, App2, ...) that can use different available paths ($P_{1,1}$, $P_{1,2}$, $P_{n,j}$, ...) attached to the respective interfaces (IF1, IF2, ...) allowing the connection to the destination node (D). This model is inline with a modern multihoming practice and represents a significant departure from the one-to-one address-interface mapping which up to now has been prevalent in the literature. The MeTHODICAL network model also highlights the different path usage models. For instance, App3 can use paths from distinct interfaces to implement the concurrent model. Moreover, each path has specific multihoming and traffic performance charac-

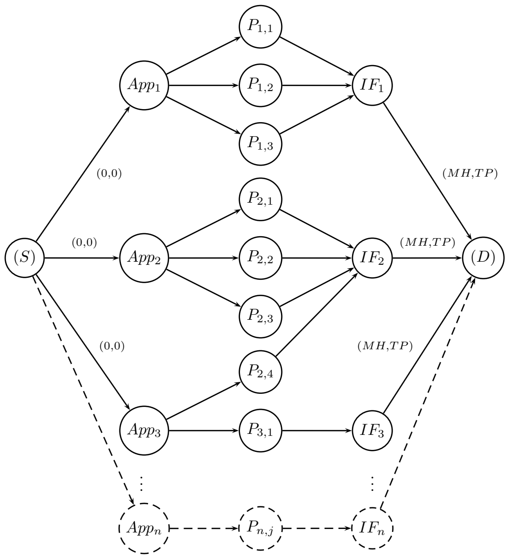


Figure 4.6: MeTHODICAL network model.

teristics, which are derived from the interfaces to which they are linked.

4.4.3 Path Optimization Algorithm

The values of multihoming and traffic performance criteria combine B-benefits and K-costs into $\mathbf{B}_{n,B}$ benefits and $\mathbf{K}_{n,K}$ costs matrices. This step is performed according to the network model, and includes all the available paths. The output of this algorithm is the path ranking score $\mathbf{s}_{i,t}$, which is based on the distances to ideal values.

Commonly, distance is interpreted as the length of space between two points. In this regard, distinct forms of determining distance [Deza and Deza, 2009] exist. The Euclidean distance, used by TOPSIS, defines a line segment between two points. The Manhattan distance or city-block, used by DiA, defines the distance that would be travelled to get from one point to another if a grid-like path is followed. Nonetheless, both distance methods only apply to gaussian data (i.e. follow a normal distribution) and do not consider the path selection problem. Indeed, the traditional interpretation of distance as the length of space is not adequate for problems with multiple criteria, as they introduce high error rates [Lahby et al., 2012]. The Mahalanobis distance overcomes these limitations and uses the covariance to correlate data, which can be gaussian or non-gaussian. Nonetheless, the use of covariance introduces overhead due to its computational complexity, and has only a statistical meaning when high-volume

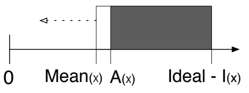


Figure 4.7: Range of Relevant Benefits

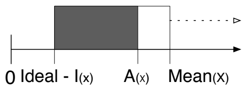


Figure 4.8: Range of Relevant Costs

of data is available.

In the MeTHODICAL path optimization algorithm, distance is abstracted from a space perspective and is considered in a relevant range, as per Definition 4.1. Such relevant ranges establish bounds based on the type of criteria, as illustrated in Figure 4.7 and Figure 4.8 for benefits and costs, respectively. The function $A(X)$ determines the range where performance of a path criterion (e.g. path capacity) is known to be above average or close to ideal values. For benefits the ideal values correspond to the maximum value of benefits $max(X_i)$, while for costs they correspond to the minimum value of costs $min(X_i)$. For such, $A(X)$ relies on the arithmetic mean and variance functions. $A(X)$ depends on the type of criteria; for B-benefits in the $\mathbf{B}_{n,B}$ matrix it is formulated according to Equation 4.15, and for K costs in the $\mathbf{K}_{n,K}$ matrix it is determined as per Equation 4.16.

$$A(\widehat{\mathbf{B}}_j) = m(\widehat{\mathbf{B}}_j) + v(\widehat{\mathbf{B}}_j);\ m(), v() \text{ are mean and variance} \tag{4.15}$$

$$A(\widehat{\mathbf{K}}_j) = m(\widehat{\mathbf{K}}_j) - v(\widehat{\mathbf{K}}_j);\ m(), v() \text{ are mean and variance} \tag{4.16}$$

The proposed distance, determined according to Equation 4.17 for a criterion i, introduces correlation by using simple functions, such as minimum, maximum, arithmetic mean and variance functions. Ideal values are determined by the $I(X)$ function and Φ value relies on input data, herein $\Phi = 0.01$.

$$\Delta(\widehat{\mathbf{M}}_i) = \sum_{j=1}^{B} \left[\frac{[I(\widehat{\mathbf{M}}_j) - \widehat{\mathbf{M}}_{i,j}]^2}{[I(\widehat{\mathbf{M}}_j) - A(\widehat{\mathbf{M}}_j)] + \Phi} \right] \tag{4.17}$$

The MeTHODICAL distance is lower for values close to ideal and within relevant ranges, and is higher for values far away from ideal and outside relevant ranges. Moreover, the proposed distance has the following advantages:

Correlation Correlates path criterion values using functions based on arithmetic mean, variance, minimum and maximum functions, that do not impose any restriction regarding the volume of data, as happens with covariance in the Mahalanobis distance [Lahby et al., 2012].

Gnostic Considers the type of criteria, and for each type determines the respective relevant ranges.

Algorithm 4.2 details the different phases of the path optimization algorithm. As a MADM technique, common principles with DiA [Tran and Boukhatem, 2008] and NMMD [Lahby et al., 2012] can be found.

Algorithm 4.2 - MeTHODICAL path optimization

```
Require: $\sum_j^B \mathbf{b}_j = 1$ #Benefits weights vector
Require: $\sum_j^K \mathbf{k}_j = 1$ #Costs weights vector
Require: $\sum_i^m \sum_j^B \mathbf{B}_{i,j} \geq 0$ #Benefits matrix
Require: $\sum_i^m \sum_j^K \mathbf{K}_{i,j} \geq 0$ #Costs matrix
Require: $\mathbf{s}_{i,(t-1)} = 0$ #Initialize Score vector for $(t)ime - 1$
$\overline{\mathbf{N}_{ij}} = \frac{\mathbf{M}_{i,j} - min(\mathbf{M}_{n,m})}{Max(\mathbf{M}_{n,m}) - min(\mathbf{M}_{n,m})}, i = 1, \cdots, n$ #Normalization
$\widehat{\mathbf{G}}_{i,j} = \mathbf{n}_j \times \overline{\mathbf{N}_{ij}}$ with $i = 1, 2, \cdots, n$ and $j = 1, 2, \cdots, m$
$I(\widehat{\mathbf{B}}_j) = max\{\widehat{\mathbf{B}}_{i,j} | i = 1, 2, \cdots, n\}$ #Ideal Benefits solution
$I(\widehat{\mathbf{K}}_j) = min\{\widehat{\mathbf{K}}_{i,j} | i = 1, 2, \cdots, n\}$ #Ideal Costs solution
$\Delta(\widehat{\mathbf{B}}_i) = \sum_{j=1}^{B} \left[ \frac{[I(\widehat{\mathbf{B}}_j) - \widehat{\mathbf{B}}_{i,j}]^2}{[I(\widehat{\mathbf{B}}_j) - A(\widehat{\mathbf{B}}_j)] + 0.01} \right] A(\widehat{\mathbf{B}}_j) = m(\widehat{\mathbf{B}}_j) + v(\widehat{\mathbf{B}}_j)$
$\Delta(\widehat{\mathbf{K}}_i) = \sum_{j=1}^{K} \left[ \frac{[I(\widehat{\mathbf{K}}_j) - \widehat{\mathbf{K}}_{i,j}]^2}{[I(\widehat{\mathbf{K}}_j) - A(\widehat{\mathbf{K}}_j)] + 0.01} \right] A(\widehat{\mathbf{K}}_j) = m(\widehat{\mathbf{K}}_j) - v(\widehat{\mathbf{K}}_j)$
$\mathbf{s}_i = \sqrt{\alpha \times \Delta(\widehat{\mathbf{B}}_i) + (1 - \alpha) \times \Delta(\widehat{\mathbf{K}}_i)}, \ i = 1, 2, \cdots, n$
$\mathbf{s}_{i,t} = \mathbf{s}_i + v\big(\mathbf{s}_i, \mathbf{s}_{i,(t-z)}\big), \ i = 1, \cdots, n$ #Set current score
$\mathbf{r}_i = order\big(\mathbf{s}_{i,t}\big)$ #Vector in crescent order
```

The MeTHODICAL path optimization algorithm has the following phases:

Phase 1 - Matrix normalization with benefits type $\mathbf{B}$ and costs type $\mathbf{K}$ using the Min-Max method, of Equation 4.18 for a matrix $\mathbf{M}$ with n paths and m criteria.

$$\begin{aligned} \overline{\mathbf{N}_{ij}} &= \frac{\mathbf{M}_{i,j} - min(\mathbf{M}_{n,m})}{Max(\mathbf{M}_{n,m}) - min(\mathbf{M}_{n,m})}, \\ &with \ i = 1, 2, \cdots, n \ j = 1, 2, \cdots, m \end{aligned} \tag{4.18}$$

The Min-Max method is able to keep criteria differences. For instance, after normalization it is possible to know which was the criterion with the maximum original value, which does not happen with the vector normalization [Chakraborty and Yeh, 2009]. This phase relies on the $max()$-maximum and $min()$-minimum functions to calculate the normalized matrices $\overline{\mathbf{B}}$ and $\overline{\mathbf{K}}$ for benefits and costs, respectively.

Phase 2 - Weighting of normalized benefits and costs matrices by multiplying the respective weight vectors, $\widehat{\mathbf{B}}_{i,b} = \mathbf{b}_b \times \overline{\mathbf{B}_{i,b}}$ benefits and $\widehat{\mathbf{K}}_{i,c} = \mathbf{k}_c \times \overline{\mathbf{K}_{i,c}}$, with

$i = 1, 2, \cdots, n$, $b = 1, 2, \cdots, B$ and $c = 1, 2, \cdots, K$. This step provides the weighted normalized $\widehat{\mathbf{B}}$ benefits and $\widehat{\mathbf{K}}$ costs matrices.

Phase 3 - Determine the ideal benefits solution, by retrieving the vector with the maximized values of benefits criteria, $I(\widehat{\mathbf{B}}_j) = max\{\widehat{\mathbf{B}}_{i,j} | i = 1, 2, \cdots, n\}$ for n paths and m criteria. Ideal solutions, in this case, correspond to those that provide more profit.

Phase 4 - Determine the ideal costs solution, by retrieving the vector with the minimized values of costs criteria, $I(\widehat{\mathbf{K}}_j) = min\{\widehat{\mathbf{K}}_{i,j} | i = 1, 2, \cdots, n\}$ for n paths and m criteria. Ideal solutions, in this case, are those that have a minimum overhead.

Phase 5 - The MeTHODICAL distance, Equation 4.17, is used to determine the distance of each path to the ideal solution. $\Delta(\widehat{\mathbf{B}}_i)$-distance of benefit criteria $\widehat{\mathbf{B}}_{i,j}$ to ideal benefits solution $I(\widehat{\mathbf{B}}_j)$ is determined according to Equation 4.17, for B-benefits.

Phase 6 - Determine $\Delta(\widehat{\mathbf{K}}_i)$-distance of cost criteria $\widehat{\mathbf{K}}_{i,j}$ to ideal costs solution $I(\widehat{\mathbf{K}}_j)$ according to Equation 4.17, for K-costs of each path.

Phase 7 - Assign scores to each path ($\mathbf{s}_i$) through the combination of distances to the ideal solutions, as per Equation 4.19 for n-paths. α enables the differentiation between the distance of benefits and the distance of costs. For instance, with α the ranking can mainly be based on benefits or costs, and $\alpha \in]0, 1]$. $\alpha = 0.5$, is the recommended value for balancing benefits and costs in the final ranking.

$$\mathbf{s}_i = \sqrt{\alpha \times \Delta(\widehat{\mathbf{B}}_i) + (1 - \alpha) \times \Delta(\widehat{\mathbf{K}}_i)} \tag{4.19}$$

Optimal paths have lower score values, as distance is closer to ideal values $\Delta(X) = 0$.

Phase 8 - Set score for current time (t) for each path. Variance function $v(x)$ is employed to allow scoring stability, considering previous z and current scores $\mathbf{s}_{i,(t-z)}$ and $\mathbf{s}_{i,t}$, respectively. If $v\big(\mathbf{s}_{i,(t-z)}, \mathbf{s}_{i,(t)}\big)$ is equal to zero, such path is stable, otherwise the path can have difference in its conditions (e.g. bursts in packet loss or delay).

Phase 9 - Ranking is obtained by ordering the score vector for current time $\mathbf{s}_{i,t}$ in a crescent order $\mathbf{r}_i = order(\mathbf{s}_{i,t})$. The optimal solution is the one with the lowest score, as it is closer to the ideal solution.

The complexity of MeTHODICAL path optimization algorithm is $O\big(m \cdot n\big)$, as it performs operations in $m \cdot n$ matrices composed by m paths passive of selection and the n criteria (benefits plus costs).

4.4.4 Path Selection

The final step of MeTHODICAL is the selection of a path according to the required protection model and respective ranking of optimal paths.

Table 4.7: Heuristics summary

Heuristic	Mode	Nodes	Description
$\mathbf{h}_1(r)$	all	≥ 2 paths	Maximize resilience.
$\mathbf{h}_2(p)$	1+1	all	Keep one of the paths in the set.
$\mathbf{h}_3(i)$	all	all	Minimize interface changes.

MeTHODICAL is flexible to incorporate heuristics seeking different goals (e.g. increase resilience, improve overall performance) and adapted to a particular protection model, as depicted in Table 4.7.

The $\mathbf{h}_1(r)$ heuristic allows applications to choose a path, with the constraint of maximizing resilience. A failure on a physical interface affects all paths operating on it, therefore $\mathbf{h}_1(r)$ can maximize resilience by selecting paths from different interfaces. This heuristic has particular interest on nodes where multiple paths are operating on a single physical interface, but it is also useful when there are multiple paths available. This heuristic adds complexity to MeTHODICAL in the order of $O(m{\cdot}n)$, since lookup operations must be performed to find a new path with a distinct interface (if existing).

$\mathbf{h}_2(p)$ is a heuristic only applicable to the concurrent alternative. With this heuristic, one of the paths in the current set is selected to be used in the new set. For instance, if the current set includes a IEEE 802.11 (WiFi) path and a 3GPP Long Term Evolution (LTE) path, the next set must contain one of them. The main purpose of this heuristic is to avoid session disruption, since moving sessions to new paths, and possibly to new interfaces, typically introduces more cost. Such heuristic adds complexity to MeTHODICAL in the order of $O(m \cdot n)$, as lookup operations are needed to find a new set with one of the previous paths.

The $\mathbf{h}_3(i)$ heuristic optimizes path selection in order to minimize the cost associated with the interface change. This metric is the opposite of $\mathbf{h}_1(r)$, as another path can be chosen to avoid moving to a new interface. This heuristic also introduces complexity, in the order of $O(m \cdot n)$, as search operations must be performed to find a path that relies on the same interface.

Path selection in MeTHODICAL can be enhanced with heuristics to meet different application requirements, as demonstrated with the proposed heuristics.

4.5 MADM Accuracy Evaluation Framework

This section specifies an evaluation methodology for MADM techniques that allows to assess the accuracy of a Multiple Attribute Decision Mechanism. With the MADM accuracy evaluation framework it is possible to compare MADM techniques more efficiently and without relying on sub-representative evaluation metrics, such as handover ratios, in the path selection problem.

The MADM accuracy evaluation framework employs Design of Experiments (DoE), also known as experimental design, [Montgomery, 2008], which allows to plan experiments, in such a way that facilitates analyses and conclusions. DoE has different techniques to promote analyses, specifically the 2^k factorial design to assess the effect of several variables over a response. In the path selection problem, the several variables include benefits and costs criteria, and the response corresponds to the path score of a MADM technique. In detail, the 2^k factorial design specifies full factory experiments for the k main effects, $(\frac{k}{2})$ two-factor interactions, $(\frac{k}{3})$ three-factor interactions, and so on, in a total of $2^k - 1$ effects. By applying full factorial, a decision matrix is obtained for the k effects, considering two levels: (-) representing the minimum values and (+) the maximum values.

Table 4.8: Decision matrix for 3 criteria with 2^k factorial design.

Id	x_1	x_2	x_3	**Effect**
1	-	-	-	(1)
2	+	-	-	x_1
3	-	+	-	x_2
4	+	+	-	x_1x_2
5	-	-	+	x_3
6	+	-	+	x_1x_3
7	-	+	+	x_2x_3
8	+	+	+	$x_1x_2x_3$

Table 4.8 exemplifies the decision matrix for 3 factors (x_1, x_2, x_3), considering a 2^k factorial design. The n^k factorial design considers n levels of the criteria. In the path selection problem with 3 paths, the n levels can correspond to the maximum values of the diverse criteria, $max_{p1}(x1)$, $max_{p2}(x1)$, $max_{p3}(x1)$ and so on.

Algorithm 4.3 - MADM accuracy evaluation framework

```
Require: $D_n[m,k]$ #$n$ Decision matrices for $n$ paths with $m$ measurements and $k$ criteria
$m(D_j) = min\{D_i[,j] \; |i = 1,\cdots,n; \; j = 1,\cdots,k\}$ #Minimum level (-) for criterion $j$
$M(D_j) = max\{D_i[,j] \; |i = 1,\cdots,n; \; j = 1,\cdots,k\}$ #Maximum level (+) for criterion $j$
if $m(D_j) \neq 0$ and $M(D_j) \neq 0$ then
    $a = 2^k$ #Follow $2^k$ factorial design
    $F_{a,k} = \binom{a}{2}$ with $m(D_j)$ and $M(D_j)$ levels #Factorial design matrix
else
    $a = n^k$ #Follow $n^k$ factorial design
    $\widehat{M}(D_j) = \left[max(D_1[,j]),\cdots,max(D_n[,j])\right] \; with \; j = 1,\cdots,k$
    $F_{a,k} = \binom{a}{n}$ with $\widehat{M}(D_j)$ levels #Factorial design matrix
end if
$W_{z,k} = \{W_{i,j}|i,\cdots,z; \; j = 1,\cdots,k;$ and $\sum W_j = 1\}$ #Set weights matrix for $z$ experiments
$I_{a,k+z} = \begin{array}{c|ccccccc|} & k_1 & \cdots & k_k & z1 & z2 & \cdots & z_z \\ 1 & e_{1,1} & \cdots & e_{1,k} & s_{1,k+1} & s_{1,k+2} & \cdots & s_{1,k+z} \\ 2 & e_{2,1} & \cdots & e_{2,k} & s_{2,k+1} & s_{2,k+2} & \cdots & s_{2,k+z} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ a & e_{a,1} & \cdots & e_{a,k} & s_{a,k+1} & s_{a,k+2} & \cdots & s_{a,k+z} \end{array}$ #Input matrix with $s_{a,z}$ score
$s = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \epsilon$ #Run ANOVA for $s$
$o = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_{1,2} x_1 : x_2 \epsilon$ #Run ANOVA with p-value $< 0.05$
$R^2$ and F-statistic and p-value #Perform statistical analysis
```

With the results of several experiments, s (score), the response variable, can be estimated through a regression model, as depicted in Equation 4.20, where x_1, x_2 and, x_3 represent effects/criteria, β_0 is the intercept coefficient, β_1, β_2 are effect coefficients and σ is the error estimate. Experiments are based on the same criteria values (+) and (-) levels, but with different weight sets.

$$s = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_1 x_2 + \beta_5 x_1 x_3 + \beta_6 x_2 x_3 + \beta_7 x_1 x_2 x_3 + \epsilon \tag{4.20}$$

Analysis of Variance (ANOVA) applies regression to formulate a linear model in the form of the Equation 4.20 and has associated statistical values that determine the efficiency of the model. Such statistical values include the goodness of fit and F-statistic. The goodness of fit can be assessed by the coefficient of determination R^2, which corresponds to the total variance in response variable (s) due to effects/criteria. Higher values of R^2, close to one, indicate that the model explains almost 100% of the variation in s due to the effects/criteria and their possible interactions.

The F-statistic is also important to assess the variation between groups and within groups. Such groups represent the different experiments. For instance, higher values of the F-statistic indicate that mean variation between experiments is greater than variation within experiments. If variation is between experiments, it highlights that the score varies due to the different configured weights.

The MADM accuracy evaluation framework is summarized in Algorithm 4.3. The different phases of the MADM accuracy evaluation framework are detailed in the next paragraphs.

Phase 1 - Gather data of the different paths for each criterion. Such step can be performed in a controlled way or relying on data collected by others, outside control of a researcher employing the proposed accuracy evaluation framework. In this step n decision matrices $D_n[m, k]$ are obtained, with m measurements for the n paths with k criteria.

Phase 2 - Determine the levels of each criterion for the diverse paths. Levels correspond to the minimum, min_j, and maximum, max_j, for path i in the n overall paths. $m(D_j)$ corresponds to the minimum level (-) while $M(D_j)$ corresponds to the maximum level (+), and are determined according to Equation 4.21 and Equation 4.22 for the n paths with k criteria, respectively.

$$m(D_j) = min\{D_i[, j]\ |i = 1, \cdots, n;\ j = 1, \cdots, k\} \tag{4.21}$$

$$M(D_j) = max\{D_i[, j]\ |i = 1, \cdots, n;\ j = 1, \cdots, k\} \tag{4.22}$$

This step determines the logic of employing 2^k or n^k factorial design. If there are no zeros in both levels, 2^k factorial design can be followed, otherwise n^k factorial design must be employed. Data with zeros can represent issues in ANOVA, such as outliers. With a 2^k factorial design, the levels correspond to the vectors $m(D_j)$ and $m(D_j)$. On a n^k factorial design, $\widehat{M}(D_j)$, the levels for criteria j are based on the maximum (+) values for the n paths, assuming maximum values are different from zero, and are determined according to Equation 4.23.

$$\widehat{M}(D_j) = \big[max(D_1[, j]), \cdots, max(D_n[, j])\big]\ with\ j = 1, \cdots, k \tag{4.23}$$

Phase 3 - Determine factorial design matrix $F_{a,k}$, with a relying on the factorial design, $a = 2^k$ or $a = n^k$. For instance, Table 4.8 depicts the combinations of three criteria under 2^k factorial design, resulting in $a = 8$, $F[8, 3]$. If a n^k factorial design is employed considering $n = 3$ for three criteria, it is obtained a $F[27, 3]$ factorial design matrix.

Phase 4 - Specify weights matrix for the different z experiments. Each j criterion in the k criteria has associated a weight. $W_{z,k}$, the matrix with weight sets is determined for the z experiments. Weights define how important a criterion is over another, tailoring the final ranking determined by MADM techniques.

Phase 5 - Run MADM technique for the full set of factors specified in the $F_{a,k}$ matrix with the respective weight sets in the $W_{z,k}$ matrix, for the z experiments. The output of MADM in each experiment is the respective experiment score $s_{a,z}$. Such experiments scores are combined with the full set of factors to form the input matrix $I_{a,k+z}$ as illustrated in Matrix 4.24, where $e_{a,k}$ holds the minimum and maximum levels, determined as follows $e_{a,k} =< m(D_{a,k}); M(D_{a,k}) >$.

$$I_{a,k+z} = \begin{array}{c} \\ 1 \\ 2 \\ \vdots \\ a \end{array} \begin{array}{c} \begin{array}{ccccccc} k_1 & \cdots & k_k & z1 & z2 & \cdots & z_z \end{array} \\ \begin{bmatrix} e_{1,1} & \cdots & e_{1,k} & s_{1,k+1} & s_{1,k+2} & \cdots & s_{1,k+z} \\ e_{2,1} & \cdots & e_{2,k} & s_{2,k+1} & s_{2,k+2} & \cdots & s_{2,k+z} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ e_{a,1} & \cdots & e_{a,k} & s_{a,k+1} & s_{a,k+2} & \cdots & s_{a,k+z} \end{bmatrix} \end{array} \tag{4.24}$$

Phase 6 - Perform ANOVA where the response variable corresponds to the $s_{a,z}$ score determined by the MADM technique according to the diverse covariates (k criteria). The initial linear model must include all the covariates and their possible interactions, as exemplified in Table 4.8 and Equation 4.20 for 3 covariates (x_1, x_2, x_3). Interactions are important as the values of one criterion might be related with the values of other criteria. For instance, the score, besides being based on bandwidth, round trip time and IPDV can be based on a relation between these parameters. Interactions between criteria are important, as they can be typical in path selection problems. For instance, higher bandwidths have associated lower RTT, as well as lower IPDV values.

Phase 7 - Reformulate the linear model by including only the effects that are significant, those with *p-value* < 0.05. Run ANOVA with the reformulated model and validate if assumptions for ANOVA models are fulfilled. Namely the model must comply with normality, homogeneity and independence assumptions [Montgomery, 2008]. Normality assumes that under the same conditions, the observations are normally distributed for each value of X. Homogeneity assumes that the variance for all X values is the same. Independence means that Y values of one observation (X_i) should not influence the Y values for other observations. In DoE, with the factorial design, the independence assumption is assured. The normality assumption can be checked via histograms, where bars must follow the trend of the normal curve. Homogeneity can be checked by plotting the residuals versus the fitted models, determined with ANOVA. If the model complies with normality and homogeneity assumptions, then statistical analysis of the regression model must be performed as detailed in the next step.

Phase 8 - Analyse the model regarding its completeness, if all the criteria are included, as well as interactions. The analysis must also rely on coefficient of determination, R^2, that assesses how the model explains the variance of score and F-statistic that complements R^2 in the sense that it measures if variance is inside experiments or between experiments. F-statistic assesses how a MADM technique deals with weights. Higher values of R^2 (close to one) and higher values of F-statistic are preferred. In addition, the significance of the effects and interactions must be considered. Significant effects indicate strong contribution to the score.

Table 4.9: Summary of performed evaluations

Evaluation	MADM	Type[a]	Criteria[b]	Goals	Evaluation metrics	Scenarios
MADM accuracy	MeTHODICAL, TOPSIS, DiA	A	subset	Accuracy, Weights Impact	R^2, F-statistic	Dropbox, Heterogenous
Analytical	MeTHODICAL, TOPSIS, DiA, NMMD	A	all	all	CRR[c], RHR[d]	Dropbox-A, Dropbox-B, Operator
VoIP quality	MeTHODICAL, TOPSIS, DiA	A	subset, Rscore	all	MOS[e], steadiness of quality	Normal, Wireles
Cloud Testbed	MeTHODICAL, TOPSIS	T	all, faulty server	Accuracy	Transfer time, server usage ratio	Testbed

[a] (A)nalytical; (T)estbed;

[b] all - Benefits and costs criteria proposed by MeTHODICAL; subset - only a set of the proposed MeTHODICAL criteria

[c] Correct Rankings Ratio (CRR)

[d] Required Handover Ratio (RHR)

[e] Mean Opinion Score (MOS)

4.6 Evaluation Methodology

This section details the evaluation methodology of MeTHODICAL. The evaluation of MeTHODICAL has the following goals:

Accuracy Assess the accuracy of the path optimization algorithm in MeTHODICAL, in terms of choosing the optimal path and reducing handover side effects.

Protection models support Assess the support of primary-backup (1:1) and concurrent (1+1) protection models in MeTHODICAL.

Heuristics Determine the performance gain that MeTHODICAL heuristics introduce and their accuracy, in tems of choosing the optimal path and reducing handover side effects.

Weights Impact Determine the impact of benefits and costs distances (α) configurations.

Different evaluations were performed, as summarized in Table 4.9, to accomplish the aforementioned goals.

4.6.1 MADM Accuracy

The MADM accuracy evaluation framework has been applied to assess the accuracy of MeTHODICAL, in two distinct scenarios: *Dropbox* and *Heterogenous* scenarios, which are described bellow. These scenarios use the same criteria for benefits and costs, as well as different measurement mechanisms between scenarios. The full set of benefits and costs criteria specified in MeTHODICAL was not used here to avoid high number of combinations in the n^k factorial design. Instead, a set of representative criteria in path selection problems was chosen [Li et al., 2013]. Benefits include security, coverage and bandwidth. Costs include Round Trip Time (RTT), IP Delay Variation (IPDV) and packet loss.

4.6.1.1 Dropbox scenario

The Dropbox scenario considers a cloud environment where Dropbox services [Drago et al., 2012] were evaluated. The evaluation of this scenario uses data collected from TCP applications in a university campus, accessing Dropbox facilities. The collected traces contain application network performance values, such as RTT, IPDV, packet retransmissions and packet duplicates. The evaluation considers a multihomed node with four distinct paths for a Dropbox service. In addition, data acquisition was outside the control of the candidate, since it was performed by other authors [Drago et al., 2012]. The wireless network is configured by considering one path according to the IEEE 802.11n and the remaining as per the IEEE 802.11g standard. Moreover, the different paths are configured with different security values, to simulate open networks and networks with stronger security mechanisms.

Table 4.10: Levels of each criterion for the different paths in Dropbox scenario. Levels are represented in the form of minimum;maximum

Paths	Benefits Criteria			Costs Criteria		
	security	coverage	bandwidth	IPDV	RTT	Loss
P1	$1;7$	$0;250$	$0;300$	$0.20;00575.31$	$62.48;0171.79$	$0.00;0.40$
P2	$1;7$	$0;100$	$0;054$	$1.50;00999.15$	$46.32;0166.27$	$0.00;0.11$
P3	$1;3$	$0;100$	$0;054$	$0.20;10105.49$	$75.35;5141.21$	$0.00;0.00$
P4	$1;5$	$0;100$	$0;054$	$0.00;01126.61$	$00.00;0259.78$	$0.00;0.18$

4.6.1.2 Heterogeneous scenario

The *Heterogenous* scenario comprises a multihomed node with three available paths, provided through a wired link (IEEE 802.3ab) and two wireless links, namely IEEE 802.11n and IEEE 802.16e. This scenario was under the control of the candidate and includes data acquired during several weeks. To collect criteria values, the OWAMP protocol [Shalunov et al., 2006] was used, specifically with the Owping [Jeff Boote and Anatoly Karp , 2012] and bwctl [Jeff Boote and Aaron Brown , 2012] tools. Such tools implement the OWAMP protocol and enable an accurate data acquisition of RTT, IPDV, packet loss and bandwidth (corresponds to the available path capacity in METHODICAL) criteria. NTP [Mills et al., 2010] was employed to synchronize the clock of machines.

4.6.1.3 Methodology

The different experiments, as per the MADM accuracy evaluation framework, were based on different criteria weights. Weights, for both scenarios, were organized in sets to include a full representation of the possible and most representative combinations $W_{z,k}$. Table 4.12 depicts the different combinations of benefits and costs weights, for the $z = 16$ experiments.

Table 4.11: Levels of each criterion for the different paths in Heterogeneous scenario. Levels are represented in the form of minimum;maximum

Paths	Benefits Criteria			Costs Criteria		
	security	coverage	bandwidth	IPDV	RTT	Loss
P1	$1;7$	$0;54000$	$00.88;16.81$	$0.00;312.0$	$0.00;202.70$	$0.00;0.67$
P2	$1;7$	$0;00250$	$32.27;56.85$	$0.10;006.4$	$1.10;021.60$	$0.00;0.00$
P3	$1;7$	$0;00100$	$89.99;91.26$	$0.00;003.5$	$0.20;021.20$	$0.00;0.00$

Table 4.12: Weights of different experiments

Experiment	$w_{security}$	$w_{coverage}$	$w_{bandwidth}$	w_{IPDV}	w_{RTT}	w_{Loss}
1	0.33	0.33	0.33	0.33	0.33	0.33
2	0.33	0.33	0.33	0.60	0.20	0.20
3	0.33	0.33	0.33	0.20	0.60	0.20
4	0.33	0.33	0.33	0.20	0.20	0.60
5	0.60	0.20	0.20	0.33	0.33	0.33
6	0.60	0.20	0.20	0.60	0.20	0.20
7	0.60	0.20	0.20	0.20	0.60	0.20
8	0.60	0.20	0.20	0.20	0.20	0.60
9	0.20	0.60	0.20	0.33	0.33	0.33
10	0.20	0.60	0.20	0.60	0.20	0.20
11	0.20	0.60	0.20	0.20	0.60	0.20
12	0.20	0.60	0.20	0.20	0.20	0.60
13	0.20	0.20	0.60	0.33	0.33	0.33
14	0.20	0.20	0.60	0.60	0.20	0.20
15	0.20	0.20	0.60	0.20	0.60	0.20
16	0.20	0.20	0.60	0.20	0.20	0.60

The n^k factorial design was chosen, as many parameters had values of zeros in both scenarios. The factorial design matrices rely on maximum values for each criterion of the distinct paths, depicted in Table 4.10 and Table 4.11 for Dropbox and Heterogenous scenarios, respectively. Indeed the matrices for these scenarios were $F_{Drop}[4^6, 6]$ and $F_{Het}[3^6, 6]$. The input matrix $I_{a,k+z}$ for ANOVA considers the defined experiments (Table 4.12) and factorial design matrices. In this evaluation, $I_{Drop}[4^6, 6 + 16]$ and $I_{Het}[3^6, 6 + 16]$ matrices were set for Dropbox and Heterogeneous scenarios, respectively.

4.6.2 Analytical

The analytical evaluation was the most complete, in terms of goals fulfillment and compared techniques, namely MeTHODICAL with TOPSIS [Tong et al., 2004], DiA [Tran and Boukhatem, 2008] and NMMD [Lahby et al., 2012]. Moreover, the performance of MeTHODICAL heuristics is also assessed with different protection models, and different configurations for benefits and costs distances.

The Correct Rankings Ratio (CRR) and the Required Handover Ratio (RHR) metrics were introduces in this thesis. Common evaluations rely on handover ratios or metrics that are specific to scenarios or applications [Stevens-Navarro and Wong, 2006]. CRR assesses the ratio on which a MADM is able to rank the diverse paths in a correct order. For such, CRR establishes the theoretical optimal path vector $\mathbf{o}_n$, which is determined according to Algorithm 4.4. For all benefits and costs criteria, the optimal path is a vector containing the ordered paths, by their identifier. Ordering is performed according to three costs criteria preferences (c_1, c_2, c_3), where c_1=OWD, c_2=IPDV, c_3=Loss, if considering ITU Y.1541 CoS0 applications. If paths are not of the same type, then the first optimal path ($\mathbf{o}_0$) corresponds to the one with the maximum available path capacity, followed by costs criteria preferences.

The RHR metric determines the ratio of handovers required during the evaluation. For such, thresholds based on the limits imposed by applications are considered, if there is an overflow at instant t, then RHR sets for this instant a required handover Γ. For instance, for CoS0 applications the limit of One Way Delay (OWD) is 100ms, $L(OWD) = 100$, as per Table 4.4. In the case of paths of different physical types, for instance, IEEE 802.11g and IEEE 802.11n, RHR considers only the path configured with better benefits, p, (e.g. IEEE 802.11n), and not every path in the matrix of costs $\mathbf{K}_{n,K}$ exceeding the limits.

Algorithm 4.4 - Theoretical Optimal path/Set

```
Require: $\mathbf{B}_{n,B}$ with $B$ benefits and n paths
Require: $\mathbf{K}_{n,K}$ with $K$ costs and n paths
  if paths have same interfaceType then
    $\mathbf{o}_n$ = order($\mathbf{K}_{n,K}$ by=vector($c_1$, $c_2$, $c_3$))
  else
    $\mathbf{o}_0$ = order($\mathbf{B}_{n,B}$, by=availablePathCap)
    $\mathbf{A}_{n-1,K} = \mathbf{K}_{n,K}$, without $\mathbf{o}_0$
    $\mathbf{a}_{n-1}$ = order($\mathbf{A}_{n-1,K}$, by=vector($c_1$, $c_2$, $c_3$))
    $\mathbf{o}_n$ = append($\mathbf{o}_0$, $\mathbf{a}_{n-1}$)
  end if
```

Benefits and costs criteria are configured according to the protection model and the scenario under evaluation. The Dropbox scenario includes clients accessing cloud-based online storage services. The Operator scenario includes services running in the cloud of Portugal Telecom operator. Both scenarios consider all the criteria proposed by MeTHODICAL for path optimization. Therefore, criteria like coverage and velocity are configured according to the theoretical values of the technology under assessment. Moreover, security is configured in a 1-7 scale where stronger security mechanisms have the maximized values, 7, while weak security schemes have low security values. Due to the characteristics of the evaluated scenarios, different evaluation goals were considered in each one. With accuracy and heuristics as common goals, the Dropbox scenario considered the protection models support and heuristics, while the Operator scenario has focused mainly on the weights impact of benefits and costs distances.

Algorithm 4.5 - Required Handover

```
Require: $\mathbf{K}_{n,K}$ with K costs and n paths for iteration i
Require: $p$ with p as preferred path
  $\Gamma = FALSE$
  if $\mathbf{K}[\cdots, “OWD”]$ or $\mathbf{K}[p, “OWD”] > L(OWD)$ then
    $\Gamma = TRUE$
  end if
  if $\mathbf{K}[\cdots, “IPDV”]$ or $\mathbf{K}[p, “IPDV”] > L(IPDV)$ then
    $\Gamma = TRUE$
  end if
  if $\mathbf{K}[\cdots, “Loss”]$ or $\mathbf{K}[p, “Loss”] > L(Loss)$ then
    $\Gamma = TRUE$
  end if
  if $\mathbf{K}[\cdots, “Reorder”]$ or $\mathbf{K}[p, “Reorder”] > L(Reorder)$ then
    $\Gamma = TRUE$
  end if
  return $RequiredHandover$, for iteration i
```

4.6.2.1 Dropbox scenario

The Dropbox scenario considers a cloud environment where Dropbox services [Drago et al., 2012] were evaluated and has already been described in subsection 4.6.1.1, for the MADM accuracy evaluation. Nonetheless, some minor modifications have been performed, to allow a complete evaluation in order to include the different protection models. As such, the wireless environment was configured in two flavors: First, *Dropbox-A* all the paths are configured as per IEEE 802.11n standard; Second, *Dropbox-B* only one path is set according to IEEE 802.11n and the remaining are configured as per IEEE 802.11g standard. As such, the following configurations are considered in the evaluation: $\{n,g,g,g\}$, $\{g,n,g,g\}$, $\{g,g,n,g\}$ and $\{g,g,g,n\}$, where "g" stands for IEEE 802.11g and "n" for 802.11n.

The Dropbox scenario considers TCP applications, according to ITU-Y.1541 [ITU-T, 2006], weights are configured as per Class 7, where high-capacity TCP transfers are included. This class gives preference to path capacity, IPDV, loss and reorder, as per Table 4.4. Thus, the three costs criteria used in Algorithm 4.4 are respectively: $c_1 = IPDV$, $c_2 = loss$ and $c_3 = reorder$.

The Dropbox scenario is also employed to test the concurrent protection model. As four paths are assumed, there is a total of six sets, formed by combining the different paths. The benefits and costs criteria for the sets are derived from the respective paths. For instance, the capacity of a set corresponds to the sum of its path capacities, while the OWD of the set considers the maximum OWD of its paths. As stated, *Dropbox-B* uses different technologies and is employed to assess the performance of MeTHODICAL and its heuristics, namely $\mathbf{h}_2(p)$, that is tailored for the concurrent model.

4.6.2.2 Operator scenario

The Operator scenario includes the cloud testbed of Portugal Telecom, a Telecommunication operator working in Portugal. The cloud configuration [Casimiro et al., 2012] includes physical machines, where several virtual machines are hosted. In addition, each virtual machine is configured with *eth0* and *eth1* Gigabit Ethernet interfaces, and has Debian GNU Linux x86_64 as the operating system.

During the period of one calendar month, the performance of the machines working in the cloud was monitored. Throughout this period, Traffic Performance (TP) data was observed where path capacity, available path capacity (benefits criteria type), OWD, IPDV, RTT, reordering, packet loss and packet duplication (costs criteria type) were gathered using the OWAMP protocol [Shalunov et al., 2006]. The owping [Jeff Boote and Anatoly Karp , 2012] and bwctl [Jeff Boote and Aaron Brown , 2012] tools were used, as previously employed in the heterogenous scenario of the MADM accuracy evaluation. In addition, network conditions were modified via the Linux traffic shaper [Graf et al., 2013], as this tool allows to differentiate interfaces performance via the introduction of packet loss and delay in specific interfaces. These events were randomly assigned to *eth0* or *eth1* interfaces within a frequency of 5 minutes and also lasting 5 minutes. For instance, in instant $t = 5m$, *eth0* could have packet loss of 5%, while *eth1* would be working in normal conditions.

The Operator scenario includes measured data according to IPPM recommendations, providing therefore, a finer control on the evaluation of MeTHODICAL and related approaches. Moreover, the evaluation in this scenario includes diverse configuration of weights for the different types of applications, namely CoS0 and CoS5, and also multiple α configurations of MeTHODICAL. MeTHODICAL 20% and MeTHODICAL 80% explore opposite configurations of α, where the first gives more importance to the results of costs criteria, while the latter to the results of benefits criteria.

4.6.3 VoIP Quality

The evaluation of VoIP quality introduced the application performance criteria, as depicted in Figure 4.9. Since this metric relies on costs criteria, such as packet loss and delay, costs criteria were also reorganized, as illustrated in Figure 4.10, to consider such fact.

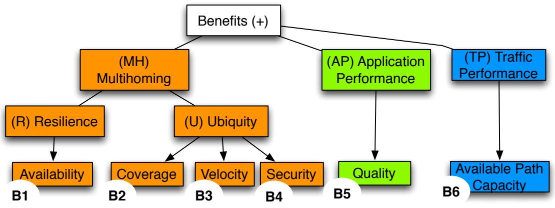


Figure 4.9: VoIP quality benefits tree.

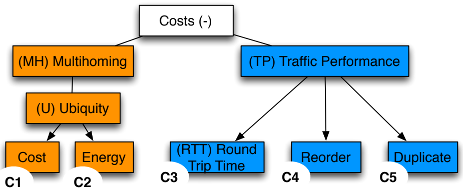


Figure 4.10: VoIP quality costs tree.

Application Performance (AP), namely, VoIP quality can be assessed by a plethora of techniques [Jelassi et al., 2012]. Intrusive methods, like Perceptual Evaluation of Speech Quality (PESQ) [ITU, 2001], are very accurate regarding the determination of quality, but have the disadvantage of requiring both transmitted and received signals to determine quality. Such kind of methodology is only useful for offline analysis. As such, PESQ is not useful for applications that want to estimate quality before transmission and that may have path information for the different paths.

With a before-transmitting perspective, the E-model [ITU-T, 2011] is well-suited for online analysis, as it defines a R factor, based on diverse impairments that account for delay, coded voice signals and loss bit rate effects. In addition, due to its non intrusive nature, it is employed in several works assessing VoIP quality [Li, 2010; Gong, Qipeng and Kabal, Peter, 2011; Halas et al., 2012]. The E-model has been adapted to IP networks [Cole and Rosenbluth, 2001], where the R factor is based on I_d - delay and

I_{e-eff} - bit rate loss impairments, as shown in Equation 4.25.

$$R = 93.4 - I_d(D) - I_{e-eff}(codec, lossRate) \tag{4.25}$$

The delay impairment, I_d, depends on one way delay - D, as per Equation 4.26, where $H(x)$ is a unity or step function, as such H is 0 if $x \leq 0$ otherwise H is 1.

$$I_d = 0.024 \times D + 0.11 \times (D - 177.3) \times H(D - 177.3) \tag{4.26}$$

The bit rate loss impairment, I_{e-eff}, relies on Bpl- packet-loss robustness factor, which depends on the employed codec, as per ITU-T G113. I_{e-eff} is determined in Equation 4.27, where besides packet loss, jitter buffer size and network jitter are included [Halas et al., 2012; Voznak et al., 2012].

$$I_{e-eff} = I_{ef_{opt}} + (95 - I_{ef_{opt}}) \times \frac{Ppl_{ef}}{Ppl_{ef} + Bpl} \tag{4.27}$$

The effect of effective packet loss Ppl_{ef} is determined by considering effective packet loss - *Epl*, jitter buffer size - *JB*, and σ network jitter, as shown in Equation 4.28. *JB* corresponds to the number of packets that buffer can accommodate to mitigate jitter effects: 1 for 20ms; 2 for 40ms and 4 for 80ms of jitter.

$$Ppl_{ef} = Epl + \frac{1 + (\frac{-0.1 \times JB}{\sigma})^{20}}{2} - Epl \times \frac{1 + (\frac{-0.1 \times JB}{\sigma})^{20}}{2} \tag{4.28}$$

The evaluation of VoIP quality considered data collected in the heterogeneous scenario described in subsection 4.6.1.2 for the MADM accuracy evaluation. Three different VoIP codecs are used for this purpose, namely, G.711, G729 and G.723. Moreover, the flexibility introduced in MeTHODICAL to differentiate the importance of costs and benefits criteria is evaluated, considering situations where costs are more important ($\alpha = 20\%$, named as MeTHCost) and situations where benefits are more relevant ($\alpha = 80\%$, named as MeTHBen). MeTHODICAL considers balanced benefits and costs criteria ($\alpha = 50\%$) to promote comparison with NMMD, TOPSIS and DiA. Finally, the capability of the optimization techniques to maintain a stable quality level while adapting to network changes is evaluated.

MeTHODICAL, NMMD, TOPSIS and DiA were assessed in two multihomed scenarios:

➤ A *hybrid* scenario comprising a multihomed node with three available paths, provided through IEEE 802.3ab, IEEE 802.11n and IEEE 802.16e links.

➤ A *wireless* scenario comprising a multihomed node with two available paths, provided through IEEE 802.11n and IEEE 802.16e links.

As stated, both of these scenarios are based on the heterogeneous scenario employed in the MADAM accuracy evaluation. The different multihomed scenarios were employed to assess the performance of VoIP in divergent configurations.

The path selection optimization techniques were compared in both scenarios in two conditions: First, the buffer size (JB) was varied with different values, JB = {1, 2, 4}, to represent situations where the buffers support 20ms, 40ms, and 80ms of voice data. Large buffer sizes tolerate delay variation but may fail to meet one way delay requirement (i.e. bellow 150ms according to ITU-T Y.1540). Finally, failures were introduced with different probabilities (FP): FP = {5%, 10%, 20%}.

The parameters regarding traffic performance on the different paths of each of these scenarios were collected through the OWAMP framework. VoIP application performance was derived from the traffic performance measures as per Equation 4.25.

MeTHODICAL, NMMD, TOPSIS and DiA performance was compared using two evaluation metrics. First, VoIP performance is assessed with the Mean Opinion Score (MOS) as the quality of experience metric. MOS uses a scale with five levels, where 5 stands for excellent, 4 for good, 3 for fair, 2 for poor and 1 for bad quality. Second, the steadiness of the quality provided by each approach was assessed through the quality stability metric, which evaluates how the techniques maintain quality levels throughout each session, as depicted in Equation 4.29, where $QualStability = \frac{q_i}{tot\_iterations}$.

$$q_i = \begin{cases} += 1 & \text{if } S_{i,t} \geq S_{i,(t-1)} \\ += 0 & \text{otherwise, } (q_i = 0 \; when \; t = 0) \end{cases} \tag{4.29}$$

4.6.4 Cloud Testbed

This evaluation was performed in the new cloud infrastructure at Portugal Telecom (PT) Datacenter which is currently a strategic platform for enterprise services and new consumer services. It is based on three main technologies, namely Cisco infrastructure for the networking and computing part, VMWare solutions for virtualization and EMC^2 for storage. MeTHODICAL was integrated in the Trustworthy and Resilient Operations in a Network Environment (TRONE) architecture [Casimiro et al., 2012] to enable fast-reconfiguration of Stream Control Transport Protocol (SCTP) and enhance the multihoming support of nodes with several paths/links. In this context, MeTHODICAL was adapted to include the trace score criterion that corresponds to the output of the anomaly-detection algorithm. This algorithm, also included in the TRONE architecture, determines if a server is facing any kind of failure (e.g. high CPU utilization, no disk space). The trace score works as a cost criterion, since 0 stands for a working server, while 1 stands for a server with failures.

Evaluation considered a communication intensive service [Gamage et al., 2011]. As such, a file transfer service was employed and included transmission of data in different sizes: *CD* (750MB) considers ISO images that could be stored in compact discs. *DVDExtra* (2GB) considers the ISO images that could be stored in DVDs containing both operating system and applications. This way, it was tested a service where the user, paying premium royalties, needs to create virtual machines on request and installs software and additional applications. Redundant and resilient connections to the ISO image files repositories are performed. Redundancy is achieved through the employment of two Gigabit Ethernet links, and resilience is assured by SCTP, which supports a primary-backup protection model out-of the box. For instance, when a failure occurs in an active link/path there is an automatic switch to another working link/path.

Table 4.13: Configuration of failures sets

ID	**Type**	**Server 1**	
		eth0	*eth1*
W1	warning	$l = 5\%$	none
W2		$l = 15\%$	none
W3		$d \approx N(50, 20)$ms	none
W4		$d \approx N(100, 20)$ms	none
C1	critical	down	none
C2		down	$d \approx N(100, 20)$ms
C3		resource fail	

To assess the effectiveness of MeTHODICAL, three types of configurations were considered. The first scenario considers transfer of images, as a regular user. The fast-reconfiguration mechanisms are not active and the standard TCP protocol is used. The second scenario features standard SCTP multihoming mechanisms. The final scenario combines MeTHODICAL, SCTP and includes Ganglia collecting CPU, disk, memory and network usage metrics, to allow anomaly detection and enhanced reconfiguration.

In addition, in each scenario two types of failures were introduced [Nagappan and Peeler, 2011]. The *Critical* failures are configured by activating CPU-intensive, disk-intensive, and memory-intensive applications. The *Warning* failures are configured by introducing high delay or packet loss. More specifically, *Warning* failures are emulated by introducing delay, *d*, (normally distributed, with $\mu = 50$ ms and $\sigma^2 = 20$), and $d \approx N(100, 20)$ms; and packet losses, *l*, (5%, 15%) at the network interfaces of the repository nodes. Configurations where failures are not applied are labelled as *none*. Table 4.13 summarizes the sets of all failures and the interfaces where they have been applied. Resource failures were created to overcharge CPU utilization (in rates $\approx 100\%$), by introducing a high number of computer-intensive processes in the background. Specifically, 1000 processes determining the checksum of the transferred files (CD and DVDExtra) were configured to run concurrently. Checksum was determined employing the *md5sum* utility [Drepper et al., 2013]. During the resource failures, Ganglia reported CPU utilization rates around $\approx 98\%$.

4.7 Results and Discussion

This section discusses the results achieved with the analytical and testbed evaluations performed by the candidate. All the analytical evaluations have been performed using R-project [Team, 2010].

4.7.1 MADM Accuracy evaluation

This section presents and discusses the results achieved with the MADM accuracy evaluation. The linear regression models are compared using model completeness, effects significance, R^2 and F-statistics. The beta terms of ANOVA regression model, as depicted in Equation 4.20, are not specified in the models obtained to simplify comparison between MADM techniques.

4.7.1.1 Dropbox Scenario

The model obtained by TOPSIS and DiA (lmTOPSIS) using the MADM accuracy evaluation framework includes all the criteria, and is specified according to Equation 4.30.

$$Y_{lmTOPSIS} = BW + RTT + Jitter + Loss + Cov \tag{4.30}$$

The lmTOPSIS model is an incomplete model, as it does not include any interaction (e.g. relations between criteria), and defines score as a function of bandwidth, RTT, jitter, loss and coverage (e.g. all criteria).

$$Y_{lmMeTHODICAL} = BW + RTT + Jitter + Loss + Cov + \text{BW:Cov}+ \\ \text{BW:RTT:Cov} + \text{BW:Jitter:Cov} + \text{BW:Loss:Cov} + \text{BW:RTT:Jitter:Cov}+ \\ \text{BW:RTT:Loss:Cov} + \text{BW:Jitter:Loss:Cov} \tag{4.31}$$

MeTHODICAL outputs a different model (lmMeTHODICAL) and besides including all the criteria, it also includes interactions between them, as per Equation 4.31. The lmMeTHODICAL model can be considered as a complete model, in comparison to lmTOPSIS, since criteria and respective interactions are included.

Table 4.14: Results of Dropbox

method	model	signif	interactions	R^2	F-statistic
TOPSIS	lmTOPSIS	yes	no	0.5274	14624.2727
DiA	lmTOPSIS	yes	no	0.4452	10518.2098
MeTHODICAL	lmTOPSIS	yes	no	0.7240	34376.5185
TOPSIS	lmMeTHODICAL	no	yes	0.5274	6093.3300
DiA	lmMeTHODICAL	no	yes	0.4452	4382.2384
MeTHODICAL	lmMeTHODICAL	yes	yes	0.7413	15649.5765

Table 4.14 summarizes the statistical values obtained in the Dropbox scenario. With lmTOPSIS model, the TOPSIS technique can explain $\approx 53\%$ of variation of data, since $R^2 = 0.5274$. DiA is only able to explain $\approx 45\%$ of the variance, nonetheless, MeTHODICAL explains $\approx 72\%$ of the score variance. Values close to 1 are fully explained by the model, therefore are more interesting in terms of statistical meaning. The F-statistic also reports higher values in MeTHODICAL, namely, $F_5 = 34376.5185, p < 0.005$, which means that the variation of score is higher between experiments than within experiments. Thus, MeTHODICAL considers more properly the weights sets configured on the diverse experiments, when compared to TOPSIS or DiA approaches. F-statistic for TOPSIS follows the lmMeTHODICAL model, namely, $F_5 = 14624.2727, p < 0.005$. MeTHODICAL within the lmTOPSIS model is the technique with more satisfactory statistical values, followed by TOPSIS. The main issue with this model is that is lacks interactions, that is, it does not consider the relations between criteria (e.g. if one criterion increases the other criterion will increase as well, or vice-versa). In this context the lmMeTHODICAL model is more complete, mainly due to the enhanced distance function of MeTHODICAL that correlates data criteria

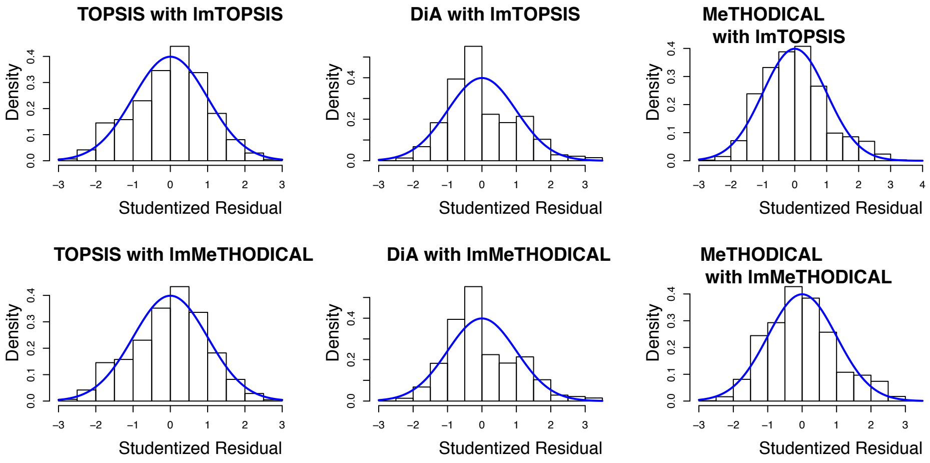


Figure 4.11: Normality for analysed techniques in Dropbox scenario

of the distinct paths.

In the lmMeTHODICAL model, MeTHODICAL presents, again, the best performance regarding statistical values, since R^2 is higher and F-statistic is also higher $F_{12} = 15649.5765, p < 0.005$, in comparison to TOPSIS and DiA results. In addition, when comparing both models, (the main difference relies on the interactions), lmMeTHODICAL model with MeTHODICAL technique is able to explain $\approx 74\%$ of score variance, against the $\approx 72\%$ of lmTOPSIS. F-statistic in the lmMeTHODICAL model is not higher in comparison to lmTOPSIS model, as the model complexity justifies such fact. The former model includes 14 terms in Equation 4.31 while the latter model contains only 5 in Equation 4.30. It is also relevant to point out for the lmMeTHODICAL model that with TOPSIS and DiA not all the effects are significant, which means that these techniques are not able to find relations between criteria.

According to the Phase 7 of the MADM accuracy evaluation framework, assumptions for ANOVA need to be checked, in order to guarantee that the results have high confidence and are statistically significant. Figure 4.11 depicts a graphical test to assess normality of lmTOPSIS and lmMeTHODICAL models within the different MADM techniques evaluated, relying on histograms and normal curve. At a first glance, DiA is the only technique violating normality in lmTOPSIS and lmMeTHODICAL models, which may indicate that the distance or scoring functions perform transformations that break such assumption. MeTHODICAL and TOPSIS are able to present normality in the scoring for both models. In these techniques bars follow the trend of the normal curve (pictured in blue), that is, there is a pattern of ascending and descending “stairs”, without any exception.

The results in this scenario demonstrate that the distance and associated score functions lead to different results, mainly in terms of supporting interactions and statistical importance. MeTHODICAL is the technique that provides the most significant and confident results.

4.7.1.2 Heterogenous Scenario

Similarly to the Dropbox scenario, the model obtained by TOPSIS (lmTOPSIS) is inline with the model obtained by DiA. This scenario included only three paths, as such less data exists in comparison to the Dropbox scenario, $3^6 = 729$ rows when compared to $4^6 = 4096$. Notwithstading, MeTHODICAL is also able to provide interactions, as demonstrated in Equation 4.32. In particular, the lmMeTHODICAL model in the heterogenous scenario is more complete with 14 effects, in comparison to the Dropbox model, which has only 12 effects, as obtained in Equation 4.32 and Equation 4.31.

$$\begin{aligned} Y_{lmMeTHODICAL} &= BW + RTT + Jitter + Loss + Cov + \text{BW:Jitter}+ \\ &\text{BW:Loss} + \text{BW:Cov} + \text{BW:RTT:Cov} \ + \text{BW:Jitter:Cov} + \text{BW:Loss:Cov} + \\ &\text{BW:RTT:Jitter:Cov} + \text{BW:RTT:Loss:Cov} + \text{BW:Jitter:Loss:Cov} \end{aligned} \tag{4.32}$$

Table 4.15: Results of Heterogeneous scenario

method	model	signif	interactions	R^2	F-statistic
TOPSIS	lmTOPSIS	yes	no	0.5352	2684.5152
DiA	lmTOPSIS	yes	no	0.4313	1768.3257
MeTHODICAL	lmTOPSIS	yes	no	0.7514	7046.4885
TOPSIS	lmMeTHODICAL	no	yes	0.5352	958.0181
DiA	lmMeTHODICAL	no	yes	0.4313	631.0595
MeTHODICAL	lmMeTHODICAL	yes	yes	0.7963	3253.4246

Table 4.15 summarizes the statistical values obtained in the heterogenous scenario. With the lmTOPSIS model, the TOPSIS technique can explain $\approx 53\%$ of variation of data, since $R^2 = 0.5352$. DiA is only able to explain $\approx 43\%$ of the variance. MeTHODICAL is able to explain $\approx 75\%$ of the score variance. The F-statistic also reports higher values with MeTHODICAL, namely, $F_5 = 7046.4885, p < 0.005$, meaning that the variation of score is higher between experiments than inside the respective experiment. TOPSIS follows MeTHODICAL performance in terms of the F-statistic. This in-

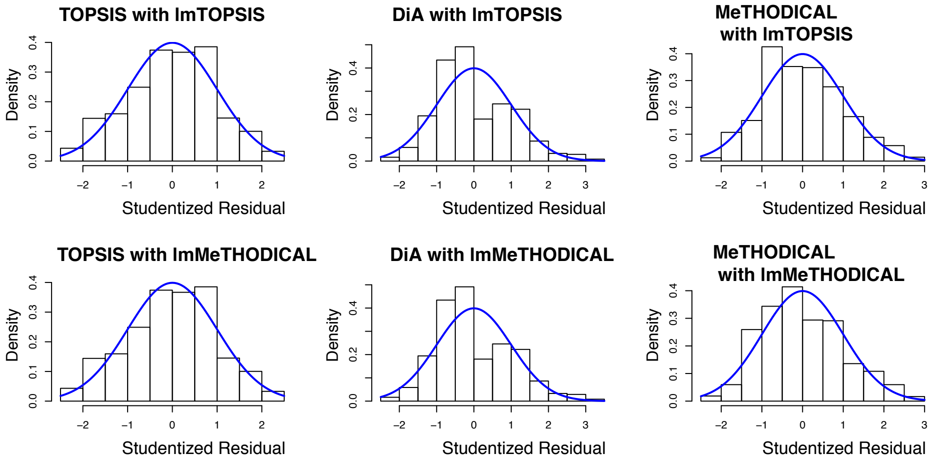


Figure 4.12: Normality for analysed techniques in Heterogeneous scenario

dicates that DiA is the technique that has less impact on scoring regarding the weights configurations. Considering weights as applications preferences (i.e. one might prefer more security while another prefers higher bandwidth), DiA may not provide a scoring adapted to the requirements of distinct applications.

With the lmMeTHODICAL model, MeTHODICAL explains $\approx 80\%$ of score variation. Therefore, contrasting with TOPSIS and DiA techniques that do not increment values of R^2 in the this model.

Figure 4.12 depicts a graphical test to assess normality of lmTOPSIS and lmMeTHODICAL models within the different techniques, relying on histograms and normal curve. With the lmTOPSIS model, normality is supported only by the MeTHODICAL technique, as bars follow the trend of the normal curve (pictured in blue). DiA and TOPSIS techniques present some exceptions to the normality assumption.

The values in the heterogenous scenario regarding R^2 are higher for MeTHODICAL and TOPSIS in comparison to the Dropbox scenario. The reason for such performance increase relies on the complexity of the scenario, from 3 to 4 paths. This fact indicates that TOPSIS and MeTHODICAL adapt more efficiently to the problem size in comparison to DiA. In fact, MeTHODICAL is able to explain $\approx 80\%$ of the values of score with all the criteria and respective interactions.

4.7.2 Analytical

This section discusses the results achieved with the complete analytical evaluation of MeTHODICAL in the Dropbox and Operator scenarios.

4.7.2.1 Dropbox-A scenario

Resuls in the Dropbox-A scenario include the Correct Rankings Ratio (CRR), which is determined according to Algorithm 4.4, and Required Handover Ratio (RHR).

Table 4.16: CRR of *Dropbox-A* in 1:1 - primary and 1+1 - concurrent models

Optimization Technique	**prefTP** (%)		**prefMH** (%)	
	1:1	1+1	1:1	1+1
MeTHODICAL	69.886	71.25	73.558	73.43
NMMD	4.731	0.00	4.515	0.00
TOPSIS	3.953	0.00	3.694	0.00
DiA	3.953	0.00	3.867	0.00
MeTHODICAL $\mathbf{h}_1(r)$	68.935	70.66	72.607	72.78
MeTHODICAL $\mathbf{h}_3(i)$	20.955	16.96	21.905	17.00
MeTHODICAL $\mathbf{h}_2(p)$	–	25.84	–	26.59

Higher values of Correct Rankings Ratio (CRR) are preferable as correct path ranking is performed more frequently. Table 4.16 shows CRR for Dropbox-A scenario with 1:1 – primary-backup and 1+1 – concurrent protection models. Overall, MeTHODICAL performs correct path ranking with higher ratios than the other evaluated techniques, in both protection models. Techniques like NMMD, TOPSIS and DiA do not perform correct ranking in the concurrent model $\approx 0\%$. The reason is related with the increased number of alternatives in the decision process, 6 sets in concurrent model vs. 4 paths in the primary model. NMMD, by correlating data based on the distance of Mahalanobis, is the technique providing the second best value for CRR, after MeTHODICAL.

MeTHODICAL heuristics also impact the correct ranking as they introduce more changes. $\mathbf{h}_1(r)$ heuristic leads to a change in paths when criteria bounds of CoS7 applications are exceeded. This heuristic has almost the same performance of basic MeTHODICAL $\approx 69\%$ and $\approx 70\%$ for 1:1 and 1+1 models, respectively, since OWD, packet loss, jitter and reorder criteria rarely override bounds of CoS7 applications. With the opposite effect, $\mathbf{h}_3(i)$ aims to decrease the number of path changes. As such, CRR values of this heuristic tend to be lower, as path change is only performed if bounds are exceeded. The $\mathbf{h}_2(p)$ heuristic is specific to the concurrent model, and aims to keep one of the paths in the set that was previously selected. This heuristic is more effective than keeping last sets used, as CRR is higher with $\mathbf{h}_2(p)$ in comparison to the $\mathbf{h}_3(i)$ heuristic.

Table 4.17: RHR and Handover ratios of *Dropbox-A* in 1:1 - primary and 1+1 - concurrent models

Optimization Technique	**prefTP** (%)		**prefMH** (%)	
	1:1	1+1	1:1	1+1
RHR	24.368	24.368	24.368	24.368
MeTHODICAL	76.668	82.976	76.366	82.804
NMMD	0.129	11.579	0.604	16.310
TOPSIS	0.043	0.172	7.863	0.388
DiA	0.043	0.129	0.129	0.086
MeTHODICAL $\mathbf{h}_1(r)$	78.893	85.137	78.699	85.007
MeTHODICAL $\mathbf{h}_3(i)$	24.368	24.368	24.368	24.368
MeTHODICAL $\mathbf{h}_2(p)$	–	76.884	–	76.949

In this scenario, the different weight configuration do not introduce changes in CRR. For instance, the values obtained with *prefTP* and *prefMH* cases are very similar. Configuration of MeTHODICAL uses balanced preferences between benefits and costs ($\alpha = 0.5$, in Equation 4.19) and for CoS7 applications this configuration does not introduce impacts in results.

The Required Handover Ratio (RHR) determines the handover ratio, which corresponds to handovers that must be performed in face of an event. These events include moments where criteria bounds of the CoS7 application are overridden. Thus, RHR establishes the correct value regarding handover ratios. Values bellow RHR indicate no reaction and therefore, handovers are not performed even when good conditions are not verified; values higher than RHR demonstrate that handovers are performed more frequently than they should. Table 4.17 depicts RHR and the handover ratios of the different optimization techniques for Dropbox-A scenario with 1:1 and 1+1 protection models. In both models, RHR is $\approx 24\%$, which means that values $< 24\%$, such as those in TOPSIS, DiA and NMMD, indicate that the respective technique does not perform path changes when they are needed. On the other hand, values $> 24\%$, such as those of MeTHODICAL, demonstrate that techniques perform path changes more often than required.

DiA is the technique with the worst performance, as handover ratios are almost null in all the cases. TOPSIS also does not perform path change in most of the cases, with the exception of the 1:1 model in the *prefMH* configuration, where TOPSIS has an handover ratio $\approx 8\%$. These results demonstrate that TOPSIS is inconsistent, as opposed to NMMD, that performs handovers in the 1+1 model for the different weights configurations. Nonetheless, NMMD has no reaction for the 1:1 model ($\approx 0\%$), which means that the correlation of NMMD is not efficient with a low number of path alternatives. If techniques do not adapt to path conditions (e.g. perform handover), then they are not effective, as higher packet loss ratios or long delays in packet delivery can be introduced for CoS7 applications.

MeTHODICAL behaves differently from DiA, TOPSIS and NMMD, as it performs handovers in all the cases and with ratios above RHR. These results of MeTHODICAL can be translated in ping-pong effects, as unnecessary handovers are carried out. Notwithstanding, this drawback can be superseded by the $\mathbf{h}_3(i)$ heuristic, as handovers are performed in the required rate, equally to RHR. As such, this heuristic avoids ping-pong effects and higher packet loss ratios and long delays in packet delivery for CoS7 applications.

4.7.2.2 Dropbox-B scenario

In the Dropbox-B scenario, the path configured according to IEEE 802.11n leads to multiple cases, as it can be configured as the last path {g,g,g,n} or as the first path {n,g,g,g}. In the presented graphics MeTHODICAL is labelled as MeTH for graphical reasons.

DiA and TOPSIS only perform correct ranking in the {g,g,g,n} case, while NMMD only ranks correctly in the {n,g,g,g} case. In the remaining cases, these techniques are not able to select paths correctly, as depicted in Figure 4.13 for primary-backup model. In the concurrent model, as depicted in Figure 4.14, NMMD, TOPSIS and DiA are not able to select optimal paths accurately, just like in the Dropbox-A scenario. Such ranking abnormalities have already been reported for DiA and TOPSIS [Lahby et al., 2012]. Moreover, optimization techniques should be able to determine optimal paths despite the position they have in the decision matrix. MeTHODICAL and respective heuristics are able to select paths in all the cases regarding the path configured as IEEE 802.11n. This fact demonstrates that MeTHODICAL is able to select optimal paths, regardless of the position (e.g. first, second alternative) in the decision matrix, or the envisioned protection model.

Considering the concurrent model, see Figure 4.14, the $\mathbf{h}_2(p)$ heuristics is more

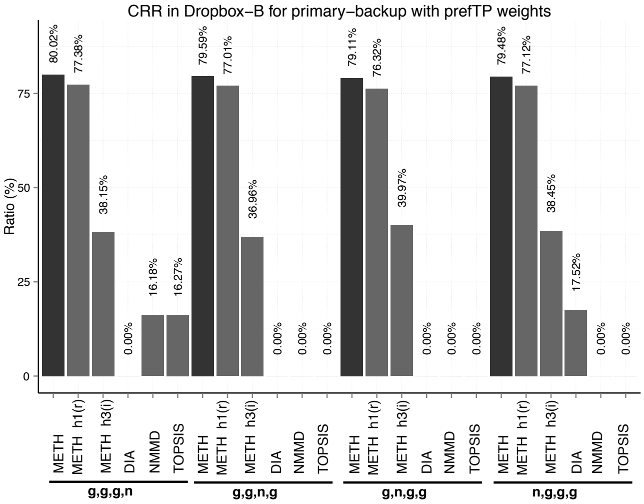


Figure 4.13: CRR for *Dropbox-B* scenario with primary-backup model.

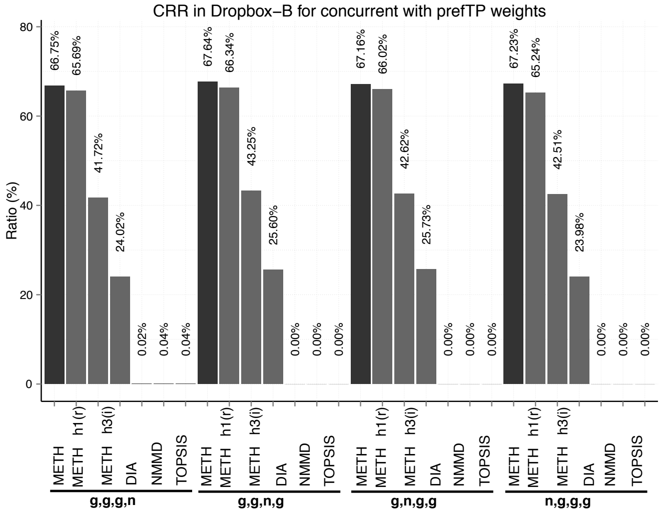


Figure 4.14: CRR for *Dropbox-B* scenario with concurrent model.

efficient than $\mathbf{h}_3(i)$, as CRR is higher for almost all the cases. Thus, keeping a path of the previous set can represent a gain in performance, instead of choosing a set with paths that have not been used yet. CRR results are coherent with those achieved in Dropbox-A for the different protection models. MeTHODICAL is the technique with higher values of CRR in both scenarios.

The different techniques perform distinctly regarding handovers, as Figure 4.15 and Figure 4.16 show for primary-backup and concurrent models, respectively. In

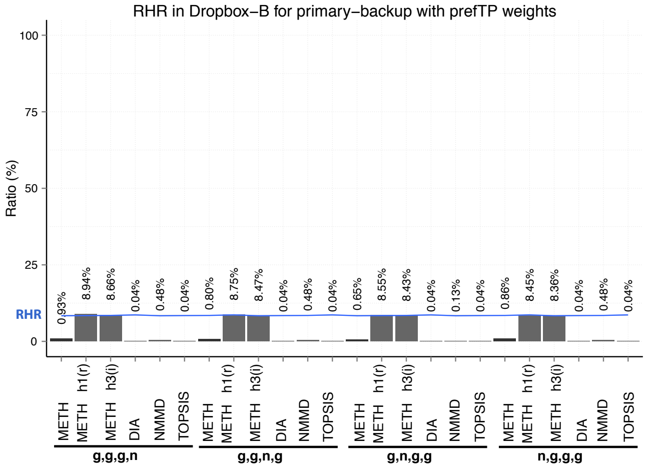


Figure 4.15: RHR and handover ratios for *Dropbox-B* with primary-backup model.

the former model, DiA, TOPSIS and NMMD do not lead to handovers, as ratios are close to null $\approx 0\%$. As such, these techniques can lead applications to experience degradation of quality, as they do not adapt to different conditions. MeTHODICAL in the Dropbox-B scenario for the primary backup protection model has lower handover ratios $\approx 1\%$ and RHR has lower ratios $\approx 8\%$. In the Dropbox-B the need to perform handovers is lower $\approx 8\%$, in comparison to RHR of Dropbox-A scenario $\approx 24\%$. This is justified by the fact that the IEEE 802.11n path has better performance leading to less handovers. The $\mathbf{h}_1(r)$ heuristic introduces the correct number of handovers.

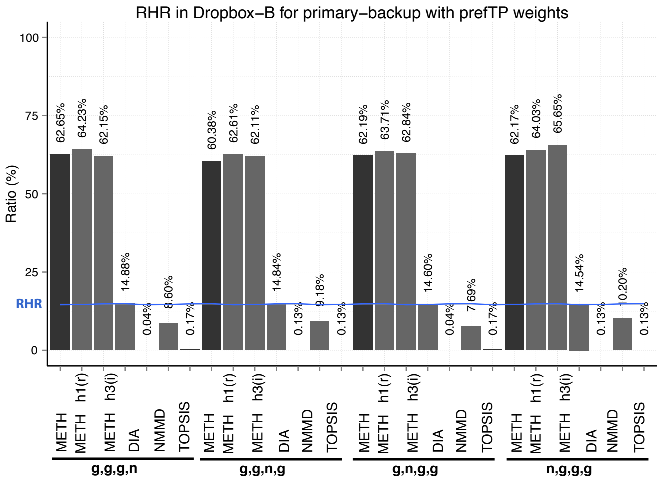


Figure 4.16: RHR and handover ratios for *Dropbox-B* with concurrent model.

In the concurrent model, NMMD, in comparison to DiA and TOPSIS, is the only technique that performs handovers in considerable ratios $\approx 8\%$, no matter the configuration case. Nonetheless, handovers are bellow what is required (RHR). Again, the most performant technique is MeTHODICAL with $\mathbf{h}_3(i)$, which has the correct handover ratio equal to RHR. The difference between primary and concurrent scenarios relies on the number of alternatives. RHR is also higher in the concurrent model $RHR \approx 15\%$ as the IEEE 802.11n path belongs to, at least two sets, leading to a frequent change between these more profitable sets, in comparison to the primary-backup protection model. MeTHODICAL and NMMD consider the number of alternatives, since with increased paths/sets, handover ratios are higher. DiA and TOPSIS do not perform proactively, as handover ratios are equal in 1:1 and 1+1 protection models. The correlation in MeTHODICAL and NMMD justifies such performance gain. Nonetheless, NMMD fails to be efficient with low number of alternatives.

4.7.2.3 Operator scenario

The *Operator* is a simple scenario since it contains only two paths. With this number of paths NMMD cannot be employed, due to the low-volume of data, which does not allow to determine covariance. In addition, this scenario does not include the concurrent model, as only one set could be configured with these paths. This scenario is based on real measurements of traffic performance criteria in the cloud testbed of Portugal Telecom.

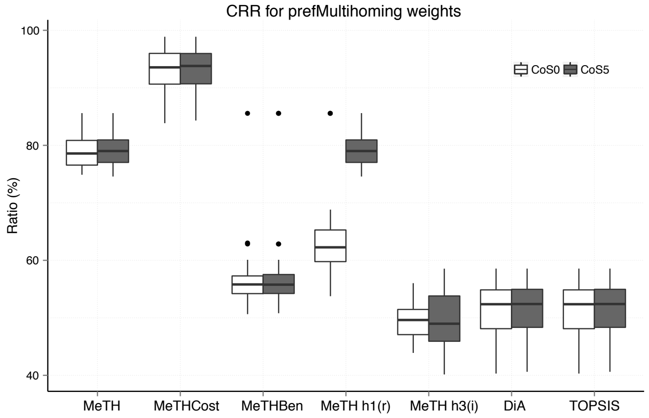


Figure 4.17: Operator scenario CRR for *prefMH* weights

CRR for the operator scenario is depicted in Figure 4.17 and Figure 4.18 for *prefMH* and *prefTP*, respectively. Graphics picture results using boxplots due to the reduced number of cases and to highlight the comparison between CoS0 and CoS5 applications.

MeTHODICAL in all the weights configuration achieves higher CRR, $\approx 80\%$ for CoS0 and CoS5 applications. Both DiA and TOPSIS have the same rate $\approx 50\%$ for both classes. Nonetheless, DiA presents inconsistency, as in *prefTP* configuration with CoS5 applications CRR is higher, which is not verified for *prefMH* case.

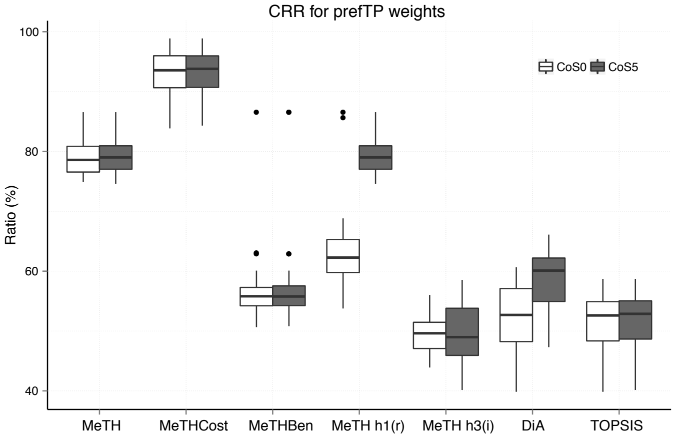


Figure 4.18: Operator scenario CRR for *prefTP* weights

As expected, MeTHCost puts more emphasis on the distance cost, as formulated in Equation 4.17, therefore the optimal paths are selected mainly based on costs criteria. On the opposite side, MeTHBen has lower CRR, as benefits criteria are equal in both paths. This kind of configuration is not possible in DiA, TOPSIS and NMMD techniques. Only MeTHODICAL allows to accentuate the importance of costs or benefits, which represents a gain in scenarios where one of the types of criteria, benefits or costs, are similar in the different alternatives. Moreover, it adds another level of configuration, as weights are specified for each criterion, but no differentiation is possible for the two types of criteria (costs and benefits) with DiA, TOPSIS and NMMD.

Heuristics depend on the type of applications. For instance, CoS0, in comparison to CoS5, is bounded, as such any criteria exceeding bounds will lead to lower scores for $\mathbf{h}_1(r)$ heuristic. Such fact is due to the need to perform path changes more often than with CoS5 applications. The $\mathbf{h}_3(i)$ heuristic has the opposite effect from the $\mathbf{h}_1(r)$ heuristic. It minimizes interface changes, and as such CRR for CoS0 applications is higher, since $\mathbf{h}_3(i)$ keeps the same path.

RHR, determined according to Algorithm 4.5, for each approach is depicted in Figure 4.19 and Figure 4.20, for *prefMH* and *prefTP* configurations, respectively.

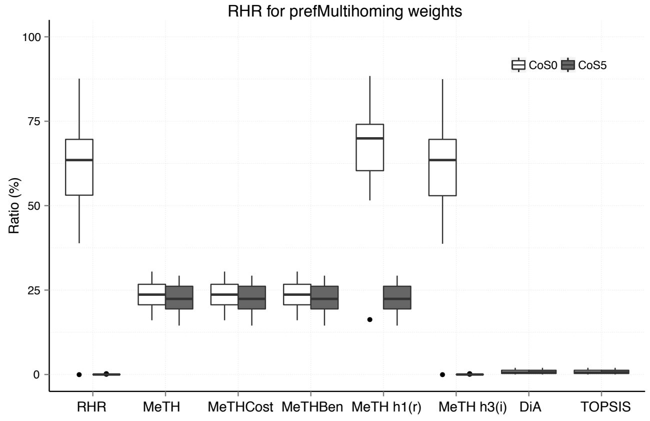


Figure 4.19: Operator scenario RHR and handover ratios for *prefMH*

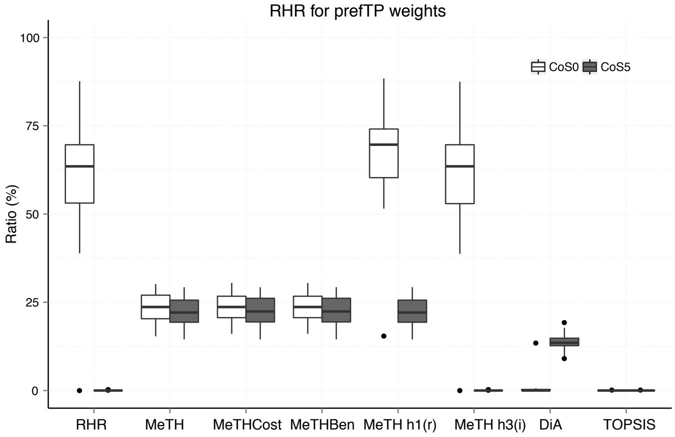


Figure 4.20: Operator scenario RHR and handover ratios for *prefTP*

Handovers depend on the type of application, as RHR is determined by the criteria bounds. As such, CoS0 applications require more handovers, $\approx 60\%$ against $\approx 0\%$ for CoS5 applications. Indeed, techniques like TOPSIS and DiA do not perform any handover in the different cases and applications. These results of TOPSIS and DiA are not correct, as they do not perform handover when they should, i.e. criteria bounds have been exceeded in a certain period of time. MeTHODICAL performs handovers in the different weights configurations, despite not reaching the RHR value. The $\mathbf{h}_1(r)$ heuristic introduces more handovers than the necessary, i.e. above RHR, which means that this heuristic is subperformant for applications that do not tolerate handovers. On the opposite side, $\mathbf{h}_3(i)$ plays the role it was designed for, reducing path changes and,

Table 4.18: Steadiness of quality for the different techniques in the evaluation scenarios

Scenario	MeTHODICAL %			NMMD %			DiA %			TOPSIS %		
	G711	G729	G723	G711	G729	G723	G711	G729	G723	G711	G729	G723
Hybrid[a]	54.69	54.53	54.53	54.95	54.80	54.80	55.63	55.48	55.63	55.63	55.48	55.63
HybridFail[b]	55.80	55.59	55.53	54.59	54.23	54.31	57.50	57.06	57.16	57.50	57.06	57.16
Wireless[a]	53.96	53.81	53.80	—	—	—	54.95	54.79	54.79	54.95	54.79	54.79
WirelessFail[b]	53.69	53.52	53.53	—	—	—	54.39	54.22	54.22	54.39	54.22	54.22

[a] Results with buffer size $JB = 1$ (20ms). [b] Results with Failure Probabilities of 5%.

as consequence, decreasing handover ratios. This heuristic leads MeTHODICAL to perform handovers in the adequated ratio, according to the requirements of applications. For instance, CoS5 applications do not perform handover with this heuristic as RHR is $\approx 0\%$.

4.7.3 VoIP quality

This section presents VoIP quality evaluation of MeTHODICAL and related techniques, NMMD, TOPSIS and DiA, in hybrid and wireless scenarios.

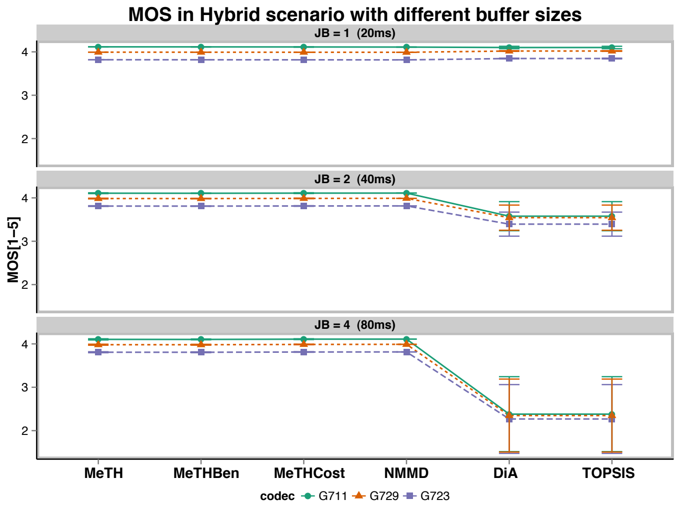


Figure 4.21: MOS for Hybrid scenario with different buffer sizes (JB=1, 2, 4)

Figure 4.21 shows the MOS obtained by the VoIP application, using the G.711, G729 and G.723 codecs, in the hybrid scenario when the buffer size is varied. In this scenario, the different versions of MeTHODICAL and NMMD provide good quality, for all the buffer size configurations and for all the codecs. The behaviours of MeTHBen, MeTHCost and MeTH are coherent for the codecs types, since the G.711 codec achieves the best quality (above 4). However, when the buffer size increases, TOPSIS and DiA result in application performance degradation, as these techniques do not adapt ranking to criteria values. For instance, with JB=4, MOS in some paths has poor quality (≈ 2). TOPSIS and DiA techniques, by choosing paths with lower quality, are slightly more stable than MeTHODICAL and NMMD, as depicted in Table 4.18. MeTHODICAL and NMMD do not choose underperforming paths as optimal, nonetheless these techniques are able to support stability in approximated rates ($\approx 55-56\%$) of TOPSIS and DiA.

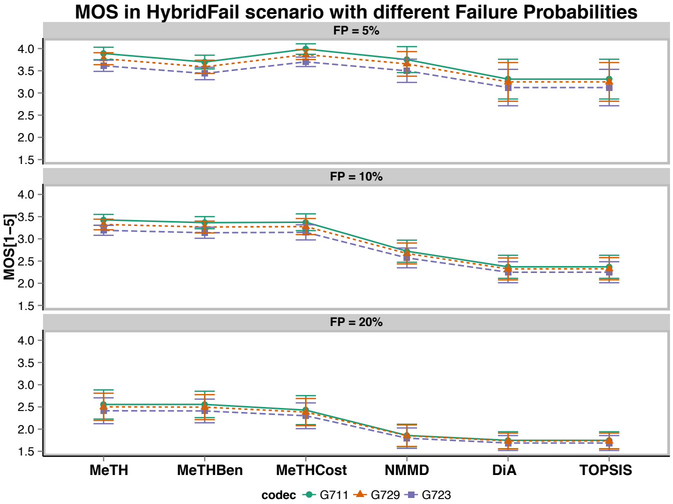


Figure 4.22: MOS for Hybrid scenario with different Failure Probabilities for JB=1

Figure 4.22 shows the MOS obtained by the VoIP application in the hybrid scenario when failures occur with different probabilities. As expected, the G.711 codec is more robust to failures, however, when the failure probability is high ($FP = 20\%$) MOS drops bellow fair levels. The three versions of MeTHODICAL are able to react to the different failures, in comparison to the related approaches. MOS is higher, with fair levels, in MeTHODICAL, MeTHBen and MeTHCost. NMMD has better performance than TOPSIS and DiA, but in $FP = 20\%$ cases, quality falls to bad levels. In terms of application quality, MeTHODICAL and NMMD outperform the DiA and TOPSIS techniques, because they correlate data, which avoids the ranking abnormality that results in the choice of unsuitable paths.

The *wireless* scenario only includes two paths to demonstrate the effectiveness of MeTHODICAL in situations with a minimum number of alternatives. The small num-

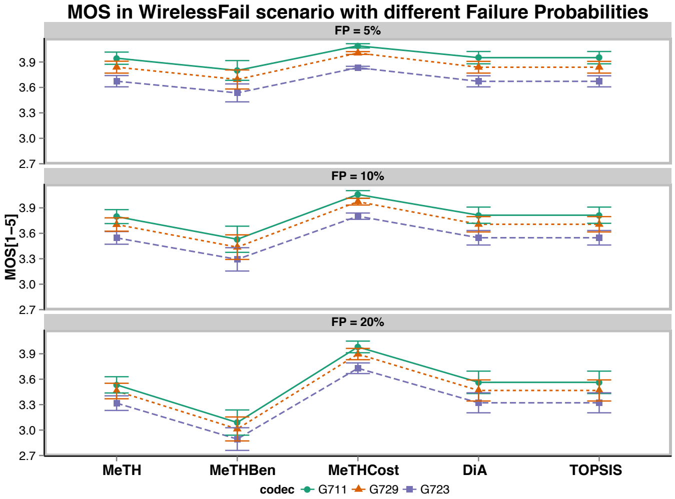


Figure 4.23: MOS for WirelessFail scenario with different Failure Probabilities for JB=1

ber of paths prevents the use of NMMD, which is tied to functions that only have statistical meaning with high volume of data. The performance of this scenario, not pictured, is similar to the hybrid scenario, with MeTHODICAL providing the best quality for all the buffer size configurations. Figure 4.23 shows the application quality for the wireless scenario with different failure probabilities. All the optimization techniques have similar results, since decisions are only about selecting one out of two available paths. However, the results show that the different configurations for costs and benefits in MeTHODICAL provide the desired impact. MeTHCost is able to support higher quality, almost in good levels, as opposed to fair levels of the remaining techniques. The reason for such performance relies on the fact that MeTHCost is configured to put more importance on cost criteria type (80%). Failures impact more costs criteria type, for instance RTT increases, as such any variation in this type of criteria is detected by MeTHCost. In addition, MeTHCost is slightly more stable than the remaining techniques, $\approx 54.5\%$ (value not pictured in Table 4.18). This fact is inline with the MOS performance and is explained by the reduced number of paths to choose as optimal, only two.

The evaluation results presented above have shown the advantages of MeTHODICAL in comparison to the remaining techniques. First, the heterogeneity of scenarios regarding the number of paths, demonstrates that MeTHODICAL is flexible and adapts well to the number of available paths. Second, MeTHODICAL, by correlating criteria values, is able to determine optimal paths, as those supporting higher levels of quality. Related techniques may choose optimal paths as the ones with lower levels of quality. Third, MeTHODICAL adapts well to the different conditions and, at the same time, it is able to keep steady and high quality paths.

4.7.4 Evaluation in Cloud testbed

This section presents and discusses the results achieved in the different scenarios and configurations. Results are discussed for the server usage ratio and for the diverse types of failures introduced in the evaluation.

4.7.4.1 Server usage ratio

Server usage ratio allows to assess the ratio of use for the two used servers. All the failures were configured in server 0. Server usage ratio for CD images is summarized in Table 4.19. All the failures were configured in server 0. This way approaches choosing this server, do not select the optimal server.

Table 4.19: Server usage ratio for CD and DVD images

Case	Server	CD images				DVD images			
		MeTH	TOPSIS	SCTP	TCP	MeTH	TOPSIS	SCTP	TCP
Normal	0	023.31	000.00	100.00	100.00	000.00	000.00	100.00	100.00
	1	076.69	100.00	000.00	000.00	100.00	100.00	000.00	000.00
W1	0	000.00	000.00	100.00	100.00	000.00	000.00	100.00	100.00
	1	100.00	100.00	000.00	000.00	100.00	100.00	000.00	000.00
W2	0	000.00	027.05	100.00	100.00	000.00	000.00	100.00	100.00
	1	100.00	072.95	000.00	000.00	100.00	100.00	000.00	000.00
W3	0	000.00	000.00	100.00	100.00	012.16	000.00	100.00	100.00
	1	100.00	100.00	000.00	000.00	087.84	100.00	000.00	000.00
W4	0	000.00	000.00	100.00	100.00	000.00	000.00	100.00	100.00
	1	100.00	100.00	000.00	000.00	100.00	100.00	000.00	000.00
W5	0	000.00	000.00	100.00	100.00	000.00	000.00	100.00	100.00
	1	100.00	100.00	000.00	000.00	100.00	100.00	000.00	000.00
C1	0	041.32	069.45	100.00	000.00	000.00	065.18	100.00	100.00
	1	058.68	030.55	100.00	000.00	100.00	034.82	000.00	000.00
C2	0	007.77	032.28	100.00	100.00	000.00	053.82	100.00	100.00
	1	092.23	067.72	000.00	000.00	100.00	046.18	000.00	000.00
C3	0	000.02	100.00	100.00	100.00	000.01	100.00	100.00	100.00
	1	099.98	000.00	000.00	000.00	099.99	000.00	000.00	000.00

Warning failure cases, such as the W1-W4 cases only affect one of the paths in the failing server. Therefore, the standard multihoming support of SCTP is able to recover and enable data transfer. TCP as it has no multihoming support has a significative performance degradation, as discussed in the following subsections.

Considering MeTHODICAL and TOPSIS in critical failures cases (i.e. C1-C3 cases) it can be observed that MeTHODICAL is able to use in higher ratios the server with the best performance (server 1). Such different between these approaches is justifiable with the stability and correlation functions of MeTHODICAL.

In the DVDExtra transfer cases, as summarized in Table 4.19, MeTHODICAL has a coherent behaviour regarding the usage ratio of the optimal server in critical failures.

4.7.4.2 Normal - without failures

The evaluation in these scenarios is based on the transfer time with and without failures. In normal conditions (i.e without failures), as depicted in Figure 4.24, the transfer time is almost similar between MeTHODICAL, SCTP and TCP. The difference between the less performant and the more performant is $\approx 3s$ and $\approx 5s$ for CD and DVDExtra cases, respectively.

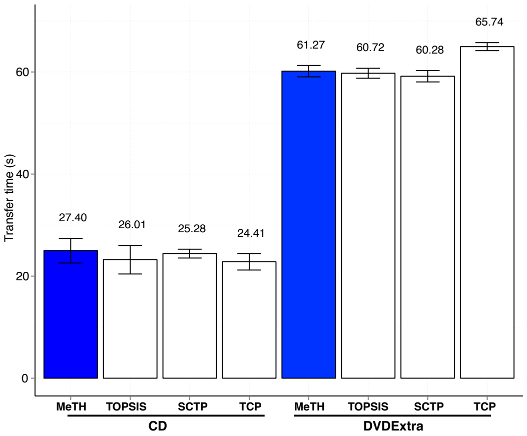


Figure 4.24: Mean transfer time in normal scenario

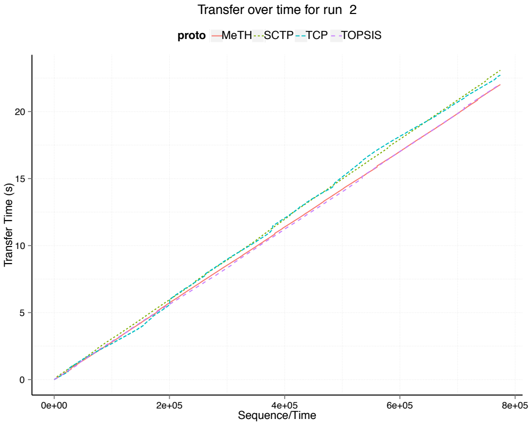


Figure 4.25: Transfer over time in normal scenario for CD images

The transfer time is $\approx 25s$ and $\approx 62s$ for CD and DVDExtra cases, respectively. This scenario is used as a reference regarding the transfer time performance, establishing acceptable limits for file transfer. For CD images the acceptable range is considered $]0; 1.5 * 25] =]0; 37.5]$ and for DVDExtra as $]0; 1.5 * 62] =]0; 93]$. Acceptable ranges are configured to limit performance degradation above 50% of normal conditions [Cholda et al., 2009]. The transfer time for big size files is optimized in MeTHODICAL and SCTP scenarios that explore multihoming configuration between servers and clients.

For instance, MeTHODICAL is able to perform load balancing between servers to avoid overloading a specific server. This fact justifies the low performance of transfer time for CD images, but in contrast, it represents a gain in performance for DVDExtra cases.

MeTHODICAL and TOPSIS techniques are stable and transfer time increases linearly, as pictured in Figure 4.25. The different approaches have almost the same performance in terms of transfer time. Nonetheless, it should be noticed that MeTHODICAL introduces load balancing between servers, which represents a gain in terms of resources management but can affect transfer time.

4.7.4.3 Loss Failures

With loss failures and other kind of failures, the transfer time of TCP exceeds the acceptable limits, by a very large margin. For instance, in the *W1* test case, with CD images, TCP clocks in a transfer time around $\approx 93s$ (not pictured).

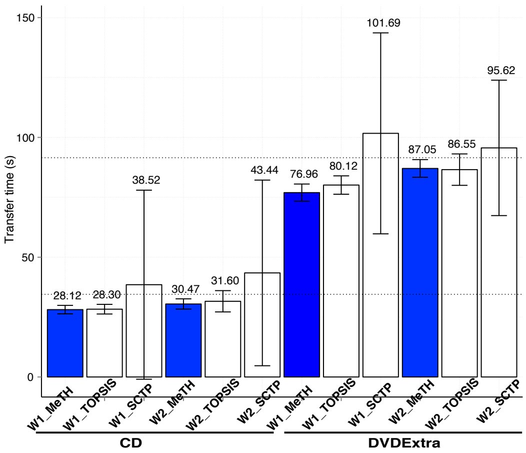


Figure 4.26: Mean transfer time in Losses scenario

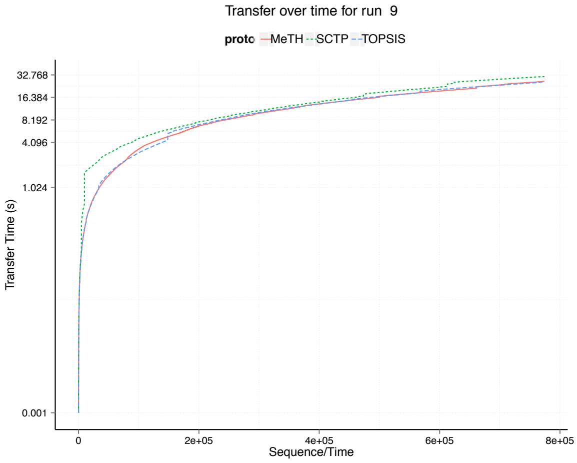


Figure 4.27: Transfer over time in Loss0 scenario for CD images

In the loss failures, as pictured in Figure 4.26, standard SCTP cannot meet the acceptable limits for 5% and 15% of loss ratios. It can be observed that SCTP starts to have higher delay in transfer from the first sequences, as pictured in Figure 4.27, for loss0 failures. As expected, MeTHODICAL, TOPSIS and SCTP are impacted with higher failure losses, as data transfer takes more time to conclude. In fact, there were cases where SCTP had a fast recovery, while in others it took longer time to recover, justifying thus the high variation. In contrast, MeTHODICAL and TOPSIS are able to provide acceptable and more predictable performance, bellow the defined performance limits for CD and DVDExtra cases. Both approaches are able to choose a server without losses.

4.7.4.4 Delay Failures

Regarding failures with delay, as depicted in Figure 4.28, standard SCTP fails to meet the acceptable limits with all delay failures, namely, 50 and 100ms.

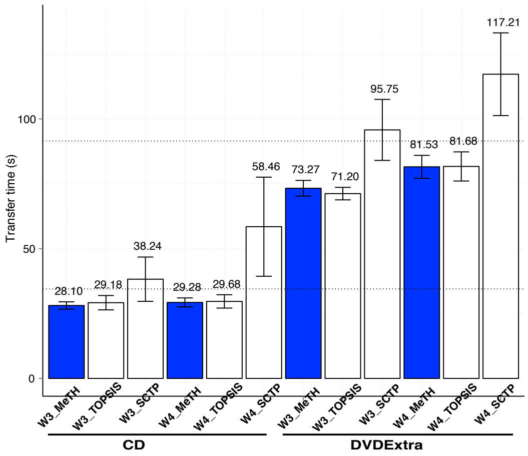


Figure 4.28: Mean transfer time in Delay scenario

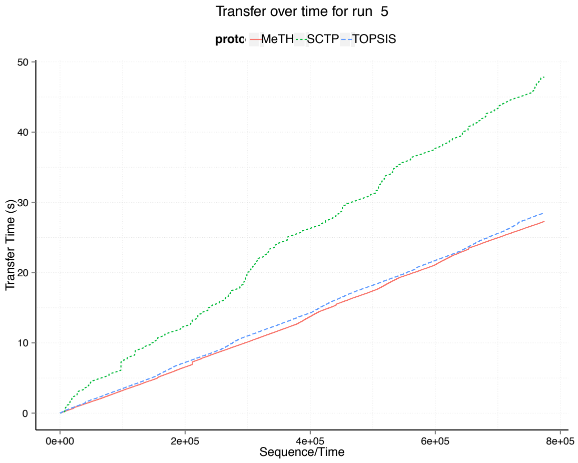


Figure 4.29: Transfer over time in Delay1 scenario for CD images

MeTHODICAL and TOPSIS are able to provide acceptable performance with values bellow the limits for the CD and DVDExtra cases. Of course, again, higher delays lead to worse performance across the board. Note that SCTP takes more time to react to this kind of failures, comparatively to loss failures. Data packets, despite being delayed, can be received within the retransmission timeout of SCTP, which lead the protocol to maintain the current link/path. In loss failures, SCTP performs the recovery to a backup path as soon as n packets are lost consecutively. In fact, as pictured in Figure 4.29 the difference between SCTP and remaining approaches is higher, when compared to loss failures, where the different techniques have such discrepancy.

With MeTHODICAL and TOPSIS the optimal server is the one with lower delay in its primary path, which lead to a gain in performance regarding SCTP.

4.7.4.5 Congestion Failures

Congestion failures, as depicted in Figure 4.30 impact performance of the different approaches as well.

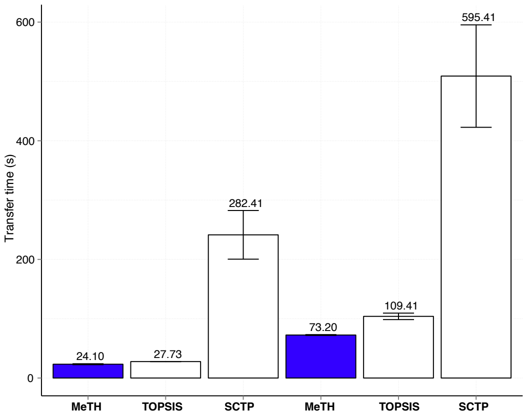


Figure 4.30: Mean transfer time in congestion scenario

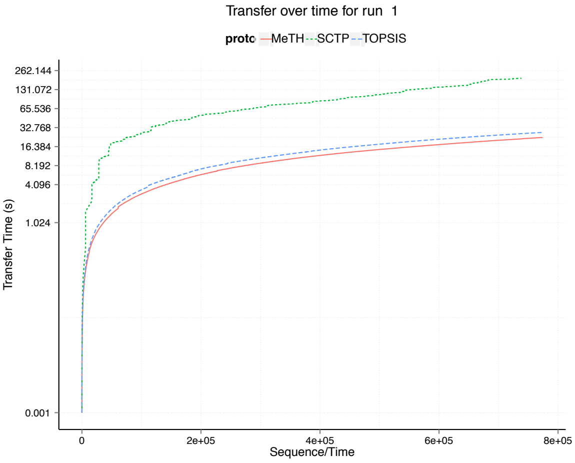


Figure 4.31: Transfer over time in congestion scenario for CD images

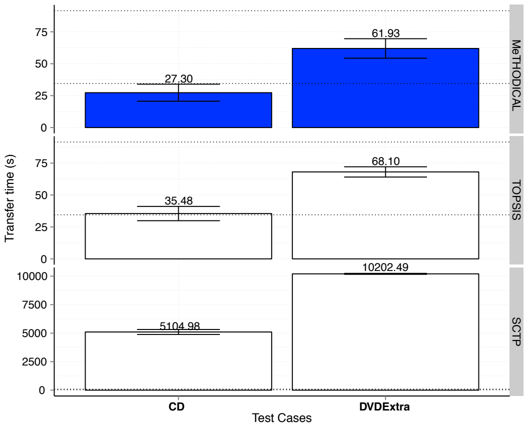
Indeed, SCTP and TOPSIS, especially in the DVDExtra transfer images, have a degradation in performance in which acceptable limits are not respected. This is not the case with MeTHODICAL for CD and DVDExtra cases, since the server without congestion is selected as the optimal.

In comparison to the failures presented so far, namely loss and delay, the congestion failure introduces more impact in the performance of SCTP. SCTP does not change to a backup path so reactively as in loss failures. In fact, as demonstrated in Figure 4.31, the performance of SCTP and TOPSIS are clearly worst than MeTHODICAL. Regarding the difference between TOPSIS and MeTHODICAL it should be pointed that the values of the diverse criteria are equal, nonetheless, the ability of MeTHODICAL to correlate criteria and therefore, determine the optimal server in a more efficient way.

4.7.4.6 Resource Failures

Resources failures are characterized by CPU overloading and are not detected by SCTP.

In any case, this type of failure affects all the available paths of a server, therefore the standard multihoming support of SCTP does not represent a direct gain in terms



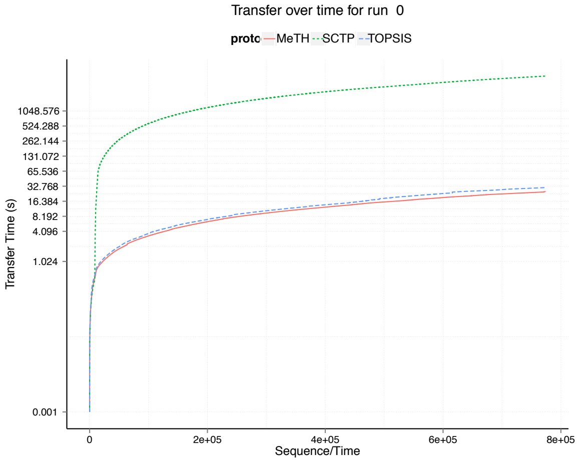


Figure 4.32: Mean transfer time in resources scenario

Figure 4.33: Transfer over time in resources scenario for CD images

of performance, as pictured in Figure 4.32.

SCTP has the worst performance values for all the test cases. In fact, as demonstrated in Figure 4.33 the performance of SCTP for DVDExtra transfer images reaches unacceptable values $\approx 10200s$. The fault tolerance mechanisms of SCTP are not able to detect such kind of failures. In any case, even if SCTP performs switching of paths, as CPU has a high utilization rate, it would not have any improvement in performance.

Both MeTHODICAL and TOPSIS approaches were able to select the server without resource failures, which lead to acceptable transfer times.

4.7.4.7 Critical and mixed failures

In critical and mixed failures the candidate aimed to assess the performance difference, mainly between MeTHODICAL and TOPSIS, as for SCTP the mixed failures have the same impact as resources failures.

SCTP can recover from a failing link/path to a backup path that is also characterized with a delay failure. In this case, the standard multihoming support of SCTP is a gain in terms that there is recovery from a critical failure, as pictured in Figure 4.34 and Figure 4.35.

All the approaches recover from *C1*- critical failure cases and *C2*- mixed failure cases. Nonetheless, in mixed failures, TOPSIS introduces a significative performance degradation, besides the high delay in transfer time the variation is also quite high. Such facts highlight the inconsistency of TOPSIS in choosing the best server, as in

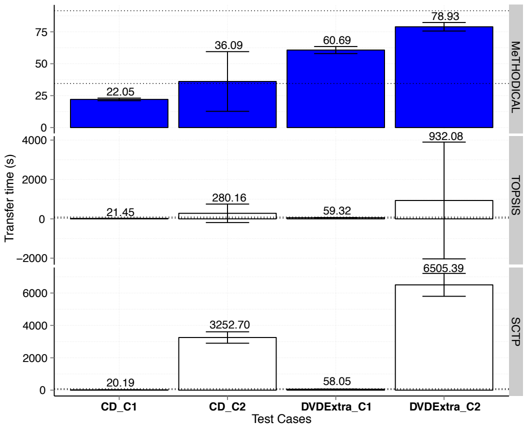


Figure 4.34: Mean transfer time in critical and mixed scenario

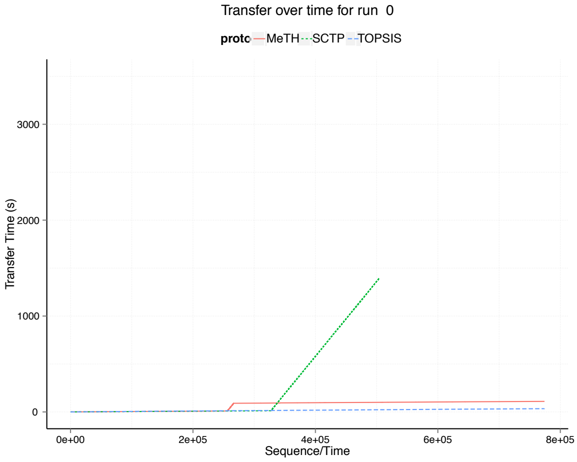


Figure 4.35: Transfer over time in mixed scenario for CD images

some cases, TOPSIS has chosen the server with the worst performance. In contrast, MeTHODICAL provides the best data transfer performance as the choice of the optimal server is consistent and efficient. For instance, MeTHODICAL does not choose the server with mixed failures in any of the tests runs.

4.8 Summary

The criteria weighting algorithm of MeTHODICAL establishes the foundation to set weights for diverse criteria in objective and precise ways, according to the desired consistency. Therefore, it can be used by any optimization technique that employs weights to establish criteria preferences. Additionally, multihoming criteria and traffic performance criteria are combined in two major types, namely benefits and costs, where the importance of each criterion is established. The versatility of the criteria weighting algorithm is demonstrated for the different ITU-Y 1541 classes of service, each one with different requirements.

MeTHODICAL is an optimization technique that enables optimal path selection with the same time complexity, $O(m \cdot n)$, of similar optimization techniques, but with improved performance, in terms of ranking stability and adaptation to network conditions. Achieved results demonstrate that MeTHODICAL is accurate, since it is able to select paths according to correct rankings, and performs handovers when they are really required.

When compared to related techniques, MeTHODICAL does not have ranking abnormality, as DiA or TOPSIS techniques. Furthermore, it does not present any requirement, such as high-volume data for NMMD, that limits its applicability. Last but not least, MeTHODICAL is also able to adapt to the number of paths/sets that can be chosen as optimal.

This chapter resulted in the following publications:

1. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**EVA: Enhancing VoIP Applications**",in proceedings of the 11th IEEE Global Communications Conference Exhibition & Industry Forum (GLOBECOM), December, 2013, Atlanta, USA.
2. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Enhancing Path Selection in Multihomed Nodes**", in proceedings of the 5th EAI International Conference on Mobile Networks and Management (MONAMI), September, Ireland, 2013.
3. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**Expedient Reconfiguration in the Cloud**", in proceedings of the 18th IEEE International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD), September, 2013, Berlin, Germany.

This chapter also includes a poster submission in the SAIL summer school, Spain, 2012, entitled "**MeTHODICAL: Multihoming for Urban Networks**".

This chapter resulted in the following papers:

1. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**MeTHODICAL: Towards the Next Generation of Multihomed Applications**", Submitted to Computer Networks, 2013.

—*Computers are useless. They can only give you answers.*

Pablo Picasso

5 Improving Multihoming

THIS chapter presents a contribution towards multihoming improvement in Mobile IPv6 (MIPv6) and related protocols. The chapter is organized as follows: Section 5.1 introduces the goals to achieve multihoming improvement and introduces MIPv6 and related protocols and overviews related works. Section 5.2 details an implementation of Multiple Care of Address (MCoA), mCoA++. Section 5.3 presents the evaluation methodology and Section 5.4 discusses the results achieved in the evaluation. Section 5.5 concludes the chapter.

5.1 Introduction

This section introduces the goals and requirements for implementations enabling multihoming support in MIPv6 protocol, considered the core mobility management protocol for IPv6 networks [Johnson et al., 2011]. Despite the proliferation of extensions to improve MIPv6 functionalities, namely in terms of multihoming. There are still a lack of implementations that allow to test the multihoming support of MIPv6 in network simulators.

5.1.1 Objectives and Requirements

The objectives to improve multihoming support include:

1. Improve the multihoming support of MIPv6.
2. Provide a standard implementation regarding multihoming support in MIPv6.

Mobile IPv6 (MIPv6) is the mobility management protocol for IPv6 networks. Its multihoming support is very limited, but can be extended in a standardized form, as demonstrated in this chapter.

5.1.2 Mobile IPv6 and Multiple Care of Address

This subsection introduces Mobile IPv6, Multiple Care of Address (MCoA) [Wakikawa et al., 2009] and Flow Bindings [Tsirtsis et al., 2011a; de la Oliva et al., 2011] protocols.

Mobile IPv6 (MIPv6) [Johnson et al., 2011] as mobility management protocol, includes several mechanisms and entities to assure that sessions are not disrupted when mobile nodes move between different networks. MIPv6 assures session survivability, through the registration of addresses configured in the visited network on the Home Agent (HA). HA assures that all the packets destined to the mobile node are delivered to this one, even if it is at a foreign network. For such, tunnels are employed, as the HA is aware of the location/address of Mobile Node (MN) after the registration of the addresses configured in the visited/foreign networks. Moreover, MIPv6 also allows MN to communicate directly with the Correspondent Node (CN), by employing specific security mechanisms (i.e. return routability), which assist the MN to prove its identity to the CN.

The registration performed in MIPv6, through Binding Update (BU) and Binding Acknowledgment (BA) messages, establishes bindings, a kind of mapping, between the Home Address (HoA) and the Care of Address (CoA). MIPv6 performs the binding of a single CoA, which is a limitation for mobile nodes with several addresses. The Multiple Care of Address (MCoA) protocol [Wakikawa et al., 2009] overcomes this limitation by extending Mobile IPv6 to support the registration of multiple addresses. MCoA introduces a new Binding Unique Identification (BID) number to identify bindings, thus allowing multiple CoAs to be bound to the home address, HoA.

MCoA also introduces enhancements in the BU messages to include the Binding Identifier Mobility Option that contains the BID(s) to register. On the reception event of a BU message, the HA and/or CN create or update the respective bindings in the Binding Cache (BC). To support multiple bindings for a home address, the lookup on

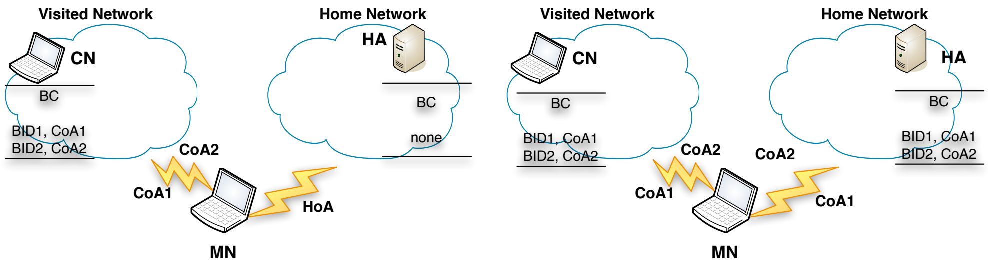


Figure 5.1: Multiple Care of Address bindings illustration

the Binding Cache is performed by the home address and the BID pair, as opposed to MIPv6 that relies only on the home address. If the HA or the CN do not support registration of multiple addresses, they acknowledge the MN in the BA, so that in the next message exchange MN resorts to standard MIPv6.

Figure 5.1 depicts the operation of MCoA by illustrating the multiple bindings at CN and HA Binding Caches and in the Binding Update List (BUL) of the MN. Moreover, MCoA considers two possible cases for the returning home operation. First, only one interface is attached to the home link. Second, the multiple interfaces can exist and one can be associated with the home network, while other with the visited network. In the last case, the Home Agent and the CN have binding entries in the Binding Cache, and the home agent forwards packets to the home link or foreign link.

The Binding Identifier Mobility Option is included in the Binding Acknowledgment (BA), Home of Test (HoT) and Care of Test (CoT) messages. This option includes several fields, such as the length that depends on the IP version (e.g. IPv4 or IPv6), the Binding ID and the status field, which reports the registration state of the respective Care of Address (CoA).

When the MN wants to register, it generates a Binding ID (value between 1 and 65535) per address, and sends a Binding Update message to the home agent and correspondent nodes, keeping the BID in the Binding Update List. When the MN has several addresses to register, it can use the bulk registration mode that includes several Binding Identifier mobility options in a single BU message. The bulk registration, where a single Binding Update message conveys multiple BID options, is only supported with the HA. Thus, the registration with the CN must be performed per address, to avoid issues with the return routability procedure, which assures identity protection for MN.

MCoA does not specify how the multiple registered addresses can be used. As such, usage address can be tailored to specific application requirements. Indeed, Flow

Bindings specification [Tsirtsis et al., 2011a; de la Oliva et al., 2011] enables the associations of flows to bindings. This way, policies can be specified, such as the choice for the link/CoA with higher (nominal) capacity. Flow Bindings extends the MCoA specification adding new options and fields to manage flows.

5.1.3 State of the Art

This subsection overviews works that aim to overcome the limitations of Multiple Care of Address protocol (e.g. use of addresses), as well as available implementations of MCoA.

The Capacity-aware preferred Multiple Care of Address (CAPMCoA) [Pan et al., 2008a] allows a mobile node to choose a Care of Address from the several addresses, based on the best throughput of a specific link-address pair. CAPMCoA does not meet the requirements of today's applications, since it only considers a throughput metric. That is, applications interested in paths with low delay do not have benefits with CAPMCoA. In addition, the implementation is not publicly available and refers to an old version of the MCoA specification [Wakikawa, 2008].

Different approaches may be followed to explore multiple addresses in mobile networks. HIPSim++ [Bokor et al., 2009] is an implementation of the Host Identity Protocol (HIP) [Moskowitz and Nikander, 2006] that supports multiple addresses for the OMNeT++ network simulator [OMNeT++, 2009], Nevertheless, HIP is not compatible with MIPv6, thus MIPv6-aware nodes do not have mechanisms to explore multiple addresses. Another implementation explores multipath at the transport layer [Dreibholz et al., 2010], by extending the Stream Control Transport Protocol (SCTP) [Stewart, 2007] to support concurrent multipath transfers. Once again, this solution does not allow MIPv6 nodes to support multiple addresses without the assistance of another protocol such as SCTP.

xMIPv6 [Yousaf and Bauer, 2013] is a simulation model that implements MIPv6 in OMNeT++. xMIPv6 provides an accurate implementation of MIPv6 protocol and related protocols, such as Fast Mobile IPv6 (FMIPv6) [Koodli, 2008] or Hierarchical Mobile IPv6 (HMIPv6) [Soliman et al., 2008]. Nonetheless, xMIPv6 does not have support for MCoA or Flow Bindings.

There are MCoA implementations in Linux [Kuntz, 2013b], as an extension to the Implementation of Mobile IPv6 and NEMO for Linux (UMIP) [Kuntz, 2013a]. Moreover, there are other implementations of MCoA and Flow Bindings but are not open to the research community [de la Oliva et al., 2011]. Indeed, there is a gap of MCoA implementations in network simulators that enable experiments with multihomed configurations. To fill such gap, in this thesis it is proposed an implementation of MCoA, in the OMNeT++ network simulator, the mCoA++, that has been made available to the community.

5.2 mCoA++: Multiple Care of Address and Flow Bindings Model

This section presents the architectural aspects of the Multiple Care of Address Registration implementation in OMNeT++ [Wehrle et al., 2010], labeled as mCoA++. Such implementation has been performed by the PhD candidate and two students, namely Marco Silva and Alexandre Santos. The mCoA++ implementation is publicly available [Sousa, 2013a].

5.2.1 Design Considerations

The goals for the development of mCoA++ include an accurate implementation of MCoA and Flow Bindings specifications, and source code availability to the research community. Moreover, diverse requirements have been established, to meet such goals, namely:

- mCoA++ ought to be RFC 5648 [Wakikawa et al., 2009] compliant.
- mCoA++ should not break the compatibility with MIPv6.
- mCoA++ should support MCoA protocol [Wakikawa et al., 2009] and Flow Bindings specification [Tsirtsis et al., 2011a].

With such design goals, mCoA++ was developed in two phases:

Phase 1 This phase extended MIPv6 to support the registration of multiple addresses. MCoA support was implemented in this phase.

Phase 2 This phase extended the previous version to support Flow Bindings.

In phase 1, mCoA++ was derived from xMIPv6 [Yousaf et al., 2008] implementation in OMNeT++. xMIPv6 was chosen because it implements all the features of MIPv6 for mobility management (e.g. tunnel creation/modification/deletion) and it is a flexible framework for easy extensions. As mentioned above, the way the multiple addresses can be used is not specified in MCoA. Taking this into account, two major types of use were implemented, namely, *ALL* and *SINGLE*. In both cases all interface addresses are registered and a separate tunnel is created for each address. However, with *ALL*, applications use the several addresses simultaneously by replicating packets for each tunnel, while with *SINGLE*, only one address is used, which can be selected according to different schemes (i.e. in a round-robin fashion or using the first registered address).

Mobile IPv6 informs upper layers (e.g. applications) when tunnels are created or deleted to assure that the addresses chosen by applications are valid (reachable through a certain path). The cross-layer mechanisms, implemented in mCoA++ rely on the notification schemes of the *INET* framework [Community, 2013], which implements protocols such as SCTP and IPv6.

In the phase 1 of mCoA++ implementation the application chooses the type of use. For instance, data applications may be interested on addresses associated with paths with higher bandwidth, while VoIP applications are interested on paths with reduced end-to-end delay. This approach is inline with recent proposals for cross-layer design, including architectures based on IEEE 802.21 [Piri and Pentikousis, 2009], for example. In the phase 2 of mCoA++ implementation, the preference for the different flows is configured in terms of priority per application, or per address.

5.2.2 Classes and Nodes

This subsection highlights the classes and nodes that were introduced in the mCoA++ implementation or that were modified to accommodate the needed functionalities .

Table 5.1 summarizes the classes introduced and those that have been modified in mCoA++. The class `MCoA` is added at the network layer of the MN, HA, and CN nodes. The MCoA class works as a configuration class, and the respective configuration directives are implemented in the `xMIPv6` class, for instance in the `SendPeriodicBU()` method. Moreover, the class `MCoA` configures several MCoA parameters in MIPv6 aware nodes. The *m_prohibited* flag indicates if a node supports the registration according to MCoA and Flow Bindings. Standard MIPv6 corresponds to $m\_prohibited = true$. The *m_bulk_reg_prohibited* flag indicates if a node supports bulk registration. The *mc_sim_home_and_foreign_prohibited* flag allows the simultaneous use of home and foreign interfaces. The *TypeUseMCoA* is a string field to define the type of use to employ for the registered addresses. The possible values defined in the `MCoADefs.h` file, include *ALL*, *SINGLEFIRST* and *SINGLERANDOM*. Moreover, the *deregisterALL* is an integer field to indicate how the deregistration should be performed (e.g. 1 to deregister one-by-one). In Phase 2, the type of use, was deactivated, as flow bindings allows to map application flows to specific addresses (i.e. BIDs.).

Table 5.1: Classes in mCoA++

Class	Phase	Purpose
KeyMCoABind	1	Key in the BUL and BC.
KeyMCoADAD	1	For operations with DAD.
XMIPv6SM	1	State Machine for MIPv6 operation.
IPv6TunAdr	1	Information for created/deleted tunnels.
IPv6PrefAdr	1	Information about preferred address.
BIDPRIList	2	Association of priority with BIDs.
BindingCache	1	Introduce new key, KeyMCoABind.
BindingUpdateList	1	Introduce new key.
IPv6Tunneling	1	Notification for created/deleted tunnels.
IPv6	1	To activate and de-activate IPv6 forwarding.
BIDPRIList	2	Association of priority with BIDs.
FlowBindingPolicy	2	Implements policies regarding flows.
FlowBindingList	2	To manage Flow Bingings.
TrafficSelector	2	Traffic Selectors [Tsirtsis et al., 2011b].

The class XMIPv6SM works as a simplified state machine for MIPv6 operations, for instance if the node is returning home, or if it has initiated MIPv6 procedures, but it is employed mainly as a helper for the address selection mechanism, at the network layer. This class holds information about the preferred address and flags for different operations (e.g. return home, address selection).

The class IPv6TunAdr is introduced to provide information about the created or deleted tunnels to the applications. The fields include entry, exit and destination trigger IPv6 addresses of tunnels.

The class IPv6 was modified to allow the activation and de-activation of IPv6 forwarding to simulate errors at the network layer. Also the detection of the correspondent nodes by the MN was reformulated when MN forwards or receives packets from a node with a different address from HA. The parse_ipv6_datagram_for_mcoa() method was introduced to update the Correspondent Nodes list for packets Transport Connection Protocol (TCP), User Datagram Protocol (UDP) or Stream Control Transport Protocol (SCTP). The previous implementation of *xMIPv6* did not include such mechanism. This detection mechanism is needed to identify the multiple addresses of a correspondent node on the MN. Moreover, such identification is filtered by the transport protocol type to avoid the identification of spurious correspondent nodes (e.g. sending signalling messages to multicast or anycast addresses).

Table 5.2: Data structures and methods in `xMIPv6` class

Data Structure/method	**Purpose**
`KeyTimer`	Modified to include the BID field.
`InterfaceCoAList`	Modified to include the BID field.
`CoABIDList`	Introduced to perform the mapping of CoA and BIDs.
`NodesMCoACap`	Introduced to hold information about nodes MCoA capabilities.
`FlowBindingList`	Introduced to hold information about Flow Bindings.
`get_and_calcBID()`	Method to assign BIDs and avoid the home address to be included in the `CoABIDList`.
`get_adr_from_bid()`	Method to retrieve an address from a BID.
`set_mobilityoptions_for_ha()`	Method to create mobility options for HA.
`set_mobilityoptions_for_cn()`	Method to create mobility options for CN.

The `xMIPv6` class is the core class of the Mobile IPv6 implementation, as such major features for MCoA and Flow Bindings support have been coded in this class. Several data structures were modified to accommodate information about BIDs, as summarized in Table 5.2.

When MIPv6 is triggered, timers to enable the creation of bindings are created (e.g. *KEY_BUL*). These timers are created for the HA and for each CN (identified in the *CNListBID*). When sending binding updates, through the `sendPeriodicBU()` method, the support for MCoA is checked, which restricts the fulfillment of options, namely `MobilityBIDOptions`. The destination of binding messages is considered, therefore a specific method is employed if registering with the HA and another method is used when registering with the CN. These methods set the `MobilityBIDOptions` according to the BIDs defined in the `CoABIDList` and flows in the `FlowBindingList`. On the Binding Update message reception, Home Agent and Correspondent Node process this message, checking each option in `MobilityBIDOptions`. Timers to expired entries, refresh request timers are created, as well as the respective tunnels. MN is informed about the registration operation in the HA and CN through Binding Acknowledgment messages, which also convey the Mobility Options. The Mobile Node proceeds according to the status of the reply message. On a successful binding operation, the Mobile Node updates the Binding Update List and initiates the return routability procedure for each BID, if the BA message comes from the HA.

The returning home operation involves several operations (e.g. remove addresses, deregister BID) that are triggered in the `returningHomeMCoA()` method. When deregistering, the tunnels are removed and the timers have $bindinglifetime = 0$. The state machine `XMIPv6SM` is also updated. In order to allow the Mobile Node to roam again, a notification message is employed to guarantee that all the auxiliary structures and respective states are initialized.

5.2.3 Headers and Mobility Options

mCoA++ adds support for `MobilityBIDOptions` - Binding Identifier Mobility Option, in phase 1. This option includes a status field for the BID, a flag to indicate if it is a home binding, and the respective BID key. Messages that can include information about BIDs were modified to include support for a vector of Binding Identifier Mobility Options, such as Binding Update (BU), Binding Acknowledgment (BA), Home of Test Init (HoTI), Home of Test (HoT), Care of Test Init (CoTI), Care of Test (CoT) and Binding Refresh Request (BRR) messages.

mCoA++ in phase 2 includes support for the Flow Identification Mobility Option `MbolityFIDOptions`, which includes a status field for the FID, the priority of the FID and the respective sub-options, which can include the Binding Reference sub-Option and the Traffic Selector sub-Option. To avoid excessive signalling different flows can be referenced in a single message, through the Flow Summary Mobility Option. Message including mobility options were modified to include the options defined in Flow Bindings, namely, BU and BA messages.

5.2.4 Notifications

Table 5.3 summarizes the notifications acting in a cross-layer fashion to inform applications of events occurring at the network layer or to configure this layer, regarding the addresses to employ.

The `NF_MCOA_APP_PREFERED_ADDRESS` notification is used to inform the network layer about the preferred address selected by applications and the respective priority. In mCoA++ phase 1, MCoA considers two types of uses, the *single* uses of a CoA selected randomly, and the *all* uses all the addresses simultaneously. This choice relies, mainly, on divergent performance gains that can be achieved. The em-

Table 5.3: mCoA++ notifications

Notification	Purpose
NF_MIPv6_MN_RETURNED_HOME	To notify return home event.
NF_IPv6_TUNNEL_ADDED	To notify creation of new tunnel.
NF_IPv6_TUNNEL_DELETED	To notify removal of tunnel.
NF_MCOA_APP_PREFERED_ADDRESS	Notify network layer about preferred address.

ployment of multiple addresses can lead to a better resilience support, notwithstanding with increased overhead levels. In mCoA++ phase 2, MCoA chooses addresses based on the applications flows, which can be identified by the pair of `<source IP; destination IP>` or simply by ports.

5.2.5 MCoA Application Support

In order to receive notifications about the creation of tunnels and to use the information received on such notifications, applications have to be extended. The class `MCoAUDPBase` acts as a base class for UDP applications. This class contains information about sockets, namely source, destination addresses and sockets ID. The class `MCoAUDPBase` implements methods for diverse socket bindings/unbindings, and methods for sending packets according to the configured type of use. The application sends packets according to the type of use, as per $typeUse$ variable, in the method `sendToUDPMCOA()`:

- ALL, packet is duplicated for n addresses.
- $SINGLERANDOM$, preferred address is chosen randomly from the vector with all the addresses, `adrsAvailable`.
- $SINGLEFIRST$, packets are sent to the first address.

In phase 2, the $typeUse$ of method `sendToUDPMCOA()` was modified to send packets according to pre-configured flows information.

The `MCoAUDPBase` class works as a base class that can be used by other applications. Initially it performs binding to the default port and configured addresses , but when receiving notifications about the creation and deletion of tunnels, it performs the socket binding using the information received with the notification messages (e.g. source, destination addresses). On the deletion operation, the socket (identified by an integer) is marked as deleted to avoid using this socket on future events.

Table 5.4: Applications MCoA-aware

Application	**Description**
`MCoAVideoStreamCli`	Video MCoA capable server.
`MCoAVideoStreamServer`	Video MCoA capable client.
`MCoAUDPApp`	VoIP MCoA capable applications .

The `MCoAUDPBase` class includes various parameters that affect the MCoA operation. The *localPort* on which socket bindings should be done, the possible *destAddresses*, the *useMode* parameter that dictates the type of use and the *isDestiny* flag indicates if the node is acting as a receiver (`true`), or as a sender (`false`).

Applications needing MCoA facilities need to extend `MCoAUDPBase` class and implement their own sending mechanisms, (sending rate, packet size). Table 5.4 summarizes applications that were introduced, extending the `MCoAUDPBase` class to support MCoA facilities.

List 5.1: MCoA application example code

```
1  int sockID=bindToPort(localPort, ipSrc_Address);
2  // msg = new cPacket();
3  if (useMode == MCOA_TUN_ALL_ADR_SINGLE_RR){
4    int idx =  (int)intrand(lenAdrs);
5    IPvXAddress adrtoSend = adrsAvailable[idx].mSrc;
6    sendToUDP(msg, adrtoSend, srcPort,
7                         destAddr, destPort, appendCtrlInfo);
8   }
9   // Unbind operation
10  unBindPort(localPort, ipSrc_Address, sockID);
```

List 5.1 provides some excerpts of code that exemplify the creation and use of MCoA in UDP applications. Line 1 depicts the binding to a local port. The `bindToPort` returns a socket ID for future operations (e.g. unbinding operation). Lines 4-5 exemplify random address selection. Line 6-7 call the send method that appends control information to the message (source and destination addresses). The last line illustrates the deletion of socket, by performing the unbinding operation.

5.2.6 Configuration

The current `FlatNetworkConfigurator6` module configures the whole simulation as a big subnet. In addition, it assigns a simple prefix per router. To enable the advertisements of several prefixes by a router, and to have distinct networks, the `MCoANetConf6` module was introduced. This module implements the methods `addOwnAdvPrefixRoutes()` and `addStaticRoutes()` to add the advertisement prefixes and static routes, for routers and hosts, respectively.

List 5.2: Routing and addressing configuration Example

```
<local node=‘‘R_1”>
<interface name=‘‘eth1” AdvSendAdvertisements=‘‘on”>
        <AdvPrefixList>
          <AdvPrefix AdvOnLinkFlag=‘‘on” AdvValidLifetime=‘‘4”
                AdvPreferredLifetime=‘‘4” AdvAutonomousFlag=‘‘on”
                advRtrAddr=‘‘on”  rtrAddr=‘‘2001:db8::0299:2B2”>
                                2001:db8::0299:00/112</AdvPrefix>
          <AdvPrefix AdvOnLinkFlag=‘‘on” AdvValidLifetime=‘‘4”
                AdvPreferredLifetime=‘‘4” AdvAutonomousFlag=‘‘on”
                advRtrAddr=‘‘on”  rtrAddr=‘‘2001:db8::0199:2B2”>
                                2001:db8::0199:00/112</AdvPrefix>
        </AdvPrefixList>
        <inetAddr tentative=‘‘off”>
                2001:db8::0299:2B2 </inetAddr>
        <inetAddr tentative=‘‘off”>
                2001:db8::0199:2B2      </inetAddr>
</interface>
</local>
```

All prefixes can be configured in a XML file, as illustrated in List 5.2. This implementation provides flexibility to configure more realistic network scenarios, as for instance subnets can be configured.

List 5.3: Configuration of BIDs priority

```
<root>
 <bid priority=”20”>20:00:00:00:01:01</bid>
 <bid priority=”30”>20:00:00:00:01:02</bid>
 <bid priority=”30”>01:80:C2:00:00:03</bid>
</root>
```

Flow Bindings includes different configurations. The `FlowBindingPolicy` module includes methods to assign priority to BIDs. Such assignment is configured for each interface via the MAC address, as illustrated in List 5.3.

List 5.4: Configuration of FIDs

```
<policy priority="20" family="IPv6" protocol="TCP">
        <src ip="2001:db8::33a1:1"/>
        <macaddress>20:00:00:00:01:01</macaddress>
</policy>
<policy priority="30" protocol="UDP">
        <macaddress>20:00:00:00:01:01</macaddress>
        <macaddress>20:00:00:00:01:02</macaddress>
</policy>
```

The specification of policies are performed in the module `FlowBindingPolicy`, which includes the method `parseXMLConfigFileTS()` to load the configurations of policies for the different flows. List 5.4 depicts examples for the configuration of policies for UDP and TCP applications.

5.3 Evaluation Methodology

This section details the methodology followed in the evaluation of mCoA++.

Table 5.5: Values of configuration parameters per scenario.

Item	mCoA++ Performance	Application Performance
Ethernet links	delay=10ms	
Internet links	delay=30ms	delay={30,100}ms
Video streaming	packet size=300B, CBR[a]=50ms	packet size=500B, CBR[a]=50ms
VoIP Application	(G.723.1) packet interval=10ms	packet interval=20ms
MN Velocity	pedestrian-3km/h and vehicular-30km/h	
Mobility Models	random way point-rwp, rectilinear-rect	
Network failures	each 20s, duration=150ms	
Use of addresses	*MCoA_ALL*- all addresses, *MCoA_SINGLE_FIRST*-first CoA, *MCoA_SINGLE_RANDOM*-random CoA	
Session length	200s	

[a] Constant Bit Rate (CBR)

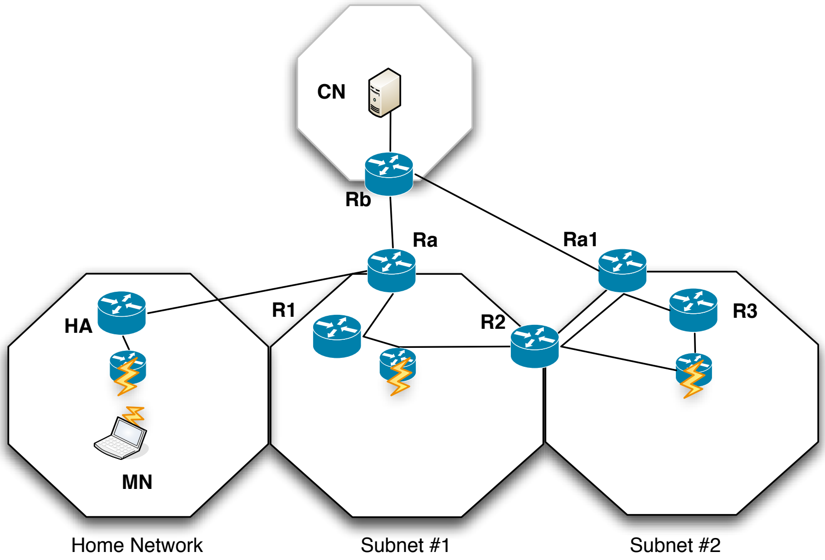


Figure 5.2: Simulation scenario for mCoA++ performance evaluation.

Two evaluation approaches were followed, namely, one to assess the performance and accuracy of the mCoA++ implementation and the other to assess the performance of applications, as detailed in the following subsections. Table 5.5 summarizes the diverse configuration parameters for both scenarios.

5.3.1 mCoA++ Performance

The evaluation of mCoA++ performance has two purposes: First, to validate the mCoA++ model through a comparison with xMIPv6. Second, to demonstrate the applicability of mCoA++ in multihoming contexts (e.g. several addresses).

The simulation scenario, as depicted in Figure 5.2, includes the Correspondent Node (CN) network, the home network and two foreign networks. Multiple prefixes are advertised on the foreign networks (*Subnet #1*, and *#2*). Moreover, router *R2* is connected to both networks, and router *R1* advertises multiple prefixes on *Subnet #1*. The Wi-Fi technology (IEEE 802.11b) is employed due to its wide deployment. Configuration parameters are depicted in Table 5.5. The scenario also encompasses Video and VoIP applications. Video is transmitted at a constant rate of $50ms$ with a packet size of $500B$, to simulate video streaming, while VoIP applications are set with packet interval of $10ms$ (G.723.1).

Network failures were introduced, to assess the advantages of using multiple addresses, namely in terms of resilience performance. The network failures include disruption of IPv6 forwarding facilities with a duration of $150ms$ and are generated each 20s between *R1* and *R2* routers.

Different ways of using the multiple available addresses were considered. The *MCoA_ALL* uses all the addresses simultaneously, *MCoA_SINGLE_FIRST* chooses the first CoA, *MCoA_SINGLE_RANDOM* chooses a CoA randomly from the several that are available, while *MIPv6* corresponds to the standard Mobile IPv6. This last case is used as reference, since MIPv6 accuracy has already been demonstrated on the xMIPv6 implementation [Yousaf et al., 2008]. In addition, the bulk registration mode is enabled for the registration procedures with MCoA cases, in order to reduce the exchange of signalling messages. With this mode, multiple addresses/multiple FIDs are conveyed in a single signalling message. As in the xMIPv6 [Yousaf et al., 2008] and Mobility Management Simulation Engine for IPv6 (MMSEv6) [Yousaf et al., 2010] the time of handover T_{HO} and the signalling cost were employed as comparison metrics. The time of handover T_{HO}, includes delay between movement detection and node registration at the CN t_{CR}. T_{HO} was measured according to Equation 5.1, in order to be agnostic of layer 2 handover delay.

$$T_{HO} = t_{CR} - t_{ASSOC} \tag{5.1}$$

t_{ASSOC} corresponds to the instant on which the MN associates with an Access Point, t_{CR} corresponds to the time where tunnels are created or destroyed due to the reception of a successful registration.

The signalling cost is based on the total signalling cost, which corresponds to the sum of the message size of the MIPv6 signalling messages, namely BU, BA, CoTI and HoTI. The message size, in bytes, includes header(s) size and respective payload size. Signalling cost has also been evaluated in the Ubiquity Evaluation Framework (UEF) specification, for MIPv6 and HIP protocols.

5.3.2 Application Performance

This section details the methodology followed in the evaluation of applications performance in mobile nodes with multiple interfaces. The evaluation was performed using mCoA++.

VoIP and video streaming traffic was used in the application performance evaluation, to assess the impact of multiple care-of addresses in the performance of multimedia applications. Video streaming traffic was generated through the transmission of packets with 500B and interarrival rate of $50ms$ according to [Zhang et al., 2008]. VoIP applications are configured with packet interarrival rate of 20ms, within a compressed bit rate of 128kbps, a sampling rate or 8kHz and 16 bits per sample, which correspond to speech characteristics [Yao et al., 2008].

Table 5.6: Mean Opinion Score

MOS	Impairment/Description
5	Imperceptible / Excellent
4	Perceptible but not annoying / Good
3	Perceptible and slightly annoying / Fair
2	Annoying but not objectionable / Poor
1	Very annoying and objectionable / Bad

The VoIPTool [Bohge and Renwanz, 2008] was employed to generate VoIP packet streams, because it allows the use of real audio data, in such a way that a recorded phone-conversation was used as the input audio. Moreover, the ITU Perceptual Evaluation of Speech Quality (PESQ) tool [ITU-T, 2013] was used to assess the Mean Opinion Score (MOS). ITU PESQ [ITU-T, 2011a; Qiao et al., 2008] is a standard that establishes a quality score, by comparing the original signal with the degraded version. PESQ allows listening quality objective measurements, which in part justifies its wide-use for VoIP quality assessments. Values of PESQ rely in the $[-0.5, 4.5]$ range and are mapped in the MOS scale, as per Table 5.6, according to the mapping function of Equation. 5.2, which is specified in ITU P.862.2 recommendation [ITU-T, 2011b].

$$y = 0.999 + \frac{4.999 - 0.999}{1 + e^{-1.3699 \cdot x + 3.8224}}, \text{ where x is PESQ} \tag{5.2}$$

The simulation scenario, depicted in Figure 5.3, includes wireless LAN subnets (*Subnet #1*, *#2* and home network) and a wireless network with high transmission power (*Subnet #3* - to model a 3G network, in terms of coverage). Routers *Ra* and *R2a* connect to *Rb* that manages the correspondent node network. The links simulating an Internet connection (links *Ra-Rb* and *R2a-Rb*) have a propagation delay of *30ms* and *100ms*. Router *R2*, managing *Subnet #3*, is connected to a wireless point configured with high transmission power, in order to provide a wide wireless coverage.

The handovers were triggered by the availability of new addresses and by the unreachability of neighbours, as in standard MIPv6. For instance, when roaming from the home network, to *subnet #1*, the Home Agent is no longer reachable, according to Neighbour Unreachability Detection (NUD) protocol [Narten et al., 2007], and a

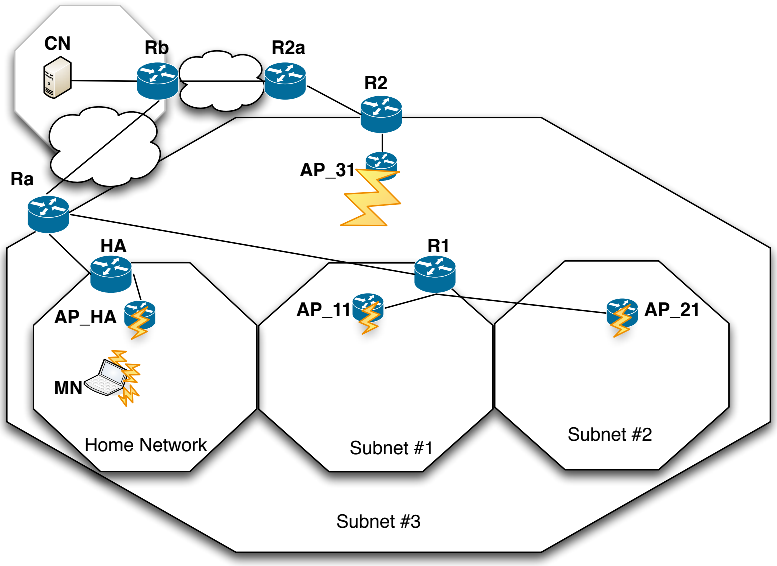


Figure 5.3: Simulation scenario for application performance evaluation

new prefix is available. After the connection to a new access point, mobile node receives prefixes, from which Care-of-Addresses are formed. Moreover, procedures like DAD [Narten et al., 2007] are executed to assure that the CoA is a unique address. Thus, handover execution time, besides including the association at the link layer also includes time to execute procedures at the IP layer, lying in values $\approx 1s$ [Yousaf et al., 2008].

The analysis has considered two failure cases. The first one includes failures due to handovers-*HO*, which were caused by the movement of the MN when roaming between networks. The second corresponds to failures on the elements of the networks-*Net* (e.g. routers). *HO* cases are equivalent to failures due to mobility of nodes. Despite that the same recovery procedures are used in both failure situations the consequences are different. On the first case, the mobile node switches to a new network, while on the second case, the MN stays on the current network, but needs to determine a new default router. The network failures included non working periods of $5s$. Such long periods were considered to allow the expiration of bindings. These failures were generated systematically each $20s$, alternately between *HA*, *R1* and *R2* routers. The network failures consist on dropping all packets in the Ethernet interfaces of routers. The handover failures were caused by the different speeds of the MN, namely 3km/h and 30km/h, configured to simulate pedestrian and vehicular speeds [ITU-R, 1997]. When correspondent nodes support Mobile IPv6 procedures, routing optimisation mechanisms can be used. Thus, failures in the Home Agent should not impact Mobile Nodes when at foreign networks. Traditional evaluations [Andersson et al., 2007; Bellavista et al., 2010] only consider the failures due to mobility, corresponding only to *HO* cases. The evaluation performed also included failures in the network, in order to assess the resilience gain of multimedia applications empowered by MCoA.

Different ways of using the multiple addresses available were considered, as depicted in Table 5.5 and employed in the mCoA++ performance evaluation.

5.4 Results

This section presents and discusses the results achieved in the mCoA++ and Application performance evaluations, as detailed in the following subsections. Both evaluations report results with a confidence interval of 95%.

5.4.1 mCoA++ Performance

Figure 5.4 depicts the handover latency for all the test cases with MCoA and MIPv6 test case, in VoIP and Video applications.

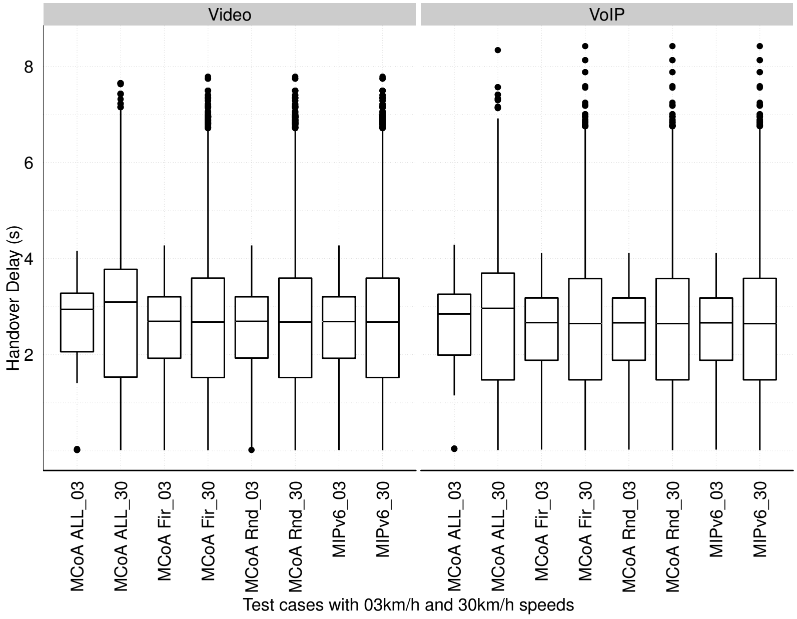


Figure 5.4: Handover time for Video and VoIP applications with MCoA ALL, MCoA ONE First (*MCoA Fir*), MCoA ONE Random (*MCoA Rnd*) and MIPv6 test cases.

To assess mCoA++ performance, Router Advertisements were configured with minimum = 0.03s and maximum = 0.07s, a similar set of xMIPv6 evaluation [Yousaf et al., 2008]. Single test cases of mCoA++ have similar delay and are equal to the delay in the MIPv6 test cases. Performance degradation is not observed in mCoA++, when compared to xMIPv6, when considering the handover delay. The mean delay in the MCoA ALL test cases is higher than in MCoA single and MIPv6 tests. The registration of multiple addresses and their simultaneous use require the establishment of tunnels for each address. While in single use of MCoA and MIPv6 cases only one tunnel is established, in the MCoA ALL test cases multiple tunnels are created, one per each registered address, consequently handover delay is higher. The 30km/h cases have more handovers, around $\sim$ 12 in opposition to $\sim$ 2 for 3km/h speed cases. In all the test cases with 30km/h, the handover delay has more variations, as it can be observed in the area of boxplots.

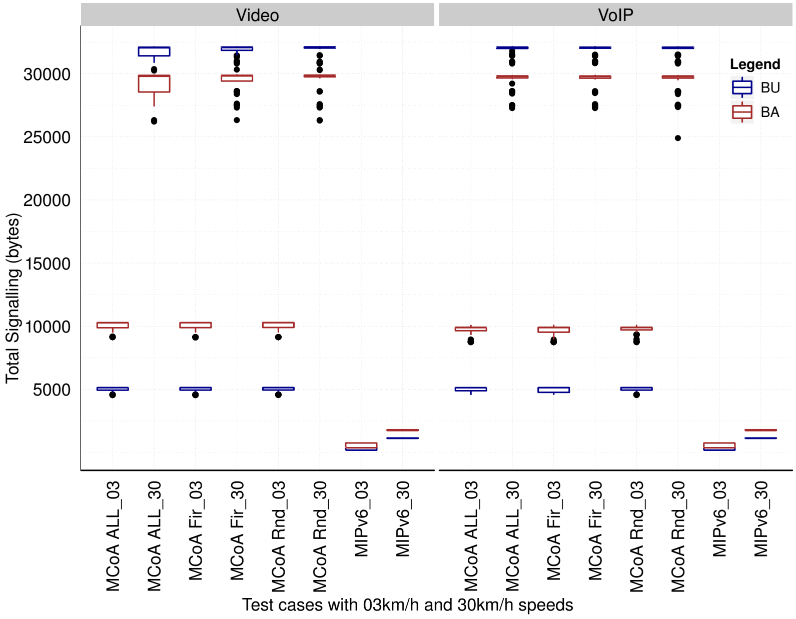


Figure 5.5: Total signalling cost for Video and VoIP applications on MCoA ALL, MCoA ONE First (*MCoA Fir*), MCoA ONE Random (*MCoA Rnd*) and MIPv6 test cases.

Despite the gain in resilience, MCoA has drawbacks, namely in the signalling cost. The modified signalling messages in the MCoA specification include Mobility Options, which carry information for each address to register. The single binding nature of MIPv6, only registers one care of address. MCoA, by enabling the registration of multiple addresses, introduces more overhead, as demonstrated in Figure 5.5. Signalling messages in mCoA++ convey multiple binding options, one per address. In addition, the number of handovers introduces more overhead as further messages are exchanged. Signalling cost between all the MCoA cases (ALL, ONE FIRST, ONE RANDOM) is similar since all the addresses are registered. As such, the several addresses are conveyed in the Mobility Options of signalling messages.

Both handover latency and signalling cost results depict the accuracy of mCoA++ implementation in comparison to xMIPv6. First, results are similar regarding handover latency. Second, mCoA++ introduces higher signalling costs, as expected due to the increased message size.

5.4.2 Applications Performance

Packet loss measurement was based on the sequences lost of the different messages. That is, each packet sent by the application was numbered and on the arrival event, packet loss ratio was determined based on the sequences that were not received. This methodology was applied to VoIP and Video applications, since duplicated packets could lead to faulty results. Duplicated packets, for each tunnel in the *MCoA ALL* mode, do not affect the payload (e.g. message sequence numbers), only headers (employed as control information) were modified, according to the respective tunnels (e.g. source and destination addresses).

Table 5.7: Applications Packet Loss (%)

App.	Speed	MCoA ALL		MCoA First		MCoA Random		MIPv6	
		Rect	Rwp	Rect	Rwp	Rect	Rwp	Rect	Rwp
VoIP	3km/h	01.43	15.90	01.43	15.90	01.44	13.72	11.32	17.39
VoIP	30km/h	35.11	55.06	34.80	58.69	35.08	56.52	52.66	63.60
Video	3km/h	01.40	16.49	01.41	17.13	01.43	16.49	17.53	20.90
Video	30km/h	35.33	56.65	35.35	57.30	35.33	56.74	56.49	64.67

Resilience can be related to packet loss. For instance, with higher packet loss ratios there are lower resilience levels. With higher speeds (e.g. 30km/h) and with random way point mobility model, indeed the level of resilience is minimized. Nodes can move to areas without coverage of Access Points, or have higher packet loss ratios due to the increased handover delay at layer 2. MCoA-aware applications improve their resilience levels, even with higher speeds, as illustrated in Table 5.7 for Video and VoIP applications. The registration of multiple addresses is the key of such improvement.

Based on the achieved results, it can be pointed that MIPv6, due to its single-binding nature does not provide resilience support. With MIPv6, applications can have packet loss ratios around $\sim 17.5\%$ with low speeds and moving rectilinearly. With the single MCoA test cases (First and Random) the use of a fixed address (e.g. the first to be configured) does not provide any gain in the performance as it leads to higher packet loss when compared to the approach of choosing an address randomly. Such results are inline with the issues identified in chapter 2, on which standard address selection do not provide multihoming support.

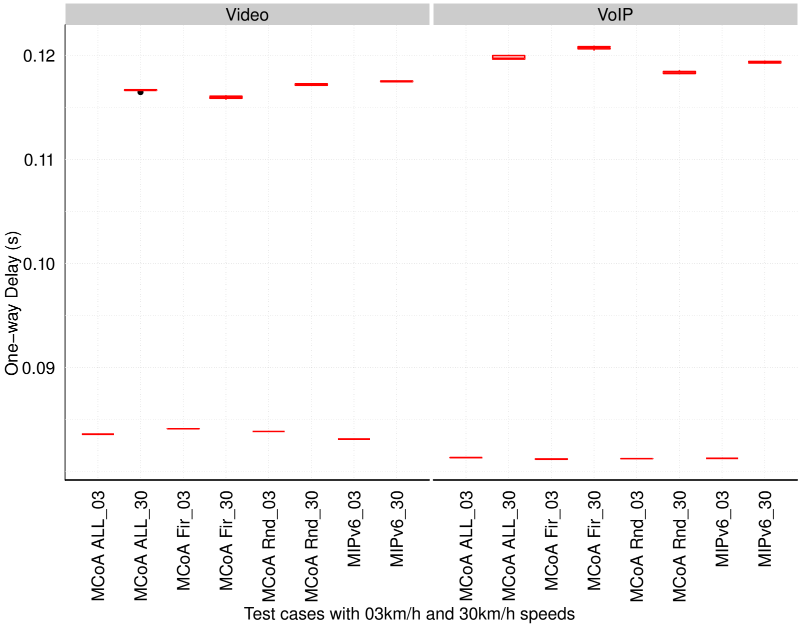


Figure 5.6: One-way delay for Video and VoIP applications on MCoA ALL, MCoA ONE First (*MCoA Fir*), MCoA ONE Random (*MCoA Rnd*) and MIPv6 test cases

One-way delay was determined by relying on message timestamps. Each message sent is also timestamped and on the reception event, one-way delay is calculated as being the difference between the received time and the message creation time. One-way delay depends on the underlying technology. In addition, different channel propagation delays are associated to the fixed links, to simulate Ethernet and Internet connections, respectively. Figure 5.6 depicts one-way delay results for the different applications. With 3km/h all the tests have similar values, around $\sim 0.08s$, but with increased speeds delay has some variations. In random and first mCoA++ cases, the address selected might be associated with a path with more failures. In addition, VoIP applications are more susceptible to higher speeds, due to the high number of sent packets.

MCoA can enhance application performance by increasing levels of resilience or supporting optimized path selection mechanisms (e.g. select a path with lower end-to-end delay). Application performance results obtained with mCoA++ put in evidence two aspects: First, MCoA *per si* is not synonym of performance gain, as for instance the cost of using all the addresses is higher. Finally, applications and network protocols must have synchronized path selection schemes to meet application requirements.

5.5 Summary

This chapter presented mCoA++, a multiple care of address model for the OMNeT++ network simulator. The candidate has released the code to the research community, in the belief that mCoA++ can be used as valuable building block in simulation studies of cross-layer architectures, evaluations of mobility management solutions and assessments of multihoming solutions.

mCoA++, a publicly available implementation of MCoA for OMNeT++ [Sousa, 2013a], was evaluated comparatively with xMIPv6, the simulation model of MIPv6 widely used by the OMNeT++ community. The mCoA++ simulation model extends xMIPv6 significantly and enables the registration of multiple care of addresses and the support of Flow Bindings. Achieved simulation results show that mCoA++ adds MCoA support in OMNeT++, without introducing any significant overhead when compared with the base xMIPv6 code for typical simulation scenarios.

The outcome of this chapter includes mCoA++, an implementation of MCoA [Sousa, 2013a] for OMNeT++ network simulator, which is publicly available, and the following publications:

1. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**A Multiple Care of Addresses Model**", ISCC, 2011 [Sousa et al., 2011d].

2. Bruno Sousa, Kostas Pentikousis, Marilia Curado, "**A study of multimedia application performance over Multiple Care-of Addresses in Mobile IPv6**", MediaWin, 2011 [Sousa et al., 2011c].

—It would behoove you to have your thesis finely tuned and the logical arguments utilized in support of it tightly woven into a credible, and creatively persuasive tapestry.

Rod Alan Woods, in *The Journey Is the Destination: A Book of Quotes With Commentaries*

6

Conclusion and Future Work

THIS final chapter provides an overview of the work that was performed, the problems that were addressed and the contributed developments to the field of study.

It is organized as follows. Section 6.1 provides a synthesis of the work hereby presented, followed by an overview of the research goals that were accomplished in Section 6.2. Finally, Section 6.3 discusses ongoing and future research directions.

6.1 Summary of the Thesis

The field of multihoming is composed by a diversity of topics related to evaluation, optimization and implementations. The following paragraphs summarize the contents of the thesis.

Chapter 2 corresponds to the multihoming state of the art. Several protocols, operating on distinct layers, have been compared regarding their multihoming support. This state of the art compares protocols regarding resilience, ubiquity, load sharing and flow distribution goals of multihoming and introduces the main types of multihoming, namely end-host, end-site and hybrid.

Chapter 3 introduced the Multihoming Evaluation Framework (MEF), which allows the evaluation of multihoming support in a protocol. More specifically, this thesis has specified frameworks to assess the multihoming support in protocols according to multihoming goals fulfilment. Indeed, the Resilience Evaluation Framework (REF) specifies methods to assess resilience support, whilst the Ubiquity Evaluation Framework (UEF) introduces methods to evaluate the ubiquity support of a protocol. Both of these frameworks constitute the basis for the Multihoming Evaluation Framework (MEF) and have the advantage of being easily used by non-experts as well as experts of resilience and UbiComp fields.

Chapter 4 specified an optimization technique for path selection problems. METHODICAL includes a path optimization algorithm that mitigates the *NP-hard* problem, by including multiple criteria and by specifying processes to score the diverse paths. This algorithm follows a Multiple Attribute Decision Mechanism (MADM) approach, and introduces an enhanced distance function to determine how far path criteria values are from ideal values. Such function, by correlating the different criteria, is able to cope with ranking abnormality, an issue that is pointed to MADM techniques, such as Technique for Order Preference by Similarly to Ideal Solution (TOPSIS) and Distance to Ideal Alternative (DiA). Moreover, a scoring stability function is introduced to avoid ping-pong effects on mobile networks. The optimization also includes an algorithm to specify weights for the several criteria in an objective and consistent way, according to a desired consistency ratio. Besides the optimization and criteria weighting algorithms, an objective and easy to use evaluation technique is also proposed to assess the performance of MADM techniques.

Chapter 5 introduced multihoming enhancements in protocols. A protocol supporting mobility in IPv6 networks has been considered and enhanced to enable multihoming support. Multiple Care of Address (MCoA) and Flow Bindings proposals extend the multihoming support of Mobile IPv6 (MIPv6) protocol. mCoA++ is an implementation of these proposals, in the OMNeT++ network simulator. The candidate has also taken the decision to release the code to the global research community, so that evaluation of future proposals mitigating multihoming issues in IPv6 or mobile networks have a basis simulation model.

6.2 Revisiting the Thesis Objectives

Briefly, the goals of this thesis were to propose a mechanism to evaluate multihoming support and to specify a mechanism to optimize multihoming experience in nodes with multiple interfaces/paths. Such goals have tailored the research in the thesis, leading to sub-goals, as presented in the beginning of each chapter. This section, revisits such goals and summarizes how they have been achieved.

In Chapter 2, the following goals were fulfilled:

- "Identify what is multihoming and the different types of multihoming, with their respective advantages and disadvantages". Multihoming has been discussed in detail, as well as different types of multihoming. In addition, diverse proposals in the state of art have been identified in the respective types of multihoming.

- "Identify the goals that multihoming solutions must pursue". Multihoming goals are four-fold: Resilience, Ubiquity, Load Sharing and Flow Distribution. Through the identification of such goals, the diverse proposals in the state-of-art have been compared.

In Chapter 3, the following objective was achieved:

- "Propose frameworks that allow to assess how multihoming goals are supported in a certain protocol. Such kind of framework, aims to establish a baseline to compare the multihoming support between protocols with the same purpose". The Multihoming Evaluation Framework (MEF) allows to assess the multihoming support of a protocol. More specifically, Resilience Evaluation Framework (REF) assesses resilience support and Ubiquity Evaluation Framework (UEF) assesses ubiquity support. These frameworks have also been applied to study the resilience and ubiquity support of different protocols, such as Stream Control Transport Protocol (SCTP), Mobile IPv6 (MIPv6) and Host Identity Protocol (HIP).

MeTHODICAL was specified in Chapter 4, leading to the accomplishment of the following objectives:

- "Specify a technique that allows an user to map her preferences in terms of criteria weighting. A scheme that allows to choose the importance of criteria over another objectively". An algorithm was specified to determine weights using linguistic terms, easily understood by humans are mapped into numeric scales to allow the determination of consistency. This way, the subjectivity of similar approaches is mitigated, by allowing to set weighs within a certain threshold, for instance 100% consistent.

- "Specify an optimization technique that is flexible enough to accommodate multiple criteria and is tailored to multihoming improvement". The *NP-hard* problem, in the face of multiple criteria, has been solved through an enhanced MADM approach. Indeed, the path optimization algorithm with a MADM approach introduces a distance function that correlates the criteria of different paths and a scoring stability function. Both enhanced functions are able to mitigate issues of MADM techniques, such as ranking abnormality or ranking identification.

- "Specify a mechanism to assess the accuracy of the Multiple Attribute Decision Mechanism (MADM) optimization techniques". Diverse MADM techniques are proposed in the literature. This thesis has also proposed a MADM technique (see previous goal). Nonetheless, this thesis has also proposed an evaluation mechanism based on the Design of Experiments (DoE) to assess the accuracy of diverse MADM techniques. The evaluation framework for MADM techniques enables an objective comparison between MADM approaches.

Multihoming has been improved in an implementation, namely the mCoA++ that accomplishes the following goals:

- "Improve the multihoming support of MIPv6". Multiple Care of Address (MCoA) and Flow Bindings improve multihoming support of MIPv6 by supporting the registration of multiple addresses, and by introducing policies for the different flows of applications.

- "Provide a standard implementation promoting enhanced multihoming support in MIPv6". mCoA++ is a public implementation of MCoA and Flow Bindings in the OMNeT++ network simulator.

The next subsection describes further research directions in the areas addressed in this thesis.

6.3 Future Work

Research is an endless process, where different iterations are required over time. The multihoming research topic is not an exception.

Future Internet architectures will coexist to explore multiple technologies, to accommodate high number of connected devices, to support more demanding applications and to guarantee acceptable levels of user satisfaction. Heterogeneity will be a constant, as it is already happening. Devices have different characteristics, access technologies are also increasing, and all need to coexist to enable high levels of resilience or simply to allow the always, anytime and anywhere paradigm.

Multihoming is, therefore, a natural evolution that future Internet architectures must pursue. The benefits of multihoming are vast. For instance, single point of failures when connections rely on a single interface or technology can be avoided. Notwithstanding, multihoming advantages in terms of resilience (e.g. higher levels of availability), ubiquity (e.g. the always, anytime and anywhere connected paradigm) have also overheads associated. For instance, energy consumption, security issues or costs aspects may arise.

Optimization techniques in the context of multihoming are imperative to establish a balanced tradeoff between the benefits and multihoming costs. Indeed, optimization techniques will have to be associated with cross-layer mechanisms on end-nodes to guarantee that the node acts in "unissimo" regarding multihoming. Optimization techniques need to have synchronized and cooperative schemes between network and nodes to overcome overloading issues that might appear.

Multihoming will be effective in future Internet architectures with cooperation schemes between network and end-nodes. The hybrid multihoming support can rely on mechanisms that promote the exchange of data between different technologies. For instance, an IEEE 802.11 network can report network load in a standardized way, so that the network load metric can be compared between heterogeneous technologies.

The synchronization is not only between nodes and networks. Applications running on end-nodes may need to map their requirements in a dynamic way, as in the occurrence of certain events, specific metrics may be more interesting. Such dynamics require optimization mechanisms to adapt, in order to include more or less criteria, or simply to adjust the frequency of measurements to improve accuracy.

Multihoming optimization mechanisms must include support for multiple applications at the same time and perform path selection according to a set of applications priority, or another relevant criterion. Without such "cooperation" an application might exhaust resources and degrade performance of others. In a cloud context, this "cooperation" is essential for a correct and sustainable management of resources. Virtualization is fundamental in a cloud environment to assure levels of availability and to maximize resilience support. Moreover, load balancing can be performed using optimized decision mechanisms to enable advanced distribution of load, as demonstrated in this thesis.

References

[Abley et al., 2003] Joe Abley, Benjamin Black, and Vijay Gill. Goals for IPv6 Site-Multihoming Architectures. IETF RFC: 3582, August 2003. 12

[Adkins, 2006] Daniel Adkins. Internet Indirection Infrastructure (i3). [Online] `http://i3.cs.berkeley.edu/` [Last Visit: 29-July-2013], 2006. 60

[Adkins et al., 2003] Daniel Adkins, Karthik Lakshminarayanan, and Adrian Perrig. Towards a More Functional and Secure Network Infrastructure. Technical Report UCB/CSD-03-1242, EECS Department, University of California, Berkeley, 2003. 59, 60

[Ahlgren et al., 2005] Bengt Ahlgren, Lars Eggert, Borje Ohlman, Jarno Rajahalme, and Andreas Schieder. Names, Addresses and Identities in Ambient Networks. In *Proceedings of the 1st ACM workshop on Dynamic Interconnection of Networks, DIN'05*, pages 33–37. ACM, August-September 2005. 34

[Akella et al., 2003] Aditya Akella, Bruce Maggs, Srinivasan Seshan, Anees Shaikh, and Ramesh Sitaraman. A Measurement-Based Analysis of Multihoming. In *proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 353–364. ACM, 2003. 69, 70, 75

[Al-Kuwaiti et al., 2009] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein. A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability. *Communications Surveys & Tutorials, IEEE*, 11(2):106–124, 2009. 69, 70

[Anand et al., 2011] Ashok Anand, Fahad Dogar, Dongsu Han, Boyan Li, Hyeontaek Lim, Michel Machado, Wenfei Wu, Aditya Akella, David G. Andersen, John W. Byers, Srinivasan Seshan, and Peter Steenkiste. XIA: An Architecture for an Evolvable and Trustworthy Internet. In *proceedings of the 10th ACM Workshop on Hot Topics in Networks, HotNets-X '11*, HotNets-X, pages 2:1–2:6. ACM, November 2011. 62

[Andersson et al., 2007] Karl Andersson, Daniel Granlund, and C. Åhlund. M4: Multimedia Mobility Manager: A Seamless Mobility Management Architecture Supporting Multimedia Applications. In *Proceedings of the 6th international conference on Mobile and ubiquitous multimedia*, pages 6–13. ACM, 2007. 194

[Anjali et al., 2010] Tricha Anjali, Alexander Fortin, Gruia Calinescu, Sanjiv Kapoor, Nandakiran Kirubanandan, and Sutep Tongngam. Multipath Network Flows: Bounded Buffers and Jitter. In *proceeginds of IEEE International Conference on Computer Communications, INFOCOM'10*, pages 1–7. IEEE, March 2010. 111

[Antucheviciene et al., 2011] Jurgita Antucheviciene, Algimantas Zakarevicius, and Edmundas Kazimieras Zavadskas. Measuring Congruence of Ranking Results Applying Particular MCDM Methods. *Informatica*, 22(3):319–338, 2011. 115, 117

[Arkko and van Beijnum, 2009] Jari Arkko and Iljitsch van Beijnum. Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming . IETF RFC: 5534, June 2009. 36

[Arshad and Mian, 2008] M. Junaid Arshad and M. Saleem Mian. Issues of Multihoming Implementation Using FAST TCP: A Simulation Based Analysis. *IJCSNS International Journal of Computer Science and Network Security* , 8(9):104–114, September 2008. 22

[Atkinson et al., 2010] Randall Atkinson, Saleem Bhatti, and Stephen Hailes. Evolving the Internet Architecture Through Naming. *J. Sel. Areas Commun.*, 28(8):1319–1325, October 2010. 50

[Autenrieth, 2003a] Achim Autenrieth. *Differentiated Resilience in IP-Based Multilayer Transport Networks*. PhD thesis, Technische Universitat Munchen, Munchen, April 2003a. 69, 70, 80

[Autenrieth, 2003b] Achim Autenrieth. Recovery Time Analysis of Differentiated Resilience in MPLS. In *proceedings of Fourth International Workshop on Design of Reliable Communication Networks, 2003. (DRCN 2003).* , pages 333–340, 2003b. 77

[Babiarz et al., 2006] Jozef Babiarz, Kwok Ho Chan, and Fred Baker. Configuration Guidelines for DiffServ Service Classes. IETF RFC: 4594, August 2006. 126

[Bagnulo et al., 2006] Marcelo Bagnulo, Alberto Garcia Martinez, Arturo Azcorra, and Cédric de Launois. An Incremental Approach to IPv6 Multihoming. *Computer Communications*, 29(5):582–592, March 2006. 1, 10, 11, 16

[Balakrishnan et al., 2004] Hari Balakrishnan, Karthik Lakshminarayanan, Sylvia Ratnasamy, Scott Shenker, Ion Stoica, and Michael Walfish. A Layered Naming Architecture for the Internet. *SIGCOMM Comput. Commun. Rev.*, 34(4):343–352, August 2004. 34, 36

[Ballani et al., 2009] Hitesh Ballani, Paul Francis, T. Cao, and Jia Wang. Making Routers Last Longer with ViAggre. In *proceedings of the 6th USENIX symposium on Networked systems design and implementation, NSDI '09*, pages 453–466. USENIX symposium, April 2009. 45, 47

[Behzadian et al., 2012] Majid Behzadian, S. Khanmohammadi Otaghsara, Morteza Yazdani, and Joshua Ignatius. A State-of The-Art Survey of TOPSIS Applications. *Expert Systems with Applications*, 39(17):13051 – 13069, 2012. 4, 112, 114

[Belhaj and Tagina, 2008] Salem Belhaj and Moncef Tagina. VFAST TCP: An improvement of FAST TCP. In *proceedings of tenth International Conference on Computer Modeling and Simulation, UKSIM' 08*, pages 88–93. IEEE, April 2008. 22

[Bellavista et al., 2010] Paolo Bellavista, Antonio Corradi, and Luca Foschini. IMS-Compliant Management of Vertical Handoffs for Mobile Multimedia Session Continuity. *IEEE Communications Magazine*, 48(4):114–121, April 2010. 194

[Benvenutti, 2005] Christian Benvenutti. *Understanding Linux Network Internals*. O'Reilly, December 2005. ISBN 0-596-00255-6. 20

[Bernardos, 2013] Carlos J. Bernardos. Proxy Mobile IPv6 Extensions to Support Flow Mobility. IETF Draft: draft-ietf-netext-pmipv6-flowmob (work in progress), February 2013. 30

[Blanchet and Seite, 2011] Marc Blanchet and Pierrick Seite. Multiple Interfaces and Provisioning Domains Problem Statement. IETF RFC: 6418, November 2011. 11, 15, 16

[Bohge and Renwanz, 2008] Mathias Bohge and Martin Renwanz. A Realistic VoIP Traffic Generation and Evaluation Tool for OMNeT++. In *proceedings of the 1st International Workshop on OMNeT++, SIMUTools'08*. ICST, 2008. 192

[Bokor, 2013] Laszlo Bokor. Host Identity Protocol (HIP) Simulation Framework for INET/OMNeT++. [Online] `http://www.ict-optimix.eu/index.php/HIPSim` [Last Visit: 29-July-2013], 2013. 35

[Bokor et al., 2009] László Bokor, Szabolcs Nováczki, László Tamás Zeke, and Gábor Jeney. Design and Evaluation of Host Identity Protocol (HIP) Simulation Framework for INET/OMNeT++. In *proceedings of MSWIM'09*. ACM, 2009. 180

[Boutet et al., 2008] Antoine Boutet, B. Le Texier, J. Montavont, Nicolas Montavont, and Guillaume Schreiner. Advantages of Flow Bindings: An Embedded Mobile Network Use Case. In *proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities, TRIDENTCOM '08*, pages 1–5. ICST, March 2008. 31

[Braden, 1989] Robert Braden. Requirements for Internet Hosts – Communication Layers. IETF RFC: 1122, October 1989. 11

[Brian Dickson, 2008] Brian Dickson. V6DH: Incremental IPv6 Dual-Homing Approach for addressing end-site reliability needs (per RADIR problem statement). IETF Draft: draft-dickson-rrg-v6dh (work in progress), 2008. 42

[Budzisz et al., 2008] L. Budzisz, R. Ferrús, A. Brunstrom, K.-J. Grinnemo, R. Fracchia, G. Galante, and F. Casadevall. Towards Transport-Layer Mobility: Evolution of SCTP multihoming. *Computer Communations*, 31(5):980–998, March 2008. 14, 70, 84

[Calle et al., 2004] Eusebi Calle, Jose L. Marzo, and Anna Urra. Protection Performance Components in MPLS Networks. *Computer Communications*, 27 (12):1220–1228, July 2004. 80

[Camarillo et al., 2010] Gonzalo Camarillo, A. Kera nen, and S. Pierrel. Automatic Flow-Specific Multi-Path Management for the Host Identity Protocol (HIP). In *proceedings of the IEEE Wireless Communications and Networking Conference, WCNC '10*, pages 1–6. IEEE, April 2010. 33

[Casimiro et al., 2012] Antonio Casimiro, Paulo Veríssimo, Diego Kreutz, Filipe Araujo, Raul Barbosa, Samuel Neves, Bruno Sousa, Marilia Curado, Carlos Silva, Rajeev Gandhi, and Priya Narasimhan. TRONE: Trustworthy and Resilient Operations in a Network Environment. In *proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN'12*, pages 1–6. IEEE, 2012. ISBN 978-1-4673-2264-5. x, 147, 150

[CCNx, 2013] CCNx. CCNx Release. [Online] `www.ccnx.org` [Last Visit: 29-July-2013], 2013. 48

[Chakraborty and Yeh, 2009] Subrata Chakraborty and Chung-hsing Yeh. A Simulation Comparison of Normalization Procedures for TOPSIS. In *proceedings of International Conference on Computers & Industrial Engineering, CIE'09*, pages 1815–1820. IEEE, 2009. 134

[Chakraborty and Yeh, 2012] Subrata Chakraborty and Chung-Hsing Yeh. Rank Similarity Based MADM Method Selection. In *proceedings of International Conference on Statistics in Science, Business, and Engineering, ICSSBE'12*, pages 1–6, 2012. 117

[Chan et al., 2008] Kwok Ho Chan, Jozef Babiarz, and Fred Baker. Aggregation of Diffserv Service Classes. IETF RFC: 5127, February 2008. 126

[Charilas and Panagopoulous, 2010] D.E. Charilas and A.D. Panagopoulous. Network Selection Problem: Multiaccess Radio Network Enviroments. *Vehicular Technology Magazine, IEEE*, 5(4):40–49, 2010. 4, 109, 111, 112

[Charoenpanyasak and Paillassa, 2007] S. Charoenpanyasak and B. Paillassa. SCTP Multihoming with Cross Layer Interface in Ad Hoc Multihomed Networks. In *proceedings of Third IEEE International Conference on Wire-*

less and Mobile Computing, Networking and Communications, WiMOB'07 , page 46. IEEE, October 2007. 25

[Chawla et al., 2007] M Chawla, BG Chun, and A Ermolinskiy. A Data-Oriented (and beyond) Network Architecture. *SIGCOMM Comput. Commun. Rev.*, 37(4):181–192, August 2007. 48, 49

[Chimento and Ishac, 2008] P. Chimento and J. Ishac. Defining Network Capacity. IETF RFC: 5136, February 2008. 122

[Choi, 2010] HyonYoung Choi. Proxy Mobile IPv6 for NS-2. [Online] `http://commani.net/pmip6ns/` [Last Visit: 29-July-2013], 2010. 31

[Choi et al., 2007] Nakjung Choi, Sungjoon Choi, Yongho Seok, Taekyoung Kwon, and Yanghee Choi. A Solicitation-Based IEEE 802.11p MAC Protocol for Roadside to Vehicular Networks. In *procedings of Mobile Networking for Vehicular Environments*, pages 91–96. IEEE, 2007. 126

[Choi et al., 2006] Younghwan Choi, Bongsoo Kim, Sang-Ha Kim, Minkyo In, and Seungyun Lee. A Multihoming Mechanism to Support Network Mobility in Next Generation Networks. In *proceedings of Asia-Pacific Conference on Communications, APCC '06*, pages 1–5. IEEE, August 2006. 13, 30

[Cholda et al., 2008] P. Cholda, A. Jajszczyk, and K. Wajda. A Unified Quality of Recovery (QoR) Measure. *International Journal of Communication Systems*, 21(5):525–548, September 2008. 2, 69

[Cholda et al., 2009] Piotr Cholda, János Tapolcai, Tibor Cinkler, Krzysztof Wajda, and Andrzej Jajszczyk. Quality of Resilience as a Network Reliability Characterization Tool. *Network, IEEE*, 23(2):11–19, March/April 2009. 2, 69, 70, 74, 75, 79, 80, 169

[Choque et al., 2011] Johnny Choque, Ramón Agüero, and Luis Muñoz. Optimum Selection of Access Networks Within Heterogeneous Wireless Environments Based on Linear Programming Techniques. *Mobile Network Applications*, 16(4):412–423, August 2011. 110, 111

[Choque et al., 2012] Johnny Choque, Ramón Agüero, and Luis Muñoz. Simulation Framework for the Evaluation of Access Selection Algorithms over

Heterogeneous Wireless Networks. In *Mobile Networks and Management*, volume 97 of *LNICS*, pages 46–60. Springer, 2012. 111

[Chowdhury et al., 2009] N. M. Mosharaf Kabir Chowdhury, Fida-E Zaheer, and Raouf Boutaba. iMark: An Identity Management Framework for Network Virtualization Environment. In *proceedings of IFIP/IEEE International Symposium on Integrated Network Management, IM '09*, pages 335–342. IEEE, June 2009. 52, 55

[Christian Dannewitz, 2013] Christian Dannewitz. NetInf - Network of Information. [Online] `http://www.netinf.org/home/home/` [Last Visit: 29-July-2013], 2013. 48, 49

[Clark et al., 2003] David Clark, Robert Braden, Aaron Falk, and Venkata Pingali. FARA: Reorganizing the Addressing Architecture. *SIGCOMM Comput. Commun. Rev.*, 33(4):313–321, August 2003. 34

[Clevenger, 2010] Bryan Clevenger. *HIDRA: Hierarchical Inter-Domain Routing Architecture*. PhD thesis, Faculty of California Polytechnic State University San Luis Obispo, 2010. 42, 44, 45, 46, 47, 54, 55, 56, 58, 61

[Cole and Rosenbluth, 2001] Rrobert Cole and J.H. Rosenbluth. Voice over IP Performance Monitoring. *SIGCOMM Computer Communication Review*, 31 (2), 2001. 148

[Community, 2013] INET-OMNeT++ Community. INET Framework. [Online] `http://inet.omnetpp.org/` [Last Visit: 29-July-2013], 2013. 182

[Crowcroft et al., 2003] Jon Crowcroft, Steven Hand, Richard Mortier, Timothy Roscoe, and Andrew Warfield. Plutarch: An Argument for Network Pluralism. *SIGCOMM Computer Communication Review*, 33(4):258–266, 2003. 39, 40

[CUBINLab, 2007] CUBINLab. FAST TCP Simulator Module for ns-2. [Online] `http://www.cubinlab.ee.unimelb.edu.au/ns2fasttcp/` [Last Visit: 29-July-2013], 2007. 23

[Dave, 2008] Meyer Dave. The Locator Identifier Separation Protocol (LISP). *The Internet Protocol Journal*, 11(1):23–36, March 2008. 43, 44, 46, 59

[Day, 2008] John Day. *Patterns in Network Architecture: A Return to Fundamentals*. Prentice Hall PTR, 2008. ISBN 0132252422. 13

[de la Oliva et al., 2010] Antonio de la Oliva, Ignacio Soto, Alberto Garca-Martnez, Marcelo Bagnulo, and Arturo Azcorra. Analytical Characterization of Failure Recovery in REAP. *Computer Communications*, 33(4):485–499, March 2010. 32

[de la Oliva et al., 2011] Antonio de la Oliva, Carlos J. Bernardos, Maria Calderon, Telemaco Melia, and J.C. Zuniga. IP Flow Mobility: Smart Traffic Offload for Future Wireless Networks. *Communications Magazine, IEEE*, 49 (10):124–132, 2011. 3, 178, 180

[de Launois and Bagnulo, 2006] Cédric de Launois and Marcelo Bagnulo. The Paths Toward IPv6 Multihoming. *Communications Surveys Tutorials*, 8(2):38–51, Second Quarter 2006. 2, 3, 9, 17, 26, 28

[Dedu, 2013] Eugen Dedu. Wireless DCCP patch in NS2. [Online] `http://lifc.univ-fcomte.fr/home/~ededu/ns2/` [Last Visit: 29-July-2013], 2013. 27

[Deleplace et al., 2007] Angeline Deleplace, Theirry Ernst, and Thomas Noel. Multihoming in Nested Mobile Networks with Route Optimization. In *proceedings of International Symposium on Applications and the Internet Workshops, SAINT '07*, page 49. IEEE, January 2007. 30

[Demichelis and Chimento, 2002] C. Demichelis and P. Chimento. IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). IETF RFC: 3393, November 2002. 122

[Demter and Fu, 2006] Jan Demter and Xiaoming Fu. GONE – GIST Overlay Networking Extension. [Online] `http://user.informatik.uni-goettingen.de/~fu/gone/` [Last Visit: 29-July-2013], 2006. 60

[Devarapalli et al., 2005] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol. IETF RFC: 3963, January 2005. 32

[Devarapalli et al., 2009] Vijay Devarapalli, Nishi Kant, Heeseon Lim, and Christian Vogt. Multiple Interface Support with Proxy Mobile IPv6. IETF Draft: (work in progress), March 2009. 29

[Deza and Deza, 2009] Michel Deza and Elena Deza. *Encyclopedia of Distances*. Encyclopedia of Distances. Springer, 2009. ISBN 9783642002342. 132

[Dhraief and Montavont, 2008] Amine Dhraief and Nicolas Montavont. Toward Mobility and Multihoming Unification-The SHIM6 Protocol: A Case Study. In *proceedings of the IEEE Wireless Communications and Networking Conference, WCNC '08*, pages 2840–2845. IEEE, March-April 2008. 12, 33

[Dionysiou et al., 2010] Theodoros Dionysiou, Vasilios A Siris, and George Stamatakis. Utility-based Channel Assignment and Topology Control in Wireless Mesh Networks. In *proceedings of IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM'10*, pages 1–9, 2010. 111, 120

[Do and Onozato, 2007] Hung Tuan Do and Yoshikuni Onozato. A Comparison of Different Paging Mechanisms for Mobile IP. *Wireless Networking*, 13(3): 379–395, 2007. 72

[Drago et al., 2012] Idilio Drago, Marco Mellia, Maurizio Munafo, Anna Sperotto, Ramin Sadre, and Aiko Pras. Inside Dropbox: Understanding Personal Cloud Storage Services. In *proceedings of the 12th ACM Internet Measurement Conference, IMC'12*, 2012. 142, 143, 146

[Dreibholz et al., 2010] Thomas Dreibholz, Martin Becke, Jobin Pulinthanath, and Erwin P. Rathgeb. Implementation and Evaluation of Concurrent Multipath Transfer for SCTP in the INET Framework. In *proceedings of 3rd International ICST Conference on Simulation Tools and Techniques, SIMUTOOLS '10*, pages 1–8. ICST, 2010. 180

[Drepper et al., 2013] Ulrich Drepper, Scott Miller, and David Madore. md5sum(1) - Linux man page. [Online] `http://linux.die.net/man/1/md5sum` [Last Visit: 29-July-2013], 2013. 152

[Droms, 1997] Ralph Droms. Dynamic Host Configuration Protocol. IETF RFC: 2131, March 1997. 15

[Dunmore et al., 2005] Martin Dunmore, Njal T. Borch, Tim Chown, Oliver Kramer, and Pekka Savola. Deliverable D4.5.3 Evaluation of Multihoming Solutions. [Online] `http://www.6net.org/publications/deliverables/D4.5.3.pdf` [Last Visit: 29-July-2013], February 2005. 34

[Dutta et al., 2007] Rudra Dutta, G.N. Rouskas, I. Baldine, A. Bragg, and D. Stevenson. The SILO Architecture for Services Integration, Control, and Optimization for the Future Internet. In *proceedings of IEEE International Conference on Communications, ICC '07*, pages 1899–1904. IEEE, June 2007. 47, 49

[Eklund et al., 2009] Johan Eklund, Karl-Johan Grinnemo, Stephan Baucke, and Anna Brunstrom. Tuning SCTP Failover for Carrier Grade Telephony Signaling. *Computer Networks*, August 2009. 6, 70, 84

[Ernst, 2002] Thierry Ernst. MobiWan: NS-2 Extensions to Study Mobility in Wide-Area IPv6 Networks. [Online] `http://www.inrialpes.fr/planete/mobiwan/` [Last Visit: 29-July-2013], 2002. 31

[Ernst and Charbon, 2004] Thierry Ernst and Julien Charbon. Multihoming with NEMO Basic Support. In *proceedings of First International Conference on Mobile Computing and Ubiquitous Computing, ICMU '04*. IPSJ, January 2004. 13

[Espi et al., 2009] Jorge Espi, Robert Atkinson, Ivan Andonovic, and John Dunlop. Proactive Route Optimization for Fast Mobile IPv6. In *proceedings of IEEE 70th Vehicular Technology Conference, VTC-Fall'09*, volume 6, pages 1–5. IEEE, September 2009. 1, 14, 18

[Eswaran et al., 2010] Sharanya Eswaran, David Shur, and Sunil Samtani. Information Utility in Mission-Oriented Networks. In *proceedings of IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM'10*, pages 1–9, 2010. 111

[Faigl et al., 2011] Zoltn Faigl, Lszl Bokor, Pedro Miguel Neves, Khadija Daoud, and Philippe Herbelin. Evaluation of Two Integrated Signalling Schemes for the Ultra Flat Architecture Using SIP, {IEEE} 802.21, and HIP/PMIP Protocols . *Computer Networks*, 55(7):1560 – 1575, 2011. 104

[Farinacci et al., 2012] D. Farinacci, D. Lewis, D. Meyer, and C. White. LISP Mobile Node. IETF Draft: draft-meyer-lisp-mn (work in progress), October 2012. 57, 59

[Farinacci et al., 2013] Dino Farinacci, Darrel Lewis, Dave Meyer, and Chris White. LISPMob - A Deployable Network Layer Mobility Implementation for

Linux. [Online] http://lispmob.org/ [Last Visit: 29-July-2013], October 2013. 57, 60

[Fekete and Hämäläinen, 2009] Gábor Fekete and Timo Hämäläinen. State of Host-Centric Multihoming in IP Networks. In *proceedings of the IFIP International Conference on New Technologies, Mobility and Security, NTMS '09*, pages 1–5. IEEE, December 2009. 2, 9, 17, 18

[Fekete, 2010] Gbor Fekete. *Network Interface Management in Mobile and Multihomed Nodes*. PhD thesis, University of Jyväskyla, Faculty of Information Technology, June 2010. 33, 74

[Feldmann et al., 2009] Anja Feldmann, Luca Cittadini, Wolfgang Mühlbauer, Randy Bush, and O. Maennel. HAIR: Hierarchical Architecture for Internet Routing. In *proceedings of Re-architecting the Internet, ReArch '09*, pages 43–48. ACM, 2009. 54, 55

[Feldmann et al., 2012] Anja Feldmann, Luca Cittadini, Wolfgang Mühlbauer, Randy Bush, and O. Maennel. Proof-of-Concept Implementation of HAIR. [Online] http://sites.google.com/site/hairarchsite/ [Last Visit: 29-July-2013], 2012. 54, 56

[Figueira et al., 2005] José Figueira, Salvatore Greco, and Mathias Ehrgott. *Multiple Criteria Decision Analysis: State of The Art Surveys*. Springer, 2005. ISBN 978-0-387-23067-2. 4, 7, 112, 115, 118, 122

[Fitzpatrick et al., 2009] John Fitzpatrick, S. Murphy, Mohammed Atiquzzaman, and John Murphy. Using Cross-Layer Metrics to Improve the Performance of End-to-End Handover Mechanisms. *Computer Communications*, 32(15):1600–1612, June 2009. 16, 26

[Floyd and Kohler, 2006] Sally Floyd and Eddie Kohler. Profile for Datagram Congestion Control Protocol (DCCP) Congestion Control ID 2: TCP-Like Congestion Control. IETF RFC: 4341, March 2006. 26

[Floyd and Kohler, 2009] Sally Floyd and Eddie Kohler. Profile for Datagram Congestion Control Protocol (DCCP) Congestion ID 4: TCP-Friendly Rate Control for Small Packets (TFRC-SP). IETF RFC: 5622, August 2009. 26

[Ford et al., 2011] Alan Ford, Costin Raiciu, Mark Handley, Sebastien Barre, and Janardhan Iyengar. Architectural Guidelines for Multipath TCP Development. IETF RFC: 6182, March 2011. 21, 24

[Ford et al., 2013] Alan Ford, Costin Raiciu, Mark Handley, and Olivier Bonaventure. TCP Extensions for Multipath Operation with Multiple Addresses. IETF RFC: 6824, January 2013. 21, 24

[Ford, 2008] Bryan Alexander Ford. *UIA : A Global Connectivity Architecture for Mobile Personal Devices*. PhD thesis, Massachusetts Institute of Technology, September 2008. 57

[Foundation, 2013] Apache Software Foundation. Apache Virtual Host documentation. [Online] `http://httpd.apache.org/docs/2.2/vhosts/` [Last Visit: 29-July-2013], 2013. 20

[Francis and Gummadi, 2001] Paul Francis and Ramakrishna Gummadi. IPNL: A NAT-Extended Internet Architecture. *SIGCOMM Comput. Commun. Rev.*, 31:69–80, August 2001. 38, 39, 40

[Franken, 2013] Kommunikationsnetz Franken. Stream Control Transmission Protocol (SCTP). [Online] `http://www.sctp.de/sctp.html` [Last Visit: 29-July-2013], 2013. 27

[Fu and Atiquzzaman, 2004] Shaojian Fu and M. Atiquzzaman. SCTP: State of the Art in Research, Products, and Technical Challenges. *IEEE Communications Magazine*, 42(4):64–76, April 2004. 93

[Fu and Crowcroft, 2006] Xiaoming Fu and Jon Crowcroft. GONE: An Infrastructure Overlay for Resilient, DoS-Limiting Networking. In *proceedings of Network and Operating Systems Support for Digital Audio and Video, NOSSDAV '06*, pages 18:1–18:6. ACM, May 2006. ISBN 1-59593-285-2. 59, 61, 64

[Gamage et al., 2011] Sahan Gamage, Ardalan Kangarlou, and Ramana Rao Kompella. Opportunistic Flooding to Improve TCP Transmit Performance in Virtualized Clouds. *Symposium on Cloud*, 2011. 151

[Garcia-Martinez et al., 2010] A. Garcia-Martinez, Marcelo Bagnulo, and I. Van Beijnum. The SHIM6 Architecture for IPv6 Multihoming. *Communications Magazine*, 48(9):152–157, September 2010. 32

[GNU, 2013] GNU. GNU Linear Programming Kit (GLPK) . [Online] `http://www.gnu.org/software/glpk/` [Last Visit: 29-July-2013], 2013. 109, 111

[Gong, Qipeng and Kabal, Peter, 2011] Gong, Qipeng and Kabal, Peter. Improved Quality for Conversational VoIP using Path Diversity. In *proceedings of Twelfth Annual Conference of the International Speech Communication Association, INTERSPEECH '11*, 2011. 148

[Graf et al., 2013] Thomas Graf, Greg Maxwell, Remco van Mook, Martijn van Oosterhout, Paul B Schroeder, Jasper Spaans, and Pedro Larroy. Linux Advanced Routing & Traffic Control . [Online] `http://www.lartc.org/` [Last Visit: 29-July-2013], 2013. 147

[Griffith et al., 2003] David Griffith, Kotikalapudi Sriram, Stephan Klink, and Nada Golmie. Optimal Mixtures of Different Types of Recovery Schemes in Optical Networks. [Online] `http://www.antd.nist.gov/pubs/paper1.pdf` [Last Visit: 29-July-2013], 2003. 80

[Gritter and Cheriton, 2001] M. Gritter and D.R. Cheriton. An Architecture for Content Routing Support in the Internet. In *Proceedings of the 3rd conference on USENIX Symposium on Internet Technologies and Systems, USITS '01*, pages 4–4. USENIX, March 2001. 38, 40

[Gundavelli et al., 2008] Sri Gundavelli, Kent Leung, Vijay Devarapalli, Kuntal Chowdhury, and Basavaraj Patil. Proxy Mobile IPv6. IETF RFC: 5213, August 2008. 31

[Gurtov, 2008] Andrei Gurtov. *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley Series, 2008. ISBN 978-0-470-99790-1. 32, 33, 36, 87, 94, 95

[Gurtov, 2013] Andrei Gurtov. InfraHIP Infrastructure for HIP . [Online] `http://infrahip.hiit.fi/` [Last Visit: 29-July-2013], 2013. 35

[Gurtov et al., 2008] Andrei Gurtov, Dmitry Korzun, and Andrey Lukyanenko. HI3: An Efficient and Secure Networking Architecture for Mobile Hosts. *Comput. Commun.*, 31(10):2457–2467, June 2008. 59, 60

[Gurtov et al., 2009] Andrei Gurtov, Miika Komu, and Robert Moskowitz. Host Identity Protocol: Identifier/Locator Split for Host Mobility and Multihoming. *The Internet Protocol Journal*, 12(1):27–32, March 2009. 33

[Guy Almes and Zekauskas, 1999a] Sunil Kalidindi Guy Almes and Matthew Zekauskas. A One-way Delay Metric for IPPM. IETF RFC: 2679, September 1999a. 122

[Guy Almes and Zekauskas, 1999b] Sunil Kalidindi Guy Almes and Matthew Zekauskas. A One-way Packet Loss Metric for IPPM. IETF RFC: 2680, September 1999b. 122

[Guy Almes and Zekauskas, 1999c] Sunil Kalidindi Guy Almes and Matthew Zekauskas. A Round-trip Delay Metric for IPPM. IETF RFC: 2681, September 1999c. 122

[Habib et al., 2007] Ahsan Habib, N. Christin, and J. Chuang. Taking Advantage of Multihoming with Session Layer Striping. In *proceedings of the IEEE International Conference on Computer Communications, INFOCOM '07*, pages 1–6. IEEE, April 2007. 34, 36

[Hagen, 2006] Silvia Hagen. *IPv6 Essentials*. O'Reilly Media, Inc., 2006. ISBN 0596100582. 15

[Halas et al., 2012] M. Halas, A. Kovac, M. Orgon, and I. Bestak. Computationally Efficient E-model Improvement of MOS Estimate Including Jitter and Buffer Losses. In *proceedings of the International Conference on Telecommunications and Signal Processing, TSP '12*. IEEE, 2012. 148, 149

[Hanka et al., 2009] O. Hanka, G. Kunzmann, C. Spleiss, J. Eberspacher, and A. Bauer. HiiMap: Hierarchical Internet Mapping Architecture. In *proceedings of First International Conference on Future Information Networks, ICFIN '09*, pages 17 –24. IEEE, October 2009. 52, 55

[Herrin, 2007] William Herrin. Tunneling Route Reduction Protocol (TRRP). [Online] `http://bill.herrin.us/network/trrp.html` [Last Visit: 29-July-2013], 2007. 45

[Hillier and Lieberman, 1995] Frederick Hillier and Gerald Lieberman. *Introduction to Operations Research - Sixth Edition*. McGraw-Hill, 1995. ISBN 9780078414497. 4, 110

[Hopps, 2000] Christian E. Hopps. Analysis of an Equal-Cost Multi-Path Algorithm. IETF RFC: 2992, November 2000. 20

[Hou et al., 2009] Jie Hou, Liu Yaping, and Gong Zhenghu. SILMS: A Scalable and Secure Identifier-to-Locator Mapping Service Sytem Design for Future Internet. In *proceedings of Second International Workshop on Computer Science and Engineering, WCSE '09*, volume 1, pages 54–58. IEEE, October 2009. 52, 55, 64

[Huang et al., 2007] Song Huang, Yong Xu, and Ling Zhang. A Path Diversity Metric for End-to-End Network. In *proceedings of 13th Pacific Rim International Symposium on Dependable Computing, PRDC'07*, pages 115–122, 2007. 69, 70, 75

[Huszak and Imre, 2010] A. Huszak and S. Imre. Eliminating Rank Reversal Phenomenon in GRA-Based Network Selection Method. In *proceedings of the IEEE International Conference on Communications, ICC'10*, pages 1–6, 2010. 115

[IBM, 2001] IBM. iSeries TCP/IP Configuration and Reference Version 5 (SC41-5420-04), May 2001. 20

[İç, 2012] Yusuf Tansel İç. An Experimental Design Approach Using TOPSIS Method for The Selection of Computer-Integrated Manufacturing Technologies. *Robot. Comput.-Integr. Manuf.*, 28(2):245–256, April 2012. 118

[IEEE, 1990] IEEE. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries 610, 1990. 88, 246, 247, 248, 249

[INET, 2012] INET. INET Framework - Implemented Protocols. [Online] `http://inet.omnetpp.org/index.php?n=Main.Status` [Last Visit: 29-July-2013], 2012. 27

[INL, 2013] INL. LinShim6. [Online] `http://inl.info.ucl.ac.be/LinShim6` [Last Visit: 29-July-2013], 2013. 35

[International Electrotechnical Commission, 2013a] International Electrotechnical Commission. Electropedia: The World's Online Electrotechnical Vocabulary. [Online] `http://www.electropedia.org/` [Last Visit: 29-July-2013], 2013a. 88, 246, 247, 248, 249

[International Electrotechnical Commission, 2013b] International Electrotechnical Commission. International Electrotechnical Commission Glossary. [Online] `http://std.iec.ch/glossary` [Last Visit: 29-July-2013], 2013b. 88, 246, 247, 248, 249

[ITU, 2001] ITU. Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs . Recommendation P.862, February 2001. 148

[ITU-R, 1997] ITU-R. Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000. ITU-R Recommendation M.1225, 1997. 193

[ITU-T, 1993] ITU-T. Recommendation M.495, Transmission Restoration and Transmission Route Diversity: Terminology and General Principles, 1993. 69, 77

[ITU-T, 1996] ITU-T. ITU-T Recommendation G.723.1, Dual Rate Speech Coder For Multimedia Communications Transmitting at 5.3 and 6.3 kbit/s , 3 1996. 84

[ITU-T, 2006] ITU-T. ITU-T Recommendation Y.1541, Network Performance Objectives for IP-Based Services, February 2006. 126, 127, 147

[ITU-T, 2007] ITU-T. ITU-T Recommendation G.1050, Network Model for Evaluating Multimedia Transmission Performance over Internet Protocol, November 2007. 127

[ITU-T, 2008] ITU-T. ITU-T Recommendation E.800, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors - Quality of Telecommunications Services: Concepts, Models, Objectives and Dependability Planning - Terms and Definitions Related to the Quality of Telecommunication Services , 9 2008. 74, 75

[ITU-T, 2011] ITU-T. The E-model: A Computational Model for Use in Transmission Planning. Recommendation G.107, December 2011. 122, 148

[ITU-T, 2011a] ITU-T. Perceptual Evaluation of Speech Quality (PESQ), An Objective Method for End-to-End Speech Quality Assessment of Narrowband Telephone Networks and Speech Codecs. ITU-T Recommendation P.862, February 2011a. 192

[ITU-T, 2011b] ITU-T. Mapping Function for Transforming P.862 Raw Result Scores to MOS-LQO. ITU-T Recommendation P.862.2, February 2011b. 192

[ITU-T, 2013] ITU-T. PESQ tool. [Online] `http://www.itu.int/rec/T-REC-P.862-200511-I!Amd2/en` [Last Visit: 29-July-2013], 2013. 192

[Iyengar et al., 2006] J.R. Iyengar, P.D. 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. 15, 26, 28, 74

[Jacobson et al., 2009] Van Jacobson, Diana Smetters, James Thornton, Michael Plass, Nicholas Brighs, and Rebecca Braynard. Networking Named Content. In *proceedings of the International Conference on emerging Networking EXperiments and Technologies, CoNEXT '09*, pages 1–12. ACM, December 2009. 48, 49

[Jain et al., 2012] Raj Jain, Subharthi Paul, and Chakchai Soin. Future Wireless Networks: Key Issues and a Survey (ID/Locator Split Perspective). *International Journal of Communication Networks and Distributed Systems*, 8(1/2): 24–52, December 2012. 18

[Jeff Boote and Aaron Brown , 2012] Jeff Boote and Aaron Brown . Internet 2 Bandwidth Test Controller (BWCTL). [Online] `http://www.internet2.edu/performance/bwctl/index.html` [Last Visit: 29-July-2013], 2012. 143, 147

[Jeff Boote and Anatoly Karp , 2012] Jeff Boote and Anatoly Karp . Internet 2 One-Way Ping (OWAMP). [Online] `http://www.internet2.edu/performance/owamp/index.html` [Last Visit: 29-July-2013], 2012. 143, 147

[Jelassi et al., 2012] Sofiene Jelassi, Gérard Rubino, H. Melvin, Habib Youssef, and G. Pujolle. Quality of Experience of VoIP Service: A Survey of Assessment Approaches and Open Issues. *Communications Surveys & Tutorials*, 14, 2012. 148

[Jen et al., 2007] D. Jen, M. Meisel, Daniel Massey, L. Wang, B. Zhang, and L. Zhang. APT: A Practical Transit Mapping Service. IETF Draft: draft-jen-apt-01 (work in progress), November 2007. 44, 46

[Johnson et al., 2011] David Johnson, Charles Perkins, and Jari Arkko. Mobility Support in IPv6. IETF RFC: 6275, July 2011. 2, 31, 87, 94, 95, 177, 178

[Jonsson et al., 2003] Andreas Jonsson, M. Folke, and Bengt Ahlgren. The Split Naming/Forwarding Network Architecture. In *proceedings of First Swedish National Computer Networking Workshop, SNCNW '03*. ACM, September 2003. 59, 60

[Kaleem, 2012] Faisal Kaleem. *VHITS: Vertical Handoff Initiation and Target Selection in a Heterogeneous Wireless Network*. PhD thesis, Florida International University, March 2012. 4, 113

[Karopoulos et al., 2010] Giorgos Karopoulos, Georgios Kambourakis, Stefanos Gritzalis, and Elisavet Konstantinou. A Framework for Identity Privacy in SIP. *J. Netw. Comput. Appl.*, 33(1):16–28, January 2010. 18

[Kent and Atkinson, 1998] Stephen Kent and Randall Atkinson. Security Architecture for the Internet Protocol. IETF RFC: 2401, November 1998. 97

[Khan, 2013] Shahbaz Khan. OPNET Application and Network Performance. [Online] `https://enterprise1.opnet.com/tsts/4dcgi/MODELS_FullDescription?ModelID=873` [Last Visit: 29-July-2013], 2013. 35

[Khare et al., 2010] V. Khare, D. Jen, Xin Zhao, Yaoqing Liu, Daniel Massey, Lan Wang, Beichuan Zhang, and Lixia Zhang. Evolution Towards Global Routing Scalability. *J. Sel. Areas Commun*, 28(8):1363 –1375, October 2010. 41, 42

[Kim and Choi, 2010] H.J. Kim and S.G. Choi. A Method to Support Multiple Interfaces a Mobile Node in Next Generation Wireless Network. In *proceedings of Sixth International Conference on Networked Computing and Advanced Information Management, NCM '10*, pages 276–281. IEEE, August 2010. 29

[Kim et al., 2012] Jong-Hwan Kim, Ji-Hyeong Han, Ye-Hoon Kim, Seung-Hwan Choi, and Eun-Soo Kim. Preference-Based Solution Selection Algorithm for Evolutionary Multiobjective Optimization. *Trans. Evol. Comp*, 16(1):20–34, February 2012. 111

[Kim and Shin, 2007] Kyu-Han Kim and Kang G. Shin. PRISM: Improving the Performance of Inverse-Multiplexed TCP in Wireless Networks. *IEEE*

Transactions Mobile Computers, 6(12):1297 –1312, December 2007. ISSN 1536-1233. 21, 23, 24, 27, 28

[Kohler, 2006] Eddie Kohler. Generalized Connections in the Datagram Congestion Control Protocol. IETF Draft: draft-kohler-dccp-mobility (work in progress), June 2006. 26

[Kohler et al., 2006] Eddie Kohler, Mark Handley, and Sally Floyd. Congestion Control Protocol (DCCP). IETF RFC: 4340, March 2006. 21, 26

[Komu et al., 2011] M. Komu, M. Bagnulo, K. Slavov, and S. Sugimoto (Ed.). Socket Application Program Interface (API) for Multihoming Shim. IETF RFC: 6316, July 2011. 33

[Komu and Henderson, 2011] Miika Komu and Thomas Henderson. Basic Socket Interface Extensions for Host Identity Protocol (HIP). IETF RFC: 6317, July 2011. 33

[Kong et al., 2008] Ki-Sik Kong, Wonjun Lee, Youn-Hee Han, Myung-Ki Shin, and HeungRyeol You. Mobility Management for All-IP Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6. *Wireless Communications*, 15(2):36–45, April 2008. 28, 29, 71, 72

[Kong, 2008] Ruoshan Kong. The Simulation for Network Mobility Based on NS2. In *proceedings of International Conference on Computer Science and Software Engineering, CSSE'08* , volume 4, pages 1070–1074. IEEE, December 2008. 31

[Koodli, 2008] Rajeev Koodli. Mobile IPv6 Fast Handovers. IETF RFC: 5268, June 2008. 3, 31, 180

[Koodli and Ravikanth, 2002] Rajeev Koodli and Rayadurgam Ravikanth. One-way Loss Pattern Sample Metrics . IETF RFC: 3357, August 2002. 122

[Krishnan et al., 2007] Suresh Krishnan, Nicolas Montavont, Eric Njedjou, Siva Veerepalli, and Alper E. Yegin. Link-Layer Event Notifications for Detecting Network Attachments. IETF RFC: 4957, August 2007. 15

[Kuntz, 2007] Romain Kuntz. Deploying Reliable IPv6 Temporary Networks Thanks to NEMO Basic Support and Multiple Care-of Addresses Registration. In *proceedings of the International Symposium on Applications and* *the Internet Workshops, SAINT '07*, page 46. IEEE, January 2007. ISBN 0769527574. 30

[Kuntz, 2013a] Romain Kuntz. UMIP - Mobile IPv6 and NEMO for Linux. [Online] `http://umip.org/` [Last Visit: 29-July-2013], 2013a. 3, 180

[Kuntz, 2013b] Romain Kuntz. MCoA / DSMIPv6 implementation for UMIP. [Online] `http://umip.org/contrib/umip-mcoa-dsmipv6.html` [Last Visit: 29-July-2013], 2013b. 3, 180

[Kwon and Kim, 2006] Ohbyung Kwon and Jihoon Kim. A Multi-Layered Assessment Model for Evaluating the Level of Ubiquitous Computing Services. In *Ubiquitous Intelligence and Computing*, volume 4159, pages 1059–1068. Springer, 2006. 2, 71, 72, 90

[Laganier and Eggert, 2008] J. Laganier and L. Eggert. Host Identity Protocol (HIP) Rendezvous Extension. IETF RFC: 5204, April 2008. 34

[Lahby et al., 2012] Mohamed Lahby, Leghris Cherkaoui, and Abdellah Adib. Article: New Optimized Network Selection Decision in Heterogeneous Wireless Networks. *International Journal of Computer Applications*, 54(16): 1–7, September 2012. Published by Foundation of Computer Science. 4, 114, 132, 133, 134, 145, 159

[Lahde et al., 2010] Sven Lahde, Martin Wegner, and Lars Wolf. Efficient Network Selection in Heterogeneous Communication Scenarios using Arbitration. In *proceedings of IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM'10*, 2010. 120

[Launois et al., 2003] Cédric De Launois, Olivier Bonaventure, Marc Lobelle, and Universit Catholique De Louvain. The NAROS Approach for IPv6 Multihoming with Traffic Engineering. In *proceedings of International Workshop on Quality of Future Internet Services, QoFIS '03*, pages 112–121. Springer, October 2003. 32, 34, 36

[Lee et al., 2008] Jong-Hyouk Lee, Tai-Myoung Chung, Sangheon Pack, and Sri Gundavelli. Shall We Apply Paging Technologies to Proxy Mobile IPv6? In *Proceedings of MobiArch'08*, pages 37–42. ACM, 2008. 72, 94

[Li, 2010] Hong Li. *Quality-of-Service Routing for Voice-over-IP in Service Overlay Networks*. PhD thesis, Department of Electrical & Computer Engineering of McGill University, November 2010. 148

[Li et al., 2012] J Li, M Manley, M Veeraraghavan, and RD Williams. A Less-Is-More Architecture (LIMA) for a Future Internet. In *proceedings of IEEE Conference on Computer Communications Workshops, INFOCOM '12*, pages 55–60. IEEE, March 2012. 51, 55

[Li and Macy, 2009] Qing Li and Kip Macy. Optimizing the BSD Routing System for Parallel Processing. In *proceedings of PRESTO '09*. ACM, August 2009. 20

[Li, 2011] Tony Li. Recommendation for a Routing Architecture. IETF RFC: 6115, February 2011. 40, 42, 50

[Li et al., 2013] Xi Li, Olivier Mehani, Ramn Agero, Roksana Boreli, Yasir Zaki, and Umar Toseef. Evaluating User-Centric Multihomed Flow Management for Mobile Devices in Simulated Heterogeneous Networks. In *Mobile Networks and Management*, volume 58 of *LNICS*, pages 84–98. Springer, 2013. ISBN 978-3-642-37934-5. 142

[Liu et al., 2007] Yi Liu, Mingxiu Li, Bo Yang, Depei Qian, and Weiguo Wu. Handover for Seamless Stream Media in Mobile IPv6 Network. In *proceedings of Wired/Wireless Internet Communications, WWIC'07*, volume 4517 of *LNCS*, pages 55–66. Springer, 2007. 71, 72, 92

[Louta et al., 2011] Malamati D. Louta, Philippos Zournatzis, Stylianos KraounaWs, Panagiotis G. Sarigiannidis, and Ioannis Demetropoulos. Towards Realization of The ABC Vision: A Comparative Survey of Access Network Selection. In *proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC'11*, pages 472–477. IEEE, July 2011. 88

[Mahmoodzadeh et al., 2007] S Mahmoodzadeh, J Shahrabi, M Pariazar, and MS Zaeri. Project Selection by Using Fuzzy AHP and TOPSIS Technique. *International Journal of Humanities and Social Sciences*, 1:135–140, 2007. 118

[Makaya and Pierre, 2008] C. Makaya and S. Pierre. An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols. *IEEE Transactions Wireless Communications*, 7(3):972–983, 2008. 72, 91

[Marler and Arora, 2004] R.T. Marler and J.S. Arora. Survey of Multi-Objective Optimization Methods for Engineering. *Structural and Multidisciplinary Optimization*, 26(6):369–395, 2004. 4, 111

[Massey et al., 2009] Daniel Massey, Lan Wang, and B Zhang. NeTS-FIND: Enabling Future Internet Innovations Through Transit Wire (eFIT). [Online] `http://www.nets-find.net/Funded/eFIT.php` [Last Visit: 29-July-2013], 2009. 41, 42

[Matouek and Gärtner, 2006] Jirí Matouek and Bernd Gärtner. *Understanding and Using Linear Programming*. Springer-Verlag New York, Inc., 2006. ISBN 3540306978. 126

[Matsumoto et al., 2003] Arifumi Matsumoto, Masahiro Kozuka, Kenji Fujikawa, and Yasuo Okabe. TCP Multi-Home Options. IETF Draft: draft-arifumi-tcp-mh (work in progress), October 2003. 21, 22

[Mehani et al., 2011] Olivier Mehani, Roksana Boreli, Michael Maher, and Thierry Ernst. User- and Application-Centric Multihomed Flow Management. In *proceedings of IEEE 36th Conference on Local Computer Networks, LCN'11*, pages 26 –34, October 2011. 110, 111

[Mehbod et al., 2013] Abolfazl Mehbod, Faisal Kaleem, Kang K. Yen, and Fumiyuki Adachi. A Fuzzy Extension of VIKOR for Target Network Selection in Heterogeneous Wireless Environments. *Physical Communication*, pages 145–155, 2013. 115

[Melia and Gundavelli, 2012] Telemaco Melia and Sri Gundavelli. Logical Interface Support for Multi-Mode IP Hosts. IETF Draft: draft-ietf-netext-logical-interface-support (work in progress), October 2012. 29

[Menth et al., 2010] Michael Menth, Matthias Hartmann, and Dominik Klein. Global Locator, Local Locator, and Identifier Split (GLI-split). Technical Report 470, University of Würzburg, Institute of Computer Science, April 2010. 37, 40

[Mikhailov, 2003] Ludmil Mikhailov. Deriving Priorities from Fuzzy Pairwise Comparison Judgements. *Fuzzy Sets and Systems*, 134(3):365–385, March 2003. 118, 124

[Mikhailov and Singh, 2003] Ludmil Mikhailov and M.G. Singh. Fuzzy Analytic Network Process and Its Application to the Development of Decision Support Systems. *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, 33:33–41, Feb. 2003. ISSN 1094-6977. 118, 124

[Mills et al., 2010] David Mills, Jim Marti, Jack Burbank, and William Kasch. Network Time Protocol Version 4: Protocol and Algorithms Specification. IETF RFC: 5905, June 2010. 143

[Ming et al., 2012] Zhong Xing Ming, Javier Ubillos, and Mingwei Xu. Name-based Shim6: A Name-based Approach to Host Mobility. *SIGMOBILE Mob. Comput. Commun. Rev.*, 15(4):46–48, March 2012. 19

[Mitsuya et al., 2007] Koshiro Mitsuya, Romain Kuntz, Shinta Sugimoto, Ryuji Wakikawa, and Jun Murai. A Policy Management Framework for Flow Distribution on Multihomed End Nodes. In *proceedings of 2nd ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture, MobiArch '07*, pages 1–7. ACM, August 2007. 29

[Montavont et al., 2008] N. Montavont, R. Wakikawa, T. Ernst, C. Ng, and K. Kuladinithi. Analysis of Multihoming in Mobile IPv6. IETF Draft: draft-ietf-monami6-mipv6-analysis (work in progress), May 2008. 15

[Montgomery, 2008] Douglas C. Montgomery. *Design and Analysis of Experiments*. John Wiley & Sons, 2008. ISBN 9780470128664. 118, 137, 140

[Morton et al., 2006] Al Morton, Len Ciavattone, Gomathi Ramachandran, Stanislav Shalunov, and Jerry Perser. Packet Reordering Metrics . IETF RFC: 4737, November 2006. 122

[Moskowitz and Nikander, 2006] Robert Moskowitz and Pekka Nikander. Host Identity Protocol (HIP) Architecture. IETF RFC: 4423, May 2006. 120, 180

[Munier, 2011] Nolberto Munier. *A Strategy for Using Multicriteria Anlaysis in Decision-Making: A guide for Simple and Complex Environmental Projects*. Springer, 2011. ISBN 978-94-007-1511-0. 115, 116

[Muscariello et al., 2009] L Muscariello, D Perino, and D Rossi. Do Next Generation Networks Need Path Diversity? In *proceedings of IEEE International Conference on Communications, ICC'09*, pages 1–6. IEEE, 2009. 3, 109

[Nacef and Montavont, 2008] B. Nacef and Nicolas Montavont. A Generic End-Host Mechanism for Path Selection and Flow Distribution. In *proceedings of Personal, Indoor and Mobile Radio Communications, PIMRC'08*, pages 1–5. IEEE, Sep 2008. 120

[Nagappan and Peeler, 2011] M Nagappan and Aaron Peeler. Modeling Cloud Failure Data: A Case Study of The Virtual Computing Lab. In *proceedigs of SECLOUD'11*, pages 8–14, 2011. 151

[Narten et al., 2007] Thomas Narten, Erik Nordmark, William Allen Simpson, and Hesham Soliman. Neighbor Discovery for IP version 6 (IPv6). IETF RFC: 4861, September 2007. 192, 193

[Nautilus, 2009] Nautilus. Nautilus6 Project Overview - Deployment of the Mobile Internet. [Online] http://www.nautilus6.org/ [Last Visit: 29-July-2013], 2009. 31, 32

[networking Lab, 2012] INL IP networking Lab. MultiPath TCP - Linux Kernel implementation, 2012. 27

[Ng et al., 2007a] Chan-Wah Ng, Thierry Ernst, Eun Kyoung Paik, and Marcelo Bagnulo. Analysis of Multihoming in Network Mobility Support. IETF RFC: 4980, October 2007a. 13

[Ng et al., 2007b] Chan-Wah Ng, Pascal Thubert, Masafumi Watari, and Fan Zhao. Network Mobility Route Optimization Problem Statement. IETF RFC: 4888, July 2007b. 30

[NICTA, 2013] NICTA. MiniZinc and FlatZinc. [Online] http://www.minizinc.org/ [Last Visit: 29-July-2013], 2013. 111

[Nishida, 2010] Yoshifumi Nishida. MPTCP Implementation on NS-2. [Online] http://www.jp.nishida.org/mptcp/ [Last Visit: 29-July-2013], 2010. 27

[Nordmark and Bagnulo, 2009] Erik Nordmark and Marcelo Bagnulo. Shim6: Level 3 Multihoming Shim Protocol for IPv6. IETF RFC: 5533, June 2009. 16, 36

[Nováczki et al., 2008] Szabolcs Nováczki, Lászlo Bokor, Gábor Jeney, and Sándor Imre. Design and Evaluation of a Novel HIP-Based Network Mobility Protocol. *Journal of Networks*, 3(1):10–24, 2008. 32

[OMNeT++, 2009] OMNeT++. OMNeT++ - discrete event simulation environment. [Online] `http://www.omnetpp.org/` [Last Visit: 29-July-2013], 2009. 84, 180

[Ong and Khan, 2008] Eng Hwee Ong and J.Y. Khan. Dynamic Access Network Selection with QoS Parameters Estimation: A Step Closer to ABC. In *proceedings of IEEE Vehicular Technology Conference, VTC Spring'08*, pages 2671–2676, 2008. 111

[OpenAir3, 2013] OpenAir3. [Online] `http://www.openairinterface.org/openairfiles/documents/papers_and_ppt_presentations/Nutshell.pdf` [Last Visit: 29-July-2013], 2013. 31

[OpenHIP, 2012] OpenHIP. OpenHIP. [Online] `http://www.openhip.org/` [Last Visit: 29-July-2013], 2012. 60

[OpenLisp, 2013] OpenLisp. The OpenLisp Project. [Online] `http://www.openlisp.org/` [Last Visit: 29-July-2013], 2013. 39, 46

[Oxford University Press, 2013] Oxford University Press. Oxford Dictionaries. [Online] `http://oxforddictionaries.com/` [Last Visit: 29-July-2013], 2013. 90, 246, 247, 248, 249

[Pan et al., 2008a] Jen-Yi Pan, Jing-Luen Lin, and Kai-Fung Pan. Multiple Care-of Addresses Registration and Capacity-Aware Preference on Multi-Rate Wireless Links. In *proceedings of International Conference on Advanced Information Networking and Applications - Workshops, AINA '08*, pages 768–773. IEEE, March 2008a. 3, 29, 180

[Pan et al., 2008b] Jianli Pan, S. Paul, R. Jain, and M. Bowman. MILSA: A Mobility and Multihoming Supporting Identifier Locator Split Architecture for Naming in the Next Generation Internet. In *proceedings of the Global*

Communications Conference Exhibition & Industry Forum, GLOBECOM '08, pages 1–6. IEEE, November-December 2008b. 53, 55

[Pan et al., 2009] Jianli Pan, Raj Jain, Subharthi Paul, Mic Bowman, and Shanzhi Chen. Enhanced MILSA Architecture for Naming, Addressing, Routing and Security Issues in the Next Generation Internet. In *proceedings of IEEE International Conference on Communications, ICC '09*, pages 1–6. IEEE, June 2009. 54

[Paul et al., 2010a] S. Paul, R. Jain, and J. Pan. An Identifier/Locator Split Architecture for Exploring Path Diversity through Site Multi-Homing - A Hybrid Host-Network Cooperative Approach. In *proceedings of IEEE International Conference on Communications, ICC '10*, pages 1–5. IEEE, May 2010a. 58

[Paul et al., 2009] Subharthi Paul, Jianli Pan, and Raj Jain. A Survey of Naming Systems: Classification and Analysis of the Current Schemes Using a New Naming Reference Model. Technical report, Washington University - Department of Computer Science & Engineering, October 2009. 2, 38, 58

[Paul et al., 2010b] Subharthi Paul, Raj Jain, and Jianli Pan. Multi-Tier Diversified Service Architecture for Internet 3.0: The Next Generation Internet. Technical Report 314, Washington University - Department of Computer Science & Engineering, June 2010b. 61, 62

[Paul et al., 2011] Subharthi Paul, Jianli Pan, and Raj Jain. Architectures for The Future Networks and The Next Generation Internet: A Survey. *Computer Communications*, 34(1):2–42, January 2011. 48, 61, 62, 63

[Pekka Nikander, 2008] Pekka Nikander. HIP for inter.net Project. [Online] `http://hip4inter.net/` [Last Visit: 29-July-2013], 2008. 36

[Pentikousis and Rautio, 2010] Kostas Pentikousis and Teemu Rautio. A Multiaccess Network of Information. In *proceedings of IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM '10*, pages 1–9. IEEE, June 2010. 48, 49

[Pierrel et al., 2007] S. Pierrel, P. Jokela, J. Melen, and K. Slavov. A Policy System for Simultaneous Multiaccess with Host Identity Protocol. In *proceedings of*

1st IEEE Workshop on Autonomic Communications and Network Management, ACNM '07, pages 71–77. IEEE, May 2007. 33, 36

[Pioro and Medhi, 2004] M. Pioro and D. Medhi. *Routing, Flow and Capacity Design in Communication and Computer Networks*. Elsevier, July 2004. ISBN 978-0-12-557189-0. 2, 69, 70, 74, 75, 76

[Piri and Pentikousis, 2009] Esa Piri and Kostas Pentikousis. IEEE 802.21: Media Independent Handover Services. *The Internet Protocol Journal*, 12(2):7–27, June 2009. 182

[Pujol et al., 2005] Jordi Pujol, Stefan Schmid, Lars Eggert, Marcus Brunner, and Jürgen Quittek. Scalability Analysis of the TurfNet Naming and Routing Architecture. In *proceedings of the 1st ACM workshop on Dynamic Interconnection of Networks, DIN '05*, pages 28–32. ACM, September 2005. 54

[Qi Wang and Mosa Ali Abu-Rgheff, 2006] Qi Wang and Mosa Ali Abu-Rgheff. Signalling Analysis of Cost-Efficient Mobility Support by Integrating Mobile IP and SIP in all IP Wireless Networks. *International Journal of Communication Systems*, 19(2):225–247, 2006. 92

[Qiao et al., 2008] Zizhi Qiao, Lingfen Sun, and Emmanuel Ifeachor. Case Study of PESQ Performance in Live Wireless Mobile VoIP Environment. In *proceedings of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC'08*, pages 1–6. IEEE, September 2008. 192

[Qureshi and Saleem, 2007] M.J.A. Qureshi and M. Saleem. Simulation and Visualization of Transmission Control Protocol's (TCP) Flow-Control and Multi-Home Options. In *proceedings of International Bhurban Conference on Applied Sciences & Technology, IBCAST '07*, pages 139–146. IEEE, January 2007. 21, 23

[Rathnayake et al., 2010] Upendra Rathnayake, Henrik Petander, Maximilian Ott, and Aruna Seneviratne. Protocol Support for Bulk Transfer Architecture. In *proceedings of IEEE International Conference on Wireless Communications, Networking and Information Security, WCNIS '10*, pages 598–602. IEEE, June 2010. 16

[RedHat, 2013a] RedHat. Configuring a Multihomed DHCP Server. [Online] https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sect-Configuring_a_Multihomed_DHCP_Server.html [Last Visit: 29-July-2013], 2013a. 20

[RedHat, 2013b] RedHat. Starting and Stopping vsftpd. [Online] https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s2-ftp-vsftpd-start.html [Last Visit: 29-July-2013], 2013b. 20

[Resatsch, 2010] Florian Resatsch. *Ubiquitous Computing Developing and Evaluating Near Field Communication Applications*. Gabler, 2010. ISBN 978-3-8349-2167-3. 2, 70, 71, 72

[Richard, 2010] Clayton Richard. *Internet Multi-Homing Problems: Explanations from Economics*, chapter 5, pages 67–78. Springer, 1 edition, 2010. ISBN 978-1-4419-6966-8. 2, 9

[Roland Bless and Waldhorst, 2011] Christoph P. Mayer Roland Bless, Christian Hbsch and Oliver P. Waldhorst. *SpoVNet: An Architecture for Easy Creation and Deployment of Service Overlays*, chapter 2. River Publishers, 2011. 59, 60

[Rosen et al., 2001] Eric C. Rosen, Arun Viswanathan, and Ross Callon. Multiprotocol Label Switching Architecture. IETF RFC: 3031, January 2001. 68

[Rosenberg et al., 2002] Jonathan Rosenberg, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley, and Eve Schooler. SIP: Session Initiation Protocol. IETF RFC: 3261, June 2002. 18

[Rossini et al., 2013a] Giuseppe Rossini, Dario Rossi, and Raffele Chiocchetti. ccnSim. [Online] http://perso.telecom-paristech.fr/~drossi/index.php?n=Software.ccnSim [Last Visit: 29-July-2013], 2013a. 49

[Rossini et al., 2013b] Giuseppe Rossini, Dario Rossi, and Raffele Chiocchetti. CCNx team. [Online] http://www.ccnx.

`org/software-download-information-request/download-releases/` [Last Visit: 29-July-2013], 2013b. 49

[Rungeler et al., 2008] Irene Rungeler, Michael Tuxen, and Erwin P. Rathgeb. Integration of SCTP in the OMNeT++ Simulation Environment. In *proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems \& workshops, SIMUTOOLS'08*, pages 1–8, Marseille, France, 2008. ICST. 84

[Sandanayake et al., 2008] Y.G. Sandanayake, C.F. Oduoza, and D.G. Proverbs. A Systematic Modelling and Simulation Approach for JIT Performance Optimisation . *Robotics and Computer-Integrated Manufacturing*, 24(6): 735 – 743, 2008. 7, 118

[Savola and Chown, 2005] P. Savola and T. Chown. A Survey of IPv6 Site Multihoming Proposals. In *proceedings of the 8th International Conference on Telecommunications, ConTEL '05*, volume 1, pages 41–48. IEEE, June 2005. 34

[Scharf and Ford, 2013] Michael Scharf and Alan Ford. Multipath TCP (MPTCP) Application Interface Considerations. IETF RFC 6897, March 2013. 25

[Schmid et al., 2005] Stefan Schmid, Lars Eggert, and Marcus Brunner. TurfNet: An Architecture for Dynamically Composable Networks. In *proceedings of the 1st ACM workshop on Dynamic Interconnection of Networks, DIN '05*, pages 28–32. ACM, September 2005. 54

[Scholtz and Consolvo, 2004] J. Scholtz and S. Consolvo. Toward a Framework for Evaluating Ubiquitous Computing Applications. *Pervasive Computing, IEEE*, 3:82–88, 2004. 2, 71, 72, 90

[Schulzrinne et al., 2013] Henning Schulzrinne, Srinivasan Seetharaman, and Volker Hilt. Collaborative Research: FIND: NetSerV Architecture of a Service-Virtualized Internet. [Online] `http://www.nets-find.net/Funded/Netserv.php` [Last Visit: 29-July-2013], 2013. 47, 50

[Schütz et al., 2010] Simon Schütz, Henrik Abrahamsson, Bengt Ahlgren, and Marcus Brunner. Design and Implementation of the Node Identity Internetworking Architecture. *Computer Networks*, 54(7):1142–1154, May 2010. 51, 55, 56

[Seta et al., 2007] Naoya Seta, Haruya Miyajima, and Liang Zhang. All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment. In *proceedings of the IEEE Vehicular Technology Conference, VTC-Sprint'07*, pages 1121–1126. IEEE, April 2007. 18

[Shalunov et al., 2006] Stanislav Shalunov, Benjamin Teitelbaum, Anatoly Karp, Jeff Boote, and Matthew Zekauskas. A One-Way Active Measurement Protocol (OWAMP). IETF RFC: 4656, September 2006. 122, 143, 147

[Shenoy, 2013] Victor Perotti Shenoy. Switched Internet Architecture. [Online] `http://www.nets-find.net/Funded/SWA.php` [Last Visit: 29-July-2013], 2013. 61, 62

[Shinta et al., 2006] Sugimoto Shinta, Kato RyoJi, and Oda ToshiKane. A Comparative Analysis of Multihoming Solutions. *Information Processing Society of Japan (IPSJ)*, pages 209–216, November 2006. 2, 9

[Siddiqui and Zeadally, 2006] F. Siddiqui and S. Zeadally. SCTP multihoming support for handoffs across heterogeneous networks. In *proceedings of Communication Networks and Services Research Conference, CNSR '06*, pages 8 pp.–250. IEEE, May 2006. 25

[Soliman et al., 2008] Hesham Soliman, Claude Castelluccia, Karim ElMalki, and Ludovic Bellier. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. IETF RFC: 5380, October 2008. 3, 31, 180

[Sousa, 2013a] Bruno Sousa. Multiple Care of Address Registration in OMNet++. [Online] `http://mcoa.dei.uc.pt/` [Last Visit: 29-July-2013], 2013a. xi, 31, 181, 198

[Sousa, 2013b] Bruno Sousa. Evaluating MADM techniques. [Online] `http://mcoa.dei.uc.pt/doe/` [Last Visit: 29-July-2013], 2013b. xi

[Sousa et al., 2010] Bruno Sousa, Kostas Pentikousis, and Marilia Curado. REF: Resilience Evaluation Framework. In *proceedings of International Workshop on Mobile Computing and Networking Technologies, WMCNT '10)*. IEEE, October 2010. x, 105

[Sousa et al., 2011a] Bruno Sousa, Kostas Pentikousis, and Marilia Curado. Multihoming Management for Future Networks. *Mobile Networks and Applications (MONET)*, 16:505–517, August 2011a. x, 65, 94

[Sousa et al., 2011b] Bruno Sousa, Kostas Pentikousis, and Marilia Curado. UEF: Ubiquity Evaluation Framework. In *proceedings of Wired/Wireless Internet Communications, WWIC'11*, volume 6649 of *LNCS*, pages 92–103. Springer, 2011b. x, 105

[Sousa et al., 2011c] Bruno Sousa, Kostas Pentikousis, and Marilia Curado. A Study of Multimedia Application Performance over Multiple Care-of Addresses in Mobile IPv6. In *proceedings of IEEE Symposium on Computers and Communications, ISCC '11*, pages 7–12. IEEE, 2011c. x, 198

[Sousa et al., 2011d] Bruno Sousa, Marco Silva, Kostas Pentikousis, and Marilia Curado. A Multiple Care of Addresses Model. In *proceedings of IEEE Symposium on Computers and Communications, ISCC '11*, pages 485–490. IEEE, June-July 2011d. x, 198

[Sousa et al., 2013] Bruno Sousa, Kostas Pentikousis, and Marilia Curado. *Multihoming: A Comprehensive Review*, volume 90, chapter 2. Elsevier, 2013. x, 65

[Srinivasan and Shocker, 1973] V. Srinivasan and AllanD. Shocker. Linear Programming Techniques for Multidimensional Analysis of Preferences. *Psychometrika*, 38(3):337–369, 1973. 118

[Srisuresh and Egevang, 2001] Pyda Srisuresh and Kjeld Borch Egevang. Traditional IP Network Address Translator (Traditional NAT). IETF RFC: 3022, January 2001. 38

[Stankiewicz et al., 2011] Rafal Stankiewicz, Piotr Cholda, and Andrzej Jajszczyk. QoX: What is it really? *Communications Magazine*, pages 148–158, April 2011. 126

[Stevens-Navarro and Wong, 2006] E. Stevens-Navarro and V.W.S. Wong. Comparison between Vertical Handoff Decision Algorithms for Heterogeneous Wireless Networks. In *proceedings of the IEEE 63rd Vehicular Technology Conference, VTC-Spring'06*, volume 2, pages 947–951, 2006. 117, 145

[Stevenson et al., 2009] G. Stevenson, S. Knox, S. Dobson, and P. Nixon. Ontonym: A Collection of Upper Ontologies for Developing Pervasive Systems. In *Proceedings of the 1st Workshop on Context, Information and Ontologies*, pages 1–8. ACM, 2009. 70, 71, 72

[Stewart et al., 2011] R. Stewart, K. Poon, M. Tuexen, V. Yasevich, and P. Lei. Sockets API Extensions for Stream Control Transmission Protocol (SCTP) . IETF RFC: 6458, December 2011. 25

[Stewart, 2007] Randall Stewart. Stream Control Transmission Protocol. IETF RFC: 4960, September 2007. 16, 21, 25, 28, 84, 180

[Stewart et al., 2007] Randall Stewart, Qiaobing Xie, Michael Tuexen, Shin Maruyama, and Masahiro Kozuka. Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration. IETF RFC: 5061, September 2007. 25, 28

[Stoica et al., 2004] Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, and S. Surana. Internet Indirection Infrastructure. *IEEE/ACM Transactions Networking*, 12(2):205–218, April 2004. 58, 59

[Subramanian et al., 2005] Lakshminarayanan Subramanian, Matthew Caesar, Cheng Tien Ee, Mark Handley, Morley Mao, Scott Shenker, and Ion Stoica. HLP: A Next Generation Inter-domain Routing Protocol. Technical Report UCB/CSD-04-1357, EECS Department, University of California, Berkeley, October 2005. 40

[SUN, 2009] SUN. System Administration Guide: IP Services, April 2009. 20

[Sun, 2010] Chia-Chi Sun. A Performance Evaluation Model by Integrating Fuzzy AHP and Fuzzy TOPSIS Methods. *Expert Systems with Applications*, 37 (12):7745–7754, December 2010. 118, 123

[Symonds, 2009] Judith Symonds. *Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools, and Applications*, volume I. Information Science Reference, 2009. 70

[Tang et al., 2007] Haitao Tang, P. Poyhonen, O. Strandberg, Kostas Pentikousis, J. Sachs, F. Meago, J. Tuononen, and Rámon Aguero. Paging issues and methods for multiaccess. In *proceedings of International Conference on Communications and Networking in China, CHINACOM '07.*, pages 769 –776, August 2007. 72

[Team, 2010] R Development Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, 2010. ISBN 3-900051-07-0. xi, 101, 152

[Templin, 2007] F. Templin. The IPvLX Architecture. IETF Draft: draft-templin-ipvlx-08 (work in progress), November 2007. 45, 46

[Templin, 2011] Fred Templin. The Internet Routing Overlay Network (IRON). IETF RFC: 6179, March 2011. 41, 42

[Thompson et al., 2006] Nathanael Thompson, Guanghui He, and Haiyun Luo. Flow Scheduling for End-Host Multihoming. In *proceedings of the IEEE International Conference on Computer Communications, INFOCOM '06*, pages 1–12. IEEE, April 2006. 32, 34, 36

[Toledo et al., 2011] N. Toledo, J.-M. Bonnin, M. Higuero, and E. Jacob. Host Identity Protocol Based NEMO Solutions: An Evaluation of the Signaling Overhead. In *proceedings of IEEE 73rd Vehicular Technology Conference, VTC '11*, pages 1–5, 2011. 104

[Tong et al., 2004] Lee-Ing Tong, Chung-Ho Wang, and Hung-Cheng Chen. Optimization of Multiple Responses Using Principal Component Analysis and Technique for Order Preference by Similarity to Ideal Solution. *The International Journal of Advanced Manufacturing Technology*, 27:407–414, 2004. 114, 145

[Toseef et al., 2008] Umar Toseef, Asanga Udugama, Carmelita Goerg, Changpeng Fan, and Frank Pittmann. Realization of Multiple Access Interface Management and Flow Mobility in IPv6. In *proceedings of 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, MOBILWARE '08*, pages 1–8. ICST, February 2008. ISBN 978-1-59593-984-5. 3, 29, 30

[Touch et al., 2011] Joe Touch, Ilia Baldine, Rudra Dutta, Gregory G. Finn, Bryan Ford, Scott Jordan, Dan Massey, Abraham Matta, Christos Papadopoulos, and Peter Reiher. A Dynamic Recursive Unified Internet Design (DRUID). *Computer Networks*, 55(4):919–935, March 2011. 59

[Tran and Boukhatem, 2009] Phuoc Nguyen Tran and N. Boukhatem. An Utility-Based Interface Selection Scheme for Multi-homed Mobile Terminals. In *proceedings of the IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC'09*, pages 767–772, 2009. 114

[Tran and Boukhatem, 2008] Phuoc Nguyen Tran and Nadia Boukhatem. The Distance to The Ideal Alternative (DiA) Algorithm for Interface Selection in Heterogeneous Wireless Networks. In *proceedings of the 6th ACM International Symposium on Mobility Management and Wireless Access, MobiWac '08*, page 61. ACM Press, 2008. 4, 7, 114, 134, 145

[Tse, 2006] Ronald Tse. TCP Fairness in Multipath Transport Protocols. Bachelor Thesis, Brown University, Department of Computer Science, May 2006. 21, 22, 23

[Tseng, 2010] Ming-Lang Tseng. Implementation and Performance Evaluation Using the Fuzzy Network Balanced Scorecard . *Computers & Education*, 55 (1):188 – 201, 2010. 118

[Tsirtsis et al., 2011a] G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, and K. Kuladinithi. Flow Bindings in Mobile IPv6 and Nemo Basic Support . IETF RFC: 6089, January 2011a. 3, 29, 31, 178, 180, 181

[Tsirtsis et al., 2011b] George Tsirtsis, Gerardo Giaretta, Hesham Soliman, and Nicolas Montavont. Traffic Selectors for Flow Bindings . IETF RFC: 6088, January 2011b. 183

[Turányi and Valkó, 2003] Zoltán Turányi and András Valkó. Design, Implementation and Evaluation of IPv4+ 4, 2003. 39

[Turányi et al., 2003] Zoltán Turányi, András Valkó, and Andrew T. Campbell. 4+ 4: an Architecture for Evolving the Internet Address Space Back Toward Transparency. *SIGCOMM Computer*, 33(5):43–54, 2003. 38, 40

[Tzeng and Huang, 2011] Gwo-Hshiung Tzeng and Jih-Jeng Huang. *Multiple Attribute Decision Making: Methods and applications*. CRC Press, 2011. ISBN 978-1-4398-6157-8. 115, 118

[Ubillos et al., 2010] Javier Ubillos, Mingwei Xu, Zhongxing Ming, and Christian Vogt. Name-Based Sockets Architecture. IETF Draft: draft-ubillos-name-based-sockets (work in progress), September 2010. 18, 19

[UCL, 2012] Networks Research Group UCL. HTSim - MultiPath TCP Simulator, 2012. 27

[Uijterwaal, 2009] Henk Uijterwaal. A One-Way Packet Duplication Metric. IETF RFC: 5560, May 2009. 122

[Union, 2013] European Union. InterArchive Terminology for Europe (IATE). [Online] `http://iate.europa.eu/` [Last Visit: 29-July-2013], 2013. 88, 246, 247, 248, 249

[Valdovinos and Diaz, 2009] I.A. Valdovinos and J.A.P. Diaz. TCP Extension to Send Traffic Simultaneously through Multiple Heterogeneous Network Interfaces. In *proceedings of the Mexican International Conference on Computer Science, ENC '09*, pages 89–94. IEEE, September 2009. 22, 23

[van Beijnum, 2002] Iljitsch van Beijnum. *BGP–Building Reliable Networks with the Border Gateway Protocol*. O'Reilly Media, 2002. 37

[Verma, 2012] Rohit Verma. Media Multihoming in SIP Sessions. IETF Draft: draft-rverma-media-multihoming-over-sctp (work in progress), January 2012. 19

[Vogt, 2008] Christian Vogt. Six/One Router: A Scalable and Backwards Compatible Solution for Provider-Independent Addressing. In *proceedings of ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture, MobiArch '08*, pages 13–18. ACM, August 2008. 58, 59

[von Neumann et al., 2007] J. von Neumann, O. Morgenstern, and A. Rubinstein. *Theory of Games and Economic Behavior (Commemorative Edition)*. Princeton Classic Editions. Princeton University Press, 2007. ISBN 9780691130613. 91

[Voznak et al., 2012] Miroslav Voznak, Adrian Kovac, and Michal Halas. Effective Packet Loss Estimation on VoIP Jitter Buffer. In *proceedings of the NETWORKING'12 Workshops*, volume 7291 of *LNCS*. Springer, 2012. 149

[Wakikawa, 2008] R. Wakikawa. Multiple Care-of Addresses Registration. IETF Draft: draft-ietf-monami6-multiplecoa-03 (work in progress), 2008. 180

[Wakikawa et al., 2009] Ryuji Wakikawa, Vijay Devarapalli, George Tsirtsis, Thierry Ernst, and Kenichi Nagami. Multiple Care-of Addresses Registration. IETF RFC: 5648, October 2009. 31, 178, 181

[Walfish et al., 2004] Michael Walfish, Jeremy Stribling, Maxwell Krohn, Hari Balakrishnan, Robert Morris, and Scott Shenker. Middleboxes no longer considered harmful. In *proceedings of the 6th conference on Symposium* *on Opearting Systems Design & Implementation, OSDI '04*, pages 15–15. USENIX Association, December 2004. 58, 60

[Wang et al., 2010] J. Wang, K. Fan, and W. Wang. Integration of Fuzzy AHP and FPP with TOPSIS Methodology for Aeroengine Health Assessment. *Expert Systems with Applications*, 37(12):8516–8526, 2010. 118, 122, 124

[Wang and Abu-Rgheff, 2006] Qi Wang and Mosa Ali Abu-Rgheff. Signalling Analysis of Cost-Efficient Mobility Support by Integrating Mobile IP and SIP in All IP Wireless Networks. *International Journal of Communication Systems*, 19:225–247, 2006. 71, 72, 91

[Wang et al., 2008] Qi Wang, Robert Atkinson, and John Dunlop. Design and Evaluation of Flow Handoff Signalling for Multihomed Mobile Nodes in Wireless Overlay Networks. *Computer Networks*, 52(8):1647–1674, June 2008. ISSN 1389-1286. 30

[Wasserman and Seite, 2011] W Wasserman and P. Seite. Current Practices for Multiple Interface Hosts. IETF RFC: 6419, November 2011. 20

[Wehrle et al., 2010] Klaus Wehrle, Mesut Günes, and James Gross. *Modeling and Tools for Network Simulation*. Springer, 2010. ISBN 978-3-642-12330-6. 181

[Wei et al., 2006] D. X. Wei, C. Jin, S. H. Low, and S. Hegde. FAST TCP: Motivation, Architecture, Algorithms, Performance. *IEEE/ACM Transactions Networking*, 14(6):1246–1259, December 2006. 22

[Wei and Ansari, 2001] Dong Wei and Nirwan Ansari. IP Traffic Monitoring: An Overview and Future Considerations. *Advances in Multimedia Information Processing*, 2195:335–342, January 2001. 121

[Wolf, 2006] Tilman Wolf. Service-Centric End-to-End Abstractions in Next-Generation Networks. In *proceedings of 15th International Conference on Computer Communications and Networks, ICCCN '06*, pages 79 –86. IEEE, October 2006. 47, 49

[Wong et al., 2007] K. Daniel Wong, A. Dutta, H. Schulzrinne, and K. Young. Simultaneous Mobility: Analytical Framework, Theorems and Solutions. *Wireless Communications and Mobile Computing*, 7(5):623–642, 2007. 72

[Xia et al., 2006] Hui-Cheng Xia, Deng-Feng Li, Ji-Yan Zhou, and Jian-Ming Wang. Fuzzy LINMAP Method for Multiattribute Decision Making Under Fuzzy Environments . *Journal of Computer and System Sciences*, 72(4): 741 – 759, 2006. 118

[Xu et al., 2010] Mingwei Xu, Zhongxing Ming, Javier Ubillos, and Christian Vogt. Name Based Sockets - Shim6. IETF Draft: draft-xu-name-shim6 (work in progress), September 2010. 19

[Xu and Guo, 2008] Xiaohu Xu and Dayong Guo. Hierarchical Routing Architecture (HRA). In *proceedings of the Next Generation Internet Networks, NGI '08*, pages 92–99. IEEE, April 2008. 51, 55

[Xue et al., 2007] Guoliang Xue, Arunabha Sen, Weiyi Zhang, Jian Tang, and Krishnaiya Thulasiraman. Finding a Path Subject to Many Additive QoS Constraints. *IEEE/ACM Transactions Network*, 15(1):201–211, February 2007. 3, 109, 112

[Yang, 2006] X. Yang. An Internet Architecture for User-Controlled Routes. [Online] `http://www.nets-find.net/Funded/InternetArchitecture.php` [Last Visit: 29-July-2013], 2006. 62, 63

[Yang et al., 2007] X.. Yang, D.. Clark, and A.W. Berger. NIRA: A New Inter-Domain Routing Architecture. *IEEE/ACM Transactions Networking*, 15(4):775 – 788, August 2007. ISSN 1063-6692. doi: 10.1109/TNET.2007.893888. 61, 63

[Yang et al., 2010] Zhe Yang, Lin Cai, and Wu-sheng Lu. Practical Scheduling Algorithms for Concurrent Transmissions in Rate-adaptive Wireless Networks. In *proceedings of the IEEE International Conference on Computer Communications, INFOCOM'10*, pages 1–9. IEEE, March 2010. 111

[Yao et al., 2008] Aihong Yao, Junjun Gu, Gang Qu, and Shuvra Bhattacharyya. Energy Efficient Implementation of G.729 for Wireless VoIP Application. In *proceedings of the 2008 International Conference on Advanced Infocomm Technology, ICAIT '08*, pages 133:1–133:7. ACM, 2008. 192

[Yi Gai and Jain, 2012] Bhaskar Krishnamachari Yi Gai and Rahul Jain. Combinatorial Network Optimization with Unknown Variables: Multi-Armed

Bandits with Linear Rewards and Individual Observations. *IEEE/ACM Trans. Netw.*, 20(5):1466–1478, October 2012. 111

[Ylitalo et al., 2008] Jukka Ylitalo, Jan Melén, Patrik Salmela, and Henrik Petander. An Experimental Evaluation of a HIP Based Network Mobility Scheme. In *proceedings of Wired/Wireless Internet Communications, WWIC '08*, LNCS, pages 139–151. Springer, May 2008. 59, 64

[Yousaf and Bauer, 2013] Faqir Zarrar Yousaf and Christian Bauer. xMIPv6. [Online] `http://www.kn.e-technik.tu-dortmund.de/en/forschung/ausstattung/xmipv6.html` [Last Visit: 29-July-2013], 2013. 3, 31, 180

[Yousaf et al., 2008] Faqir Zarrar Yousaf, Christian Bauer, and Christian Wietfeld. An Accurate and Extensible Mobile IPv6 (xMIPV6) Simulation Model for OMNeT++. In *proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems \& workshops, SIMUTOOLS '08*, pages 1–8. ICST, 2008. 181, 191, 193, 195

[Yousaf et al., 2010] Faqir Zarrar Yousaf, Christian Müller, and Christian Wietfeld. A Comprehensive MIPv6 Based Mobility Management Simulation Engine for the Next Generation Network. In *proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems \& workshops, SIMUTOOLS '10*, pages 1–8. ICST, 2010. 191

[Zekri et al., 2012] Mariem Zekri, Badii Jouaber, and Djamal Zeghlache. A Review on Mobility Management and Vertical Handover Solutions Over Heterogeneous Wireless Networks . *Computer Communications*, 35(17):2055 – 2068, 2012. 4, 112

[Zhang et al., 2010a] Lixia Zhang, Deborah Estrin, Jeffrey Burke, Van Jacobson, James D Thornton, Diana K Smetters, Beichuan Zhang, Gene Tsudik, Dan Massey, Christos Papadopoulos, Lan Wang, Patrick Crowley, and Edmund Yeh. Named Data Networking (NDN) Project. [Online] `http://www.named-data.net/techreport/TR001ndn-proj.pdf` [Last Visit: 29-July-2013], October 2010a. 47, 50

[Zhang et al., 2010b] Wei Zhang, Xia Yin, Jianping Wu, Wei Zhang, and S. Huang. Real Aggregation for Reducing Routing Information Base Size. *JCIT*, 5 (6):1–7, August 2010b. 44, 46

[Zhang et al., 2006] Xinyang Zhang, Paul Francis, Jia Wang, and Kaoru Yoshida. Scaling IP Routing with the Core Router-Integrated Overlay. In *proceedings of IEEE International Conference on Network Protocols, ICNP '06*, pages 147–156. IEEE, November 2006. 44, 46

[Zhang et al., 2008] Yu Zhang, Chuan Heng Foh, and Jianfei Cai. An On-Off Queue Control Mechanism for Scalable Video Streaming over the IEEE 802.11e WLAN. In *proceedings of the IEEE International Conference on Communications, ICC '08.* , pages 4958 –4962, May 2008. 192

A

Appendix A - Definitions for Ubiquity terms

THIS appendix presents the definitions employed in the Ubiquity Evaluation Framework (UEF) specified in Chapter 3.

A. Appendix A - Definitions for Ubiquity terms

Table A.1: Ubiquity evaluation criteria summary.

Term	Definition
Accessibility[c] [t]	"degree to which a product (e.g., device, service, and environment) is accessible by as many people as possible"
Accuracy[b] [t]	"A qualitative assessment of correctness, or freedom from error."
Adaptability[b] [t]	"The ease with which a system or component can be modified for use in applications or environments other than those for which it was specifically designed."
Adjustability[d] [t]	"Can be slightly modified to achieve a desired result."
Adoptability[d] [t]	"Quality of being taken up or followed."
Analyzability [d] [t]	"Quality of being examined methodically and in detail, typically in order to be explain and interpreted."
Compatibility [b] [t]	"The ability of two or more systems or components to exchange information."
Configurability[a] [t]	"Possibility of specifying various hardware and/or software configurations supported by a product."
Connectivity [b] [t]	"The state of being connected to the Internet or some other type of computer network."
Credibility[d] [t]	"The quality of being trusted and believed in."
Customizability[a] [t]	"Process of making tailor-made models, i.e.models designed to meet the specific needs."
Decomposability[d] [t]	"Break down or cause to break down into component elements or simpler constituents."
Downloadable[d] [t]	"Copy (data) from one computer system to another or to a disk."
Embeddedness[b] [t]	"A computer system or software that is part of a larger system and performs some of the requirements of that system."
Effectiveness[a] [t]	"The extent to which a component or system fulfils its function."

[a] InterArchive Terminology for Europe (IATE) [Union, 2013] [b] IEEE Standard Dictionary [IEEE, 1990] [c] IEC - Electropedia [International Electrotechnical Commission, 2013b,a]
[d] Oxford Dictionary[Oxford University Press, 2013]
[t] Technical Capability [u] Technical Extension

Table A.1: Ubiquity evaluation criteria summary (continued)

Term	**Definition**
Efficiency[b t]	”The degree to which a system or component performs its designated functions with minimum consumption of resources.”
Extensibility[b t]	”The ease with which a system or component can be modified to increase its storage or functional capacity.”
Integrability[d t]	”Quality of being combined with another to form a whole.”
Interoperability[b t]	”The ability of two or more systems or components to exchange information and to use the information that has been exchanged.”
Interpretability[a t]	”Suitability of imagery for interpretation with respect to answering adequately requirements on a given type target in terms of quality and scale.”
Invisibility[d t]	”Quality of being unable to be seen.”
Learnability[d t]	”Gain or acquire knowledge of or skill in (something) by study, experience, or being taught.”
Maintainability[d t]	”Keep in good condition by checking or repairing it regularly.”
Mobility[d t]	”The ability to move or be moved freely and easily.”
Portability[b t]	”The ease with which a system or component can be transferred from one hardware or software environment to another.”
Predictability[d t]	”Ability of always behaving or occurring in the way expected.”
Proactiveness[d t]	”Ability of creating or controlling a situation rather than just responding to it after it has happened.”
Reconfigurability[c t]	”The ability (of a functional unit) to be reconfigured.”
Reliability[d t]	”The ability of a system or compo- nent to perform its required functions under stated conditions for a specified period of time.”
Reusability[d t]	”The degree to which a software module or other work product can be used in more than one computer program or software system.”
Scalability[a t]	”The ability to add power and capability to an existing system without significant expense or overhead.”

[a] InterArchive Terminology for Europe (IATE) [Union, 2013] [b] IEEE Standard Dictionary [IEEE, 1990] [c] IEC - Electropedia [International Electrotechnical Commission, 2013b,a]
[d] Oxford Dictionary[Oxford University Press, 2013]
[t] Technical Capability [u] Technical Extension

Table A.1: Ubiquity evaluation criteria summary (continued)

Term	Definition
Security[a t]	″Combination of confidentiality-prevention of unauthorised disclosure of information-,integrity,-prevention of unauthorised modification of information-,and availability-prevention of withholding of information or resources.″
Sensibility[d t]	″The quality of being able to appreciate and respond to complex influences.″
Shareability[d t]	″Portion of application, system component that can be used other systems or applications.″
Stability[a t]	″The property of a linear system such that, after being displaced from its steady-state condition by disturbance, it comes back to that steady-state condition when the disturbance has ceased.″
Testability[d t]	″The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met.″
Understandability[a t]	″Features of programming languages which determine the readability of programs.″
Usability[b t]	″The ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component″
Wearability[d t]	″Computer or other electronic device that is small or light enough to be worn or carried on ones body.″
Authentication[a u]	″A method to establish security services by means of simple or strong authentication.″
Authorization[a u]	″The granting to a user,a program or a process the right of access.″
Automation[a u]	″The investigation, design, development and application of methods of rendering processes automatic, self-moving, or self-controlling.″
Autonomy[d u]	″The right or condition of self-government.″
Context Reusability[d u]	″Context that can be reused.″
Durability[c u]	″The ability of an item to perform a required function under given conditions of use and maintenance, until a limiting state is reached.″

[a] InterArchive Terminology for Europe (IATE) [Union, 2013] [b] IEEE Standard Dictionary [IEEE, 1990] [c] IEC - Electropedia [International Electrotechnical Commission, 2013b,a]
[d] Oxford Dictionary[Oxford University Press, 2013]
[t] Technical Capability [u] Technical Extension

Table A.1: Ubiquity evaluation criteria summary (continued)

Term	**Definition**
Entity Tracking[d u]	"The maintenance of a constant difference in frequency between two or more entities."
Identity Tracking[d u]	"The maintenance of a constant difference in frequency between two or more identities."
Inferred Context[d u]	"The set of circumstances or facts defining a particular situation or event that can be deduced."
Location Tracking[d u]	"The maintenance of a constant difference in frequency between two or more locations."
Negotiation[a u]	"The process by which two session protocol machines (SPMs) agree on a common set of functional units and protocol values and on the initial setting of available tokens."
Response Time[b u]	"The elapsed time between the end of an inquiry or command to an interactive computer system and the beginning of the system's response."
Seamlessness[d u]	"Quality of providing smooth and continuous service, with no apparent gaps or spaces between one part and the next."
Self-Control[d u]	"The ability to control oneself."
Service Coverage[b u]	"The degree to which a given service or set of services addresses all specified requirements for a given system or component."
Standardization[d u]	"To cause (something) to conform to a standard."
Trust[a u]	"An entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects."
User Context[d u]	"Context associated with an user."
User preference [d u]	"Preferences associated with an user."
User profile[d u]	"Information that characterizes an user in a system."
User Satisfaction[d u]	"Set of metrics that express means to assess how users are satisfied with a service."
Utility[b u]	"A software tool designed to perform some frequently used support function."

[a] InterArchive Terminology for Europe (IATE) [Union, 2013] [b] IEEE Standard Dictionary [IEEE, 1990] [c] IEC - Electropedia [International Electrotechnical Commission, 2013b,a] [d] Oxford Dictionary[Oxford University Press, 2013]
[t] Technical Capability [u] Technical Extension