Tuomas Taipale

Feasibility of wireless mesh for LTE-Advanced small cell access backhaul

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.
Espoo 14.9.2012

Thesis supervisor:

Prof. Jukka Manner

Thesis instructor:

M.Sc. (Tech.) Pekka Wainio

Aalto University
School of Electrical Engineering

AALTO YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Tuomas Taipale

Työn nimi: Mesh-verkon soveltuvuus LTE-Advanced liityntärunkokytkentään

Päivämäärä: 14.9.2012 Kieli: Englanti Sivumäärä: 11+82

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotekniikka Koodi: S-38

Valvoja: Prof. Jukka Manner

Ohjaaja: DI Pekka Wainio

Mobiilidatan määrä on muutaman viime vuoden aikana kasvanut voimakkaasti ja nykyiset ennustukset arvioivat eksponentiaalista kasvukäyrää tulevien vuosien aikana. Matkapuhelinjärjestelmät ovat kehittyneet nopeasti tämän trendin ohjaamana. Neljännen sukupolven matkapuhelinverkkostandardien myötä, uudet innovaatiot kuten heterogeeniset verkkoratkaisut tarjoavat ratkaisun nykyisiin skaalautuvuus- ja kapasiteettiongelmiin. Joitain ilmeisiä ongelmakohtiakin kuitenkin esiintyy kuten heterogeenisten verkkojen runkokytkennän toteuttaminen.

Yksi lupaavimmista tavoista toteuttaa heterogeenisten verkkojen runkokytkentä on langaton ja itseorganisoituva mesh-verkko. Tämän opinnäytetyön tavoitteena on varmistaa ja testata Nokia Siemens Networksin kehittämän mesh-runkokytkentäverkkokonseptin toteutettavuutta ja toiminnallisuutta soveltuvan validointijärjestelmän avulla.

Kaiken kaikkiaan validointijärjestelmä ja sen päälle toteutettu mesh-protokolla toimivat moitteettomasti koko kehitys- ja testausprosessin ajan. Konseptin eri ominaisuudet ja mekanismit todistettiin täysin toteutettaviksi ja toimiviksi. Muutamalla lisäominaisuudella ja konseptiparannuksella mesh-konsepti tarjoaa houkuttelevan ja innovatiivisen ratkaisun heterogeenisten verkkojen runkokytkentään tulevaisuudessa.

Avainsanat: LTE-Advanced, heterogeeniset verkot, Matkapuhelinverkkojen runkokytkentä, langattomat mesh-verkot, SON

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Tuomas Taipale

Title: Feasibility of wireless mesh for LTE-Advanced small cell access backhaul

Date: 14.9.2012 Language: English Number of pages: 11+82

Department of Communications and Networking

Professorship: Networking technology Code: S-38

Supervisor: Prof. Jukka Manner

Instructor: M.Sc. (Tech) Pekka Wainio

Mobile traffic demands and volumes are increasing and will dramatically keep increasing in the future. Along with this, mobile networks have evolved to better match this growth. Fourth generation cellular network standard introduced a set of new innovations for mobile communications, including support for heterogeneous network deployments. Heterogeneous networking is the likely answer for future mobile data capacity shortage but also poses some challenges, the most evident being how to implement the backhauling.

One of the most promising heterogeneous network backhaul solutions is a meshed radio system with self-organizing features. The main scope of this master's thesis is the verification of functionality and feasibility of a wireless mesh backhaul concept developed by Nokia Siemens Networks through a proof-of-concept system.

All in all, the wireless mesh proof-of-concept system performed strongly throughout the development and testing process. The different functionalities were proven to work successfully together. With further development and enhancement, the system concept displays extreme potential for a state-of-the-art heterogeneous network backhaul technology.

Keywords: LTE-Advanced, heterogeneous networks, mobile backhaul, wireless mesh, SON

Preface

I wish to thank M.Sc. (Tech.) Pekka Wainio and Professor Jukka Manner for extremely valuable and good feedback and guidance. Additionally, I wish to thank everyone from Nokia Siemens Networks, Technical Research Centre of Finland and Aalto University who contributed to the wireless mesh backhaul proof-of-concept system assembly, protocol software development and system validation process.

Otaniemi, 14.9.2012

Tuomas Taipale

Table of Contents

List of Abbreviations

3G	Third generation of mobile telecommunications
4G	Fourth generation of mobile telecommunications
3GPP	The 3rd Generation Partnership Project
AMPS	Advanced Mobile Phone System
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
AUC	Authentication Center
BGP	Border Gateway Protocol
BMCA	Best Master Clock Algorithm
BRAWE	Broadband multi-antenna radios for millimeter wave frequency bands
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CET	Carrier Ethernet Transport
CMOS	Complementary Metal Oxide Semiconductor
DiffServ	Differentiated Services
DOCSIS	Data Over Cable Service Interface Specification
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line
EDGE	Enhanced Data rates for GSM Evolution
EXP	MPLS Experimental header field
FDD	Frequency Division Duplexing
FDMA/FDM	Frequency Division Multiple Access and Multiplexing
FRR	Fast Reroute
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GNID	WMN Node Identifier
GPIO	General Purpose Input/Output
GPRS	General Packet Radio Service

GPS	Global Positioning System
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HSUPA	High Speed Uplink Packet Access
ICMP	Internet Control Message Protocols
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IMS	IP Multimedia Subsystem
IMT	International Mobile Telecommunications
IntServ	Integrated Services
IP	Internet Protocol
IS-95	Interim Standard 95
IS-IS	Intermediate System to Intermediate System
ITU	International Telecommunication Union
LDP	Label Distribution Protocol
LOS	Line-of-Sight
LSU	Link State Update
LTCC	Low temperature co-fired ceramic
LTE	Long Term Evolution
MAC	Media Access Control
MEF	Metro Ethernet Forum
MEVICO	Mobile Networks Evolution for Individual Communications Experience
MIMO	Multiple In Multiple Out
MME	Mobility Management Entity
MPLS	MultiProcotol Label Switching
MSC	Mobile Switching Center
NFL	National Football League
NGMN	Next Generation Mobile Networks
NG-SDH	Next Generation Synchronous Digital Hierarchy

NLOS	Non-line-of-Sight
NMT	Nordic Mobile Telephone
NS	Network Simulator
NSN	Nokia Siemens Networks
OAM	Operations, Administration and Maintenance
OFDMA	Orthogonal FDMA
OSPF	Open Shortest Path First
PB	Provider Bridging
PBB	Provider Backbone Bridging
PBB-TE	Provider Backbone Bridging-Traffic Engineering
PC	Personal Computer
PCM	Pulse Code Modulation
PCP	Priority Code Point
PCRF	Policy and Charging Control Function
PDC	Pacific Digital Cellular
PDH	Plesiochronous Digital Hierarchy
P-GW	Packet Data Network Gateway
POP	Point-of-Presence
PRIO	Priority
PSTN	Public Switched Telephone Network
PTP	Precision Time Protocol
RF	Radio Frequency
RFC	Request For Comments
RTP	Real-time Transport Protocol
RVSP	Resource Reservation Protocol
SCTP	Stream Control Transmission Protocol
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SON	Self Organizing Network
STID	Spanning Tree Identifier
STM	Synchronous Transport Module
TACS	Total Access Communications System
TCL	Tool Command Language

TCP	Transmission Control Protocol
TD-CDMA	Time Division CDMA
TDD	Time Division Duplexing
TDMA/TDM	Time Division Multiple Access and Multiplexing
TD-SCDMA	Time Division Synchronous CDMA
UDP	User Datagram Protocol
UNI	User-to-Network Interface
US	United States
VCID	Virtual Connection Identifier
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VoIP	Voice over IP
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
VTT	Technical Research Centre of Finland
WCDMA	Wideband CDMA
WFQ	Weighted Fair Queuing
WiMAX	Worldwide Interoperability for Microwave Access
WirelessHART	Wireless Highway Addressable Remote Transducer Protocol
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WPAN	Wireless Personal Area Network

1 Introduction

Mobile traffic demands are increasing and will dramatically keep increasing in the future. Demanding, high-speed traffic profiles mean smaller cell sizes due to physical constraints which translate to a need for more base stations and more transport capacity. In turn, more and more backhaul connections are needed, especially on the bandwidth-constrained last mile access. Traditionally mobile backhauling has been done with simple point-to-point microwave, copper or fibre connections. However, along with LTE-Advanced (Long Term Evolution) and shortening cell coverage areas, base stations need to be placed in unconventional locations in context of telecommunications equipment such as lamp post. Integrating an adequate backhaul transport for these smaller base stations becomes problematic. Therefore, there is a need for investigating smart and flexible backhaul solutions for this last mile of the backhaul. The use of directional wireless meshes used as a backhaul transport has been jointly studied by NSN (Nokia Siemens Networks) and VTT (Valtion Tieteellinen Tutkimuskeskus, Technical Research Centre of Finland). The earlier phases of this research project have resulted in specifications of completely new routing, link scheduling, resiliency and other system design algorithms as existing meshing protocols were judged unfit for the task. In this master's thesis a proof-of-concept system will be built to study and verify the functionalities and feasibility of these new algorithms.

1.1 Future outlook for mobile traffic

The rise of smartphones has been and probably will be the main driver for ever increasing mobile data volumes in the future along with new types of devices using mobile data such as tablet computers. On the other hand smartphones has caused the competition in the mobile handset markets to move towards hypercompetition between different ecosystems (i.e. Apple vs. Android vs. Windows) but also unchained consumers from the walled gardens of mobile operators by enabling access to the Internet via genuine and working web browsers. This, in turn, has fundamentally changed how people use their smartphones and the popularity of rich multimedia content streaming is growing continuously. According to estimates by Cisco and Alcatel-Lucent, mobile traffic volume is forecasted to follow exponential growth trend, being over 6 exabytes per month by the year 2015. NSN and Ericsson have slightly lower estimates, being around 3 exabytes for the same year. Numbers are summarized in Figure 1 [1]. The present 3G LTE (third generation of mobile telecommunications) technologies such as HSPA and HSPA+ (High Speed Packet Access) will take care of the high access requirements for now but as the distributed content gets richer with, for example, high definition video, the bandwidth starts to feel a bit too narrow.

LTE-Advanced (Long Term Evolution) is one of the first technologies defined capable of fulfilling the requirements for the IMT-Advanced (International Mobile Telecommunications) criteria issued by ITU (International Telecommunication Union). LTE-Advanced technology set is able to offer data speeds from hundreds of megabits all the way to the gigabit mark, which can be regarded as a genuine broadband mobile access. This is mainly achieved by streamlining and simplifying especially the core part of the radio service system and with better efficiencies in the radio access part, the

whole system converging towards an all-IP (Internet Protocol) network. [2] In addition, with present channel coding techniques, data rates are getting closer to the theoretical Shannon upper bound for radio channel capacity. This means that in order to achieve higher data rates, consumers need to be closer to the base stations, thus the trend in the radio access has been to move towards even smaller cell sizes, namely to picocells and femtocells. These take care of areas ranging from a couple of tens of square meters to hundreds of square meters, to better target certain high data rate demand areas such as city centers.

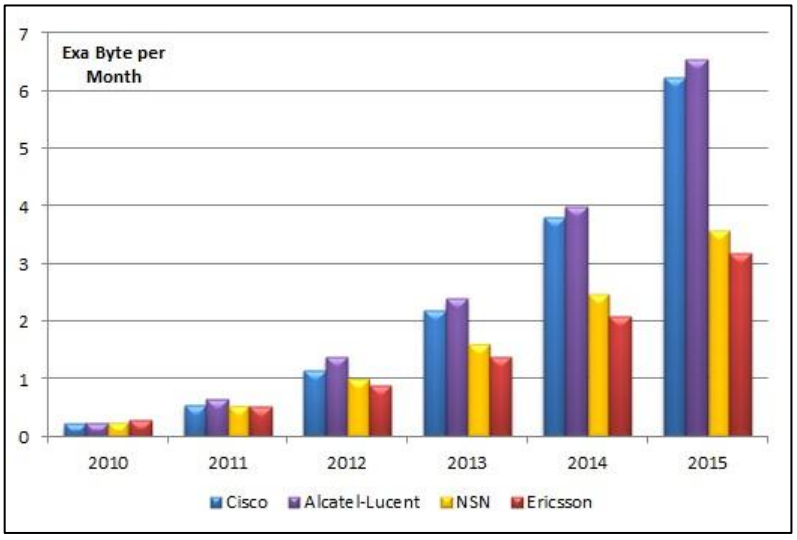

Figure 1: Mobile data traffic forecasts for the year 2015. [1]

1.2 Problem statement

Figure 2 illustrates the present direction in mobile base station coverage evolution. Capacity has been traditionally increased by simply increasing sectors within base station coverage, increasing the number of potential frequency channels or generally overhauling the radio access methods. LTE-Advanced introduced the idea of heterogeneous network deployments. Essentially, this means that a base station coverage area is enhanced with adding smaller base stations within the cell area. These smaller base stations act as hot spot access points, bringing capacity potential to densely populated areas such as city centers or railway stations. Capacity is thus increased, not only with frequency and sector overhauls, but with topology choices as well.

The smaller cell sizes along with heterogeneous network deployments can bring gigabit speeds for mobile clients. With the increasing number of smaller base station sites, backhauling these connections to nearest operator POP (Point-of-Presence) will eventually become problematic. The fiber infrastructure used in aggregation and core transport is not always feasibly extended for various reasons. Alternative copper-based solutions are not up to the task, mainly due to their insufficient transport capacities. One way to backhaul the sites is to use wireless links, directional microwave or millimeter wave radios in particular. However, as the base stations that are to be backhauled, are in places such as lamp posts, utility masts, bridge walls, often surrounded by building

"canyons", the connection to the gateway base station is not necessarily direct. This subsequently suggests a relaying functionality among the smaller base station backhaul units. One of the most promising methods for backhauling these smaller base station sites seems to be meshed infrastructure using microwave and millimeter wave radios [3] which also opens possibilities to enhance the access infrastructure with smart technologies such as SON features (Self Organizing Network), protection and load balancing methods.

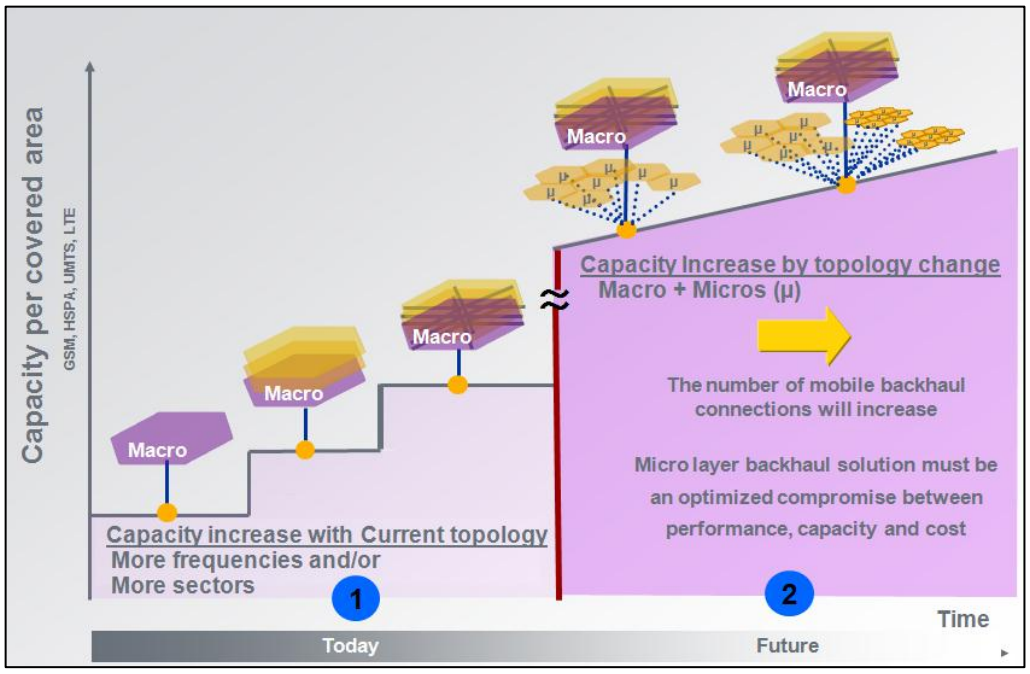

Figure 2: The problem statement.

Even though the idea of wireless meshes is quite well known, the possibilities of using directional wireless mesh networking or rather partially meshed wireless mesh networks as mobile backhaul connection is rather new and has been closely studied jointly by NSN and VTT as part of the MEVICO project (Mobile Networks Evolution for Individual Communications Experience) which is a European research project to study the network aspects of the LTE-Advanced mobile broadband network. The idea is to connect LTE-Advanced evolved NodeB base stations via point-to-point microwave links to a partially meshed directional network with advanced traffic management functionalities to provide improved resiliency and flexible usage of available transport capacity. The initial planning and specification work started in 2008 and has been slowly building in complexity, resulting in a need to verify and test developed algorithms in practice.

1.3 Earlier study

The concept of wireless mesh networks has been studied quite widely. Existing solutions around wireless mesh networks can be labeled roughly in three different categories: (mobile) ad-hoc networks, wireless sensor networks and (static) wireless mesh

networks. Ad-hoc networks are wireless networks formed by nodes without pre-existing infrastructure, for example, a set of laptops forming wireless connections without switches or routers acting as access points. Typical to these sorts of networks are that they are power-constrained, have low throughput and medium to high latency. IEEE (Institute of Electrical and Electronics Engineers) 802.11s is a wireless mesh extension for the IEEE 802.11 WLAN (Wireless Local Area Network) standard family and defines specific mesh functionality enhancements for 802.11-based networks [4]. Typical research areas over wireless ad-hoc networks include, for example, the usage of different antenna techniques [5], different medium access control algorithms and scheduling principles [6] [7] [8] and networking and routing optimization issues [9] [10].

Wireless sensor networks are usually heavily power- and energy-constrained networks that consist of simple field nodes and a sink node acting as a gateway or data storage. IEEE 802.15 standard family specifies technologies for WPANs (Wireless Personal Area Network). WPANs can be used to connect applicable devices with a range of a few meters. [11] 802.15 family has been used as a basis for many present low-rate and low-power mesh networks such as ZigBee and WirelessHART (Highway Addressable Remote Transducer) [12] [13]. Typical research areas and applications for WPANs and sensor networks are multimedia home networks, military purposes and surveillance in difficult terrains.

Static wireless mesh networks are typically better structured networks that are built around mesh nodes and a gateway connecting the mesh cloud to a wired infrastructure. IEEE 802.16 WiMAX (Worldwide Interoperability for Microwave Access) Mesh mode amendment is an example of such static mesh network [14]. 802.16j defines another method for WiMAX basic operation called Mobile Multihop Relay mode, which aims at improved coverage and throughput enhancements [15].

In addition to the standardized IEEE variants presented above, research exists also on wireless mesh networks used in backhaul solutions. Topics include overall radio access design in third and fourth generation mobile networks [16] [17], resiliency and Quality of Service aspects [18] [19] and antenna and link technology studies [20] [21] [22] [23].

As a preliminary input, a survey by VTT was undertaken to study the feasibility of existing meshing protocols to be used as a basis for the planned backhaul mesh concept. However, none was found to fulfill the pre-established performance, manageability and cost criteria.

1.4 Author's contribution and results overview

The main objective of this master’s thesis is the assembly of a proof-of-concept hardware platform system that is running a prototype version of the developed small cell access backhaul protocol discussed in Section 1.2. Furthermore, the scope of this master’s thesis includes the entire planning and execution of extensive testing scenarios to verify the different functionalities and demonstrate the feasibility of the system as well as the partial development of the concept and the prototype protocol.

The test cases cover exhaustively all the functionalities of the proof-of-concept system, including the novel routing and scheduling algorithms, resiliency, Quality of Service, traffic and load management and a set of preliminary performance tests. Based on the results of the numerous test cases, the functionality and feasibility of the wireless

mesh concept were validated. The proof-of-concept demonstrator system performed exemplarily throughout the testing process. Certain aspects in creating and expanding the demonstrator system required noteworthy amounts of work in order to get the system functional but in the end the different hardware units were integrated successfully together and they formed an impressive ensemble.

Moreover, some of the most notable test results include the cooperation of the prototype protocol, the network processor platform and the radio units in order to implement the novel routing and scheduling schemes, extremely fast resiliency scheme, outperforming the MPLS (MultiProtocol Label Switching) path and fast rerouting mechanisms and the functionality of smart traffic steering algorithms in heavily congested network situations.

1.5 Structure of this thesis

This master's thesis consists of five main chapters. Chapter 2 discusses the different aspects of mobile communication systems in terms of traffic and technology evolution. Some of the reasoning and factors behind the forecasted exponential mobile data traffic growth are presented. Moreover, a short overview on the architectures and technologies of different generations of mobile communication systems are given.

Chapter 3 discusses the purpose and technologies of mobile transport and backhauling. The most common aspects of mobile backhauling are discussed, including the general structure and hierarchy and motivation behind mobile transport in general. Additionally, different technologies utilized in legacy backhaul solutions and packet-based backhaul solutions are presented. The challenges related to LTE-Advanced and heterogeneous networks are explored in terms of mobile transport. Finally, the requirements for future LTE-Advanced heterogeneous network backhaul technologies are discussed.

Chapter 4 presents a potential wireless mesh access backhaul solution for LTE-Advanced, aiming to fulfill the requirements for heterogeneous network transport. Motivation and background is given on why an entirely new transport solution was required. The key aspects of the concept are presented shortly.

Chapter 5 introduces the proof-of-concept system built in conjunction with this master's thesis. The different elements of the system are presented as well as the concept related topology, routing and scheduling information used in this particular system. Finally, overview on the design and specification principles on the testing process, planned and carried out as part of this master's thesis, is given.

Chapter 6 presents an overview on the designed test cases for the individual functionalities of the wireless mesh concept. The results for all the test cases are also summarized. Discussion on the concept and potential future work is given with a short introduction on public demonstrations of the concept.

Finally, Chapter 7 presents a summary and conclusions for this master's thesis.

2 Mobile traffic and network evolution

Mobile data volumes have surged during past few years and are expected to grow exponentially in the near future. Behind this trend is a mixture of factors including the new smartphone era and cheaper access to mobile broadband. This chapter discusses the factors behind the ever increasing mobile data growth and how mobile networks have evolved technically to cope with higher capacity needs. Section 2.1 presents different factors and trends affecting mobile data usage with a closer look at some of the major facilitators. Section 2.2 presents a sort introduction to mobile networks and how they have evolved over time to better fulfill demands from the telecommunication industry.

2.1 Mobile traffic evolution

For a long time, the technical target in mobile network design has been to optimize the network infrastructure for voice traffic transport while reserving only a little room for mobile data traffic. However, the situation has been different for a couple of years now. Mobile data traffic is gradually growing and taking over voice in terms of traffic volumes. The trend in mobile networks has been to move towards all-IP (Internet Protocol) networks where all traffic is packet-based and voice is merely part of real-time traffic class.

In 2009, for the first time, mobile voice was overtaken by mobile data in terms of traffic generated on mobile networks. It is also expected that in the near future the mobile voice traffic growth will remain rather limited compared to the expected exponential growth of mobile data traffic. As illustrated in Chapter 1, the monthly usage volumes could rise to as high as 6 exabytes per month by the year 2015. The exponential growth for mobile data is driven by growing number of smartphones, connectivity dongles, tablet computers and other connected mobile devices. [24] As of February 2012, half of the typical traffic profile for a mobile data consumer consists of video traffic [25]. According to some forecasts the video portion will grow to 66% by the year 2014 [26], or even 90% by the end of year 2012 according to another forecast [27]. Most of the video and data traffic is generated through mobile web browsing. Other notable sources are services such as IPTV, video-on-demand and peer-to-peer sharing. Another important segment of mobile application and service evolution is social networking in form of e-mail, instant messaging, blogging, micro-blogging, VoIP (Voice over IP) and video transmissions [26].

Anyhow, this does not explain the whole story behind the tremendous traffic explosion in the packet switched domain. On top of device driven growth, demographical reasons also play an important role in traffic volume build-up. There will be around 7.6 billion people in the world by the year 2020 with the current population growth rate. The market for potential mobile broadband users is continuously growing and directly increasing the overall mobile traffic volumes. At the same time, the increasing potential user base is facilitating growth with the mobile broadband enabled handset markets, creating a synergy in which both of the parties are influencing growth in the markets of the other. As of December 2011, 25% of the world population is using the Internet while 60% is subscribed to some sort of a mobile communication system. These figures suggest that there is a major area of untapped customer potential. According to some

estimates, the growth of mobile Internet users in industrialized countries will saturate more or less somewhere in the year 2015. However, the market growth in the developing countries seems to keep growing without interruptions. In developing countries the dominant access method to the Internet in some cases is only via mobile broadband enabled handheld devices due to cost inefficiencies in fixed access deployment in sparsely lived geographical areas. The other reason for future mobile traffic growth is the portfolios of attractive business models of the mobile operators. The most visible and tempting of these models is perhaps the flat pricing packages for unlimited mobile data access. This, on the other hand, has some negative effects on the long term profitability of the operators. [26]

The telecom ecosystem as a whole is in a very disruptive phase. The main enablers for mobile Internet are mobile operator businesses, mobile operating system ecosystems, mobile terminals and mobile network technologies. They all have to be adapted and evolve in order to handle the technical and business aspect evolution that the concept of mobile broadband requires and enables. The changing role of these enablers and how they facilitate mobile data growth is further elaborated in the following sections.

2.1.1 Mobile operators

For mobile operators mobile broadband and Internet has resulted in significant changes in their tariff planning. Mobile voice tariffing has been traditionally based on time-based charging and on a fixed portion that is charged monthly or as a customer activates its operator specific subscription. Early data services were charged on a data chunk basis, for example, price per Megabyte. However, regulation and demand side economics backed up by the rise of the smartphones has forced mobile operators to change their tariffing plans to monthly flat rate pricing for unlimited data traffic for customers. In the long run, though, flat rate pricing has a dire negative effect on mobile operator revenue generation and on the ability to build new, even more capable mobile networks. Another challenge has emerged from the changing role of the operators. As the interest for mobile broadband customers lies within the Internet realm and on the online application and content world, the role of the mobile operators has reduced to offering merely a bit pipe for consumers. This in turn has resulted in mobile operators moving into charging for data chunk packages, selling a certain amount of data per user per month. The data size can vary from a few hundred megabytes per month for casual web browsers to tens of gigabytes per month for 3G heavy users (third generation mobile networks). This trend started in the US (United States) already in 2010 when AT&T ended selling unlimited data packages [28]. Some mobile operators have also presented their interest for creating mobile operator specific application stores similar to what the present mobile handset and operating system manufacturers and developers have been doing [28]. Some operators have also started offering other kinds of value added services bundled with their network access subscriptions which allow the operators to capture some of the value that the online content markets possess. For example, the Finnish operator Elisa sells value added services in form of clever and attractive IPTV product solutions (Elisa Viihde) and security solutions (Elisa Vahti) [29]. Another example is the US-based operator Verizon which has been offering premium and exclusive high quality

and high definition streaming services for NFL (National Football League) game broadcasts [30].

2.1.2 Mobile operating system ecosystems

The emergence and introduction of mobile platforms (Apple iOS and Google Android in 2007 [31]) and especially mobile web browsers that can handle web pages in their original forms enabled customers and mobile handset users break out from the walled gardens of mobile operators. On top of the smartphone platforms, application stores emerged. Apple was first with the App Store and Google came second with its Android Market. The application stores and application developers together create platform specific ecosystems.

The fight between these different ecosystems facilitates innovation for mobile platforms and rapid growth in mobile data usage as consumers adopt new applications, games and trends [32] [33]. For example, most advanced games for smartphones can be up to a few hundred megabytes in size, all downloaded via mobile networks. All of the present dominant mobile operating system platforms offer a capable and powerful platform that can run rich media content and offer several ways for consumers to be connected. These capable smartphone platforms then play a major role in the future mobile data traffic explosion.

2.1.3 Mobile terminals

Since the launch of iPhone by Apple, which can be regarded as the moment for rise of the smartphones, the market for smartphones and smart connected devices has been going rapidly in volume especially in the last two years (2010 and 2011). [34] Mobile terminal differentiation especially in the Android world has been in the technical performance side, i.e. more powerful processors, more cores, more memory, larger screens etc. Today's smartphones are actually more powerful than couple of year old desktop computers. On the other hand, even though smartphones and their software platforms are one of the main contributors for exponential mobile data growth, they still only take around 27% of the whole mobile phone market share, the rest is controlled by feature phones [34]. One can only imagine the daily mobile data volumes when this ratio starts to tip towards smartphone dominance.

2.2 Mobile network evolution

The principal concepts in mobile communication systems are global connectivity and seamless mobility, global roaming, authentication needs, secure connections and transmissions and global standardization. These form the basic requirements and basis for how mobile communication systems need to be designed, interworked and regulated. Global connectivity and seamless mobility mean that a wide area needs to covered with different access methods and connectivity equipment (i.e. base stations). From this follows that wide area coverage needs to be divided into cellular substructures which are conventionally modeled with hexagonal areas, each served by a base station. This way service needs can be better designed and targeted in heterogeneous traffic pattern areas. Furthermore, cells can be still divided into individual sectors with directional antennas.

Seamless mobility for users is implemented with a handover mechanism, meaning that active connections are kept alive during a base station switchover between coverage areas. The responsibility between two base stations is switched in such a way that already established connections are disrupted as little as possible while the serving base station changes. [35] Base station coverage can be labeled by its cell size which is essentially the maximum distance that the base station can transmit data without errors in the mobile terminal reception. The term macrocell is used to describe the widest range of cell sizes. Macrocells are preferred in rural areas or along highways. In densely populated urban areas, microcells can be used as macrocell hot spots. Picocells are for areas even smaller than microcells. An example of usage would be a large office, a mall, or train station. Currently the smallest area of coverage can be implemented with a femtocell which can be used in homes or small offices.

The architecture of a mobile communication system includes distributed systems such as the base station access part and centralized systems such as the authentication of users. The former part forms the radio access network of a mobile communication system. The latter centralized part of a mobile communication system is called the core network. General high level system architecture for mobile networks is summarized in Figure 3. Radio access network includes base stations and controllers for the base station elements. Radio access network is responsible for all the radio related functions and may also take care of some mobility management functionalities. Core network consists of switching and routing elements that forwards incoming calls and packet data from the radio access network towards other networks. Core network also includes authentications servers, signaling entities and mobility management functionalities. Traffic moves between these logical units through backhauling connections. [35]

Over time, the mobile network infrastructure model has been changing to better fulfill the demands from the telecommunication industry. The direction now seems to be towards increasingly flatter network architectures, lowered hierarchy of link-layer specific network elements and gradual introduction of IP for all parts of the mobile network. This is mandatory in order to deliver generally lowered system latency and more open interfaces. It has also been pointed out that the trend in mobile networks has been a transition from being transport-centric, where the focus is on delivery of packets and being simply a bit pipe for transient traffic, to becoming more service-centric by offering features such as comprehensive Quality of Service schemes and smart connectivity device deployments. [37]

In addition, mobile networks have the possibility to use devices functioning on the licensed spectrum namely femtocells and picocells. Femtocells have been used to offer a coverage extension in form of home access points. They have cell sizes comparable to WLAN (Wireless Local Area Network) capabilities but enable a more controlled access in terms of, for example, Quality of Service. Picocells offer slightly wider coverage areas than femtocells and have been started to use as a capacity fillers in high density areas, such as city centers. Picocells form the basis in heterogeneous networks in which macrocells and picocells interwork together forming wide coverage areas but still being able to provide high capacity hot spots. The first signs of more service-centric mobile networks were in 3G networks (third generation of mobile telecommunications) which employed the IMS (IP Multimedia Subsystem). Subsequently, 4G (fourth generation of mobile telecommunications) systems are already nearly entirely all-IP. The evolution of mobile networks is discussed more closely in the following sections. [37] [38] [39]

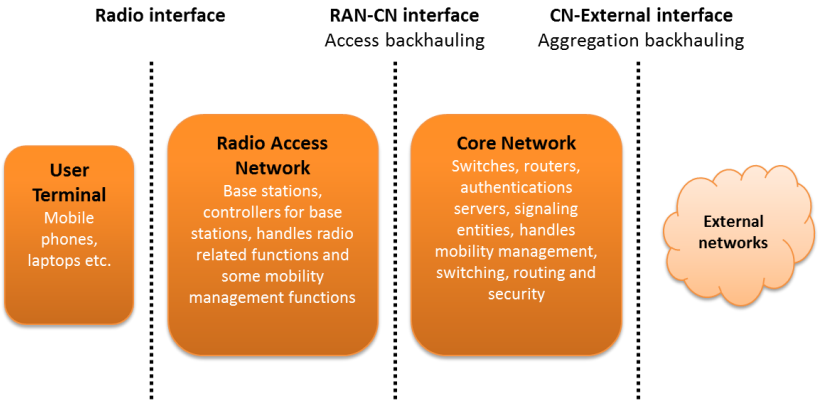

Figure 3: High level system architecture for mobile networks [36] (modified).

2.2.1 First generation cellular networks

First generation cellular networks were the first set of technology standards that introduced the cellular structure that since has persisted throughout the following technology generations. All the different mobile communication standards labeled as the first generation technologies offered voice services that were entirely analog. FDMA/FDM (Frequency Division Multiple Access and Multiplexing) was used as the multiple access and multiplexing techniques. First generation FDMA systems were so called narrowband systems as the separation of users was done with several narrowband channels occupying only a few dozen kilohertz of channel space. The whole frequency band allocated for a given mobile operator was divided into smaller frequency bands and distributed over the mobile network infrastructure. Inside a cell, the allocated frequency band was further divided into even smaller sections which were the actual usable communication channels and used as the means of data transfer between mobile customers and base stations. In addition, the signals being analog meant that the quality degraded quite linearly as a mobile client was moving further from a base station. Using narrowband FDMA meant also that the communication channels were sensitive to fading, needed powerful frequency filters and wasted air interface resources in the sense that entire communication channel was allocated to a single customer during a connection. On the other hand FDMA was the only reasonable and practicable access technique for a completely analog system. In the core network side of the first generation cellular networks, communications were routed by circuit switching. Essentially the first generation technologies were merely a rather direct extension for the existing PSTN (Public Switched Telephone Network) over the air.

The basic network architecture of a first generation cellular network is illustrated in Figure 4. The network consists of two main subsystems: base station subsystem and network and switching subsystem. Base station subsystem consists of BTS (Base Transceiver Station) and BSC elements (Base Station Controller). At minimum BTS hosts antennas for mobile terminal communication, other relevant RF (Radio Frequency) elements and software for multiple access implementation. A set of BTSs are connected to a BSC. BSCs and BTSs can be co-located and backhauled with wired (e.g. fiber or

copper) or wireless connections (e.g. directional microwave radios). BSC is responsible for controlling the attached BTSs by implementing the majority of mobility management functions, processing mobile terminal measurements, handover execution, radio channel allocation etc.

Next in hierarchy is the network and switching subsystem. Network and switching subsystem consists of the MSC (Mobile Switching Center), HLR (Home Location Register), VLR (Visitor Location Register) and AUC (Authentication Center) elements. MSC is responsible for inter-BSC mobility, paging and location update functions and interworking with PSTN. Location registers HLR and VLR are responsible for keeping track of operator specific customers and roaming customers temporarily subscribed to a network. AUC handles authentication related functions based on mobile terminal identities. [35] [40] [41]

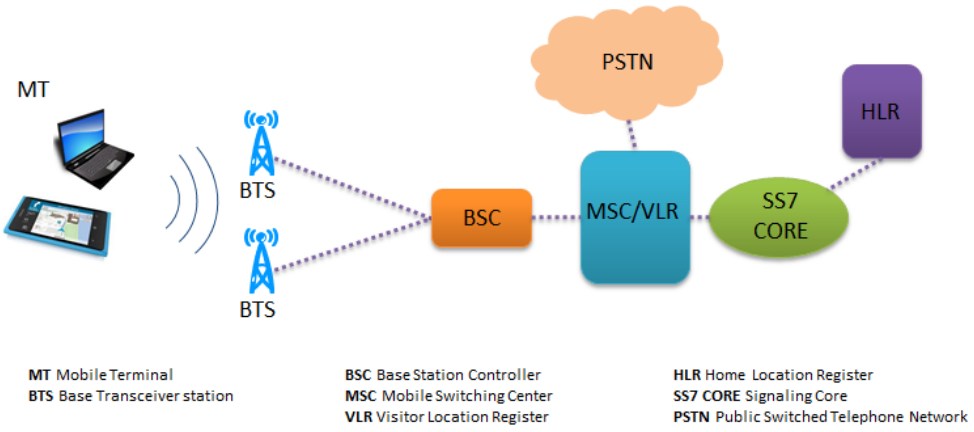

Figure 4: The structure of a first generation cellular network.

The first generation cellular systems did not really become globally united, and different set of standards were used in different countries. NMT (Nordic Mobile Telephone) was the standard used in Nordic countries, Eastern Europe and Russia. The standard established in the United States was AMPS (Advanced Mobile Phone System). Finally, TACS (Total Access Communications System) was used in the United Kingdom. [41]

2.2.2 Second generation cellular networks

The main innovation in the second generation cellular networks were digitization of the transferred speech signal which also meant that digital compression techniques was also possible to apply, improving the overall efficiency in the radio access. This also enabled the possibility to use more efficient multiple access and multiplexing techniques. The incoming analog signal (i.e. voice) in the mobile terminals was modulated using PCM (Pulse Code Modulation). After this compression techniques reduced the information rate needed to transmit over the air. Second generation mobile systems mainly used two different approaches for multiple access and multiplexing.

GSM (Global System for Mobile Communications) standard used a TDMA/TDM method (Time Division Multiple Access and Multiplexing). In TDMA, time continuum

is divided into slots which are then allocated to different customers. The time slots are filled with the digital PCM voice samples originating from the customer terminals. In addition to overall efficiency of TDMA, it also enabled higher instantaneous throughput for a given costumer, allowed discontinuous reception which meant that mobile terminals could move to a power saving state during an inactive reception/transmission period permitting longer battery life. There are also some downsides in TDMA systems. Overall, a carefully planned delay budget planning is needed due to the queuing over time. TDMA systems also perform better coupled with some other multiple access system, such as FDMA, in order to avoid system-wide waiting time accumulation. [40] [41]

GSM became quite widely spread standard. In 2010 around 2 billion people around the world was connected via GSM deployments in 212 countries around the world which in turn made global roaming possible for GSM terminals. Rival standards also existed but did not gain the same kind of global popularity as GSM has gained. PDC (Pacific Digital Cellular) was used in Japan and employed TDMA/TDM as its multiple access. IS-95 (Interim Standard 95) was used in the United States area and employed a different multiple access compared to GSM and PDC, the CDMA (Code Division Multiple Access). CDMA is a so called wideband access system, meaning that radio transmission occupies the whole system spectrum thus allowing all resources to be used in every cell and enabling a relatively high system capacity. [35] [41]

Initially second generation cellular networks did not offer any genuine data services in addition to carrying the actual digital voice samples. In GSM the first real data services came in form of the GPRS (General Packet Radio Service). Essentially, GPRS introduced a packet switched domain next to the traditional circuit switched domain enabling packet switched transmission over the air. Mobility was handled by hiding the radio access network operations (such as handovers) from external networks (such as Internet) by tunneling incoming and outgoing packet data in the edge of the core network. The air interface introduced a separate pool of TDMA slot resources that were allocated to data packet transmission. Up to eight time slots can be reserved for a single customer resulting in a maximum of 171.2 kbit/s transmission speeds. The packet switched domain introduced two new mobile network elements: SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node). SGSN is responsible for the delivery of data packets from and to the mobile terminals within a certain geographical service area. It routes packet traffic, handles mobility management tasks and also does authentication and charging related tasks. GGSN is the element responsible for communicating and interworking with external networks. The structure of GSM network architecture enhanced with GPRS elements is depicted in Figure 5 which shows the packet switched domain implemented separately next to the traditional circuit switched domain. [41] [42]

The next step in GSM data service evolution was EDGE (Enhanced Data rates for GSM Evolution). EDGE is an extension to the existing GPRS standard, employing the same packet core architecture but refining some of the air interface characteristics. Improvements were done by applying better modulation techniques and changing some of the physical layer aspects. Maximum data rates were in theory 473.6 kbit/s, later peaking up to 1 Mbit/s with further refinements. GSM evolution ends with EDGE. [42]

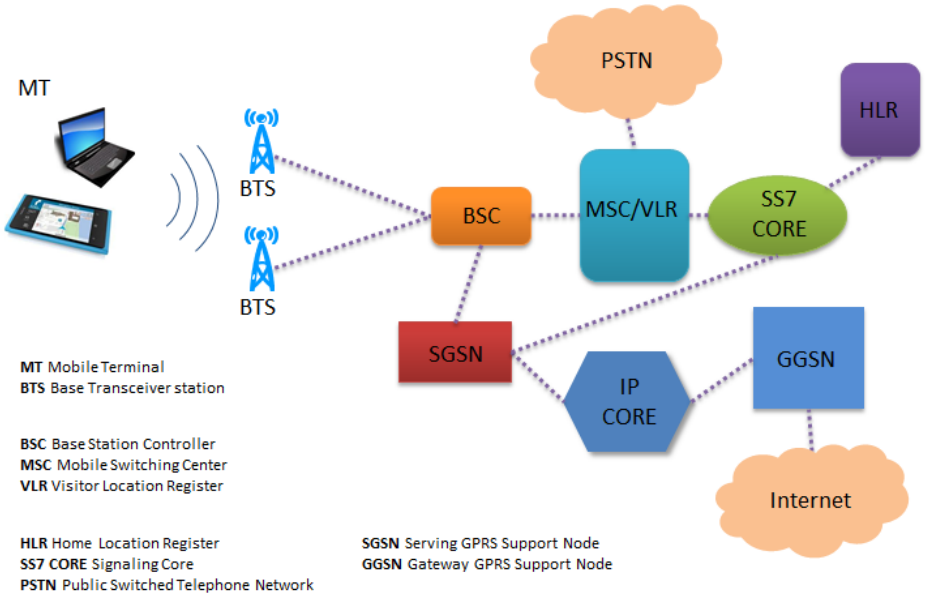

Figure 5: The structure of a GSM network enhanced with GPRS elements.

2.2.3 Third generation cellular networks

The success of second generation mobile standards motivated the development of a successor system. Certain goals were pre-established and they were to implement a system with better spectral efficiency, higher peak data rates, wider support for interactive and multimedia services and backward compatibility. CDMA was chosen as the multiple access method in the air interface. A general consensus for using a single standard in all regions of the world was not achieved, thus eventually five different access methods was accepted to be part of the IMT-2000 (International Mobile Telecommunications) standard set defining the technologies to be used in third generation cellular networks. The core side of the network stayed largely the same compared to the second generation evolution architectures. Separate switching domains were allocated for circuit and packet data. Radio access network on the other hand was changed completely. As mentioned above, there were five different access technologies in the end of the standardization cycle: WCDMA (Wideband CDMA), TD-CDMA (Time Division CDMA), TD-SCDMA (Time Division Synchronous CDMA), GERAN (GSM EDGE Radio Access Network) and CDMA2000 (Multicarrier CDMA). Different technologies were used in different countries. WCDMA ended up being the most popular of the access technologies and has been since its initial standardization rapidly adopted and deployed throughout Europe, Japan and rest of Asia. The network architecture in WCDMA stayed largely the same as in GSM systems. The core network was more or less used as is (apart from some software upgrades) and the structure in radio access also remained the same, only the element terms were changed. Base transceiver stations became NodeBs and base station controllers became radio network controllers. [35]

Third generation evolution has increased mobile data rates quite fast during the last couple of years. In 2002 the first evolutionary steps was taken in third generation technologies as HSDPA was introduced (High Speed Downlink Packet Access). Theoretical maximum data rates up to 14.4 Mbit/s could be achieved. The increased speed was the result of combining multi-code transmission towards mobile terminals and also introducing time division component on top of the CDMA code logic. By dividing the CDMA orthogonal code transmission in time, a pool of schedulable time and code resource slots were formed. These resource slots could then be assigned to customers depending on their bandwidth needs. Similar logic was later applied in the uplink and in 2004, HSUPA (High Speed Uplink Packet Access) was introduced and enabled a theoretical maximum of 5.76 Mbit/s data rates. Further evolution in third generation technologies has incorporated MIMO (Multiple In Multiple Out) antenna techniques, higher modulation schemes and radio carrier aggregation technologies to increase the mobile data rates even further. [35] [41] [42]

2.2.4 Fourth generation cellular networks

As third generation systems were on their first widespread rollout, the standardization bodies started already working on the next future mobile communication systems. It was deemed necessary as third generation system characteristics would not eventually be able to meet the demand for future mobile applications. ITU (International Telecommunication Union) defined a set of requirements for a genuine fourth generation mobile communication system named as IMT-Advanced. The requirements include all-IP base network, peak rates of 1 Gbit/s and high spectral and system efficiency among other things [43]. The major force behind fourth generation mobile network standardization has been 3GPP (The 3rd Generation Partnership Project) and the new standard became known as LTE (Long Term Evolution). It was decided that both air interface and core network sides needed a significant overhaul in order to cope with future traffic volume projections. In LTE, OFDMA (Orthogonal FDMA) was chosen as the multiple access in the radio interface. OFDMA consists of several subcarriers placed close to each other. These subcarriers can then be modulated with data and divided in time. [35]

In addition to the major changes in radio access network, core network underwent large changes. The whole underlying idea was to define a fully IP-based core network. LTE architecture also marks the elimination of the circuit switched domain present in the previous generation technologies. The LTE network architecture is illustrated in Figure 6. LTE radio access network consists entirely of evolved NodeBs that can communicate directly with each other without other controlling elements (such as the BSC and RNC). The core network in LTE consists of a MME (Mobility Management Entity), S-GW (Serving Gateway), P-GW (Packet Data Network Gateway), HSS (Home Subscriber Server) and PCRF (Policy and Charging Control Function). MME is responsible for overall mobility management and session control and mainly performs signaling functions only. S-GW is used as the core side anchor towards the radio access network. P-GW is responsible for interworking tasks with external networks. HSS is the master data base and register for subscriber information. PCRF takes care of traffic policing according to some established Quality of Service parameters. [40]

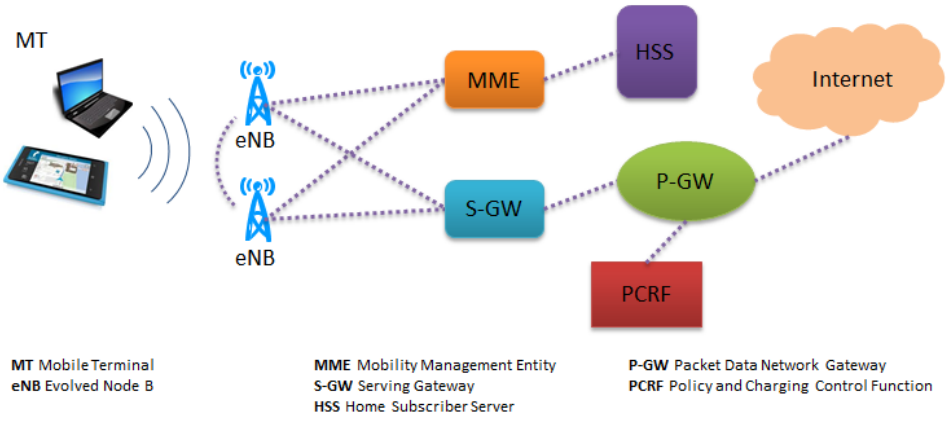

Figure 6: LTE network architecture.

LTE was the first candidate to fulfill the IMT-Advanced requirements set by ITU but did not quite meet them. More specifically, 3GPP Release 8 (as in LTE, specifications frozen in the end of 2008) enabled maximum theoretical throughputs of 300 Mbit/s in downlink and 75 Mbit/s in uplink. [44] Since the Release 8, LTE has gone through a number of evolutionary steps. To overcome some of the pitfalls that Release 8 had, 3GPP started working on the next LTE related specification set (Release 10) that would finally fulfill the IMT-Advanced requirements. Release 10 (also known as LTE-Advanced) extends the capabilities of the original LTE in numerous ways. Release 10 includes innovative techniques such as bandwidth extension and spectrum aggregation, extended multi-antenna transmission and relaying functionalities. LTE-Advanced also introduces an enhanced support for heterogeneous network deployments, which enables the usage of smaller picocells and femtocells on top of macrocell coverage. This results in densification (i.e. more base stations per area) of the radio access network which in turn enables better signal-to-noise ratios on mobile terminal and base station sites as communication end points are brought closer to each other. [45] [46] [47]

The first LTE (3GPP Release 8) networks are already commercially available. The world's first LTE mobile network was opened in the end of 2009 by mobile operator TeliaSonera [48]. The deployment pace since has picked up speed. As of May 2012 there are roughly 72 commercial LTE networks launched. The number is predicted to be roughly 134 by the end of year 2012 [49]. The first LTE-Advanced networks are projected to be deployed somewhere in the year 2013 [50].

2.3 Summary

Mobile data volumes have surged during past few years and are expected to grow exponentially in the near future. Behind this trend is a mixture of factors including the new smartphone era, cheaper access to mobile broadband and a set of demographical factors. Furthermore, the traffic growth trend is likely to remain exponential as there is a vast amount of untapped market potential for the mobile device and wireless communication infrastructure segments to expand, especially in developing countries.

Over time, the mobile network infrastructure model has been changing to better fulfill the demands from the telecommunication industry. The direction now seems to be towards increasingly flatter network architectures, lowered hierarchy of link-layer specific network elements and gradual introduction of IP for all parts of the mobile network. Moreover, mobile networks are undergoing a transition from being transport-centric, where the focus is on delivery of packets and being simply a bit pipe for transient traffic, to becoming more service-centric by offering features such as comprehensive Quality of Service schemes and smart connectivity device deployments.

In terms of technological evolution, mobile networks have been transitioning from fully circuit switched systems towards fully digitized, packet switched communication systems. The first mobile communication systems, collectively categorized as first generation cellular networks, were merely a wireless extension for the wired PSTN system. The second generation cellular networks in turn transported fully digitized voice and in the end of its evolution, also supported packet data transport. Third generation cellular networks took the first steps towards a genuine wireless and mobile broadband network access and introduced the IMS which can be regarded as the first sign towards more service-centric mobile communication systems. Finally, fourth generation systems introduced a major overhaul for mobile communication system design, renewing both core and radio access networks. Core network was designed to be simpler and flatter compared to previous generation networks. Radio access, in turn, was bolstered with more efficient radio interface technologies and topological enhancements in form of heterogeneous network deployments.

3 Mobile backhaul

The transport infrastructure between a radio access network and a core network is called the mobile backhaul. The basic function of mobile backhaul is to provide transparent connectivity service between base stations and core controllers. Along with LTE-Advanced and heterogeneous networks, the backhaul design has proven challenging.

This chapter presents the concept of mobile backhaul and transport along with the used technologies and solutions for different generation mobile communication systems. Section 3.1 discussed the basic functionalities of mobile backhaul including the service definition, tiered architecture and topologies. Used transport technologies for different mobile system generations are presented spanning from circuit switched systems to packet-based solutions. Section 3.2 discusses different aspects of how a backhaul transport should be designed for LTE-Advanced heterogeneous networks. Finally, Section 3.3 discusses what an optimal heterogeneous network backhaul solution might include.

3.1 Mobile backhaul overview

The mobile network architecture illustrations presented in Chapter 2 give a rather high-level logical view on how the elements of a mobile network are interconnected. A typical mobile (access) network consists of thousands or even tens of thousands of base station sites while the number of the core sites remains under a dozen per such base station cluster. The interconnecting network between these is the mobile backhaul transport network. Thus, the mobile backhaul unites the mobile network with other external transport networks, connecting a vast number of base station sites to a small amount of centralized control sites, transporting transparently the mobile network originated traffic and system signaling with certain Quality of Service, resiliency, security etc. requirements. The general trends in mobile data usage and the impending exponential mobile traffic growth (Chapter 2) also inevitably affect the mobile backhaul and its design requiring it to evolve accordingly. This essentially means that the mobile backhaul and transport will change from plain bit transport to giving more support to the mobile networks in terms of increased resiliency, better traffic management and Quality of Service. [51]

Due to vastly different equipment numbers, geographical issues and processing requirements between the mobile network base station sites and the core network controllers, it is evident that a hierarchical or tiered architecture is needed. Example architecture for a mobile backhaul network is given in Figure 7. The main tiers are the access, aggregation and core tiers. The access tier connects a number of base station sites to an access gateway device which is a low level device, executing typically layer 2 forwarding. Access tier technologies include microwave links, DSL (Digital Subscriber Line), plain Ethernet and NG-SDH (Next Generation Synchronous Digital Hierarchy). After the access tier, data is subsequently aggregated on the aggregation tier. Here data rates start becoming quite large, hence high capacity transport technologies are deployed including plain optical transport networks and IP/MPLS solutions (MultiProcotol Label Switching). Packet switching/routing happens here in layer 2 or in layer 3 with provider edge devices. Next in hierarchy is the core network site with relevant con-

trollers, gateways and high capacity provider core devices (e.g. BSC, RNC, MME, P-GW, GGSN etc.). The gateways subsequently direct data towards external transport networks via transit and peering points. [51]

In mobile network architecture specifications, the backhaul connection and topology is usually for simplicity illustrated as a single line (or a cloud in case of packet-based solutions) between access and core elements. However, the physical topology can be quite complex and its structure is dependent on numerous factors. The operator specific design, geographical issues, topology choices and existing network infrastructure all affect the physical implementation.

The backhaul topology choice depends largely on which tier the connections are deployed. The access tier naturally has a very large number of needed backhaul connections between mobile base station sites and the first access gateways. On the other hand, the capacities on these links are not so high. The most deployed transport technology in the mobile backhaul links is directional microwave links (55% in 2011) [52]. The topologies used in access are a tree or chain topology, main objective being high link utilization and sharing to cut down costs. In core tier, the situation is the opposite. Link and transport capacities are high and the number of links is rather low. The topology is quite often a ring type topology as resiliency is more important in the core than in the access due to the vast amounts of traffic being transported. The aggregation tier is normally a mixture between the two, capacities can rise quite high and the number of links is moderate. [51]

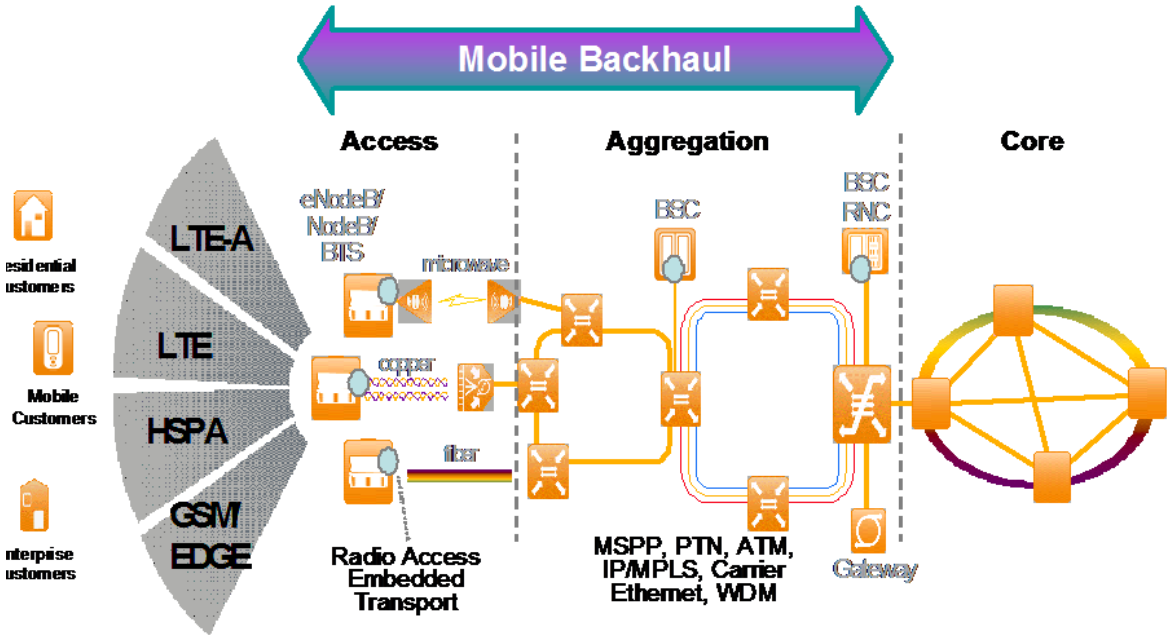

Figure 7: Example architecture for mobile backhaul.

3.1.1 Legacy backhauling

Most of the existing mobile backhaul connections or networks have been deployed to serve mobile communication systems presently considered as legacy technologies as in second and third generation mobile communications systems. The backhaul networks

have been built to serve solely second generation technologies or both second and third generation technologies. Both second and third generation systems are designed circuit switching in mind. Thus the backhauling solutions also employ TDM technologies to transport the radio access data towards the core. The most used TDM-based technologies are PDH (Plesiochronous Digital Hierarchy) and SDH transport technologies. Both are hierarchical systems multiplexing lower rate circuit switched data into high capacity transport frames and modules. PDH is mainly used near the access network to multiplex the circuit switched data originating from mobile clients. PDH hierarchy can transmit data rates up to 139.264 Mbit/s (E4 frame) [53]. Towards the core PDH capacity starts becoming insufficient requiring higher transmission capacity. SDH transmit capacity can go up to 40 Gbit/s (STM-256 (Synchronous Transport Module)) [53] and is quite widely deployed for core network transport. PDH and SDH both offer a synchronous transport service (nearly synchronous with PDH) with a fixed bandwidth and transport slotting. Any sort of configuration change traditionally needed to be performed locally, though newer equipment allow remote configuration with network management systems. The shortcomings of SDH have been partially amended in the form of NG-SDH which allows dynamic capacity allocation, multipath capacity and offers framing procedures for different protocols [51]. For third generation mobile systems ATM (Asynchronous Transfer Mode) [53] was also used over the PDH/SDH transport infrastructure. Even though ATM offers asynchronous and more packet friendly transport service with virtual circuits and cell framing, it still added another network layer and overhead to be managed and maintained. [51] [55]

3.1.2 Packet-based backhauling

The TDM-based transport solutions offer a basic and resilient transport service between base station sites and core network for legacy mobile communication systems. However, these systems are extremely inflexible in terms of dynamic capacity allocation and access capacity and are not able to handle large asynchronous traffic volumes. Packet-based solutions in the backhaul portion are then inevitable due to their capacity flexibility, low cost and high manageability features. The strategy for transition towards packet-based backhaul can be essentially two-fold. The legacy transport infrastructure can be entirely virtualized with a packet-based overlay network while new backhaul deployments can be made natively packet-based from scratch. Overlaying an existing PDH/SDH/ATM network can be cost effective but adds yet another layer of complexity. Replacing the current legacy backhaul infrastructure would lead to simplified network and layering architecture but would require substantial capital expenditure and would introduce challenges with, for example, interworking and synchronization though synchronization can be implemented quite effectively with Synchronous Ethernet [56] or Timing-over-Packet solutions. In any case, the packet-based solutions need to continue offering services and support for the current legacy technologies employed in mobile backhaul network. These services include pseudowire emulation for 2G systems (natively TDM) and 3G systems (natively ATM), services for newer IP-native 3G systems, LTE IP-native services etc. The most common packet-based backhauling technologies currently are Carrier Ethernet Transport, plain IP transport and IP/MPLS transport. [51]

Carrier Ethernet is essentially a set of amendments to plain Ethernet in order to make Ethernet transport more suitable for large, complex and demanding operator net-

work environments. Most notable set of features is the Ethernet OAM (Operations, Administration and Maintenance) [57]. Carrier Ethernet technologies offer a layer 2 transport between the radio network and core network. The most common Carrier Ethernet technologies are PB (Provider Bridging) [58], PBB (Provider Backbone Bridging) [59] and PBB-TE (Provider Backbone Bridging-Traffic Engineering) [60]. The transport network can be divided into hierarchy by using VLAN double tagging (Virtual Local Area Network) in case of PB or MAC (Media Access Control) address separation in case of PBB. The backhaul transport could be implemented, for example, by assigning two VLAN tags per an LTE evolved NodeB for control and data and then aggregating a cluster of same kind of VLAN assignments behind an operator VLAN tag for aggregation transport. Carrier Ethernet is optimal for 3G and 4G IP-native traffic transport but also supports legacy emulation for TDM and ATM with TDM over Ethernet [61] and ATM over Ethernet schemes. Carrier Ethernet protocols need a spanning tree protocol to be run alongside to prevent looping and unnecessary broadcast storming. Also, Quality of Service can be problematic in Carrier Ethernet but the situation has got better with PBB and PBB-TE. Resiliency in Carrier Ethernet solutions is largely dependent on the detection delay of error and the convergence time of used spanning tree protocol. Typical values for combined detection and convergence are around one second with Rapid Spanning Tree Protocol and Ethernet OAM. [51]

From 3G onwards, mobile communication systems have been supporting IP for fixed transport. IP can be used in conjunction with transport layer protocols TCP (Transmission Control Protocol), UDP (User Datagram Protocol) or SCTP (Stream Control Transmission Protocol). The transport stack in user plane is UDP/IP between base stations and controller units, and in control plane SCTP/IP. SCTP is preferred choice over TCP due to the ability to distinguish different users as opposed to plain byte oriented transport. [51] IP naturally requires a routing protocol to distribute the routing information. OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System) and BGP (Border Gateway Protocol) can all be found in different backhaul networks. For legacy TDM transport, IP can use specific and suitable real time upper layer protocols such as RTP (Real-time Transport Protocol). For Quality of Service, IP uses DiffServ (Differentiated Services) and IntServ (Integrated Services) schemes that control packet scheduling according to certain per-hop or per-domain target values. IP also offers some traffic engineering capabilities through its control protocols such as default routing and link weighting. Resiliency in IP networks is largely dependent on the error detection delay and the convergence time of the used routing protocol. Typical values for present routing protocols are a few seconds with IGPs (Interior Gateway Protocol) and a couple of tens of seconds with BGP [54].

IP/MPLS is perhaps the most used operator core transport technology. MPLS is effectively a layer 2.5 protocol tagging incoming packets with a special shim header and subsequently switching these shim headers across an MPLS cloud to form an MPLS tunnel. MPLS tunnels can be created by using LDP (Label Distribution Protocol) which in turn needs a routing protocol for topology knowledge, or entirely manually using RVSP (Resource Reservation Protocol). For backhaul networks, IP/MPLS offers numerous connectivity services such as layer 3 and layer 2 VPNs (Virtual Private Network) (BGP MPLS VPN [62], VPLS (Virtual Private LAN Service) [63] and VPWS (Virtual Private Wire Service) [63]) which can be used, for example, connecting a cluster of base stations with corresponding controllers over an aggregation network. MPLS

also offers extensive traffic engineering capabilities in terms of tunnel creation and incoming traffic handling. Quality of Service in MPLS networks is handled with DiffServ. Resiliency in MPLS networks can be extremely good and converge fast but can require manual configuration for best performance. Typical values are a couple of hundred milliseconds with MPLS path protection and around 50 milliseconds with MPLS FRR (Fast Reroute) [54]. Both methods require manual configuration of protective paths or links. Other possibility is to use LDP which is more automated but only converges after the control plane routing protocols have converged after a link break. [51]

3.1.3 Backhauling heterogeneous networks of LTE-Advanced

As was discussed in Chapter 2, to battle the exponential mobile data traffic growth, LTE-Advanced (and LTE to some extent) introduced the concept of heterogeneous network deployments along its antenna and radio interface specific additions. With heterogeneous networks, a coverage area of a macrocell is enhanced by adding base stations with shorter coverage to handle some of the traffic of the macrocells while the macrocell acts as a gateway between access and aggregation tiers. This is illustrated in Figure 8. These short coverage base stations are collectively called small cell base stations and can be categorized according to cell coverage and capacity as micro-, pico- and femtocells. The advantages of these deployments are obvious: Some of the traffic is offloaded to the small cells improving the overall system performance, more evenly distributed traffic volumes and generally better and faster service for mobile clients. The number of small cell sites in certain macrocell coverage are can rise up to even hundred pieces (e.g. large city center) and every one of them needs to have a fast backhaul connection. Thus, implementing the connectivity between upper transport tiers and the small cell base stations becomes problematic.

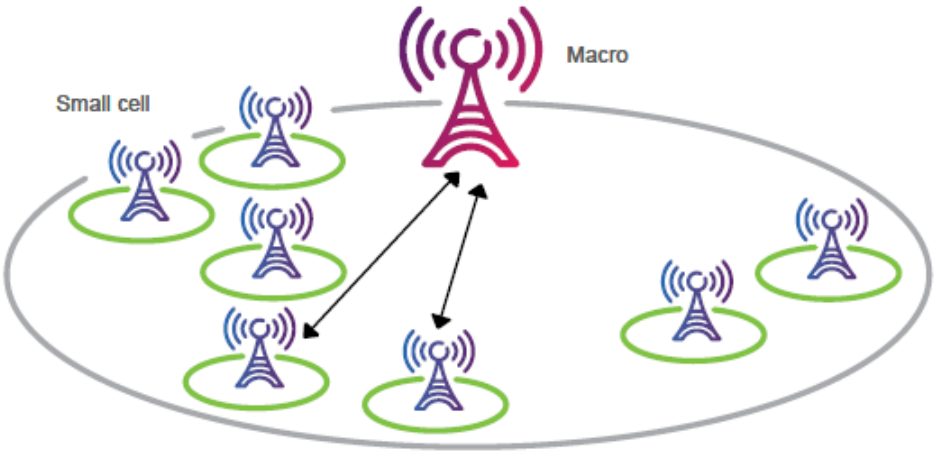

Figure 8: Heterogeneous network. [64]

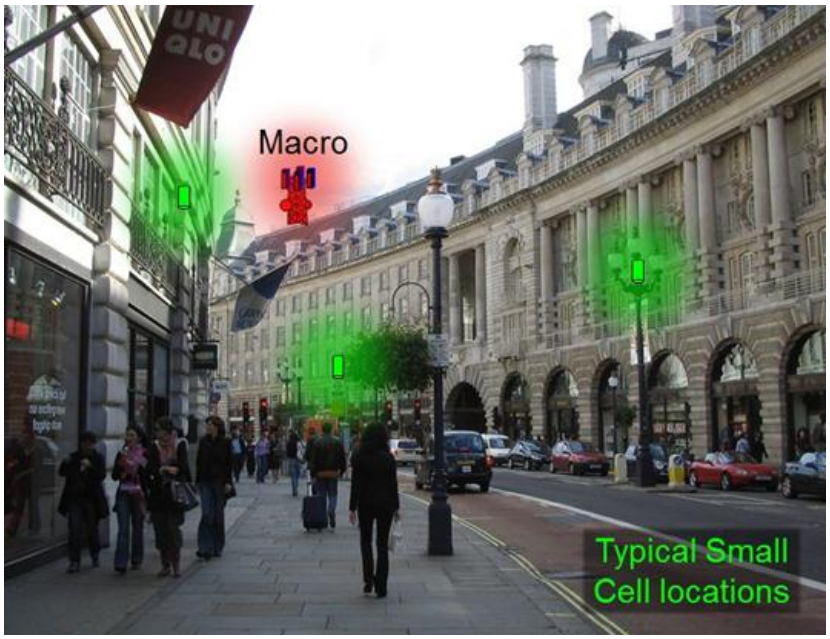

Figure 9: Typical small cell locations. [65]

Most notable challenge is the fact that the small cell base stations are deployed in locations which are not optimal for telecommunication equipment in general. Factors that have not traditionally affected telecommunications equipment will have larger impact. With macrocells, the base station is usually attached to a mast or tall building in such a way that there are no elements blocking the line of sight for backhaul connections or alternatively, the backhaul is implemented with wired connections. With heterogeneous networks and small cells, the typical deployment height for a small cell base station and a complementing backhaul transport point is three to nine meters above street levels, with installation platforms being lamp posts, bridges and building walls. Utilizing wired backhaul connections for these types of mounting places is clearly not always feasible. Wireless connections in turn will be under the effects of temporary blocking due to, for example, tall vehicles and trees and increased pole sway (lamp posts vs. broadcast masts) among other things. This is illustrated in Figure 9. With these unusual deployment locations, clear line of sight between a macrocell gateway and a small cell is not in most cases possible to guarantee. This in turn suggest a sort of relaying solution between small cells. Even so, the backhaul should still be able to fulfill the LTE-Advanced requirements with decent Quality of Service, availability, capacity etc., yet the installation and operational costs should be as low as possible. It is evident then that the access backhaul design for small cells can be quite of a challenge.

At the moment, there does not seem to be any general consensus of how exactly a small cell backhaul should be implemented as the entire concepts of heterogeneous networks and small cells are quite new. Equipment manufacturers have their own viewpoints on small cells [66] [64] [67]. However, technology forums such as MEF (Metro Ethernet Forum) and NGMN (Next Generation Mobile Networks) help to move the industry forward by clarifying consensus around the operators' requirements for small cell backhaul and have published extensive requirements reports for future small cell access backhaul systems [68].

3.2 Small cell access tier backhaul design

The most important general aspects of designing and implementing a backhaul service for LTE-Advanced small cell deployment are proper connectivity with a gateway (i.e. bit pipe), synchronization, resiliency, Quality of Service and security. These services should be offered by any modern mobile backhaul network but can cause serious challenges especially in the context of small cell backhauling. [51] [65] On top of these, additional design aspects include capacity and topology considerations, OAM mechanisms, choice of wired or wireless connectivity and hardware and physical design aspects [65]. These areas of small cell access backhaul design are discussed more closely in the following sections.

3.2.1 Wireless and wired connections

As mentioned earlier, a little over half of all the mobile backhaul connections are wireless microwave links. Wireless solutions can be either LOS (Line-of-Sight), NLOS (Non-line-of-Sight), suggesting the availability of a direct obstacle-free connection between two wireless nodes. In an urban environment, NLOS links generally can offer better coverage values but naturally offer less capacity. NLOS links are feasible only with carrier frequencies under 6 GHz, due to decreasing signal penetration capabilities. The situation is the opposite with LOS links. The most common LOS frequencies are in the 6 to 38 GHz band (microwaves) and 60-80 GHz band (millimeter waves). Both microwave and millimeter wave frequency bands can be used with highly directional antennas offering moderate to very high capacity throughputs. The potential limiting factors with millimeter wave technologies is quite high atmospheric absorption affecting the coverage of the link and precise link planning procedure requirements. Using millimeter wave links in LTE an LTE-Advanced mobile backhaul have been studied quite widely [69] [70] [71]. The general consensus seems to be that the high capacity up to 10 Gbit/s with proper configuration is recognized and that rain attenuation has great effect on the coverage in millimeter wave systems. However, these study results indicate that globally millimeter wave system can offer five nine availability with distances up to 1 kilometer which is more than fine for small cell backhauling. [65]

Another consideration in wireless systems is the spectrum licensing. The frequency bands available under 6 GHz and around 60 GHz are largely license exempt and can offer low cost backhaul solutions, however, interference may become a problem. For example, WLAN systems use 2.4, 5 and 60 GHz bands possible causing interference to backhaul systems on the same bands. 80 GHz band employs a light licensing scheme which allows the spectrum to be licensed via a simple and quick application process at a nominal cost. Generally, a licensed frequency band offers a more manageable and interference-free solution for backhaul. Traditional microwave technologies will probably decline in popularity against millimeter wave radios due to their expensive and cumbersome small cell deployment. [65]

With wired backhaul solutions, there are no interference or NLOS/LOS issues. In turn, the quality and coverage of the existing wired infrastructure need to be assessed. The most common wired technologies for access backhaul are DSL variants, DOCSIS (Data Over Cable Service Interface Specification) and fiber-based solutions. DSL and

DOCSIS are somewhat widely deployed. With the present DSL and DOCSIS technologies, which use copper in the access portion, the capacity is becoming a problem. Both can go only up to 50 – 100 Mbit/s with 1 kilometer distances which simply is not enough for LTE-Advanced access transport. Fiber-based solutions can offer the required capacity but likely do not to meet the general cost and availability requirements, though if a fiber infrastructure exists, it will be used for backhauling. Wired, fiber-based solutions are likely to grow in market share on macro cell and aggregation level connections while wireless connections are likely to grow on access level, systematically replacing copper-based solutions [72].

3.2.2 Resiliency, availability and topology choice

Resiliency and availability define the service continuation characteristics of a network system. Resiliency can be achieved with redundancy and proper control. Control can be in form of protection or restoration. Protected systems have already calculated back-up paths or routes which can be immediately activated in case of a link failure on an active link. Restoration in turn reacts to a link failure by finding another route after a convergence period. Protection is proactive while restoration is reactive. Availability on the other hand defines how big portion of a certain time span a service should be up and running. For core transport this number is typically five nines (99.999% availability), which allows merely a 5.26-minute downtime per year. With aggregation transport the number is usually four nines (99.99% availability) resulting in 52.56-minute downtime per year. For access tier and small cell portions these numbers are further relaxed, being 99% - 99.9% (87.6 hours – 8.76 hours). Availability in general is impacted by equipment failure, power outages etc. and in wireless systems further reduced by weather conditions, temporary blocks such as buses and trees, pole sway and vibration. Obviously the required availability figure largely defines if protection or restoration should be used. [65] The packet-based solutions for backhaul all offer a definitive set of resiliency mechanisms for core and aggregation transport which can achieve five nine availability. However, the access portion of the backhaul is generally unprotected due to the extensive amount redundant links needed between base station sites and aggregation. Also, even if cost factors permit, there can be other reasons why link redundancy is not implemented such as no feasible way to arrange connection to the nearest POP (Point-of-Presence), problems with laying cable and aesthetic reasons. If, however, there is redundant links available for a base station, some access backhaul protection mechanisms exist. On IP layer, redundancy can be managed with IP addressing by using connections between node loopbacks (similar to BGP loopback peer connections with TCP). The idea is that as long as there is an operational link between a base station and an aggregation device, the connection remains active. In addition, a routing protocol can be run on the base station nodes. Similarly, on the Ethernet layer, link aggregation protocols can be used. [51] Wired solutions for small cell backhaul probably can meet the availability requirements set for the service without additional redundancy. However, wireless backhaul solutions will likely need proper redundancy in order to offer the required availability defined by the industry. [65]

One way to enhance resiliency is to choose a redundant topology. As mentioned before, the typical deployment height for a small cell base station and a complementing backhaul transport point is 3 to 9 meters above street levels with installation platforms

being lamp posts, bridges, building walls etc. which likely prevents direct connections (in the likely scenario that there is no wired connectivity available) between the small cells and macrocell gateway resulting in need of relaying functionality among the small cells. Topology choices for wireless access backhaul networks are trees, rings or meshes. These different topologies can be assessed not only from resiliency point of view but from the ability to handle traffic fluctuations as well. According to a study on possible wireless backhaul topologies, which evaluates the solutions from redundancy and traffic handling capability point of views, meshed networks in general provide the best possible redundancy with smallest amount of links needed while still having the best performance in handling traffic demand fluctuations. Tree topologies need a redundant link on every single hop in order to offer some end-to-end redundancy. Moreover, if one of the primary links fails, it effectively halves the entire capacity of the tree backhaul due to the bottleneck in the single failed hop. Ring topologies do not need the additional links tree topologies need in order to provide basic redundancy. However, the capacity problem in case of link failures still haunt ring topologies in the same way as in tree topologies. If capacity need to preserved, some of the primary links in the ring topology need to be arranged into smaller rings. With large traffic demand fluctuations, the only solution in tree and ring topologies is to add larger capacity links. In turn, as the demand increase can happen anywhere in the network, all the links in the network would need an upgrade. It was discovered that after a certain traffic demand threshold it is not possible to find an optimal tree or ring topology. On the other hand, meshed solutions allow traffic to be load-balanced over the topology to mitigate congestion. Furthermore, the relative advantage only increases when traffic demand and fluctuation increase. [73] The potentiality of mesh topologies in backhaul has been recognized in other studies as well [74] [75] [76]. It is then quite evident that meshed topologies can help dramatically in availability and resiliency issues and in addition offers exceptional traffic handling capabilities.

3.2.3 Synchronization

In order for base stations to work properly and with acceptable Quality of Service, proper synchronization is needed. Frequency synchronization is crucial in the radio interface to ensure stability of the transmitted radio frequency carrier. Wandering frequency synchronization between adjacent cells would, for example, make the handover procedure more difficult. On top of proper frequency synchronization, some mobile communication systems require time or phase synchronization in order to control uplink and downlink transmissions in adjacent cells without interference. [65]

Legacy TDM systems (PDH and SDH) had synchronization properties built in to the physical transmission layers which the base stations could subsequently use for timing and frequency recovery. In PDH systems, the tributaries (PDH streams) originating or terminating at base stations all produce a nominal and standardized bit rate stream, however as this is not centrally controlled, the bit rates between two separate terminals may vary slightly (though the maximum error is defined and standardized). Thus, PDH networks are nearly, but not quite perfectly, synchronized. SDH systems on the other hand follow a tight hierarchy of clocks which in turn enables a precise synchronization over an SDH network. [51]

Along with the new packet era, transport networks employ more and more frequently Ethernet already in the physical layer, which in turn cannot be used for any sort of clock recovery as such due to the asynchronous nature of the technology. For packet-based backhaul systems, Timing-over-Packet methods are used. To provide synchronization, these methods exchange clock or other synchronization information on top of IP layer. PTP (Precision Time Protocol) is one of the most complete methods for telecom network synchronization and can offer very accurate synchronization. PTP offers hardware time stamping support, on-path bridging support, automatic clock hierarchy build-up (by using BMCA (Best Master Clock Algorithm)) and fast enough protocol packet rate. The mode of operation is straightforward, a group of network nodes (e.g. base stations) first elect one node to be the grandmaster (by using BMCA) and subsequently not elected nodes become slaves. The synchronization is achieved by exchanging PTP protocol messages (delay requests by slaves and delay responses by the grandmaster) sent to a special multicast address. PTP architecture can also include special boundary clocks that bridge received PTP messages between its client ports. With PTP, frequency and time (absolute time) synchronization can be achieved. Synchronous Ethernet is another method to obtain network wide synchronization. Synchronous Ethernet mode operation differs from PTP in some ways. [77] [51]

Synchronous Ethernet operates on the physical level as opposed to being purely packet-based. The synchronization is obtained by injecting special synchronous data framing on to the wire and with Synchronous Data Management Protocol [56]. Two Ethernet end points can recover a timing reference from the synchronous data stream and passing this onwards on a path. Synchronous Ethernet can only achieve frequency synchronization. [51]

On top of the above packet-based synchronization methods, GPS (Global Positioning System) can be used to gain system synchronization. GPS can offer both very accurate frequency and time synchronization but also poses some challenges, the main problem being loss of signal in indoor or heavily lossy environments. In addition, GPS may not be properly available in some parts of the world. [65]

The NGMN requirements report states that any of the above mechanisms can be used to gain system synchronization in small cell backhaul, the final decision being situation and solution dependent [65]. PTP and Synchronous Ethernet both provide accurate frequency synchronization while former only also delivers time reference. This aspect need to be taken into account when deciding on the access and duplexing methods for the small cell backhaul. GPS is another possibility for system synchronization, however due to its “external interference” characteristics, the packet-based solutions gain an advantage for small cell backhaul synchronization.

3.2.4 Quality of Service

The transport service provided by the mobile backhaul is an important part in delivering the end-to-end service experience for mobile clients. For example, real-time traffic flows must get a fitting service throughout the transport chain in order to fulfill the strict timing and delay requirements that, for example, voice and video traffic have. Mobile clients should have the same experience whether accessing over small cells or over macrocells. Thus, it is crucial for the backhaul to support and provide a basic Quality of Service scheme for the radio access network. The radio access network (base stations)

provides Quality of Service features for all mobile clients inside the coverage area on individual traffic flow level. The backhaul, however, provides Quality of Service for aggregate traffic flows and only with a handful of assignable traffic classes. Thus, the overall Quality of Service design for backhaul is not a trivial task. Overall, the Quality of Service mapping should be similar in radio access and backhaul with similar interpreting of the traffic classes throughout the backhaul. [51]

The performance of a backhaul system (i.e. Quality of Service) can refer to following aspects: data rate, packet delay, delay variation, packet loss, connection setup time, connection availability, connection drop rate, connection interruption times etc. The functionality of any Quality of Service more or less requires the following general functions: ingress processing, egress processing and information delivery. Information delivery means that the packets traversing through a network has information on them about the active Quality of Service scheme (e.g. header fields) and which the intermediary routers or switches act upon. Ingress processing includes marking and policing functions. Marking is the act of modifying the Quality of Service fields in incoming packets based on some predefined set of rules (for information delivery). Policing functionalities are responsible for regulating and controlling the incoming traffic, for example, by dropping traffic flows that are occupying more bandwidth than they are supposed to. Egress processing is responsible for realizing the traffic profile defined in the Quality of Service configuration. This is done by traffic shaping and scheduling. Traffic shaping is essentially temporary buffering of packets in excess data rate situations. Scheduling on the other hand schedules packets for transmission according their traffic class. The most common packet scheduler algorithms are Strict Priority Scheduler, Weighted Round Robin Scheduler and Weighted Fair Queuing. These three functions then contribute to the overall and unified Quality of Service scheme active on a network region (e.g. per-hop behavior and per-domain behavior). [51]

With the packet-based backhaul solutions presented in Section 3.1, Quality of Service can be implemented with various ways. On IP level, the most common Quality of Service scheme is DiffServ. DiffServ information is transported in the DSCP (DiffServ Code Point) of an IP packet. With MPLS applications, DiffServ mechanisms are also used, though the EXP (Experimental field) field on the MPLS shim header is used for the Quality of Service information. Thus a mapping procedure between IP DSCP and MPLS EXP is needed. On Ethernet layer, PCP (Priority Code Point) bits can be used for Quality of Service mapping or VLAN tags for more granular traffic class division. [51]

In small cell backhaul solutions, there are two different Quality of Service scenarios recognized. The first scenario is an offloading scheme, where best-effort traffic is offloaded to small cell base station in heavy traffic load situations. As the traffic is best-effort, no Quality of Service scheme is needed for user plane traffic. The second scenario is a fully operational heterogeneous network deployment for LTE-Advanced, thus needing a genuine Quality of Service scheme continuing the service of the macrocell. The small cell backhaul Quality of Service needs to support similar traffic class handling as the macrocell, grant proper prioritization of traffic classes, offer input for controllers about current situation of the access network and support congestion handling and mitigation techniques. [65]

3.2.5 Security

As with any communication technology, security is an important aspect of mobile network and backhaul design. In the context of mobile networks, security is implemented by dividing the network into security domains. A security domain is a network portion controlled by a single operator generally with a similar security levels throughout the domain. Between different security domains there can be transit security domains, forwarding traffic between security domains. Along with IP networking being increasingly used in all radio access technologies, 3GPP has defined the usage of IPsec (Internet Protocol Security) [78] [79] as mandatory between security domains and optional within security domains. IPsec can offer end-to-end confidentiality, integrity and authentication and can protect any protocol carried by it. On a general level, both base stations and core controllers have security gateways collocated with them and secure communication is performed through these gateways. Base stations and core controllers form a bidirectional IPsec tunnels between these gateways. [51]

IPsec is also the recommended security scheme for mobile backhaul, unless the backhaul is physically secure. However, along with the new packet-based backhaul solutions, IPsec protection alone may turn out to be insufficient. Some additional protection mechanisms alongside IPsec are traffic separation (e.g. VLAN tag separation, MPLS tunnel separation) and non-cryptographic protection (e.g. smart algorithms studying incoming traffic for "suspicious" patterns). [51]

With small cell backhauls, it is generally recognized that due to the outdoor and easy-to-tamper locations the small cell backhaul is considered to be more exposed to attacks. The security with small cells can be divided into physical/equipment security as well as network security. Physical security largely depends on the integration level with the corresponding small cell base station, an integrated base station with backhaul technology being the most secure solution. Complete decoupling of the backhaul and base station units contributes to deployment flexibility but potentially exposes the interface (e.g. cabling) between the units for attacks and tampering. On network level security, it is again suggested to use IPsec framework. [65] NGMN forum has also defined a general and extensive study solely on LTE and LTE-Advanced backhauling security [80].

3.3 Optimal solution for small cell backhaul

Summing up the main findings discussed in the previous section:

- Wired backhaul solutions can provide connections to small cell base stations with less interference than wireless solutions, however, the most widely deployed wired connections are DSL and DOCSIS which does not have the capacity required by LTE-Advanced. Fiber offers high capacity transport medium and is deployed if the infrastructure is available or feasible to extend. Wireless solutions can offer flexibility in the deployment but may suffer from system and external weather interference. 80 GHz band solutions offer the most tempting choice for wireless small cell backhaul links due to the light licensing scheme and high capacity potential with directional antennas.
- Resiliency in the present access backhaul links are non-existent due to the massive number of backhaul links to be protected. Small cell backhaul links

are deployed in potentially quite varying environments (i.e. city centers) thus some level of protection is needed. One way to add resiliency is to use a proper topology. Mesh topologies offer superior traffic handling and protection performance over tree and ring topologies.

- All base stations need accurate frequency synchronization and some mobile technologies need accurate time synchronization in addition. As the built-in synchronization delivered by legacy TDM-based backhaul links are being replaced by packet-based backhaul solutions, a method for synchronization signaling is needed. PTP and Synchronous Ethernet both provide very accurate packet-based synchronization, PTP providing both time and frequency while Synchronous Ethernet provides only frequency synchronization.
- Small cell backhaul is part of the overall end-to-end mobile service offered for mobile clients, thus the access backhaul needs to support the end-to-end Quality of Service scheme active in the domain with similar mappings and interpreting of the traffic classes as in higher tier network elements.
- Small cell backhaul needs to support a secure communication between base stations and core controllers. This can be done with end-to-end solutions such as IPsec and enhanced with physical and non-cryptographic security.

According to the findings listed above, the best platform for a small cell backhaul seems to be a meshed wireless network with high capacity millimeter wave radios and directional antennas, ability to transport synchronization and having a comprehensive Quality of Service scheme including delay constraints, congestion control and traffic prioritization. Also, security features and deployment features that make it easy to install and remove elements should be included. In addition, as the backhaul is essentially "carrier grade", it needs basic OAM functions and support of 3GPP interfaces similar to macrocells.

Along with 3GPP LTE (i.e. Release 8), the vision of SON (Self-Organizing Networks) was specified for future radio access networks. The point of SON features is to make radio access planning, configuring, managing, optimizing and healing easier than it has traditionally been. 3GPP and NGMN forums have published numerous documents dealing with different aspects of SON [81] [82] [83]. SON can be divided into three main subareas: self-configuration, self-optimization and self-healing. Self-configuration includes features such as automatic connectivity establishment, neighbor discovery and automatic parameter setup. Self-optimization feature is essentially the ability to adjust existing parameters and radio access behavior according to traffic fluctuations. Self-healing features include dynamic capacity redirection and general mechanisms that aim to soften the impact of malfunctioning base stations. Even though 3GPP has defined these features the radio access network in mind, they need to be supported by the backhaul as well. The small cell backhaul solution needs to be as automated and flexible as the small cell base stations themselves in order for the transport service to be as transparent as possible.

3.4 Summary

The transport infrastructure between a radio access network and a core network is called the mobile backhaul. The basic function of mobile backhaul is to unite the mobile network with other external transport networks, connecting a vast number of base station sites to a small amount of centralized control sites, transporting transparently the mobile network originated traffic and system signaling with certain Quality of Service, resiliency, security etc. requirements. Due to vastly different equipment numbers, geographical issues and processing requirements between the mobile network base station sites and the core network controllers, it is evident that a hierarchical or tiered architecture is needed. The main tiers are the access, aggregation and core tiers.

Traditionally, mobile networks have been backhauled using circuit switched technologies, such as PDH and SDH. Circuit switched technologies provide a basic synchronous transport service with a fixed bandwidth and transport slotting. They are quite inflexible and cannot handle dynamic traffic fluctuations. However, along with the trend towards fully IP-based mobile networks, the backhaul is increasingly also packet-based. Packet-based solutions offer greater degree of capacity flexibility, low cost and high manageability features. The most common packet-based transport technologies for the backhaul are Carrier Ethernet solutions, plain IP transport and IP/MPLS solutions.

The heterogeneous network deployments, or more specifically small cells, introduced along LTE-Advanced offer the likely answer for future base station capacity shortage but also introduce potential challenges, the most evident of which being how to backhaul the small cell base stations. Every small cell base station needs to have a fast backhaul connection, thus the amount of backhaul units will grow exponentially. In addition, as the mounting places for small cells and subsequently backhaul units move closer to street levels, factors that have not traditionally affected telecommunications equipment will have larger impact. These include, among other things, temporary blocking due to, for example, tall vehicles and trees and increased pole sway (lamp posts vs. broadcast masts). Even so, the backhaul service needs to fulfill certain requirements on resiliency, synchronization, Quality of Service, security and SON.

4 Wireless mesh for small cell access backhaul

Among the most promising small cell access backhaul solutions is a meshed radio system with SON features. In case of a mesh, a proper protocol suite needs to be deployed along with it, handling basic routing and MAC scheduling along with the desired self-configuring, self-optimizing and self-healing features.

This chapter discusses the present state-of-the-art mesh protocols and introduces a wireless mesh concept for small cell backhaul developed jointly by NSN (Nokia Siemens Networks) and VTT (Technical Research Centre of Finland). Section 4.1 gives an overview on the structure of wireless mesh networks and discusses the present state-of-the-art mesh protocols and what are their main shortcomings as a potential small cell access backhaul protocol. Section 4.2 introduces more specifically the wireless mesh backhaul concept by NSN including routing and forwarding, network-wide scheduling, shared resources concept, Quality of Service, traffic load balancing and management schemes, system signaling and protocol frame structures. The concepts and specifications introduced in this chapter are the basis for the proof-of-concept system which is introduced in the next chapter.

4.1 Mesh protocols for backhaul

Typical reference architecture for a wireless mesh network is illustrated in Figure 10. This structure repeats basically in all wireless mesh solutions. The used topologies are quite often only partially meshed and consist of a set of mesh routers communicating which each other. The mesh routers have minimal mobility, if any, and form the backbone of wireless mesh networks. One of the mesh routers is usually a special sink node which acts as a centralized database or gateway towards external networks. Clients for the mesh nodes can be laptops, mobile phones and other wireless devices. Meshed networks are inherently reliable and offer good redundancy. Meshed networks also provide extensive self-configuration, self-optimization and self-healing features. The routers in wireless mesh networks can establish connections dynamically and maintain mesh connectivity among the network. In case of node or link break down, transported traffic can be rerouted via several potential back-up paths. Similarly, if traffic load is exceeding certain link capacities, mesh routers can dynamically balance the load within the network via the mesh connections. The wireless communication is usually implemented with either omnidirectional or directional antennas. [84]

Chapter 3 listed an exhaustive array of requirements that a potential meshed backhaul solution for small cells should include. However, the requirements obviously do not take a stand on how the different features should be implemented in practice. On a more technical level, the requirements turn into suitable choices between connectionless and connection-oriented networking mode, centralized and distributed control, reactive and proactive routing scheme, channel and medium access method and state of interference awareness among other things. In the context of the small cell requirements, some design choices are more desirable than others. For example, connection-oriented routing scheme with centralized control has better change to match strict Quality of Service

requirements or that proactive routing mechanisms have faster resiliency and protection features than reactive routing schemes.

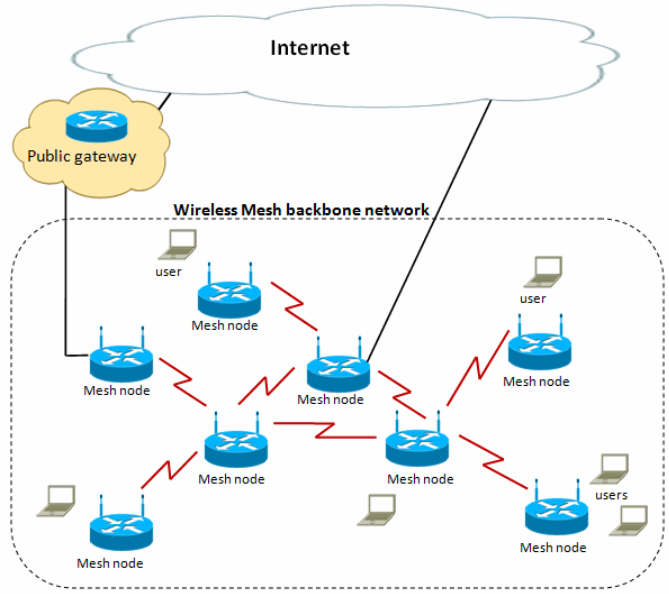

Figure 10: Reference architecture for a wireless mesh network. [85]

An extensive study was undertaken by VTT to analyze current state-of-the-art routing and MAC scheduling schemes for wireless mesh networks in order to find a potentially suitable protocol suite for wireless mesh backhaul solution [86]. Generally, there exists a lot of research on wireless mesh networks for different applications both proprietary and standardized. The framework used to identify potential solutions for a small cell backhaul included the general requirements presented in Chapter 3 in addition to design principles originating from NSN. The most popular standardized mesh technologies are the IEEE (Institute of Electrical and Electronics Engineers) 802.11s WLAN mesh, IEEE 802.15.5 WPAN mesh (Wireless Personal Area Network) and IEEE 802.16 WiMAX mesh (Worldwide Interoperability for Microwave Access) variants. They all offer quite complete mesh solutions for different scopes. The applicability for backhaul solution on the other hand is not in most cases optimal. For example, WPAN solutions have a variety of mobility management features and omnidirectional antenna control features which are unnecessary features in a static small cell deployment. WiMAX meshes provide some applicable features such as centrally controlled scheduling features but as a whole the standard is rather incomplete.

The main findings of the study [86] are that even though there is a lot of research material for wireless mesh networking, the analyzed solutions seem to only tackle one or only a few problem areas of mesh networking (e.g. protection, MAC scheduling, protection techniques, Quality of Service etc.) leaving the system level procedures omitted or vaguely defined or that the proposed solution is not directly applicable to fulfill the small cell backhaul specific requirements without extensive modifications. Also, the usage of directional antennas is possible in many of the proposed mesh solutions, however, only as static installments. This of course requires adjustments in potentially sev-

eral individual nodes if new links are added or old ones removed. The next section introduces a state-of-the-art wireless mesh solution for backhauling small cell base stations developed by NSN and VTT that aims to fulfill the small cell requirements and overcome pitfalls in the present wireless mesh network protocols.

4.2 State-of-the-art wireless mesh concept

The WMN (Wireless Mesh Network) backhaul solution is a novel concept solution targeted for next generations' small cell, ultra high capacity mobile base station first mile access backhaul. The system concepts and algorithms are also applicable for other meshed high capacity packet transport connections. Essentially the WMN system is a highly transparent network cloud offering connectivity between desired end points (e.g. a set of base stations and an aggregation transport network gateway) with advanced and smart self-optimization, self-healing and self-configuration capabilities offering traffic engineering and configuration features but requiring little or no maintenance or human intervention. Example deployment scenario is presented in Figure 11.

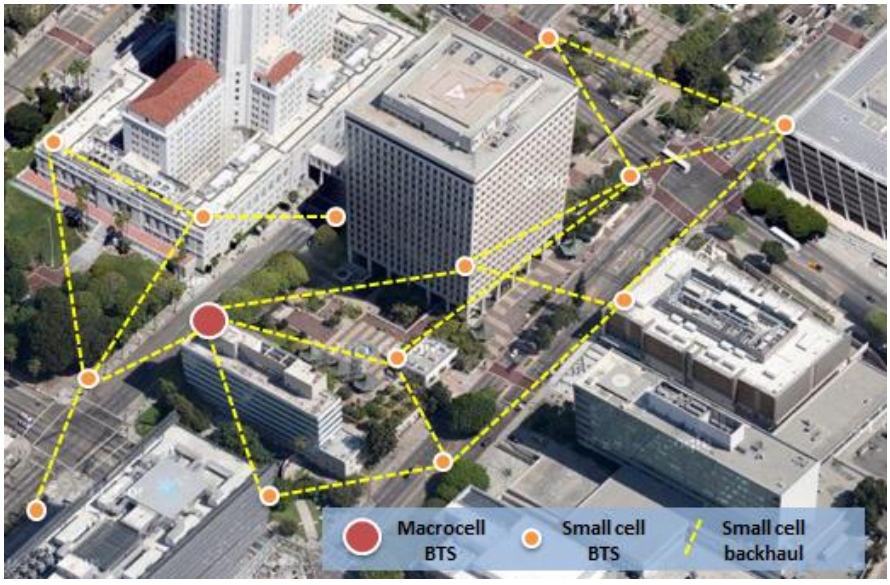

Figure 11: Example deployment for small cell backhaul. The small cell backhaul hop lengths vary from 200 to 300 meters.

The WMN system consists of a set of wireless mesh backhaul elements partially meshed with each other. The system is connected to external transport networks through special gateway elements, and all traffic coming in and out of the WMN cloud will traverse these gateways. The elements can be located essentially anywhere, offices, homes and base station sites, an example deployment being a mixture of these. The most probable deployment strategy however will likely end up being a co-location scheme with existing operator small cell base station sites. The WMN cloud offers a layer 2 transport service with WMN specific packet framing, allowing a wide range of format for incoming traffic. The backhaul elements are connected to each other mainly with directional pencil beam point-to-point millimeter wave radio links which can be

electronically steered to point to a number of different directions. However, other types of communications media can also be used such as fiber.

The wireless communication links in the WMN system are implemented by utilizing the concept of shared resources. In shared resources concept, a WMN node can communicate with only one neighbor at a time. The shared resource can be, for example, the wireless transceiver or antenna. Along with the usage of shared hardware resources and smart beam steering algorithms the equipment cost, flexibility and deployment problems of a typical meshed network can be largely avoided as the node can find new neighboring nodes without manual operative actions. The communication on the directional wireless links can be implemented with either FDD (Frequency Division Duplexing) or TDD (Time Division Duplexing) scheme. [87]

The WMN system is a centralized system in principle and the gateway mesh nodes are in an important role. The forwarding and MAC scheduling are based on pre-calculated information, and the needed calculations are entirely carried out in the gateway nodes. The resulting forwarding and schedule access tables and mappings are subsequently flooded to the rest of the WMN. The regular plain mesh nodes are then responsible for local decisions based on the current network state information received via WMN specific signaling. Local decisions are events such as regular forwarding, MAC schedule tracking, load management tasks and protection switching. [87]

Centralized and pre-calculated routing and scheduling information was chosen due to the fact that it was proven very hard [88] [89] to fulfill the small cell requirements described in Chapter 3, especially Quality of Service (delay, congestion handling, load management) with, for example, distributed reactive system. The shared resources system itself would be nearly impossible to make functional with distributed control. The next sections introduce the different aspects of the proposed concept more closely.

4.2.1 Networking, routing and forwarding

The routing and forwarding operations in the WMN system are based on centralized pre-computation of routing and forwarding information. More specifically, a central entity (i.e. a WMN gateway node) receives topology information on a planned small cell backhaul deployment including rough coordinates of the projected WMN node positions and the planned neighbor relationships between the WMN nodes. This information could be based on existing operator network base station deployments or be a completely new construction. After this information is given as input to the centralized entity, it then calculates a set of disjoint spanning trees for the target topology. An example for this operation is illustrated in Figure 12. Optionally, the calculation step can include traffic engineering parameters such as traffic estimates for certain set of links, link preferences, link capacity lists and path delay constraints. The calculation process ends in ordering the spanning trees into a precedence table for each node in the topology based on hop count and traffic engineering parameters. The spanning trees are always calculated separately for each gateway in a WMN topology and the number of spanning trees for a gateway depends on the number of links originating from the gateway. Furthermore, except for the root, other gateway nodes are not included in the spanning tree calculations. [88]

The actual routing is then based on the pre-calculated spanning tree priority list, resulting in a connection-oriented end-to-end communication through virtual circuits

formed by the underlying spanning tree infrastructure between every plain node and a gateway in the WMN system. Virtual circuits between non-gateway nodes are also supported. The routing strategy could be compared to ATM, where the end-to-end connections between plain nodes and gateway nodes following the calculated spanning trees resemble the virtual paths of an ATM system, while different classes of service between end points on the other hand resemble the virtual circuits of an ATM system. The mapping between incoming client data and a virtual connection can be based on basically anything, for example, VLANID and PCP on an 802.11Q header. The forwarding tables are formed locally by each node in the system based on the received spanning tree information. The forwarding table entries consist of spanning tree identification number, node identification number and an output interface.

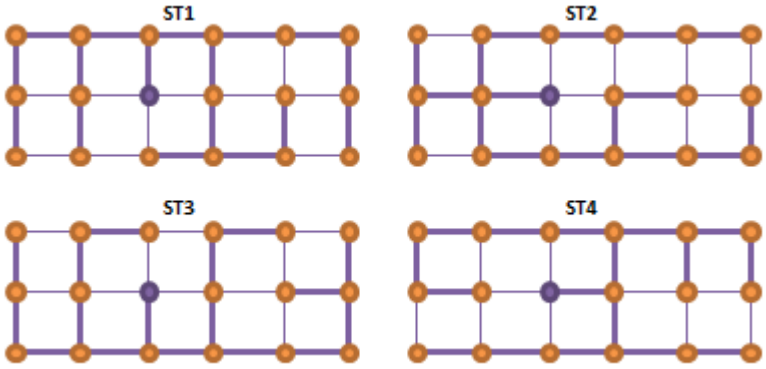

Figure 12: Example spanning tree (ST) calculation for a “chocolate bar” topology. The purple node is the gateway node.

4.2.2 Shared resources and scheduled transmission

WMN system employs a shared resources concept for wireless communication. This heavily affects the actual scheduling of data transmission in the system. This is solved by dividing a given topology into a collection of activity sets. Activity set in this context means activating (or coloring) the links in the topology in such a way that only one link per node is active (or colored) at a time. These activity sets then form the basis for shared resources communication by steering the communication direction towards other nodes according to a given activity set on all of the nodes in the topology. The idea is illustrated in Figure 13.

The calculation process first aims to find (almost) all maximal activity sets over a given topology. A maximal activity set is a matching of the above rules which cannot be enlarged further, i.e. adding more active links without breaking the searching rules. After the maximal activity set search is done, a genetic algorithm [90] [91] [92] is utilized to find a smaller collection of maximal activity sets from the search results in such a way that end-to-end delay between certain heavily used paths on a topology is optimized (input from the above route calculation needed). The result of the genetic algorithm is a small set of highly delay-optimized activity sets that are repeated cyclically. On a single node, these activity sets show as transmission slots assigned for different interfaces. Data flows through the WMN system according to these scheduled transmis-

sion slots, along the paths defined in the routing configuration. Typical values for transmission slots range from 100 to 500 microseconds. [88]

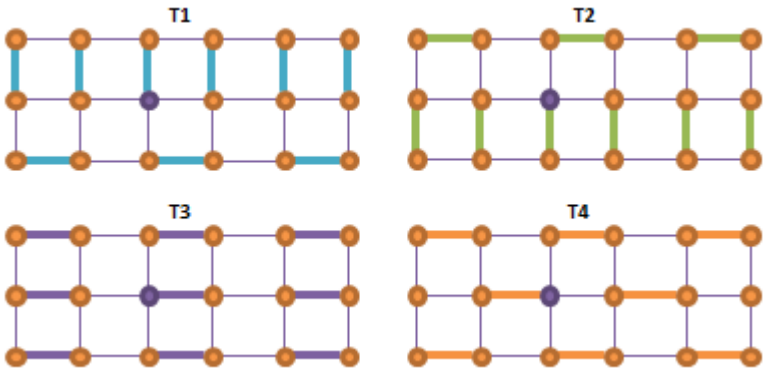

Figure 13: Example activity set (T) calculation for a “chocolate bar” topology. The purple node is the gateway node. The colored links represent the direction of the shared resources system at a given time.

4.2.3 Resiliency

Resiliency in the WMN system is based on the large amount of redundancy provided by the meshed network and pre-computed set of possible paths between two end points in a WMN topology. Fault detection is largely event-based meaning that as fault is detected (e.g. loss of light in fiber, weak received signal strength on a microwave link) the switchover to redundant paths is immediately initiated. Fault detection is extremely fast as the transport service works on layer 2 and there is no need to propagate the alarm upwards in a heavy protocol stack. Link quality is checked on a per-packet basis resulting in a nearly hitless protection scheme, a packet or two may be lost in the worst case. Furthermore, there is no need for any routing information convergence and recalculation due to the fact that all nodes already have a set of prioritized paths towards the gateway nodes. Thus, a path reselection consists of a simple search for the next intact path towards a destination. A fault always triggers a link state update that is broadcasted via the affected tree or trees. This way all the nodes will know which of the available spanning trees are affected and should not be used in subsequent packet forwarding. The routing in the WMN is done in an end-to-end fashion, thus transient packet loss may occur due to the link state update propagation delay. This is battled by introducing a fast local tree switching, which means that transient packets are rerouted along the local virtual connections towards a desired destination according to the forwarding tables in the point of failure nodes. This on the other hand may introduce packet reordering in the destination node as packets may come momentarily from several different directions towards a destination (i.e. the old route, the locally switched route and the new route), thus a re-sequencing buffer is needed in all the nodes. [93]

4.2.4 Quality of Service

The WMN system offers a basic Quality of Service scheme, offering different level high and low priority classes of service. Up to 9 different priority classes with different scheduling schemes are defined: five high priority classes and four low priority classes. The internal signaling and messaging of the WMN system is mapped to the highest priority class which is scheduled by using Strict Priority Queuing. The highest external traffic class is also scheduled using Strict Priority Queuing. Strict Priority Queuing can offer delay bounds over the system and is optimal for carrying for example real time traffic or some other low delay requiring traffic type. The rest of the traffic classes are scheduled using WFQ-scheduler (Weighted Fair Queuing) [WFQ]. Naturally the strict priority classes are scheduled first and the remaining link capacity is scheduled according to WFQ. Finally, the dynamics of the Quality of Service scheme can be adjusted as is seen fit. [93]

4.2.5 Load management

Load management of the WMN system includes a set of pre-emptive mechanisms to optimize different traffic flows and loads present in the network at a given time so that available network capacity is utilized as well as possible. The main mechanisms are congestion control and avoidance, capacity handling and link quality monitoring. All these mechanisms work on per priority and per flow basis, giving more attention to higher priority traffic classes. Congestion control detects congested links and reroutes traffic flows (lower priorities first) to lessen the traffic burden on a particular link. There is always the possibility that the congestion just moves to another point in the network. This is avoided with active capacity handling. Link specific available capacities on a certain path is monitored and reported by all the nodes in the network. This way, if a target path does not have enough capacity on the way to a destination, data is further rerouted. Also, as the majority of links in the WMN system will be wireless, the link quality is bound to change according to weather and other interfering effects. This capacity fluctuation is therefore taken into account as well. The result is that even in a highly degraded network state, high priority traffic still can be transported while low priority traffic gets poorer service or could be even dropped entirely. [93]

4.2.6 Synchronization

Rather accurate synchronization is needed for the WMN system to work optimally due to the network-wide link scheduling and possible TDD scheme. The system employs a specific Timing-over-Packet synchronization technique combining PTP mechanisms and WMN-only specific mechanisms. The synchronization is delivered in a WMN system via a synchronization tree. One of the gateway nodes act as a grandmaster clock and is the root of the tree. The plain nodes act as PTP boundary clocks offering bridged synchronization transport deeper to the tree. The gateway neighbor nodes act as slaves for the grandmaster and in turn the next tier in the tree act as slaves for the first tier thus causing the synchronization information propagate down the tree. The grandmaster clock can be chosen, for example, with the best master clock algorithm that is available in the PTP. [94]

4.2.7 Frame structure and signaling

The general frame structure used in the WMN system data encapsulation is illustrated in Figure 14. Every packet traversing the WMN system, be it control or data, is tagged with the same general header format. The header length is 32 bits consists of eight different fields. The first field (STID, Spanning Tree Identifier, 8 bits) tells which spanning tree is to be used, the second field (GNID, WMN Node Identifier, 8 bits) tells the destination this particular packet is to be forwarded. The flags in the next field are used in packet re-sequencing and fast local tree switching. The PRIO (Priority, 4 bits) tells the priority of the packet and finally the VCID (Virtual Connection Identifier, 8 bits) tells the virtual connection between two end points. Moreover, due to the radio communication, the WMN header is further divided into fixed sized portions and encapsulated into radio specific framing for transmission over a radio link. [93]

Figure 14: The general structure of the WMN header. Radio layer headers are omitted here.

System signaling consists of failure, congestion and capacity reporting according to which all the nodes form a mapping of the current state of the network. The signaling messages are collectively called link state updates. The signaling is always spanning tree specific. Events that need to be signaled to other nodes are always forwarded along the spanning trees that are affected by the triggering event. As mentioned earlier, the signaling packets are mapped to highest priority class thus getting precedence over all the other classes of service. The control data type and information is specified in the payload portion of the WMN packet while the header remains the same as in Figure 14. [93]

4.3 Summary

Among the most promising small cell access backhaul solutions is a meshed radio system with SON features. As the backhaul in this case is essentially a separate network, relaying traffic between base stations and a gateway, suitable routing and scheduling mechanisms are needed for proper traffic transport. In general, there is plenty of material available on different aspects of wireless mesh networking, the most prominent being the IEEE mesh standards. However, the existing mesh solutions seem to tackle only a few problem areas of mesh networking leaving the system level procedures omitted or vaguely defined or that the proposed solution is not directly applicable without extensive modifications.

The WMN backhaul solution developed by NSN and VTT is a novel concept solution targeted for next generations' small cell, ultra high capacity mobile base station first mile access backhaul. The concept employs innovative technologies and mecha-

nisms in terms of routing and MAC scheduling in addition to offering an extensive SON portfolio and high capacity wireless communication. More specifically, the basic connectivity between base stations and a gateway is implemented with virtual connections that are established based on pre-calculated base station topology information. Furthermore, the data transmission is scheduled with a steerable shared resource principle, resulting in a dynamic and flexible networking scheme. The mesh itself provides built-in redundancy and enables the usage of smart load management methods. Finally, the WMN system also implements a packet-based synchronization distribution mechanism and offers encapsulation service for various types of incoming traffic.

5 Wireless mesh demonstrator system

Chapter 4 introduced the WMN system concept developed by NSN and VTT. This chapter introduces the proof-of-concept system that was built to demonstrate and test out the feasibility and functionality of the developed concept. The proof-of-concept demonstrator system and test environment presented in this chapter was assembled as part of the main scope of this master's thesis.

Section 5.1 introduces the main demonstrator elements, including the used network processor platform, Lanner MR-730, wireless mesh prototype protocol software and an 80 GHz millimeter wave radio system prototype BRAWE (Broadband multi-antenna radios for millimeter wave frequency bands). Test topology with spanning tree and schedule calculations required by the concept are also introduced. In addition, all used testing software and hardware are introduced. Section 5.2 presents background and methodology information for all the test phases developed for verifying the different functionalities and performance of the demonstrator software. The testing is divided into different phases that cover a certain aspect of the protocol such as basic routing and scheduling, resiliency etc.

5.1 Demonstrator elements

As is mentioned in Chapter 1, the earlier phases of the NSN and VTT wireless mesh backhaul research project have resulted in specifications of completely new routing, link scheduling, resiliency and other system design algorithms. The functionality and feasibility of the whole concept system required practical prototype testing, thus a demonstrator environment was set up in the NSN Mobile Backhaul laboratory.

The demonstrator system was originally planned to be able to work with gigabit speeds, thus in order for the system to function and process packet data fast enough, certain aspects needed to be assessed. A simple simulation environment and simulator development would not have been feasible. For example, the present network simulator tools such as NS (Network Simulator) and OPNET simulators, as can be expected, only include the most common standardized and used networking elements to date in the fields of traffic modeling, protocols, routing and queuing processes and physical media. Adding new networking protocols and elements can be highly laborious, for example, NS employs two language planes in which users can work in, a control plane implemented in Object TCL (Tool Command Language) and a data plane (simulated packet processing) in C++. This means that developers must work and debug in two separate planes resulting in potentially large challenges and convoluted dependencies. Also, some of the network simulation tools are closed and proprietary thus making own additions to the tool set simply is not possible. One could also use general purpose languages such as C or C++ to create a simulation environment from scratch, but this would require, on top of the actual new protocol set, a complex event handling structures, time management, link modeling, traffic modeling etc. which would likely take the focus off the main objective, functionality and verification testing of the implemented prototype protocol software, and move it to the process of making a complex and working simulator. Thus simulation-based environment would not be optimal platform

for the developed WMN concept and in the end prototyping was chosen as the validation platform.

When selecting the prototype platform, commercial off-the-shelf networking devices such as Juniper or Cisco would offer the needed hardware accelerated processing capabilities but in the end could not be utilized due to the closed software environments. General-purpose processor-based (i.e. normal PC-based (Personal Computer) platform) development would offer a flexible and relatively easy way to create a partially meshed network of PCs implementing the prototype protocol software with the help of intermediary switches and hubs. Networking could be implemented through network socket programming APIs (Application Programming Interface), more particularly raw sockets, which gives the software developer access to as deep as link layer control and in this context unneeded transport and network layers could be skipped. However, the usage of socket programming APIs through an operating system (e.g. Linux or Windows) will eventually hamper the throughput and data rates of the system, and the gigabit mark could not be achieved. The last and selected alternative was to use network processor-based platforms. The introduction of network processor-based systems has combined the flexibility of a general-purpose processor without sacrificing any of the packet forwarding capabilities of for example an ASIC chip (Application Specific Integrated Circuit) manufactured specially for packet forwarding. In the end, the Lanner MR-730 network processor platform employing the Octeon network processor from Cavium Networks was chosen as the prototype platform.

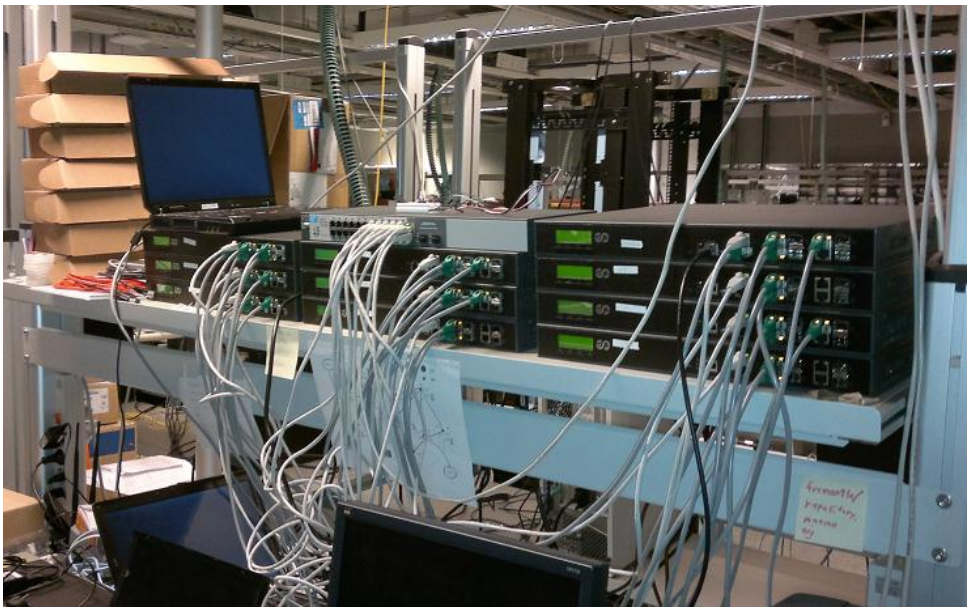

Figure 15: The wireless mesh network demonstrator in the NSN Mobile Backhaul Advanced laboratory. Ten Lanner MR-730 units forming the partial mesh and an Ethernet switch to deliver external synchronization.

The running wireless mesh demonstrator network is illustrated in Figure 15. The demonstrator environment consists of Lanner MR-730 network processor platform units running the experimental wireless mesh protocol software. The platform units are arranged in a partial mesh network via Ethernet connections. The Lanner MR-730 equip-

ment is used as the prototype hardware platform for the WMN backhaul node. In addition, the wireless connections between different WMN nodes are emulated as a set of Ethernet cable connections between the Lanner MR-730 platforms. In order to test and verify the idea of scheduled multi-direction transmission with a real wireless link, two hops in the test topology were implemented with BRAWE millimeter wave radio system that implements an experimental beam steering technology. The test topology is created with ten Lanner MR-730 units. The following sections give a more thorough overview on the different elements of the demonstrator and used test topology.

Even though a network processor-based platforms offer the required throughput and performance values, from the system design point of view, a few things are good to notice. The original design employs a millimeter wave radio with a beam steerable antenna as the wireless communication end point. Thus, by using Ethernet cabling between the mesh nodes, the communication is made slightly easier as data is always guaranteed to move between nodes. Also the communication channel is a lot "cleaner" while using proper guided medium (i.e. cabling) as opposed to the changing characteristics of a wireless multipath medium. Therefore, as pointed out above, one set of hops was implemented with a beam steerable radio system (BRAWE) to verify the operation with real wireless data path and shared resources.

The novel synchronization protocol to enable network-wide packet-based synchronization was not implemented on the prototype protocol software, thus synchronization based on IEEE 1588 PTP was delivered externally for the Lanner MR-730 units through the switch on top of the Lanner MR-730 units in Figure 15. Lastly, the incoming and outgoing client traffic in the demonstrator is solely in Ethernet format (more specifically in 802.1Q format) and all the routing and Quality of Service specific mappings are done based on the corresponding 802.1Q header fields (VLANID representing a certain destination mesh node and the PCP representing a certain Quality of Service class). Apart from these concepts, the demonstrator environment and software aims to be as close as possible to a potential pilot product solution, including the concepts of routing, scheduling, Quality of Service, advanced mechanisms, header format, signaling etc.

5.1.1 Lanner MR-730 network processor platform

The hardware platform for the wireless mesh demonstrator was chosen to be the MR-730 model from the Taiwanese Lanner Inc. [95]. Similar network processor platforms are offered by Portwell [96] and Caswell [97]. The platforms from all the manufacturers are quite similar, biggest differences are in the chosen network processor, set of available input media accesses and the amount of data interfaces. The MR-730 was chosen for its four-core Octeon CN5230 network processor.

The MR-730 platform offers four gigabit Ethernet ports with optical transceiver options. There are also two Fast Ethernet ports labeled as management access and a separate Ethernet interface for serial access. The gigabit ports are used to emulate the different wireless connections towards other WMN nodes when Ethernet cabling is used. The two management ports are used for system access and client communication emulating the potential incoming and outgoing evolved NodeB traffic. For storage the platform offers Serial ATA interfaces and a Compact Flash interface. For demonstrator purposes, a 4 gigabyte Compact Flash card that is partitioned into two separate planes is

used as the hard drive for the platform. The first partition includes a Linux image and the binary file for the data plane of the wireless mesh protocol. The other partition includes the file system for the Linux. The motherboard also employs a few GPIO (General Purpose Input/Output) pins for external communication which are needed in the BRAWE radio system integration.

The most important element on the platform is obviously the Octeon CN5230 network processor. Cavium Networks offer an extensive set of C-libraries to control the wide array of features that the chipset enables (such as hardware accelerated packet processing, Quality of Service features, TCP processing and encryption and decryption processing among other things). [98]

5.1.2 BRAWE millimeter wave radio system

BRAWE radio system is a combination of research efforts by VTT and Aalto University's Department of Micro and Nano-technology and Department of Radio Science and Engineering. Basic research on CMOS transistor technology (Complementary Metal Oxide Semiconductor), LTCC chip packaging technology (Low temperature co-fired ceramic) and lens antennae technology culminated in the creation of the BRAWE radio system incorporating all the individual research project elements into one working prototype. The research project was active during 2009 to 2011 and involved research on transmission technology on millimeter waves in short range indoor applications working on 60 GHz band and in outdoor long range applications working in the 80 GHz band. The latter prototype was employed in the demonstrator. The system integrated in the demonstrator consisted of two static transmitters without beam steering capabilities and one receiver unit that employed the experimental lens antenna and beam steering capabilities among other things. The integrated and functional system is illustrated in Figures 16 and 17.

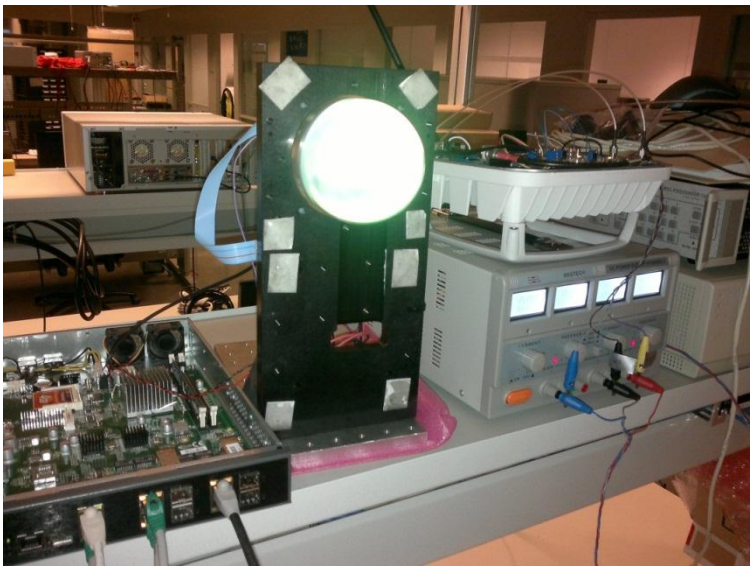

Figure 16: BRAWE receiver employing a lens antenna (in the middle) integrated to a NSN FlexiPacket Radio (right, on top of a regular power source) and to the Lanner MR-730 (left).

Figure 17: Two transmitter units (grey boxes on both sides of the power source) and NSN FlexiPacket Radios on far right and left side.

The original prototype only included the required radio frequency parts thus an external baseband signal processing element structure was needed in order to make the system applicable to genuine data communication. The baseband processing chip of the NSN FlexiPacket Radio (a packet radio solution by NSN for mobile backhaul transport) platform was chosen for the task. The FlexiPacket Radio is externally a simple wireless Ethernet hop employing a basic Ethernet input for data. Thus the data pipe integration only included plugging the Ethernet cable to one of the Lanner MR-730 platform's gigabit Ethernet interfaces. The FlexiPacket Radio baseband processing unit only accepts pure Ethernet traffic and as the protocol running in the demonstrator has its own header type, the data frames in the network needed a simple dummy Ethernet header amended in front of them in order for the data to go through the FlexiPacket Radio hop. The FlexiPacket Radio is an FDD system as opposed to a TDD system planned for the demonstrator system, but was still chosen as the baseband processor platform as suitable TDD radio solutions were not available.

5.1.3 Wireless mesh prototype protocol software

The development of the wireless mesh prototype protocol software started in the first quarter of the year 2011. The initial functionality included basic spanning tree routing mechanisms and scheduling principles. Since, the protocol has slowly grown in complexity. The structure of the software follows the basic principles of any routing software and hardware combination. There is a separate data plane that is running on one of the Octeon network processor cores and a control plane that is running on another core. The control plane is implemented in a daemon mode running on top of Debian Linux. Both the control and data plane are written in C which still offers the fastest performance among all computer programming languages. The software also includes extensive debugging possibilities which are used in the verification testing analysis. The structure of the protocol software is illustrated in Figure 18.

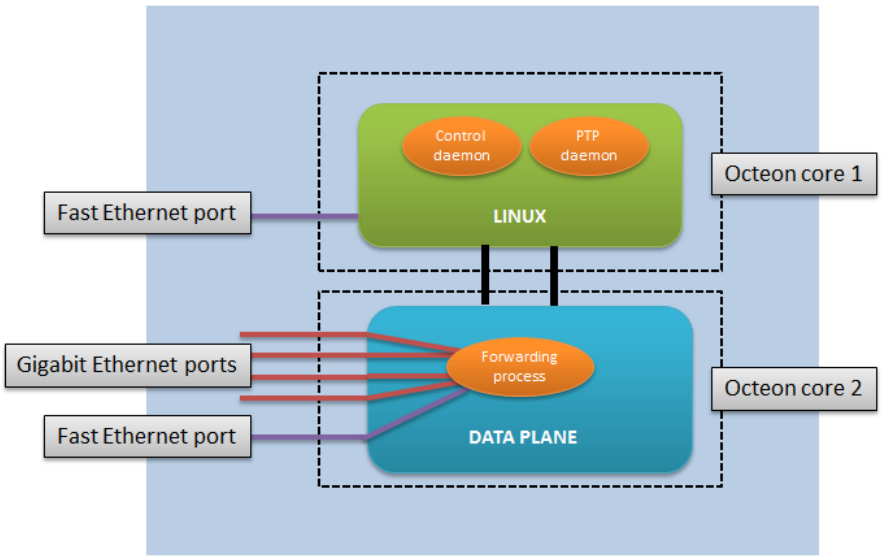

Figure 18: The structure of the prototype protocol software stack.

The data plane mainly forwards packets between the gigabit Ethernet ports of the Lanner platform which represent the mesh radio directions and one hundred megabit port which represents the UNI (User-to-Network Interface) port directed towards the client of the mesh node (i.e. the base station). It controls the selection of the antenna direction when radio link is used by setting the states of a particular GPIO to be readable by a microcontroller on the BRAWE radio platform and sends, through priority-based output packet buffering, and receives packets from one link (radio, Ethernet or combination) at a time according to given schedule. The packets are made available for the software as "works" by the Octeon packet processing hardware. The data plane also performs low level testing of the link states and reports changes to control plane among other things. It is quite important to keep the data plane functionality simple in order to achieve the needed throughput requirements.

The control plane consists of a Linux daemon handling the control tasks. At startup, it reads the general scheduling and route configuration parameters from configuration files and creates the routing table, path preferences and scheduling info to be used on the data plane. As mentioned earlier, synchronization between mesh nodes is handled externally. The Linux access ports and a desktop computer are connected to a LAN in which PTP messages are exchanged by PTP daemon software, which is an open source Linux project [99], running in the network hosts. A desktop computer is used as a master clock and the Lanner MR-730s are configured as slave clocks. The control plane subsequently sends PTP-corrected time information regularly to data plane for schedule synchronization. It also handles the control signaling with other mesh nodes. The communication between control planes of different mesh nodes is done via the link state update messages introduced in Chapter 4. The communication between control and data planes is done via shared bootmemory blocks or internal messaging, both provided by the Octeon system architecture.

The required configuration for the software is delivered at boot-up with two separate configuration files: stdata.cnf and wmn.cnf. When the platform is booted, the files

are parsed and read to a set of shared bootmemory blocks which can be accessed by both forwarding and control plane binaries. Stdata.cnf configuration file includes all the spanning tree information required to calculate the priority paths towards different nodes in the network. The file also includes a list of spanning tree priorities which are used to determine which spanning tree should be used as a primary, secondary, tertiary etc. path towards a certain destination as well as information about neighbor mesh nodes. Wmn.cnf configuration file includes information about virtual connection mappings, priority queue scheduling, schedule timing, guard timing and maximum interface specific data rates.

5.1.4 Test topology

The test topology represented an important part of the demonstrator system. To have some practical touch to the demonstrator, the topology was chosen from a real-life small cell scenario example deployed over an urban city center. The links and neighbor relationships were copied from the example scenario and used as a reference for the test topology. In addition, the testing of the concept needed a multi-hop scenario in order to properly test the features of the protocol. A network of ten prototype mesh nodes was chosen. The test topology is illustrated in Figure 19. Nodes 1 and 8 were chosen as the gateways for the topology.

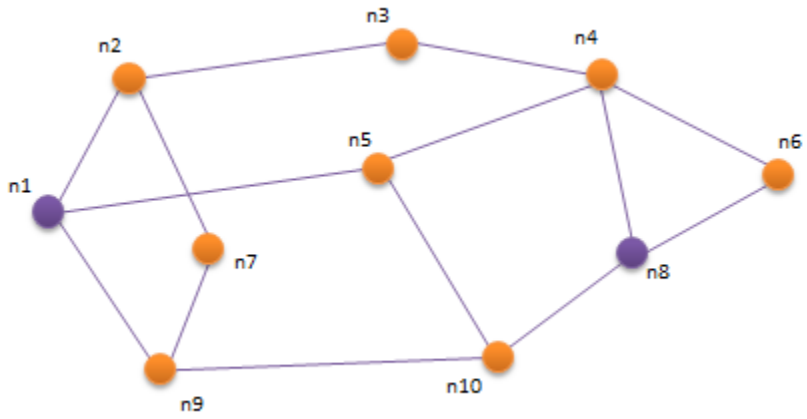

Figure 19: The ten node test topology. Purple nodes are gateways.

As was introduced in Chapter 4 the concept of shared resources needs a network-wide scheduling scheme. The schedule was calculated for the test topology with the scheduling algorithm introduced in Chapter 4. In addition, the spanning tree information and path priorities were calculated with the spanning tree routing algorithm, also introduced in Chapter 4. The schedule and the spanning tree information for the test network are illustrated in Figures 20 and 21.

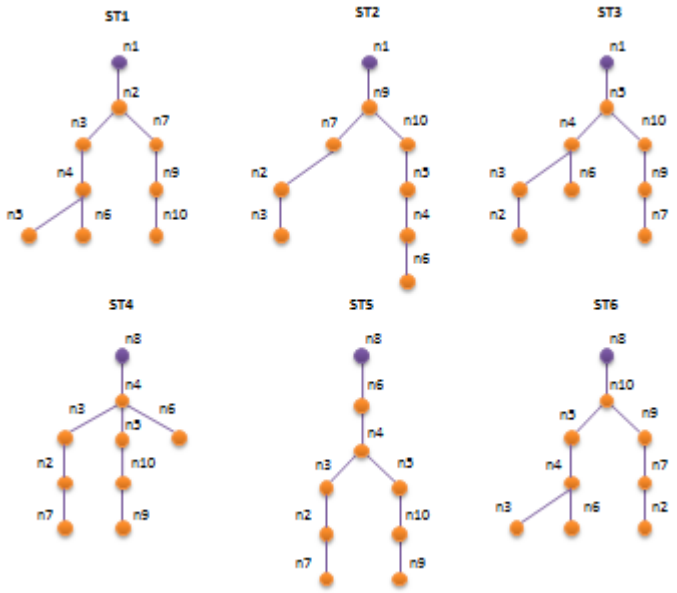

Figure 20: Calculated spanning trees for the test topology.

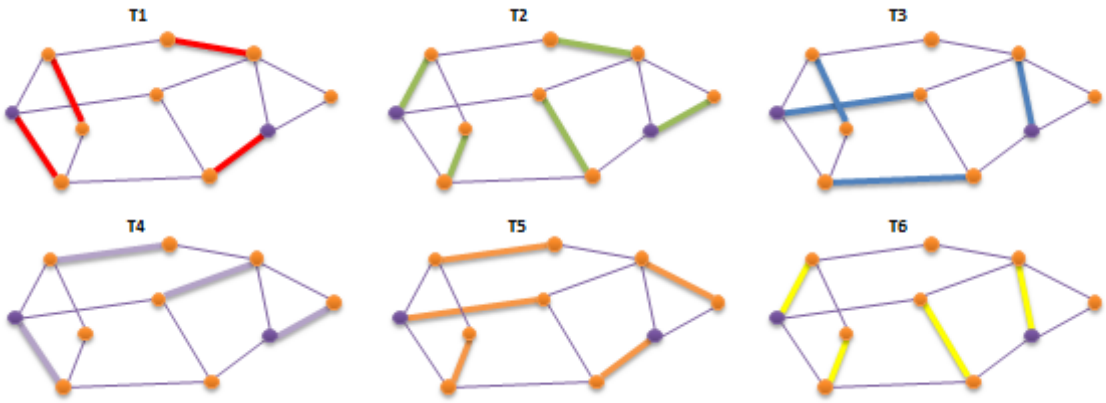

Figure 21: Calculated schedule for the test topology.

5.1.5 Test equipment

In order to inject traffic to the demonstrator system, three main elements were used: regular PCs running Linux for lighter traffic handling and injection, a Spirent TestCenter network traffic generator [100] for heavier traffic handling and Wireshark network protocol analyzer for data capture [101]. These elements were then attached to the client port of the Lanner MR-730 platform which in turn encapsulates incoming traffic. Linux itself includes a wide array of handy tools for managing outgoing network traffic and it is also quite straightforward to create own light network traffic generators with C. In order to create the right kind of Ethernet traffic in Linux, one needs to use the

vconfig [102] and ifconfig [103] utilities to modify VLANIDs and IP address configuration. This is basically everything that is needed to inject traffic to the demonstrator.

The Spirent TestCenter platform provides a selection of measurement solution for basically any kind of network. The feature palette spans from traditional performance testing to the rigorous analysis of virtualization, cloud computing, mobile backhaul, and high speed Ethernet. The traffic to be generated can be modified quite freely and the platform supports an enormous amount of different data frame types and test scenarios. The equipment can be easily attached to two different Lanner MR-730 platform client ports (source and destination pair) to form a loop which enables measurements for extremely accurate latency times and packet errors among other things.

Wireshark is a powerful network protocol analyzer available on all major operating system platforms. It is extremely useful for network troubleshooting, analysis, education and software and communications protocol development. Obviously, the protocol used here cannot be found on the supported protocol list thus the prototype protocol software analysis is largely based on the hex view provided by the Wireshark. The program supports custom dissector creation but this has not yet been implemented for the mesh protocol.

Lastly, a simple software traffic generator for Linux was created (written in C) that offers more flexibility and options in 802.1Q frame creation (e.g. sequence numbers in the payload) and also permits the creation of basically any kind of header (Ethernet or mesh protocol specific) for a specific testing purpose.

5.2 Test phases

The system under test is quite different from a regular system of network interconnect devices and does not implement any standardized protocol or a set of protocols. Thus the verification tests for the wireless mesh demonstrator were created from scratch and just for this particular system. The original test and specification documents that were created in conjunction with this master thesis are quite extensive and broad, defining several test cases per a certain functionality set. The following sections present an overview on the different functionalities of the prototype protocol, divided into separate testing phases. Each phase elaborates on the objective, background and methodology of the testing process. A basic verification test for each of the respective functionalities is described and additional testing principles are explained.

In most cases networking equipment can be tested with standardized and extensive testing procedures for different purposes, such as the “Benchmarking Methodology for Network Interconnect Devices” defined in RFC 2544 [104] (Request For Comments) and “Benchmarking Methodology for Firewall Performance” defined in RFC 3511 [105]. These sorts of documents discuss and define a number of tests that may be used to describe the performance characteristics of a certain network element. In addition to defining the tests, the documents also describe specific formats for reporting the results of the tests. They give insight and good reference platform and templates on how tests can and should be designed for network interconnect devices, but unfortunately cannot be directly applied in this case as explained earlier.

5.2.1 Test phase 1: basic routing and scheduling

Objective and background

The purpose of this test phase is to verify the functionalities of the novel spanning tree routing technique and the network-wide scheduling mechanism. As mentioned in Chapter 4, the routing in the wireless mesh network is based on a set of pre-calculated spanning trees. On top of this spanning tree structure virtual connections between the source and destination nodes are created and prioritized based on the VLANID information of the injected Ethernet data frames in the source node.

Methodology for the spanning tree-based routing

The spanning tree-based routing is one of the fundamental features of the WMN system concept, in addition to the scheduling principle. Thus it is important to test it quite thoroughly. The basic verification test is to simply send traffic with different VLANIDs across the network. The traffic should flow between different nodes in the network according to the predefined VLANID mappings and packets with undefined VLANIDs should be rejected. Furthermore, as the routing is the first feature to use the WMN specific encapsulation, it is important to verify the correct construction of the WMN header with different spanning tree and destination node combinations. The routing scheme should be tested with several traffic streams simultaneously sent to all possible destinations to verify that the forwarding operation can handle a natural network situation where traffic is forwarded between multiple base stations. Finally, the traffic type should range from raw test traffic to demanding real time traffic such as video. These testing principles should verify the correct operations of the routing scheme.

Methodology for the network-wide schedule

The basic verification testing for the scheduling principle is to send traffic between two nodes and capture the traffic on the receiving side and then observing the timing of the received packets. The timestamps should match the transmission slot timing configured for schedule cycle. Moreover, the scheduling principle need to be tested with different time scales and varying transmission slot timing within a single cycle. Also, the accuracy and wander of the timestamping carried out by the protocol software need to be clarified in order to discover the shortest possible transmission slot times achievable in the demonstrator system. The test traffic should be slow enough that the amount of samples remains reasonable low (i.e. received packets with timestamps). These testing principles should verify the correct operations of the scheduling scheme.

5.2.2 Test phase 2: integration of the BRAWE radio system

Objective, background and methodology

The purpose of this testing phase is to verify the beam steering functionality of BRAWE radio system integrated to the wireless mesh demonstrator system and test the concept of shared resources in general. The beam steering logic is controlled by the prototype protocol software implementing the network-wide scheduling procedure. As the sched-

ule is in the millisecond timescales, accurate synchronization is crucial. In the system perspective, the BRAWE radio hop is simply a bit pipe, thus the testing procedure can be very similar to what was introduced in the routing testing scenario above. If the synchronization and scheduled transmission works as specified, data should flow through the wireless hop without errors. The integration test phase also includes the link break information and steering control delivery installation to and from the Lanner MR-730 platform. The BRAWE wireless hop will be set up in the triangular area formed by nodes 2, 7 and 9 (see Figure 19). The receiver (see Figure 16) will be installed on node seven while nodes 2 and 9 will be having the BRAWE transmitter units (see Figure 17).

5.2.3 Test phase 3: resiliency

Objective and background

The purpose of this testing phase is to verify the automatic link break protection mechanisms in the prototype protocol software. Both Ethernet and BRAWE radio system link breaks are verified. As link break is detected, traffic on the broken link is routed through the best alternative path defined by the mesh routing algorithm. As link state changes back to operational again, reversion back to the last available routing path will take place. In addition to link break detection on certain links, the prototype protocol software also informs other nodes in the demonstrator system about the particular link break in form of LSUs (Link State Update). The Ethernet link break detection is based on functions offered by the Cavium Octeon development library and radio link failure is based on received signal strength measurements. On top of this a simple Hello-message-based link fault detection scheme similar to OSPF and BGP timeout event triggers was also implemented in the demonstrator system. The resiliency portfolio also includes a fast local tree switching mechanism. The fast local tree switching is a sort of fast rerouting mechanisms for transient data frames near newly broken links.

Methodology for the Ethernet link break

The basic verification testing for the link break detection in case of wired Ethernet is to unplug an Ethernet cable between two nodes and observe how the protocol software behaves. To test the Hello-message-based link break detection, the functions checking the Ethernet interface states need to be disabled, so that link break detection is solely based on the Hello messages. If the protection mechanisms work properly a reselection of path between the chosen source and destination pair should take place. With Ethernet cables, the actual hardware detection that the cable is unplugged on Lanner MR-730 platform takes up to a few hundred milliseconds so packet loss in this case is inevitable. When the cable is re-plugged, a reversion to the original routing path should take place. Further testing includes correct behavior verification with several traffic streams forwarded across the network and with several link breaks. The traffic type should range from raw test traffic to demanding real time traffic such as video. In addition, the correct link state message signaling and node specific forwarding table updates throughout the network need to be verified. These testing principles should verify the correct operations of the Ethernet-based link break detection and handling.

Methodology for the BRAWE radio system link break

The basic verification testing for the link break detection with the BRAWE radio system simply includes the blocking of the BRAWE transmitters and receiver alternatively with a physical object and observing the behavior of the protocol software. The protection mechanism should behave exactly the same as in Ethernet case, the detection mechanisms being only slightly different. With BRAWE radio system link break detection, path reselection should be nearly errorless (a frame or two might be lost). As the obstacle in the radio path is removed, the data stream should be changed to its original routing path. The detection as the receiver is blocked should be simple enough; both transmission directions should be interpreted as being broken. On the other hand, the individual blocking of one of the transmitters might expose some obscurities in the behavior of the protocol software. Furthermore, the testing needs to include iteration on different transmission slot timing to verify the shortest possible times that the integrated BRAWE radio system and the WMN system can operate correctly with. The test traffic streams should be the same as in wired Ethernet case to compare the differences. These testing principles should verify the correct operations of the BRAWE radio system-based link break detection and handling.

Methodology for the fast local tree switching mechanism

The basic verification testing for the fast local tree switching feature is to compare the performance differences in terms of packet loss between protocol software with and without the fast local tree switching mechanism. Without the fast local tree switching mechanism, transient data frames on nodes with link breaks are simply dropped, thus a decrease in packet loss should be visible as the feature is turned on. Further testing includes the verification of the feature more closely on a packet level and with several link breaks. Finally, the re-sequencing functionality needs to be verified with a traffic stream consisting of sequenced packets. These testing principles should verify the correct operations of the fast local tree switching mechanism.

5.2.4 Test phase 4: Quality of Service

Objective and background

The purpose of this test phase is to verify the Quality of Service scheme of the prototype protocol software. The Quality of Service includes verification of proper mapping of traffic class information, congestion control mechanism and load management functionalities. The Quality of Service mapping is done in the ingress of the demonstrator system according to the PCP field in the Ethernet header of incoming packets. The mapping of the traffic classes is done as specified in Chapter 4. The congestion control is based on priority specific buffer length measurements. The buffer length measurement process identifies certain thresholds after which a certain link and priority combination is regarded as slightly, highly or fully congested. The routing process then adapts to this congestion situation by reconfiguring existing traffic and again favoring higher priority traffic over lower priority traffic. The protocol software also keeps track of available capacity on all the outgoing links and calculates incoming data rate from the client port on per priority basis. If a certain traffic flow is higher than the available ca-

pacity on a certain link, this particular traffic flow is then rerouted via some other path that has the required capacity.

Methodology for the Quality of Service mapping

The Quality of Service mapping functionality is tested by injecting test traffic to the WMN system with different Ethernet PCP values and capturing the test traffic after is has been encapsulated with the WMN format. The WMN header should be updated according to incoming PCP tagged Ethernet frames following the mapping rules provided in the initial configuration files. Further testing includes the correct verification also in the egress of the WMN network and with different configured mapping values. These testing principles should verify the correct operations of the Quality of Service mapping functionality.

Methodology for congestion control mechanism

The congestion control mechanism is tested with a gradually ramped up traffic stream sent between two nodes. If the congestion control mechanism works properly, the preconfigured thresholds should trigger as the interface and link specific traffic loads in question approach their maximum capacities. Further testing includes the iteration of suitable buffer sizes and threshold levels. In addition, the signaling of the congestion control information across the network needs to be verified. These testing principles should verify the correct operations of the congestion control mechanism.

Methodology for traffic and load management

The traffic and load management methods are the primary Quality of Service enforcing features of the WMN system. The basic verification testing includes a high and a low priority traffic flows which are sent between two nodes, using the same path. When the higher priority traffic is injected on the same link that the lower priority traffic is following, it should take a higher preference. When the link capacity is adjusted to a suitable value, the link should get congested and the lower priority traffic should be rerouted via another route to the chosen destination or alternatively dropped if there are no more back-up paths available. Further testing includes several traffic flows with varying priorities forwarded across the network under different link break and congestion situations. These testing principles should verify the correct operations of the traffic and load management mechanisms.

5.2.5 Test phase 5: preliminary performance testing

Objective, background and methodology

The purpose of this test phase is to try out the performance figures of the software-based protocol suite. The demonstrator system is designed to be a gigabit system overall. Link specific throughput values will be lower than the total system capacity due to the shared resources concept. The performance of the software will be tested by injecting three different traffic flows to the client port of node 1 (see Figure 19) and receiving the traffic flows from the neighbor node client ports (nodes 2, 5, 9, see Figure 19). Short term

throughput will be interpolated and the discovered values will be used on an overnight test run to test the stability of the software at maximum data rates. Packet loss and latency will be examined.

5.3 Summary

Due to the advanced nature and novelty of the WMN system concept, the functionality and feasibility of the whole concept system required practical prototype testing. The proof-of-concept system was designed to offer gigabit speeds, thus it was deemed necessary to utilize network processor-based platforms, which combine the flexibility of a general-purpose processor without sacrificing any of the packet forwarding capabilities of, for example, an ASIC chip manufactured specially for packet forwarding. In the end, the Lanner MR-730 network processor platform employing the Octeon network processor from Cavium Networks was chosen as the prototype platform.

The proof-of-concept system consists of Lanner MR-730 network processor platform units running the experimental wireless mesh protocol software, implementing the WMN system concept functionalities. In addition, the wireless connections between different WMN nodes were emulated as a set of Ethernet cable connections between the Lanner MR-730 platforms. In order to test and verify the idea of scheduled multi-direction transmission with a real wireless link, two hops in the test topology were implemented with BRAWE millimeter wave radio system that implements an experimental beam steering technology.

The general principles for test design and specification for the different functionalities of the WMN system concept were to verify the correct operation of the mechanisms under likely traffic and network situations. This way, for example, the basic routing testing included testing with a varying traffic profile, spanning from best effort file transfer to more demanding real time traffic and with different virtual connections active. Other tests would then follow the same principles. Additionally, test cases for the WMN system concept were created from scratch due to the fact that the system under test is quite different from a regular system of network interconnect devices and does not implement any standardized protocol or a set of protocols.

6 Test results

In Chapter 5, the most important testing aspects of the different functionalities of the WMN prototype protocol were presented. In this chapter, first an overview of the used test process is given. Then a description of the basic validation test methods used in each of the functionality phases of the WMN prototype protocol development and the respective results are summarized. The extensive phase specific testing documentation is omitted here.

Section 6.1 gives an overview on the testing process used. Sections through 6.2 and 6.6 presents the actual verification results for each of the functionality phases and gives a short rationale on the designed verification tests. Section 6.7 discusses the main findings of the testing process and suggests some potential future research topics. Finally, Section 6.8 presents a summary on the public demonstrations of the WMN concept and demonstration platform.

6.1 Testing process overview

The testing took place over the period of twelve months in total. New functionalities were tested as soon as they had been implemented in the prototype protocol software. Testing was almost completely done at NSN, with only preliminary software testing at VTT. The process is depicted in Figure 22 and illustrates also the task responsibility division between NSN and VTT. The concept and protocol software development was an incremental process and consisted of a set of phased functionality milestones, all adding up towards the final version of the prototype protocol software. Specifications were first created jointly by NSN and VTT, being partially in the scope of this master's thesis as well. After the specifications were agreed upon, the protocol software was developed accordingly. The tasks of this phase were carried out entirely by VTT. In addition to building the test setup introduced in Chapter 5, the entire test planning, test case execution and result reporting were the main responsibility areas of this master's thesis.

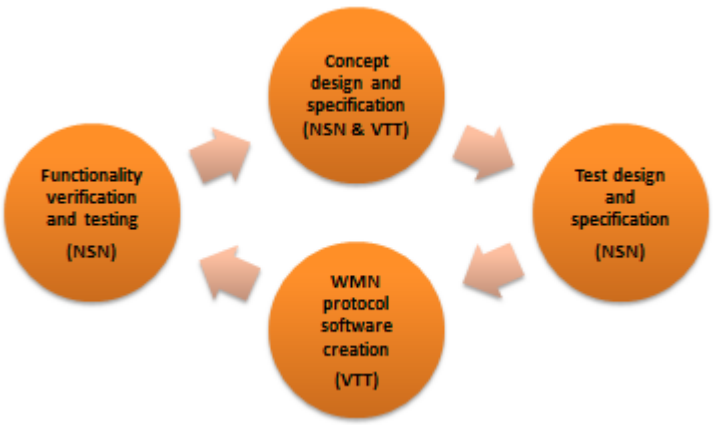

Figure 22: The concept development and testing process.

The principal testing tools introduced in Chapter 5, i.e. Spirent TestCenter traffic generator, Wireshark analyzer and Linux networking tools, are well suited for end-to-

end verification testing and analysis. However, as the correct internal messaging verification of the WMN system was also an important aspect of the system functionality, the test specification and creation phase also included definitions for certain debugging and other informative properties to be included as part of the features of the prototype protocol software. These features helped immensely in the overall testing process.

6.2 Basic routing and scheduling

Results for the spanning tree-based routing

The test aimed to validate the spanning tree-based routing mechanism, including correct mapping of ingress data, correct forwarding paths and correct and uncorrupted data on the egress of the WMN system. The test setup is illustrated in Figure 23. The client ports of the Lanner MR-730 units were attached regular PCs on both sides of a tested hop. The PCs were configured to have the same VLANIDs as defined in node configuration files. Externally, the routing principle is quite simple and the test case does not need to be very complicated. As long as incoming data is tagged with proper VLANID values, i.e. they match the configured VLANIDs in node specific mapping list configuration, data should flow through the WMN system correctly. Every aspect of the routing scheme features can be tested with the ping utility between endpoint hosts on a certain established connection. If a ping is successful, it means that data is correctly mapped on the ingress of the WMN system, that data is correctly forwarded along the planned path towards a certain destination and finally that data is correctly inverse mapped in the egress of the system. In addition, as the ping utility includes a reply ICMP message (Internet Control Message Protocols), the bi-directionality of a routing path is tested as well.

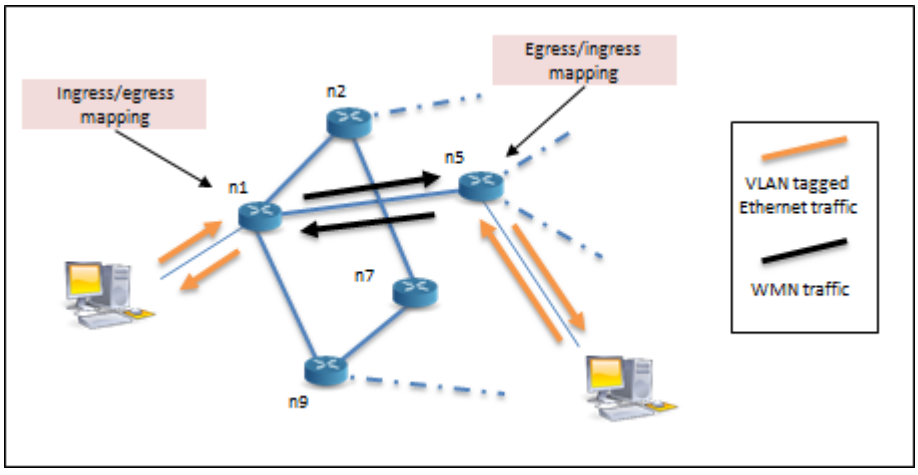

Figure 23: Test setup for basic routing testing.

As routing is one of the two fundamental mechanisms of the WMN system in addition to the scheduling principle, it was necessary to validate also the correct header format in the packets traversing the WMN system. Figure 24 illustrates a packet captured with Wireshark from a gigabit Ethernet mesh port in node 1. The correct header format can be clearly seen in the captured packet. The packet is first encapsulated with

an Ethernet dummy header, placed in order for the wireless hop to work properly (red rectangular area) and subsequently with the actual WMN header (black circular area). This particular packet was heading towards node 5, following spanning tree number 3.

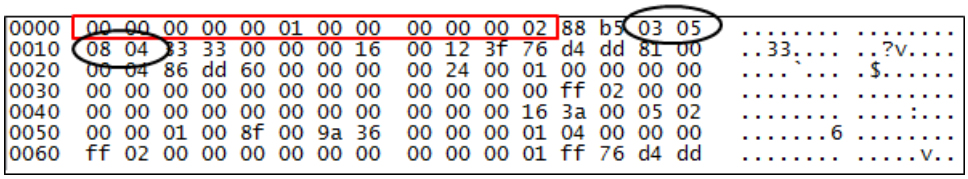

Figure 24: Captured WMN packet on direction n1-n5.

Overall, the routing works as originally specified. Incoming data on the ingress of the WMN system gets mapped correctly according to the VCID mapping tables defined in the configuration files. In case of incorrect or undefined VLAN tagged data in the ingress, the data packets simply get dropped. With the properly working routing scheme, the prototype protocol can be easily amended with functionalities utilizing the spanning tree-based routing such as internal signaling features. The scheme also allows possible traffic engineering features as certain VLANID mappings can be configured to follow suitable spanning trees or in turn special spanning trees can be created to overlay the network in a particular way.

Results for the network-wide schedule

The test aimed to validate the network-wide scheduling principle, i.e. the accordance of the observed timing with configured parameters. The test setup is illustrated in Figure 25. Traffic was captured on receiving side with Wireshark and timestamps of the received packets were examined. To verify the correct behavior of the scheduling principle a few things were taken into consideration. First of all, the amount of time reserved per transmission slot should not be extremely small. Short transmission slots could potentially be affected by timing inaccuracy introduced by the elements along a test route. Secondly, as the schedule timing is observed on receiving packet time stamps, incoming traffic needs to be fast enough to fill up every potential transmission slot, but on the other hand slow enough that the amount of samples (i.e. received packets) per slot would remain in reasonable amounts. In the end, the transmission slot timing was configured to be 100 milliseconds per slot. As can be deduced from Figure 25, 100 millisecond timing for every transmission slot in node 1 should result in data transmission towards its neighbors in 300 millisecond intervals. The test traffic was generated with the ping utility with 100 millisecond intervals originating from a regular PC.

Figure 26 presents a capture stream from one of the neighbors of node 1. As was expected, the packets have arrived more or less in 300 millisecond intervals, consisting of 100 milliseconds for the actual transmission slot in addition to the 200 milliseconds waiting time due to the transmission towards other two directions. The timestamps vary roughly 2 milliseconds around the expected 300 millisecond interval multiples. This slight timing inaccuracy is present in all captured traffic. The timing inaccuracy is likely due to relative clock differences between the used Linux PC and the Lanner MR-730. Inaccuracies can also rise if packets are sent near the end of a transmission slot, as transmission is not aborted if a packet processing is already started. In any case, in prin-

ciple the concept of scheduled transmission works correctly and can offer accurate transmission slot timing for the demonstrator system down to the millisecond scale. With further software optimization and hardware accelerated processing of the main functionalities, the microsecond transmission slot times planned for the concept should be easily achieved.

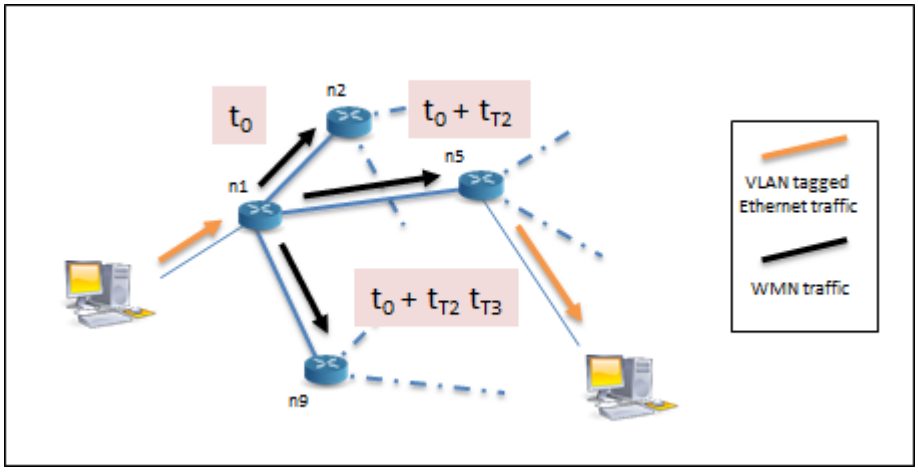

Figure 25: Test setup for basic schedule testing.

1	0.000000	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
2	0.000021	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply
3	0.296614	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
4	0.296622	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply
5	0.598354	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
6	0.598377	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply
7	0.598401	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
8	0.598407	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply
9	0.900319	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
10	0.900340	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply
11	1.196695	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
12	1.196712	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply
13	1.196747	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
14	1.196753	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply
15	1.498668	102.0.0.1	102.0.0.2	ICMP	Echo (ping) request
16	1.498688	102.0.0.2	102.0.0.1	ICMP	Echo (ping) reply

Figure 26: Captured scheduling cycle data.

6.3 Integration of the BRAWE radio system

The BRAWE radio hop is essentially just a bit pipe for the WMN system and requires very accurate synchronization between transmitting and receiving side due to the rapidly switching antenna beam direction. Obviously, if receiving and transmitting side are not following the same absolute time, their communication might not be properly aligned, meaning that, for example, transmitting side starts data transmission even though receiving side is not turned to that particular antenna direction yet.

The most important thing in the integration of the BRAWE radio system was delivery of beam steering and link break information between the Lanner MR-730 and the

BRAWE radio units. The radio unit had been amended with suitable input and output electronics by VTT before it was integrated to the WMN system. In turn, suitable GPIO pins for controlling the beam steering and interpreting the link break information from BRAWE were specified and incorporated into the prototype protocol software. The physical integration thus only included connecting the right BRAWE inputs and outputs with corresponding GPIO pins on the Lanner platform.

As mentioned in Chapter 5, the NSN FlexiPacket board used for the baseband processing is an FDD system. Since the WMN demonstrator system originally was designed to be a TDD system, this caused some challenges in the integration phase. FDD mode of operation is usually designed in such a way that a continuous connection between two communicating FDD radios exists at all times, excluding the initial device start-up phase. This is why FDD phase lock acquisition performance is not required to be that fast (roughly a few tens of milliseconds). In turn, TDD systems can acquire phase lock as fast as during an Ethernet packet preamble (i.e. in a few microseconds). Thus, the transmission slots could not be configured to be as low as the demonstrator system would allow because enough time needed to be allocated for both the phase lock acquisition and the actual data transmission as the beam direction changed. Anyhow, with slight adjustment to transmission slot timing, the system was able to perform satisfactorily. In the end roughly 40 millisecond transmission slots were configured with 20 millisecond guard time for the phase lock acquisition (i.e. the software simply waits for 20 milliseconds in the beginning of every transmission slot). The radio hop transmission was not completely errorless mainly due to the suboptimal baseband hardware used and slight wander in synchronization, but still it was able to transmit, for example, real-time traffic without visible errors.

The successful integration of the BRAWE radio system was a significant milestone in the concept verification process. It meant that the novel concepts of network-wide scheduling principle and shared resources are functional and feasible technologies and that they can be implemented in practice with real radio hardware. The basic transport mechanisms developed for the WMN system are thus entirely feasible and realizable in practice.

6.4 Resiliency

Results for the Ethernet link break

The test aimed to validate the operation of the network under link breaks, including link break detection, system signaling and end-to-end path reselection. The test setup is illustrated in Figure 27. Data was sent between gateway node 1 and the rest of the network. Regular PCs and TestCenter was used for traffic generation. As with the routing scheme, on a system level the verification of the correct protection behavior is a simple task. With bi-directional traffic, an Ethernet cable is simply unplugged on an active path and the behavior in the network is observed. If data flows correctly in both directions through the network after a link break, it implies that nodes can detect errors correctly, the information about the link break reaches relevant nodes (both ends of an active path) and that the activation of path reselection functions correctly. In addition to simply observing externally the behavior of the network, it was necessary for the nodes to log information about received and sent link state update signaling messages. Internally, the

link state messages are binary encoded, thus as part of the test planning, the human-readable format that the nodes would follow in logging the link state update messages was specified. Naturally, the log entries should include at least the links and nodes affected by the link break. Also, it was necessary for the entries to have a list of affected spanning trees, virtual connections and preferences for more accurate validation.

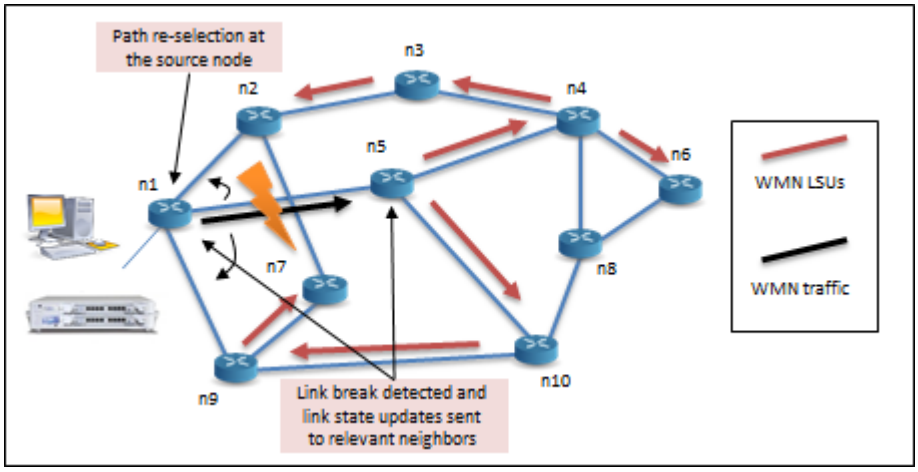

Figure 27: Test setup for resiliency testing.

The test setup depicted in Figure 27 illustrates an example link break scenario where cable between nodes 1 and 5 is unplugged. Respectively, Tables 1 and 2 illustrate the link state update message log entries that are sent or received due to the link break. As can be seen they give information on affected interface, link, spanning trees, virtual connections and preferences.

Table 1: Link state update message sent from node 5.

```
**************************************
Link manager: Inner interface status notification from SE: if index: 0, state: broken.
**************************************
ST manager: Link between nodes 1-5 broken.
ST manager: Spanning trees going through the link:
ST 3
ST manager: Sending Link State Update (link 1-5 broken, affects ST 3) to neighbour node
4
ST manager: Sending Link State Update (link 1-5 broken, affects ST 3) to neighbour node
10
**************************************
VC (outgoing) preference path states after link update (1-5 from operational to broken):
* VC 4: Pref 1: Path ST 3, GN 1, state: broken
* VC 4: Pref 2: Path ST 2, GN 1, state: operational
* VC 4: Pref 3: Path ST 1, GN 1, state: operational
```

Table 2: Link state update received at node 6.

```
****************************************
ST manager: Received Link State Update (link 1-5 broken, affects ST 3) from neighbour
node 4
ST manager: No other neighbours to forward the LSU.
****************************************
VC (outgoing) preference path states after link update (1-5 from operational to broken):
* VC 5: Pref 1: Path ST 3, GN 1, state: broken
* VC 5: Pref 2: Path ST 1, GN 1, state: operational
* VC 5: Pref 3: Path ST 2, GN 1, state: operational
```

As was expected, the link break detection with Ethernet cables is somewhat slow and causes packet loss every time cables are unplugged. Also, it was noted that as the correct behavior of the protection mechanism requires that all the nodes in the network have a consistent view of the present state of the topology, lost link state messages will affect the performance of the network. This suggests that the event-based link state update flooding needs to be enhanced with some regularly performed node originated end-to-end connectivity test along the specified paths. A good reference would be the connectivity fault management used in Ethernet OAM [57]. Overall, link break detection, signaling and the end-to-end path reselection features work as specified. Data can be forwarded between a source and destination pair as long as there is a spanning tree connection between them. The path reselection reroutes traffic traversing a breaking spanning tree but other traffic is not affected in any way.

Results for the BRAWE radio system link break

The test aimed to validate the resiliency features of the WMN system while the BRAWE radio system was integrated to the demonstrator and implementing one wireless hop of the topology. One of the more concerning and challenging areas during the link break detection testing with the radio system was the overall synchronization of the system as antenna beam directions were being changed rapidly. The link break detection in the BRAWE radio platform was done in a single element, measuring plainly the received signal strength and triggering an alarm if a certain threshold voltage was passed, independent of antenna beam direction. Thus it was up to the protocol software to determine that the link break information was read during the correct antenna beam direction.

It was found out that with short transmission slot times, the protocol software could not distinguish properly which of the two directions is affected by link break. This suggests that either it takes too much time to for the software to read the link break input value and this somehow causes transmission slot overlap (which seems unlikely as GPIO pin operations are quite fast) or alternatively the electronics on the BRAWE radio platform are too slow and cannot properly keep up with the control signaling and subsequently cause the software to read delayed values (which also seems rather unlikely as comparators can change their output value in a few nanoseconds). The only reasonable fix to this problem was to lengthen the transmission slot times. Anyhow, with the

BRAWE radio system, only the link break information delivery is changed while the link state messaging logic caused by the link break remains the same as in Ethernet case. The successful verification of the received signal strength-based link break detection meant that the overall protection switching delays can be optimized to be extremely low, even as fast as a few microseconds, though the concept will need further testing with shorter transmission slot times and more optimal hardware.

Results for the fast local tree switching mechanism

The test aimed to validate the benefits of the fast local tree switching mechanism. For proper verification of the mechanism, a link break scenario needed to be created in which there are two end-to-end connections between a source and destination pair and also a connection towards the same destination on one of the transient nodes. The most suitable spot for the test was source and destination pair node 5 – node 8. The preference list in node 5 needed a slight modification as the primary path towards node 8 needed to traverse via node 6 (see Figure 27 for reference). Furthermore, the secondary path needed to traverse via node 10. The link break was induced between nodes 4 and 6, so that transient packets could be forwarded momentarily with the fast local tree switching towards node 8 from node 4. With this single configuration all the functionalities included in the fast local tree switching portfolio could be properly verified, including the potential packet loss decrease and the correct functionality of the re-sequencing buffering. The potential advantages of transient packet forwarding in terms of decrease in packet loss were tested by using protocol software with and without the fast local tree switching. The test traffic used here was low rate and rather short burst of packets and was generated with TestCenter. In turn, the test traffic in re-sequencing tests was generated with a custom traffic generator written in C and created as part of the test specification planning. The packets created with the generator had ascending indices programmed in the payload. By capturing the packets in the receiving side and observing the payload indices, the re-sequencing buffer functionality could be verified (i.e. were the packets in or out of order).

Packet loss measurements with and without fast local tree switching are presented in Table 3. There were ten test runs for both cases with the same traffic profile and with more or less the same timing in the link break. As can be seen, the packet loss is consistently higher when local tree switching is not used, i.e. transient packets are dropped if link break is detected. Packet loss values effectively halve when local tree switching is turned on (4,049% vs. 2,228%). As already pointed out, Ethernet link break detection takes a while, causing some unavoidable packet loss. This is why packet loss occurs also with local tree switching. In any case, it is evident that the fast local tree switching mechanism certainly makes a notable difference in decreasing packet loss in link break events.

The fast local tree switching mechanism provides a clear improvement in the packet forwarding capabilities of the WMN system in link break situations. The positive impact of the mechanism is likely to only grow with higher data rates and larger topologies as the link state update messages take naturally more time to propagate in multihop topologies. The active re-sequence buffering was also found to be working correctly. The potential downside with the buffering is a slight increase in end-to-end delay as the mechanism essentially halts the packet forwarding to wait for the arrival of all tran-

sient packets. However, as in-order packet transport is part of the mobile backhaul Quality of Service requirements, the tradeoff is acceptable and in the end the buffering delay should not be that high.

Table 3: Test result with and without fast local tree switching with burst size (TX), received packets (RX) and packet loss (P-LOSS).

	With local tree switching			Without local tree switching		
	TX	RX	P-LOSS	TX	RX	P-LOSS
	29762	29163	599	29762	28570	1192
	29762	29121	641	29762	28534	1228
	29762	28553	1209	29762	28590	1172
	29762	29197	565	29762	28539	1223
	29762	29143	619	29762	28560	1202
	29762	29155	607	29762	28551	1211
	29762	29210	552	29762	28543	1219
	29762	29161	601	29762	28601	1161
	29762	29124	638	29762	28581	1181
	29762	29163	599	29762	28499	1263
AVG	**29762**	**29099**	**663**	**29762**	**28556,8**	**1205,2**
AVG %	**100**	**97,772**	**2,228**	**100**	**95,951**	**4,049**

6.5 Quality of Service

Results for the Quality of Service mapping

The test aimed to validate the basic mapping of Quality of Service information for traffic in the ingress of the WMN system. Traffic was sent between two nodes. As mentioned in Chapter 4, the WMN system has its own internal Quality of Service scheme. Thus it was important to validate that the Quality of Service information in the ingress of the system gets mapped correctly according to configured mappings and that the information is transported and mapped correctly in the egress of the system for upper transport hierarchies. The prototype protocol was specified to use Ethernet Quality of Service information for ingress mapping. Thus the correct mapping and transport of the information was tested by sending traffic between two PCs attached to different nodes with different values configured in PCP fields of the forwarded Ethernet packets. The test traffic was generated with the ping utility. Packets were subsequently captured from transient and egress nodes to verify the correct mappings. With the introduction of the Quality of Service scheme to the prototype protocol, it was again necessary to specify a suitable amendment to the link state update format.

Figure 28 illustrates a packet encapsulated in the WMN header. The Quality of Service header field is marked with a black circular area. In this particular case, the PCP mappings were chosen in such a way that the traffic class would be mapped to the highest external traffic class. Overall, the mapping mechanism works throughout the config-

ured priority range in ingress and egress cases. Table 4 illustrates the link state message log entry amended with the specified Quality of Service information. Every priority per certain destination can be individually managed.

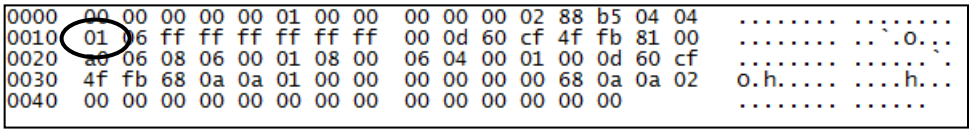

Figure 28: Captured WMN packet with the highest external traffic class.

Table 4: Quality of Service information in link state update messages.

```
****************************************
ST manager: Received Link State Update (link 5-10 broken, affects ST 3) from neighbour
node 4
ST manager: No other neighbours to forward the LSU.
GN 7, prio H2: ST changed from 3 to 1 (pref 2)
GN 7, prio H3: ST changed from 3 to 1 (pref 2)
GN 7, prio H4: ST changed from 3 to 1 (pref 2)
GN 7, prio L1: ST changed from 3 to 1 (pref 2)
GN 7, prio L2: ST changed from 3 to none (no paths left).
GN 7, prio L4: ST changed from 3 to none (no paths left).
                  .
                  .
                  .
GN 10, prio L1: ST changed from 3 to 1 (pref 2)
GN 10, prio L2: ST changed from 3 to none (no paths left).
GN 10, prio L4: ST changed from 3 to none (no paths left).
****************************************
VC (outgoing) preference path states after link update (5-10 from operational to bro-
ken):
* VC 5: Pref 1: Path ST 2, GN 1, state: operational
* VC 5: Pref 2: Path ST 1, GN 1, state: operational
* VC 5: Pref 3: Path ST 3, GN 1, state: broken
```

Naturally, the Quality of Service mapping mechanism only enables the traffic classification information available to the internal algorithms of the WMN and as such is not a very complex task. Generally, it should be also emphasized that even though the Quality of Service mapping in this demonstrator system is implemented based on Ethernet Quality of Service information, in principle the software can be easily extended to interpret, for example, DiffServ DSCP fields on IP headers or MPLS EXP fields on the MPLS shim headers if desired.

Results for congestion control mechanism

The test aimed to validate the second tool in the Quality of Service scheme of the WMN system: the congestion detection mechanism. The test setup is similar to as illustrated in Figure 23, though the PCs are replaced by TestCenter for higher data rates. A gradually ramped up traffic flow was sent from the traffic generator. Thus at some point, if the congestion detection mechanism works correctly, the prototype protocol should start recording congestion events on the particular link. Again, it was necessary to amend the

protocol specific messaging with further information fields, more specifically, with knowledge on the level of congestion and the affected links. Congestion events are similar to link breaks in the sense that the rest of the WMN network needs to know about it. Thus it was necessary to also validate the correct signaling procedures of the congestion information. This was done similarly as in link break tests, the received link state messages were recorded at all nodes and the correctness of the information was subsequently verified. The new congestion information amended to the link state updates is illustrated in Table 5.

As the congestion detection is based on measuring the buffer fill levels, the suitable buffer sizes needed to be interpolated. The rationale behind size allocation differs from, for example, regular IP router buffer dimensioning. This is mainly due to the inherent traffic shaping caused by the scheduling principle. Essentially, this means that the buffer sizes need to be long enough so that the traffic that is cumulated during transmission slot waiting times does not cause premature congestion events, i.e. there needs to be some transparent buffering. On the other hand however, the buffer sizes cannot be too long as this would start to affect negatively the system latency at some point. A good rule of thumb for the buffer lengths was derived to be the amount of bytes a certain direction could be able send if it had all the transmission slots allocated to it.

Table 5: Congestion status information in link state update messages.

```
**************************************
ST manager: Link between nodes 1-5. Congestion status:
Priority L4: Congestion status: Low.
* Updated to congestion status table.
ST manager: Spanning trees going through the link:
ST 3
ST manager: Sending Link State Update (link 1-5 congestion status, affects ST 3) to
neighbour node 5
A congestion task set to be executed after 150120 us.
**************************************
ST manager: Executing delayed congestion task (link 1-5)
Update cong blocking: GN: 2,ST 3, prio L4: Free -> Low
Update cong blocking: GN: 3,ST 3, prio L4: Free -> Low
Update cong blocking: GN: 4,ST 3, prio L4: Free -> Low
Update cong blocking: GN: 5,ST 3, prio L4: Free -> Low
Update cong blocking: GN: 6,ST 3, prio L4: Free -> Low
Update cong blocking: GN: 7,ST 3, prio L4: Free -> Low
Update cong blocking: GN: 9,ST 3, prio L4: Free -> Low
Update cong blocking: GN: 10,ST 3, prio L4: Free -> Low
No updates to current preferences.
```

The initial congestion detection tests discovered obscure behavior in terms of throughput and forwarding capabilities of the prototype protocol. The links were configured to their maximum capacity values (i.e. one gigabit) but the software could not achieve even a third of the expected throughput. Cavium Networks promises over 4 Gbit/s packet forwarding capabilities for each of the cores used in the Lanner MR-730, thus it was hard to believe that the mediocre throughput values was due to software complexity. After extensive debugging and further testing the cause of the problem was found to be a single function call provided by Cavium Networks helper library API which monitors the state of Ethernet interfaces on the Lanner MR-730. The function

was called every time prior to forwarding a packet and evidently hampered the performance of the packet forwarding process. The problem was solved by calling the function less often. The fix was seemingly simple as the problem was entirely platform and demonstrator environment specific. Ethernet-based connections are merely used to emulate the wireless connections between WMN nodes and there was no need to alter the WMN concept specifications as a result.

All in all, even though the initial throughput problems haunted the verification testing, the congestion monitoring and triggering functionalities per se were working correctly as specified. Congestion information is sent to the nodes via the affected spanning tree, similarly as in the link break case.

Results for traffic and load management

The test aimed to validate the traffic and load management procedures implemented in the protocol software. Traffic and load management features are the main processes behind the Quality of Service scheme of the WMN system. The mapping and detection mechanisms tested in the previous two phases are used as the basic tools in traffic and load management decision making. The test setup is illustrated in Figure 29. The test consists of two priority classes, one higher than the other, which are sent towards a common destination along the same path. Both of the traffic flows are sent at near maximum link speeds so that there is properly room for only one of the traffic flows. The test is started by injecting the lower priority traffic flow along the configured path. Shortly after, the higher priority traffic is injected on the same path. As the traffic flows are of different priority and as higher priority traffic classes should always get precedence over lower priority classes in congestion situations, a dramatic decrease in the throughput of the lower priority traffic flow should be seen. Thereafter, the behavior of the network is observed. The test traffic is injected with TestCenter in such a way that the traffic is sent and received on different ports of the traffic generator, effectively forming a loop. This way as the congestion situation changes in the network, the dynamics of the sent traffic flows can be observed and verified in real time and recorded for further analysis.

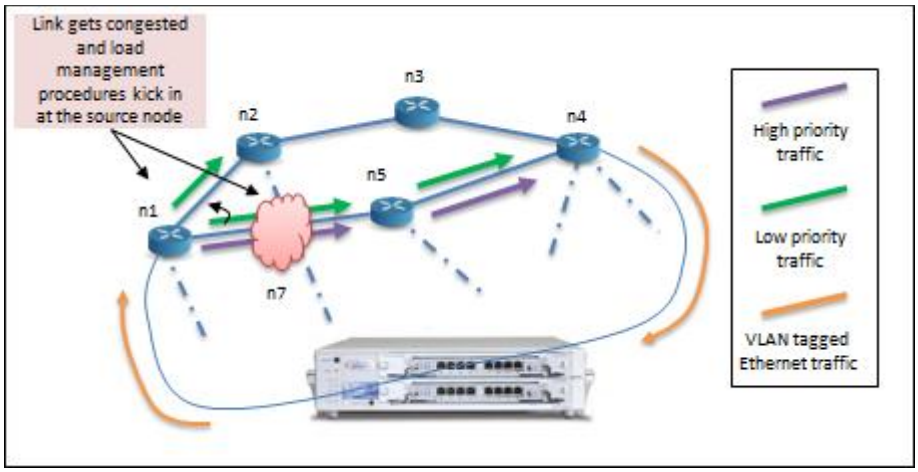

Figure 29: Test setup for traffic and load management testing.

Figures 30 and 31 present received traffic distribution snapshot diagrams from the test case results. Both figures are derived from TestCenter statistics. In this case, the back-up paths between the source and destination nodes are disabled to make the traffic and load management procedures more explicit. Figure 30 represents the initial phase of the test. The low priority traffic flow is received with 100% throughput percentage and zero packet loss. Figure 31 in turn shows the traffic distribution in the receiving side as the higher priority traffic is injected to the system. As can be seen, the lower priority traffic is immediately starting to suffer from packet loss and declining capacity. In the figure, the throughput percentage for the low priority traffic flow is roughly 56% with 44% packet loss. On the other hand, the high priority traffic flow is allocated the entire bandwidth (roughly 97% throughput percentage) with some random packet loss (roughly 3%). It will take some time for the low priority packet loss rate to reach 100% as the traffic flow statistics are cumulative.

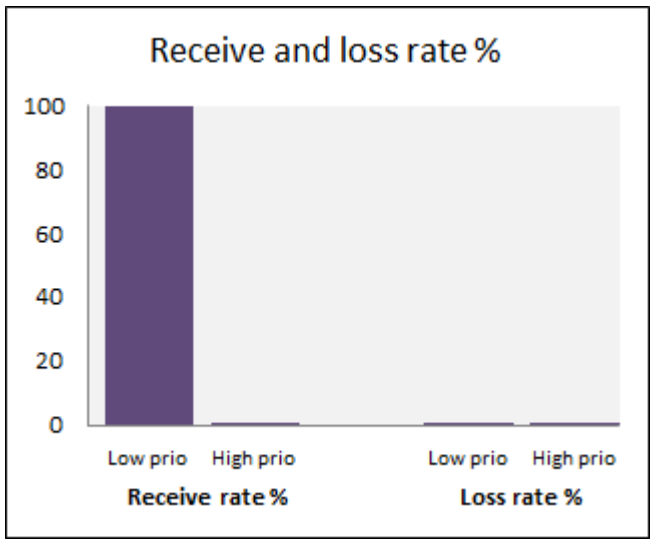

Figure 30: Received traffic distribution with only the lower priority traffic flow active.

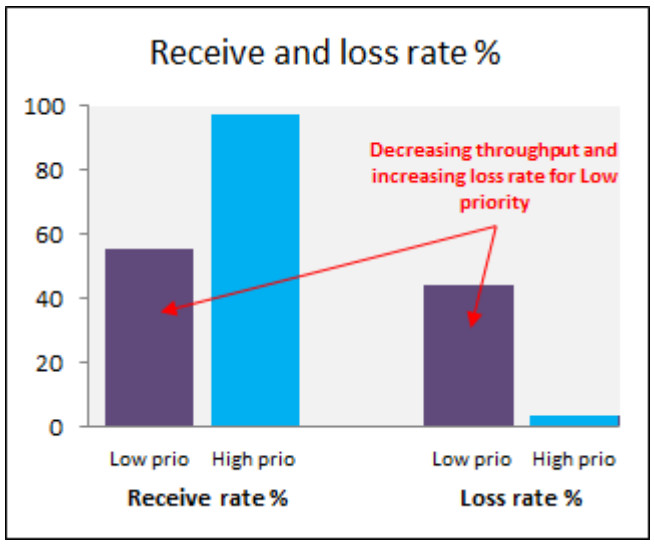

Figure 31: Received traffic distribution when both priority traffic flows are active.

This simple test case more or less verifies the correct operation of the entire Quality of Service scheme of the WMN system. The resulting traffic distribution diagrams suggest that the protocol software can distinguish the traffic classes of individual packets and can make traffic and load management decisions based on them in high traffic load and congestion situations. As mentioned, the traffic distribution diagrams presented above were recorded in a situation where back-up paths were disabled. However, if there are established back-up paths left between the particular source and destination, the lower priority traffic is always attempted to reroute through them.

The implications of the working Quality of Service scheme are that basically any real time or delay constrained traffic can be forwarded with quite deterministic delay bounds through multi-hop WMN networks, provided that they are indeed mapped to the real time traffic classes. In turn, lower priority traffic such as plain best effort traffic can be rerouted via slightly longer routes. Furthermore, the higher priority traffic flows can be preserved better, as the lowest priority traffic classes can be dropped completely in highly degraded network situations.

6.6 Preliminary performance testing

The test aimed to validate the stability features of the software over longer runs with maximum link capacities. The test setup is illustrated in Figure 32. As the WMN system uses the concept of shared resources, single traffic stream towards some destination was not going to be enough to the test the maximum forwarding capabilities of the protocol software. Thus, the test included three different traffic flows sent from node 1 towards all of its neighbors. The individual traffic streams combined would subsequently test the maximum forwarding performance. The test traffic flows were all tagged with the highest priority class so that traffic class dependent disparities would be avoided.

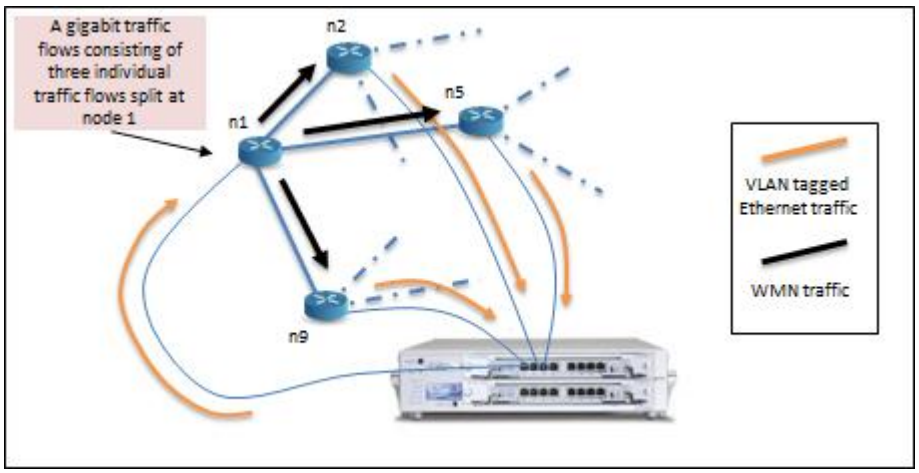

Figure 32: Test setup for performance testing.

As a preliminary step, a suitable nearly maximum value was interpolated for the three test flows. In theory, the software in the demonstrator system with the present topology and schedule can forward data at 333 Mbit/s per link direction. However, at nearly maximum capacity, the output buffers start filling up rapidly and the congestion

mechanisms start triggering. Maximum short term link capacity was found to be roughly 325 Mbit/s. After a while, the link starts building up congestion and frame loss occurs. 310 Mbit/s was found to be a stable, long term maximum capacity and thus used as the data rate for each of the three test flows. Transmission slots lengths was chosen to be 4 milliseconds. With shorter transmission slot times, the accuracy of the individual slot boundaries would not likely be good enough, as was discussed in the schedule testing phase earlier. In addition, with the schedule calculated for the demonstrator topology, every link in node 1 will be getting two transmission opportunities in one schedule cycle.

Table 6: Performance test results.

Stream ID	TX count (frames)	RX count (frames)	Dropped frames	Avg latency (us)	Min latency (us)	Max latency (us)
1	2598890027	2598882014	8013	9715.538	2643.98	111088.14
2	2598890027	2598881943	8084	9714.978	3628.01	107928.91
3	2598890026	2598881940	8086	9709.526	1155.52	108577.84

The test was running for roughly 20 hours. Table 6 lists the results of the test run, including total sent frames, total received frames, packet loss count, average latency, minimum latency and maximum latency for all the three individual traffic streams. As can be seen, the protocol software performs quite well with nearly maximum capacities over long times. The total amount of frames sent in each individual stream was nearly 2.6 billion. Furthermore, even though the chosen capacity was found to be stable for the software earlier, some frame loss still occurred. However, the packet loss ratio is something like 0.0001% which is quite good for prototype software. The cause for this level of extremely low packet loss can be basically anything. Packets might have been lost at the Lanner MR-730 input buffers which are hardware controlled and drop packets after certain thresholds. There might have been a full congestion situation at some point in the test run which also might have caused packet loss. The most important thing is, though, that this occurs rarely and packet loss stays satisfactorily low.

Latency-wise, there does not seem to be any odd behavior. Minimum latency is, as can be expected, below the 4-millisecond transmission time slot. This merely means that as a packet has entered the demonstrator ingress, it has been forwarded out during the first possible transmission slot. The average latency suggests that, in general, packets have been entering the ingress of the demonstrator in such a way that they have missed the first possible transmission slot turn, waited two transmission slots reserved for other links and subsequently have been forwarded in the second possible transmission slot. On the other hand, the maximum latency is quite high, suggesting that packets have been buffered for up to roughly 30 transmission slots. The packets being this long in the system might be most vulnerable to potential packet drops. However, as the average latency is so much shorter than the maximum, packets with 108 to 110 microsecond latency seem to be quite rare.

These results suggest that, for example, voice traffic would not suffer any sort of quality degradation if transported over the WMN system even with the 4-millisecond transmission slot timing used in the demonstrator. ITU has defined an acceptable delay

requirement for most user applications to be in the 0-150 millisecond area [106]. The WMN concept itself defines a 100-500 microsecond transmission slot timing interval. With little interpolation, for example, 200 microsecond transmission slot times would linearly result in roughly 500 microsecond latency per hop which implies extremely good performance.

6.7 Discussion and future work

Overall, the system testing process progressed quite smoothly. The demonstrator environment performed exemplarily, even though the BRAWE radio system suffered from antenna feeder chip breakdowns during the testing process. As a result, some of the tests were not able to be performed with a working wireless hop. Complex and fatal bugs were non-existent, and the few bugs, for example, the capacity problem discussed as part of the congestion testing earlier, that actually bothered the testing process were eventually sorted out and were more or less validation platform specific, having nothing to do with the concepts of the WMN system. Also, it is fair to mention that the prototype protocol was extremely high quality software and had relatively small amount of mainly minor bugs. This is largely thanks to precise and accurate specification documentation by NSN and experienced programming carried out by VTT.

It should be also emphasized that the whole objective of the testing process was to proof that the concept works under likely traffic, load and network situations, on a system level. Based on the results of the verification testing, this particular objective was fulfilled. Extensive software testing such as code coverage, mutation and fault injection testing carried out at unit, system, integration and system integration levels, generally, is not appropriate or feasible in proof-of-concept projects. Generally, the reasoning behind this is potential scope conflicts and time constraints. More specifically, the objective of a research project is the development of a new technology or functionality, rather than a deep testing of a piece of prototype software that is likely to change greatly in architecture and logic if the concept is further developed. Furthermore, eventually this sort of software testing needs to be performed in potential product development phase.

In the end of the testing process, the prototype protocol included a working and verified routing and scheduling scheme, extensive resiliency and Quality of Service feature sets as well as successfully integrated 80 GHz radio link with electronically steerable beams. In addition, as the resiliency and Quality of Service schemes are highly automated, the protocol and the system fulfill the self-healing and self-optimization features of the SON portfolio. In principle, the demonstrator environment running the newest version of the prototype protocol would be capable of proper mobile transport as such. From the basic small cell requirements discussed in Chapter 3, the prototype protocol is missing a genuine synchronization distribution method (synchronization was delivered externally to the demonstrator system) and a security scheme. The planned synchronization scheme for the WMN system has already been specified conceptually as mentioned in Chapter 4, only the actual implementation has not yet been designed.

A potential security scheme for the WMN system is still under consideration. The NGMN forum recommends the usage of IPsec for the access backhaul. In this case, the security would be taken care of in end-to-end fashion, between the small cell base stations and the core network of LTE-Advanced. This scenario would not require any security measures from the backhaul transport, as the transported packets would be se-

cured on upper levels. However, as discussed in Chapter 3, the planned deployment locations for small cell base stations and backhaul nodes are such that in theory one could be able to tamper with the elements or carry out traffic analysis. Thus, the WMN system might benefit from an optional link layer security scheme. A good reference starting point is the 802.11i standard [107], which defines a security method for wireless local area networks. With this kind of security scheme, the security would be the responsibility of every backhaul node in a WMN system. Nodes would authenticate themselves regularly with other WMN nodes according to some pre-defined patterns and subsequently transmit AES-encrypted data (Advanced Encryption Standard). Though, as with all encryption, the process will introduce additional delay. Thus, with the planned few hundred microsecond transmission slot times, encryption would likely need proper hardware acceleration.

As discussed in the resiliency results section earlier, the WMN system would also benefit from an OAM scheme. More specifically, it may need to be necessary to monitor centrally from the WMN gateway nodes all the configured virtual connections with tools similar to the ping and traceroute utilities. Also, as part of the OAM scheme, the WMN nodes could regularly report node and interface specific packet loss, packet delay and jitter to assist with, for example, SLA assurance and overall traffic distribution and capacity analysis and planning.

Finally, to fully comply with the SON feature portfolio, the WMN system also needs an extensive self-configuration feature set in addition to the self-healing and self-optimization features discussed earlier. The self-configuration aspect includes mechanisms such as fully automatic neighbor discovery and relation and fully automatic bootstrapping of the network when the nodes are powered up for the first time. The network should be able to configure itself dynamically without any expectations on prior topology, scheduling or synchronization information on any of the nodes expect the gateway nodes, which are used to centrally control the network. This leads to obvious challenges and open issues such as how to spread the topology, scheduling and synchronization to the rest of the network and how the neighbor discovery is carried out with the shared resources and highly directional link beams.

Other potential or planned research areas for the WMN spawned during testing and general concept development process are further enhanced resiliency scheme in form of spanning tree repair and rapid path discovery, dynamic traffic engineering features similar to MPLS Traffic Engineering (e.g. virtual connection injection), further enhanced traffic and load management capabilities (e.g. inverse multiplexing of best effort traffic classes for better network utilization) and hierarchical topology solutions for better scalability. Also, the wireless communication needs to be tested with more optimal TDD radio hardware at some point in time.

6.8 Public demonstrations

During the testing process, a few possibilities to showcase the demonstrator system publicly emerged. As mentioned briefly in Chapter 1, the WMN system was jointly developed and studied by NSN and VTT under the Celtic-Plus MEVICO umbrella project which had the joint agenda of researching different aspects of 3GPP LTE networks and their evolution. The project also included other research partners from universities and other telecommunication industry companies such as Aalto University, University of

Oulu, Alcatel-Lucent, Ericsson and numerous other partners, all contributing with their own research projects and items. In addition to MEVICO specific public demonstration, the WMN demonstrator platform visited a few NSN internal research seminars to inform and illustrate a potential solution and product idea for future small cell access backhaul.

Celtic-Plus organization is an "industry driven European research initiative to define, perform and finance through public and private funding common research projects" [108]. It arranges annually an event where all the participating projects with their particular research areas and topics showcase the most recent results of their findings. Furthermore, the organization also conducts regular reviews on the state of the different research projects.

The first public demonstration of the WMN concept was in January 2012 as part of Celtic-Plus and MEVICO mid-term review. Participants included personnel from Celtic-Plus organization, VTT, Aalto University and telecommunication industry representation from NSN and Alcatel-Lucent. The review meeting was held at NSN and the demonstration platform included the WMN demonstration system and the BRAWE radio system. The topology was changed slightly from the one used in the test and verification process and introduced in Chapter 5, to make the feature demonstration and elaboration clearer. The demonstrated features were the resiliency and Quality of Service schemes and the demonstration cases were similar to what was used in the testing process. The resiliency demonstration included a video stream that was forwarded through the WMN system. The topology was planned in such a way that the traffic would use the wireless links provided by the BRAWE radio system as primary and secondary paths. Thus when the primary forwarding path was blocked with an obstacle, the traffic would subsequently be forwarded via the other wireless link. The Quality of Service demonstration included a high and a low priority video streams which the prototype software would forward differently in link break situations. Overall, the demonstration was successful and the WMN concept aroused interest.

The second public demonstration was in February 2012 and was in conjunction with the annual Celtic Event which was held in Stockholm, Sweden. The topology was the same as in the MEVICO mid-term review, though the BRAWE radio system was not functional at this point. The functional setup built at the exhibition hall is presented in Figure 33. The demonstrated features were largely the same as in MEVICO mid-term review demo, though the Quality of Service scheme was amended with congestion control and load management mechanisms and were subsequently also demonstrated at the exhibition. All in all, the Celtic-Event demonstrations were successful and the WMN concept drew visitors from different universities, telecommunication operators and other research organizations.

All in all, the successful demonstrations and general interest towards the WMN concept at NSN internal seminars and public exhibitions imply strong performance of the protocol software and the demonstrator platform as well as a promising future outlook for the WMN concept itself.

Figure 33: The demonstration setup at the Celtic-Event 2012.

6.9 Summary

The WMN proof-of-concept system build up, protocol software development and the subsequent system validation took place over the period of twelve months in total. The process was incremental and consisted of a set of phased functionality milestones, all adding up towards the final version of the prototype protocol software. In the end, the WMN prototype protocol included all the planned routing and scheduling, resiliency, Quality of Service and traffic and load management features. All the different functionalities were proven to be entirely feasible and realizable in principle, though further testing need to conducted with more optimal hardware. Additionally, the WMN concept might benefit from a set of enhancements including link layer security and OAM scheme.

Overall, the system testing process progressed quite smoothly and the proof-of-concept environment performed exemplarily. Complex and fatal bugs were non-existent, and the few bugs that actually bothered the testing process were eventually sorted out and were more or less validation platform specific, having nothing to do with the concepts of the WMN system. Also, it is fair to mention that the prototype protocol was extremely high quality software and had relatively small amount of mainly minor bugs.

In addition to internal testing, the WMN concept was showcased at numerous public exhibitions, including the Cetlic Event organized by Celtic-Plus initiative. Generally the concept drew a notable amount of attention and positive feedback, thanks to the successful demonstrations. Overall, the WMN concept has a lot of potential and a promising future outlook.

7 Summary and conclusions

Mobile data traffic demands and volumes have surged considerably during the past couple of years. This has been driven by a few principal factors, including the rise of smartphones and their ecosystems, generally cheaper access to mobile broadband and the global expansion of the wireless infrastructure and mobile device markets. The growth trajectory is forecasted to increase in exponential fashion.

To meet the mobile data volume growth requirements, mobile communication system and technology standards have been evolving accordingly. The trend in cellular network design has been to move towards fully packet-based and service-centric mobile networks with incremental changes to the mobile network architecture, i.e. the radio access network, core network and the transport connections between them. Fourth generation mobile communication system standards introduced a completely overhauled core and radio access network architectures, making the architecture flatter and more efficient overall. One of the most notable features is the support for heterogeneous network deployments which allows the enhancement of macrocell coverage with shorter coverage smaller base station sites. These smaller cells are the likely answer for future scalability and capacity shortage problems.

The transport infrastructure between a radio access network and a core network is called the mobile backhaul. The basic function of mobile backhaul is to unite the mobile network with other external transport networks, connecting a vast number of base station sites to a small amount of centralized control sites. Traditionally, mobile networks have been backhauled using circuit switched technologies, such as PDH and SDH. However, along with the trend towards fully IP-based mobile networks, the backhaul is increasingly also packet-based. With the introduction of heterogeneous network deployments and the vastly increased number of smaller coverage base station, the backhaul design becomes problematic due to increasing number of needed backhaul connections, new type of base station site locations and installations. Also, factors that have not traditionally affected telecommunications networks and equipment will have larger impact. These include, among other things, temporary blocking due to, for example, tall vehicles and trees and increased pole sway (lamp posts vs. broadcast masts).

One of the most prominent future small cell backhaul solutions is a wireless mesh radio system with SON capabilities. This concept has been closely studied and developed by NSN and VTT. The wireless mesh backhaul concept utilizes virtual connections between different small cell backhaul units and a gateway. Connections are established based on pre-calculated spanning tree infrastructure overlaying a given small cell base station deployment topology. Furthermore, the data transmission is scheduled with a steerable shared resource principle, resulting in a dynamic and flexible networking scheme. Additionally, the concept utilizes extensive resiliency, Quality of Service and traffic management features.

As the wireless mesh concept specifications grew in complexity, it was deemed necessary to test out the developed technologies in practice. Thus, as part of the main objective of this master's thesis, a proof-of-concept system was built that was running a prototype mesh protocol implementing the different functionalities of the concept. The purpose behind the assembly of the proof-of-concept system was to verify the functionality and demonstrate the feasibility of the proposed small cell access backhaul network

concept. Furthermore, the testing process aimed to validate that the proof-of-concept system and the prototype protocol perform satisfactorily under likely traffic, load and network situations, on a system level. The entire specification, design and execution of the functionality verification test cases were also part of the main objective of this master's thesis.

Extensive test cases were defined for the different functionalities of the wireless mesh concept, including basic routing and scheduling, resiliency, Quality of Service, traffic and load management as well as performance testing. Based on the results of the numerous test cases, the functionality and feasibility of the wireless mesh concept were validated. Complex and fatal bugs were non-existent, and the few problems that actually bothered the testing process were eventually sorted out and were more or less due to the used validation platform, having nothing to do with the concepts of the wireless mesh. Thus the main objectives of this master's thesis can be regarded as fully and successfully completed, though further testing will need to be carried out at some point in time with more optimal radio hardware. Potential future topics include enhanced link layer security, OAM possibilities, time synchronization, further enhanced resiliency scheme, further enhanced traffic and load management capabilities and hierarchical topology solutions.

All in all, the wireless mesh proof-of-concept system performed quite strongly throughout the entire development and testing process. The different functionalities, including the mesh network algorithms and the wireless millimeter wave link, were proven to work successfully together even with slightly suboptimal hardware and software. With further development and enhancement, the WMN system concept displays extreme potential for state-of-the-art small cell access backhaul transport technology.

References

[1] Rayal, F. *Mobile Data Traffic Forecasts: A Comparative View*. Cited in 12.2.2012.Available in http://frankrayal.com/2011/11/21/mobile-data-traffic-forecasts-a-comparative-view/.

[2] 3GPP Long Term Evolution Work Item list. Cited in 12.2.2012. Available in http://www.3gpp.org/ftp/Specs/html-info/FeatureListFrameSet.htm.

[3] Schmidt, E. et al. *Mobile Backhaul Vision 2011-2015*. 2009.

[4] IEEE Standard for Information Technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking. *IEEE Std 802.11s-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011)*, pp.1-372, Sept. 10 2011. DOI 10.1109/IEEESTD.2011.6018236.

[5] Qunfeng, D. and Bejerano, *Y. Building Robust Nomadic Wireless Mesh Networks Using Directional Antennas*. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp.1624-1632, 13-18 April 2008. DOI 10.1109/INFOCOM.2008.223

[6] Gore, A.D. and Karandikar, A. *Link Scheduling Algorithms for Wireless Mesh Networks*. Communications Surveys & Tutorials, IEEE , volume 13, issue 2, pp.258-273, Second Quarter 2011. DOI 10.1109/SURV.2011.040510.00008.

[7] Cooper, I. et al. *Optimised scheduling for Wireless Mesh Networks using fixed cycle times*. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium, pp.1-6, 20-24 June 2011. DOI 10.1109/WoWMoM.2011.5986176.

[8] Marshall, R. et al. *Computationally Efficient Transmission Scheduling for Sensor Networks*. Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference, pp.203-207, 3-6 Dec. 2007. DOI 10.1109/ISSNIP.2007.4496844.

[9] Venkatesh, G. and Wang, K. *Estimation of maximum achievable end-to-end throughput in IEEE 802.11 based wireless mesh networks*. Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference, pp.1110-1117, 20-23 Oct. 2009. DOI 10.1109/LCN.2009.5355214.

[10] Gupta, B.K. et al. *Optimization of routing algorithm in wireless mesh networks*. Nature & Biologically Inspired Computing, 2009. NaBIC 2009. World Congress, pp.1150-1155, 9-11 Dec. 2009. DOI 10.1109/NABIC.2009.5393819

[11] IEEE 802.15 Working Group, home site. Cited in 12.8.2012. Available in http://www.ieee802.org/15/.

[12] ZigBee Alliance, standard specifications. Cited in 12.8.2012. Available in http://www.zigbee.org/Specifications.aspx.

[13] HART Communication Foundation, home site. Cited in 12.8.2012. Available in http://www.hartcomm.org/protocol/wihart/wireless_technology.html.

[14] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems. *IEEE Std 802.16-2009 (Revision of IEEE Std 802.16-2004)*, pp. C1-2004, May 29 2009. DOI 10.1109/IEEESTD.2009.5062485

[15] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 1: Multiple Relay Specification. *IEEE Std 802.16j-2009 (Amendment to IEEE Std 802.16-2009)*, pp.c1-290, June 12 2009. DOI 10.1109/IEEESTD.2009.5167148

[16] Bu, T. et al. *Designing wireless radio access networks for third generation cellular networks*. INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE , volume1, pp. 68- 78, 13-17 March 2005. DOI 10.1109/INFCOM.2005.1497880.

[17] Yamao, Y. et al. *Radio access network design concept for the fourth generation mobile communication system*. Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st , volume 3, pp. 2285-2289, 2000. DOI 10.1109/VETECS.2000.851680.

[18] Soh, W. et al. *Improving restorability in radio access network*. Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE, volume 6, pp. 3493-3497 1-5 Dec. 2003. DOI 10.1109/GLOCOM.2003.1258884.

[19] Hong, C. et al. *QoS Routing and Scheduling in TDMA Based Wireless Mesh Backhaul Networks*. Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE, pp. 3232-3237, 11-15 March 2007. DOI 10.1109/WCNC.2007.596.

[20] Haghighizadeh, N. and Mohammadi, A. *Characterization of wireless mesh backhaul networks with MIMO systems*. Telecommunications, 2008. IST 2008. International Symposium, pp. 388-392, 27-28 Aug. 2008. DOI 10.1109/ISTEL.2008.4651333.

[21] Baccarelli, E. et al. *Routing for multi-antenna Wireless Mesh Network backhaul*. Access Networks & Workshops, 2007. AccessNets '07. Second International Conference, pp. 1-8, 22-24 Aug. 2007. DOI 10.1109/ACCESSNETS.2007.4447128.

[22] Aburakawa, Y. et al. *Fiber and free-space hybrid optical networking for new generation mobile radio access network*. Wireless Personal Multimedia Communications, 2002. The 5th International Symposium. pp. 586- 590, Oct. 2002. DOI 10.1109/WPMC.2002.1088242.

[23] Aburakawa, Y. and Otsu, T. *Experimental evaluation of 800-nm band optical wireless link for new generation mobile radio access network*. Microwave Pho-

tonics, 2002. International Topical Meeting. pp. 261- 264, 5-8 Nov. 2002. DOI 10.1109/MWP.2002.1158913.

[24] Idate Consulting & Research. *Traffic forecasts for 2010-2020.* Cited in 20.5.2012. Available in http://www.ictbefemto.eu/fileadmin/documents/publications/ workshop_2011/F._PUJOL_IDATE_15_05_2011.pdf.

[25] Butler, B. *Video now accounts for half of mobile data traffic.* Cited in 20.5.2012. Available in http://www.networkworld.com/news/2012/022312-video-mobile-traffic-256495.html.

[26] Wanda, A. *Traffic Evolution Characteristics of the Mobile Internet.* Cited in 21.5.2012. Available in http://www.telecomstechnews.com/blog-hub/2011/ dec/08/traffic-evolution-characteristics-of-the-mobile-internet/.

[27] Nokia Siemens Networks. *Long Term Evolution (LTE) will meet the promise of global mobile broadband.* Finland, 2009.

[28] Halliday, J. and Arthur, C. *Mobile operators signal end of flat-rate data tariffs as app use grows.* Cited in 21.5.2012. Available in http://www.guardian.co.uk/ technology/blog/2010/aug/23/net-neutrality-mobilephones.

[29] Elisa Oyj, home site. Cited in 22.5.2012. Available in www.elisa.fi.

[30] Verizon Communications Inc. home site. Cited in 22.5.2012. Available in http://sponsorship.verizonwireless.com/nfl/.

[31] Kenney, M. and Pon, B. *Structuring the Smartphone Industry: Is the Mobile Internet OS Platform the Key?* Journal of Industry, Competition and Trade, volume 11, issue 3, pp. 239-26, 2011.

[32] Lin, F. and Ye, W. *Operating System Battle in the Ecosystem of Smartphone Industry*. Information Engineering and Electronic Commerce, 2009, IEEC '09, pp. 617-621, 16-17 May 2009.

[33] Basole, R.C and Karla, J. *On the Evolution of Mobile Platform Ecosystem Structure and Strategy*. Business & Information Systems Engineering, volume 3, issue 5, pp. 313-322, 2011.

[34] Perez, S. *It's Still A Feature Phone World: Global Smartphone Penetration At 27%*. Cited in 22.5.2012. Available in http://techcrunch.com/2011/11/28/its-still-a-feature-phone-world-global-smartphone-penetration-at-27/.

[35] Molisch, A. F. *Wireless Communications.* 2nd Edition. United Kingdom, John Wiley & Sons Ltd, 2011. ISBN 978-0-470-74187-0.

[36] Juniper Networks Inc. *Mobile Backhaul Reference Architecture*. United States, 2011.

[37] Cisco Systems Inc. *Evolution of the Mobile Network (white paper).* United States, Cisco Public Information, 2010.

[38] Ballot, J.M. *The IP Road to Mobile Network Evolution (white paper).* Alcatel-Lucent enriching communications, volume 1, issue 1, 2007.

[39] Brown, G. *Flat Is Back: Toward the All-IP Mobile Network*. Cited in 26.5.2012. Available in http://www.lightreading.com/document.asp?doc_id=128148.

[40] Tektronix Communications. *LTE Networks: Evolution and Technology Overview (white paper).* United States, August 2011.

[41] Bhalla, M. R. and Bhalla A. V. *Generations of Mobile Wireless Technology: A Survey*. International Journal of Computer Applications, volume 5, issue 4, August 2010.

[42] Wesolowski, K. *Mobile Communication Systems*. 1st Edition. United Kingdom, John Wiley & Sons, 2002. ISBN 978-0-471-49837-7.

[43] International Telecommunication Union, Radiocommunication Sector, IMT-Advanced global standard. Cited in 25.5.2012. Available in http://www.itu.int/ITU-R/index.asp?category=information&rlink=imt-advanced&lang=en.

[44] 3GPP Long Term Evolution. Cited in 25.5.2012. Available in http://www.3gpp.org/LTE/.

[45] 3GPP Long Term Evolution Advanced. Cited in 25.5.2012. Available in http://www.3gpp.org/lte-advanced.

[46] Nokia Siemens Networks. *The advanced LTE toolbox for more efficient delivery of better user experience (white paper).* Finland, 2011.

[47] Ericsson. *LTE – A 4G Solution*. Sweden, April 2011.

[48] Press release. *TeliaSonera first in the world with 4G services*. Cited in 26.5.2012. Available in http://www.teliasonera.com/en/newsroom/press-releases/2009/12/teliasonera-first-in-the-world-with-4g-services/.

[49] GSA. *GSA confirms 72 commercial LTE networks launched, LTE will enter mainstream in 2012*. Cited in 26.7.2012. Available in http://www.gsacom.com/news/gsa_351.php.

[50] LTE World. *The Race To Deploy LTE-Advanced Networks*. Cited in 22.7.2012. Available in http://lteworld.org/blog/race-deploy-lte-advanced-networks.

[51] Salmelin, J. and Metsälä E. *Mobile Backhaul.* 1st Edition. United Kingdom, John Wiley & Sons, 2012. ISBN 978-1-119-97420-8.

[52] Infonetics Research. *Mobile Backhaul Equipment and Services Forecasts*. March 2012.

[53] Ericsson and Telia. *Understanding Telecommunications 1*. Studentlitteratur, 2001. ISBN 91-44-00212-2.

[54] Davies, G. *Designing and Developing Scalable IP Networks*. 1st Edition. United Kingdom, John Wiley & Sons, 2004. ISBN 0-470-86739-6.

[55] Gustafsson, K. et al. *Mobile Broadband Backhaul Network Migration from TDM to Carrier Ethernet*. IEEE Communications Magazine, volume 48, issue 10, pp. 102-109, October 2010.

[56] Gildred, J. et al. *Synchronous Ethernet Specification Draft v0.39*. Cited in 24.7.2012. Available in http://grouper.ieee.org/groups/1394/c/20031216/Sync_ Ethernet_039a_draft.pdf.

[57] IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management, *IEEE Std 802.1ag-2007 (Amendment to IEEE Std 802.1Q - 2005 as amended by IEEE Std 802.1ad - 2005 and IEEE Std 802.1ak - 2007)*, pp.1-260, 2007. DOI 10.1109/IEEESTD.2007.4431836.

[58] IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges, *IEEE Std 802.1ad-2005 (Amendment to IEEE Std 802.1Q-2005)*, pp.1-74, May 26 2006. DOI 10.1109/IEEESTD.2006.6044678.

[59] IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks Amendment 7: Provider Backbone Bridges, *IEEE Std 802.1ah-2008 (Amendment to IEEE Std 802.1Q-2005)*, pp.1-110, Aug. 14 2008. DOI 10.1109/IEEESTD.2008.4602826.

[60] IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks Amendment 10: Provider Backbone Bridge Traffic Engineering, *IEEE Std 802.1Qay-2009 (Amendment to IEEE Std 802.1Q-2005)*, pp. c1-131, Aug. 5 2009. DOI 10.1109/IEEESTD.2009.5198465.

[61] Bar-Lev, D. et al. *Introduction to Circuit Emulation Services over Ethernet (white paper)*. Metro Ethernet Forum, 2004.

[62] Rosen, E. et al. *BGP/MPLS IP Virtual Private Networks (VPNs)*. RFC 4364, IETF, 2006. Available in http://tools.ietf.org/html/rfc4364.

[63] Andersson, I. et al. *Framework for Layer 2 Virtual Private Networks (L2VPNs)*. RFC 4664, IETF, 2006. Available in http://tools.ietf.org/html/rfc4664.

[64] Ericsson. *It all comes back to backhaul (white paper)*. Sweden, 2012. Available in http://www.ericsson.com/res/docs/whitepapers/WP-Heterogeneous-Networks-Backhaul.pdf.

[65] Next Generation Mobile Networks Alliance. *Small Cell Backhaul Requirements*. Germany, 2012. Available in http://www.ngmn.org/uploads/media/NGMN_ Whitepaper_Small_Cell_Backhaul_Requirements.pdf.

[66] Nokia Siemens Networks. *Deployment strategies for Heterogeneous Networks (white paper)*. Finland, 2012. Available in http://www.nokiasiemensnetworks. com/portfolio/products/small-cells.

[67] Alcatel-Lucent. Small Cell Solution (white paper). France, 2010. Available in http://www.thecom.co.il/files/wordocs/Small_Cells_Overview_Brochure.pdf.

[68] Next Generation Mobile Networks Alliance, home site. Cited in 25.7.2012. Available in http://www.ngmn.org/.

[69] Vainikainen, P. et al. *Feasibility Study of E-band Radio for Gigabit Point-to-Point Wireless Communications*. Finland, Aalto University, Department of Radio Science and Engineering, 2010.

[70] Li, Y. *E-band radios for LTE/LTE-Advanced mobile backhaul*. Integrated Nonlinear Microwave and Millimeter-Wave Circuits (INMMIC), 2010 Workshop, pp.84, 26-27 April 2010. DOI 10.1109/INMMIC.2010.5480132.

[71] Hansryd, J. and Eriksson, P. High-speed mobile backhaul demonstrators. Ericsson Review, issue 2, pp. 10-16, 2009.

[72] ABI Research. *Mobile Backhaul Market Analysis 2011*. September 2011.

[73] Kuo, F. et al. *Cost-Efficient Wireless Mobile Backhaul Topologies: An Analytical Study*. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, pp.1-5, 6-10 Dec. 2010. DOI 10.1109/GLOCOM.2010.5683870.

[74] Gruber, M. et al. *Topologies of wireless mesh networks with inband backhauling*. Personal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium, pp.2057-2062, 26-30 Sept. 2010. DOI 10.1109/PIMRC.2010.5671579.

[75] Chia, S. et al. *The next challenge for cellular networks: backhaul*. Microwave Magazine, IEEE, volume 10, issue 5, pp.54-66, August 2009. DOI 10.1109/MMM.2009.932832.

[76] Egeland, G. and Engelstad, P.E. *The reliability and availability of wireless backhaul mesh networks*. Wireless Communication Systems. 2008. ISWCS '08. IEEE International Symposium, pp.178-183, 21-24 Oct. 2008. DOI 10.1109/ISWCS.2008.4726042.

[77] IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)*, pp. c1-269, July 24 2008. DOI 10.1109/IEEESTD.2008.4579760.

[78] Kent, S. and Seo, K. *Security Architecture for the Internet Protocol*. RFC 4301, IETF, 2005. Available in http://www.ietf.org/rfc/rfc4301.txt.

[79] Houdley, R. *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP).* RFC 4309, IETF, 2005. Available in http://www.ietf.org/rfc/rfc4309.txt.

[80] Next Generation Mobile Networks Alliance. *Security in LTE backhauling.* Germany 2012. Available in http://www.ngmn.org/uploads/media/NGMN_ Whitepaper_Backhaul_Security.pdf.

[81] 3GPP Self-Organizing Networks. Cited in 28.7.2012. Available in http://www. 3gpp.org/SON.

[82] Next Generation Mobile Networks Alliance. *NGMN Use Cases related to Self Organising Network, Overall Description*. Germany, 2008. Cited in 28.7.2012. Available in http://www.ngmn.org/uploads/media/NGMN_Use_Cases_related_ to_Self_Organising_Network__Overall_Description.pdf.

[83] Next Generation Mobile Networks Alliance. *NGMN Recommendation on SON and O&M Requirements*. Germany, 2008. Cited in 28.7.2012. Available in http://www.ngmn.org/uploads/media/NGMN_Recommendation_on_SON_and_O_M_Requirements.pdf.

[84] Akyildiz, I. F. and Wang, X. *Wireless Mesh Networks*. 1st Edition. United Kingdom, John Wiley & Sons, 2009. ISBN 978-0-470-03256-5.

[85] Advanced wireless networks. Cited in 2.8.2012. Available in http://wiki.mikrotik.com/wiki/Testwiki/Advanced_MikroTik_Wireless_networks

[86] Seppänen, K. et al. *State-of-the-art of routing and medium access control in directional wireless mesh networks*. RAPTor WP 5.5, 2009.

[87] Seppänen, K. et al. *Architectural definition and requirements specification for routing and MAC scheduling in directional WMN*. RAPTor WP 5.5, 2009.

[88] Seppänen, K. et al. *Detailed specification of directional WMN protocols and algorithms*. DiMeRA WP 1.2, 2010.

[89] Seppänen, K. et al. *Analysis of directional WMN algorithms*. DiMeRA WP 1.3, 2010.

[90] Rawlins, G. J. E. *Foundations of Genetic Algorithms*. 1st Edition. United States of America, Morgan Kauffmann Publishers, Inc., 1991. ISBN 1-55860-170-8.

[91] Chambers, L. D. Practical Handbook of Genetic Algorithms, Complex Coding Systems, Volume 3. 1st Edition. United States of America, CRC Press, 1999. ISBN 0-8493-2539-0.

[92] Miettinen, K. et al. *Evolutionary Algorithms in Engineering and Computer Science*. 1st Edition. United Kingdom, John Wiley & Sons, 1999. ISBN 0-471-99902-4.

[93] Seppänen, K. et al. *Wireless Mesh Network, Algorithm Update*. MEVICO WP 3.2, 2012.

[94] Seppänen, K. et al. *Analysis of existing ToP standards for WMN internal clock synchronization and time signal distribution*. DiMeRTS, 2011.

[95] Lanner Electronics Inc. home site. Cited in 14.6.2012. Available in www.lannerinc.com.

[96] Portwell, home site. Cited in 14.6.2012. Available in www.portwell.com.

[97] Caswell Inc. home site. Cited in 14.6.2012. Available in www.cas-well.com.

[98] Cavium Networks Octeon Plus CN52XX network processor. Cited in 14.6.2012. Available in http://www.cavium.com/OCTEON-Plus_CN52XX.html.

[99] Precision Time Protocol daemon, home site. Cited in 14.6.2012. Available in http://ptpd.sourceforge.net/.

[100] Spirent TestCenter, home site. Cited in 15.6.2012. Available in http://www.spirent.com/Solutions-Directory/Spirent-TestCenter/EnterpriseAndDataCenterNetworks.

[101] Wireshark network protocol analyzer, home site. Cited in 15.6.2012. Available in http://www.wireshark.org/.

[102] Vconfig, VLAN configuration program, home site. Cited in 16.6.2012. Available in http://linux.die.net/man/8/vconfig.

[103] Ifconfig, network interface configuration program, home site. Cited in 16.6.2012. Available in http://linux.die.net/man/8/ifconfig.

[104] Bradner, S. and McQuaid, J. *Benchmarking Methodology for Network Interconnect Devices.* RFC 2544, IETF, 1999. Available in http://www.ietf.org/rfc/rfc2544.txt.

[105] Hickman, B. et al. *Benchmarking Methodology for Firewall Performance.* RFC 3511, IETF, 2003. Available in http://www.ietf.org/rfc/rfc3511.txt.

[106] ITU-T Recommendation G.114. *One-way transmission time*. Cited in 28.7.2012. Available in http://www.itu.int/rec/T-REC-G.114-200305-I/en.

[107] IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Std 802.11i-2004*, pp. 1-175, 2004. DOI 10.1109/IEEESTD.2004.94585

[108] Celtic-Plus initiative, home site. Cited in 5.8.2012. Available in http://www.celtic-initiative.org/.