Small Cell Wireless Backhaul in Mobile Heterogeneous Networks

PAVEL LEGONKOV
and
VASILY PROKOPOV

KTH Information and Communication Technology

Degree project in
Communication Systems
Second level, 30.0 HEC
Stockholm, Sweden

Small Cell Wireless Backhaul in Mobile Heterogeneous Networks

Pavel Legonkov and Vasily Prokopov

Master of Science Thesis

Communication Systems
School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden

July 4, 2012

Examiner: Professor G. Q. Maguire Jr.

Abstract

Small cells are deployed in a crowded areas with a high demand for both coverage and capacity. It is hard to address both of these requirements simultaneous with a conventional mobile network architecture based on macro cells. In many case a wire is not available to connect the small cell to the core of the mobile network. Under these circumstances a wireless link could be a convenient solution for the backhaul.

In this master's thesis IEEE 802.11n technology was evaluated to assess its suitability for backhaul from a small wireless cell. The performance of wireless equipment manufactured by several vendors has been measured. The results of these measurements were analyzed and compared to a set of requirements established for small cell backhaul. The analysis has affirmed that IEEE 802.11n is capable of providing sufficient performance to be used for small cell backhaul in various deployment scenarios. Note that in this thesis we include femtocells, picocells, wireless LAN access points, and other technologies in the category of "small cells".

Another research questions of this master's thesis is security of small cell backhaul. In addition to protecting the backhaul link itself, the security research investigated the safety of the whole mobile network architecture remodeled with the introduction of small cells. A mechanism to integrate secure small cells into a mobile network was developed.

The results obtained during the project will be used as an input for product development activities in the company hosting the project. The resulting product could become the target of future wireless system performance measurements.

Sammanfattning

Små celler sätts ut i områden med höga krav på täckning och kapacitet. Det är svårt att adressera båda dessa krav samtidigt med en konventionell mobil nätverksarkitektur baserad på makro-celler. I många fall finns ingen kabel tillgänglig att koppla den lilla cellen till kärnan i det mobila nätverket. Under dessa omständigheter kan en trådlös länk vara en lämplig lösning för backhaul.

I denna avhandling utvärderas IEEE 802.11n-teknikens lämplighet för backhaul av små celler. Prestandan hos trådlös utrustning tillverkad av flera olika tillverkare har mätts. Resultaten av dessa mätningar analyserades och jämfördes med en mängd krav uppsatta för backhaul av små celler. Analysen har förankrat att IEEE 802.11n är kapabel till att tillhandahålla tillräcklig prestanda för backhaul av små celler i diverse miljöer. Notera att i denna avhandling så inkluderas femto-celler, pico-celler, Wireless LAN-åtkomstpunkter, och andra teknologier i kategorin små celler".

Andra forskningsfrågor berörda i avhandlingen är säkerhet vid backhaul av små celler. Utöver att skydda backhaul-länken själv så undersökte säkerhetsforskningen säkerheten av hela mobilnätsarkitekturen när små celler används i arkitekturen. En mekanism för att integrera säkra små celler i ett mobilnät utvecklades.

De resultat som införskaffades under projektets genomförande kommer att användas som input till produktutvecklingsaktiviteter hos företaget som sponsrade projektet. Den resulterande produkten skulle kunna bli mål för framtida prestandamätningar av trådlösa system.

Acknowledgements

We would like to express our gratitude to the people we were closely working with during this master's thesis project, namely:

Annikki Welin, our supervisor at Ericsson, for her general project management, providing ideas, resolving technical and organizational issues, organizing meetings with people interested in the results of the project, providing the equipment, arranging our work space, taking us to the corporate parties, and helping in every aspect of this work.

Professor **Gerald Q. Maguire Jr.**, our academic supervisor at KTH, for guiding us through the project, providing valuable ideas, and generating extremely helpful feedback.

Kenneth Sandberg for presenting radio theory fundamentals, providing support during radio measurements, and help during our analysis of the results.

Tomas Thyni for asking challenging questions, motivating us to dig deeper, and for explaining the security aspects of picocell network integration.

Jaume Rius I Riu for being helpful through all stages of the project, resolving funding issues, providing feedback on the report and presentations, and sharing project-related reading material.

Per Sjöberg, who provided the lab with a shielded room for the measurements, and helped to create the antenna radiation diagrams.

Contents

1 Introduction **1**
1.1 Overview . . . 1
1.2 Problem description . . . 2
1.3 Aim, goal and sub-goals . . . 4
1.4 Structure of this thesis . . . 4
1.5 Methodology . . . 5

2 Background **7**
2.1 Mobile heterogeneous networks . . . 7
2.2 Wireless technologies . . . 8
2.2.1 UMTS and LTE . . . 8
2.2.2 IEEE 802.11n . . . 11
2.2.2.1 MIMO . . . 12
2.2.2.2 MCS . . . 12
2.2.2.3 Channel width . . . 12
2.2.3 IEEE 802.11s . . . 14
2.3 Security . . . 15
2.3.1 IPsec protocol suite . . . 15
2.3.2 IKEv2 . . . 16
2.3.3 CAPWAP over DTLS . . . 18
2.3.4 3GPP security architectures . . . 19
2.4 Related work . . . 22

3 IEEE 802.11n as backhaul for a small cell **25**
3.1 Constrains and limitations . . . 25
3.2 Performance requirements . . . 26
3.2.1 Throughput requirements . . . 26
3.2.2 Latency and jitter requirements . . . 30
3.3 Experimental study . . . 32
3.3.1 Goals . . . 32
3.3.2 Equipment . . . 33

3.3.3 Measurement scenarios 33
3.3.4 Results and analysis 38
3.3.4.1 Theoretical and practical peak throughput . . . 38
3.3.4.2 Switching fabric limitations 40
3.3.4.3 Maximum distance 42
3.3.4.4 Modulation and coding schemes 42
3.3.4.5 MIMO modes 43
3.3.4.6 Channel bandwidth 44
3.3.4.7 Antenna types 44
3.3.4.8 Interference measurement scenario 45
3.3.4.9 Indoor measurement scenario 46
3.4 Conclusions 47

4 Secure integration of a small cell into a modern cellular system 49
4.1 Problems 49
4.2 Proposed security mechanism 51
4.3 Conclusions 53

5 General conclusions and future work 55
5.1 General conclusions 55
5.2 Future work 56
5.3 Social, economic, ethical, and environmental issues 57

Bibliography 59

A Experimental study results 65

B TDMA wireless backhaul performance measurements results 83

List of Figures

2.1 The interworking architecture of UMTS and LTE 9
2.2 IPsec headers for tunnel and transport modes of operation 16
2.3 IKEv2 operation 17
2.4 CAPWAP session establishment 19
2.5 System architecture of HeNB 20
2.6 3GPP WLAN interworking 21

3.1 Wireless technologies supported by a picocell 26
3.2 Simplified small cell network topology 31
3.3 Point-to-point measurement scenario 34
3.4 Interference measurement scenario 35
3.5 Indoor measurement scenario 36
3.6 Peak data rates obtained on the tested IEEE 802.11n devices . . . 39
3.7 Large frame against IMIX 41
3.8 MCS scheme as a function of RSSI for Vendor A 43
3.9 Peak throughput for different MIMO modes for Vendor A 44

4.1 Remote picocell deployment network architecture 50
4.2 Call-flow of a secure connection establishment 51

List of Tables

2.1 Data rates for different MCSs used in IEEE 802.11n 13

3.1 Peak theoretical throughput of LTE and IEEE 802.11n 27
3.2 Average and peak LTE macro cell throughput rates 28
3.3 Calculated throughput rates for an LTE small cell backhaul 28
3.4 Technical specifications of the APs used in the measurements . . . 33
3.5 Variables changed during the measurements 35
3.6 Interference measurements: configurations and results 45

A.1 Measurement results for Vendor A, point-to-point scenario, cables, 3x3 MIMO, 40 MHz channel 66
A.2 Measurement results for Vendor A, point-to-point scenario, cables, 2x2 MIMO, 40 MHz channel 67
A.3 Measurement results for Vendor A, point-to-point scenario, cables, 1x1 MIMO, 40 MHz channel 68
A.4 Measurement results for Vendor A, point-to-point scenario, cables, 3x3 MIMO, 20 MHz channel 69
A.5 Measurement results for Vendor A, point-to-point scenario, cables, 2x2 MIMO, 20 MHz channel 70
A.6 Measurement results for Vendor A, point-to-point scenario, cables, 1x1 MIMO, 20 MHz channel 71
A.7 Measurement results for Vendor A, point-to-point scenario, small panel antenna, 3x3 MIMO, 40 MHz channel 72
A.8 Measurement results for Vendor A, point-to-point scenario, small panel antenna, 2x2 MIMO, 40 MHz channel 73
A.9 Measurement results for Vendor A, point-to-point scenario, big panel antenna, 2x2 MIMO, 40 MHz channel 74
A.10 Measurement results for Vendor B, point-to-point scenario, cables, 2x2 MIMO, 40 MHz channel 75
A.11 Measurement results for Vendor B, point-to-point scenario, cables, 1x1 MIMO, 40 MHz channel 76

A.12 Measurement results for Vendor B, point-to-point scenario, cables, 2x2 MIMO, 20 MHz channel 77
A.13 Measurement results for Vendor B, point-to-point scenario, cables, 1x1 MIMO, 20 MHz channel 78
A.14 Measurement results for Vendor B, point-to-point scenario, small panel antenna, 2x2 MIMO, 40 MHz channel 79
A.15 Measurement results for Vendor B, point-to-point scenario, big panel antenna, 2x2 MIMO, 40 MHz channel 80
A.16 Measurement results for the interference scenario 81

B.1 Measurement results for Vendor C, point-to-point scenario, cables, 2x2 MIMO, 40 MHz channel 84
B.2 Measurement results for Vendor C, point-to-point scenario, internal antenna, 2x2 MIMO, 40 MHz channel 85

List of Acronyms and Abbreviations

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AC	access controller
AH	Authentication Header
AP	access point
BER	bit error rate
BICN	Bearer-Independent Core Network
BPSK	binary phase-shift keying
BSS	Basic Service Set
CAPWAP	Control And Provisioning of Wireless Access Points
CFG	Configuration
CSMA/CA	carrier sense multiple access with collision avoidance
DCF	distributed coordination function
DCH	Duall Channel
DCH-IPT	Dual Channel Intermittent Periodic Transmit
DHCP	Dynamic Host Configuration Protocol
DL	downlink
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions

DSL	digital subscriber line
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement
EAP-SIM	Extensible Authentication Protocol Method for GSM Subscriber Identity Module
eNB	evolved NodeB
EPC	Evolved Packet Core
ESP	Encapsulating Security Payload
ESS	Extended Service Set
eUTRAN	evolved UTRAN
FPS	frames per second
GGSN	Gateway GPRS Support Node
H(e)MS	H(e)NB Management System
HeNB	Home evolved NodeB
H(e)NB	Home NodeB or Home eNodeB
HLR	Home Location Register
HNB	Home NodeB
HSS	Home Subscriber Server
IKE	Internet Key Exchange
IM	Instant Messaging
IMIX	Internet Mix
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Number

IPT	Intermittent Periodic Transmit
ISAKMP	Internet Security Association and Key Management Protocol
ITU-T	ITU Telecommunication Standardization Sector
LAN	local area network
LGI	long guard interval
LOS	line-of-sight
LTE	3GPP's Long Term Evolution
LQM	link quality metric
MBSS	Mesh BSS
MCS	modulation and coding scheme
MIMO	multiple-input and multiple-output
MME	Mobile Management Entity
MNO	Mobile Network Operator
NAT	network address translation
NAT-T	NAT traversal
NGMN	Next Generation Mobile Networks
NLOS	non-line-of-sight
OAM	Operation, Administration and Maintenance
OSI	Open Systems Interconnection
PDG	Packet Data Gateway
PDN	Packet Data Network
P-GW	PDN Gateway
PLMN	Public Land Mobile Network
PLPC	physical layer convergence procedure
POP	point of presence

PPB	parts-per-billion
PPS	packets per second
QAM	quadrature amplitude modulation
QoS	Quality of Service
QPSK	quadrature binary phase-shift keying
QR	Quick Response
RA	Registration Authority
RADIUS	Remote Authentication Dial In User Service
RAN	radio access network
RBS	Radio Base Station
RNC	Radio Network Controller
RSSI	Received Signal Strength Indicator
SA	Security Association
SCH	Single Channel
SeGW	Security Gateway
SFTP	SSH File Transfer Protocol
SGI	short guard interval
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SIM	Subscriber Identity Module
SNR	signal-to-noise ratio
SSPN	Subscription Service Provider Network
TCP	Transmission Control Protocol
TDMA	time division multiple access
TLS	Transport Layer Security

UDP	User Datagram Protocol
UE	User Equipment
UL	uplink
UMTS	Universal Mobile Telecommunications System
URI	uniform resource identifier
USIM	UMTS Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VoIP	voice over IP
WAG	WLAN Access Gateway
WCDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	wireless LAN
WTP	wireless termination point

Chapter 1

Introduction

This chapter presents a brief introduction to the research area along with a description of the problems addressed by this master's thesis. The project's aim, goal, sub-goals and research methodology are described as well.

1.1 Overview

The number of mobile broadband subscribers continues to grow at a tremendous rate. The number of mobile subscribers is expected to reach 3.5 billion by 2015 [1]. This growth is accompanied by a substantial increase in mobile traffic. Ericsson has predicted a tenfold increase in mobile traffic by 2016 as compared to 2011 [2]. Cisco expects an increase in the overall mobile data traffic of 10.8 exabytes **per month** by 2016 [3].

To satisfy these demands a new generation of mobile networks is being rapidly deployed by mobile operators. Deployment of 3GPP's Long Term Evolution (LTE) is becoming more and more ubiquitous. By January 2012 as many as 33 commercial deployments of LTE standard have been made around the globe [4]. However, even the advances offered by LTE are unable to cope with growing demands for capacity and increased data throughput. Here we should note that capacity is measured in terms of the aggregate traffic for a cell, thus it is proportional to the number of users times their data rates. With both the number of users (which increasingly includes various devices and not simply human users) and their data rates increasing the capacity must improve even faster than the increase in data rates!

Mobile operators are finding it hard to provide sufficient data rates from the cellular base stations to their core network and to ensure mobile service availability within densely populated areas, such as shopping centers and transportation terminals. The traditional macro cell oriented mobile network architecture does not suit these environments. In order to provide services to a large number of subscribers in a small area there should be many cells, thus dividing the users and their data traffic over these different cells. Moreover, it is quite expensive to deploy macro base stations within dense underlays. Additional constraints include the lack of appropriate locations meeting the requirements for macro base station deployment, e.g. a sufficient supply of power, cooling, physical space, and site security.

To meet the demands for capacity and throughput dictated by the exponential growth of traffic volumes and subscribers the architecture of the existing radio access networks (RANs) should be reconsidered and enhanced. As of today, a number of solutions have been proposed to improve RANs. For example, Landström, *et al.* propose [5]:

- Improving the macro layer by upgrading the radio access technology (e.g. upgrading from Universal Mobile Telecommunications System (UMTS) to LTE) and utilizing increased allocations of spectrum.
- Increase the density of the macro layer by increasing the number of macro base station sites.
- Complementing the RAN with small cells such as femtocells, picocells, and Wi-Fi access points.

The last option, also referred to as a heterogeneous network, is currently considered the most promising way of increasing both capacity and throughput. The advantage of small cells is that they could be deployed in a self-organizing manner at literally any location. An additional advantage is that these small cells can be located near where the users actually are.

1.2 Problem description

> It isn't that they can't see the solution. It's that they can't see the problem.
>
> G. K. Chesterton [6]

Migration towards a heterogeneous network architecture by complementing a homogeneous mobile network with small cells brings a set of new challenges to defeat and demands to fulfill.

The main aspects that should be reconsidered when introducing a heterogeneous network architecture arise from its nature. Deployment of a heterogeneous network assumes that it is possible to deploy a small cell in an **unprepared** location. Typical installation points of these small cells are the lampposts, building walls, and utility poles. This is quite different from the traditional approach used when deploying a macro cell oriented mobile networks as in this approach the base station is deployed at preplanned and carefully prepared installation site.

Since the small cell deployment site is not usually prearranged, there seldom is a wire for connecting the small cell to the core of the mobile network. Moreover, even having a wire in place is not always helpful since within the coverage area of one macro cell tens of small cells could be deployed. In such a case the number of required backhaul links is multiplied leading to scalability issues and potentially increasing the installation and operating expenses. And if the move to smaller cells is viewed as panacea regarding the coverage and capacity problems, it instantly creates another problem - how to provide suitable backhaul from all of these small cells.

In many cases a **wireless** link could be a convenient backhaul solution. However, wireless backhaul introduces such problems as spectrum allocation, radio interference, and line-of-sight (LOS) availability. Since LOS is not always available, non-line-of-sight (NLOS) technologies may need to be considered. The major question is which wireless technology among the set of available options is the optimal technology for small cell backhaul. To answer this question a specific set of evaluation metrics should be developed representing the requirements imposed on the small cell backhaul.

In addition, bringing a small cell physically closer to the actual mobile user raises new security issues. Small cells could be deployed literally anywhere, which means that sometimes the backhaul link may traverse an insecure transport network, e.g. the Internet. This change in the physical deployment of small cells leads to a set of security-related issues including secure backhaul connection establishment, cell discovery and authentication, and key distribution.

As of today, various vendors have developed their own proprietary mechanisms for deployment of the small cells which cover all or at least some of the aspects described above. However, there is no widely adopted industry standard for small cell deployment in heterogeneous networks. The diversity in implementations of heterogeneous networks raises questions of vendor interoperability and technology transparency. Lack of interoperability is viewed negatively by network operators as they believe that it can lead to vendor lock-in and higher costs. The lack of technology transparency is expect to hinder the development of new technology in the area of small cells, which could lead to increased development times and could delay the introduction of the new technology that is needed to solve the capacity and data rate demands.

1.3 Aim, goal and sub-goals

This master's thesis project was conducted in cooperation with Ericsson. One of the intentions of the company is to be a strong player in the field of mobile heterogeneous networks. To achieve this goal there is a need for a solution to the problems of small cell deployment. Consequently, the aim of this master's thesis project is to provide the company with the basis for its heterogeneous network solution which should enable smooth and secure integration of small cells into a generic modern mobile network.

Moving from general to specific goals, the goal of this thesis project can be split into two parts. The first is to investigate if the IEEE 802.11n standard is suitable for use as small cell backhaul. The second part is to propose a mechanism for secure integration of small cells into the existing LTE and Advanced LTE mobile network architecture. It is important to note that the integration is with modern network and not legacy networks, therefore a packet oriented solution is quite suitable.

The following activities are identified as the project's deliverables, hence they can be used as indicators of successful project completion:

- Conduct performance measurements of a IEEE 802.11n backhaul link under various conditions. Analyze the results and assess how suitable the IEEE 802.11n standard is small wireless cell backhaul. Under which specific conditions is it able to provide sufficient performance.

- Propose a secure mechanism of integrating a small cell into the existing modern mobile network architecture.

1.4 Structure of this thesis

Chapter 1 introduces the topic of the master's thesis, describes the problem and its context, and specifies the aim and goal of this work.

Chapter 2 lays the foundation required to understand the problem, describes the activities undertaken during the experimental study, and presents the results of the study. This chapter describes wireless architectures and security concerns due to the advent of the heterogeneous network paradigm. Finally, related work is presented and analyzed in this chapter.

Chapter 3 describes the experimental study of a IEEE 802.11n wireless link's performance. Initially a set of performance requirements for a small cell backhaul is defined. Following this an analysis of the data obtained during the experimental study is done. Finally, some conclusions are drawn as to whether the IEEE 802.11n backhaul meets the stated performance requirements.

In Chapter 4 a secure mechanism to integrate a small cell into an existing modern mobile network is proposed.

Conclusions and future work suggestions are provided in Chapter 5, which completes the thesis.

1.5 Methodology

This master's thesis project incorporates both quantitative and qualitative research techniques. The first part of the research is of a quantitative nature. It is conducted with an experimental approach which is applicable when a theoretical analysis is inadequate or unfeasible. We chose an experimental approach because there was no theoretical basis to achieve the goal and sub-goals identified above. The research question and evaluation metrics in form of performance requirements are identified, then an experimental study is conducted. We have chosen an iterative process, so that we can refine our solution incrementally (hence we initially aimed for functional correctness and then could tune for increased performance). In the final step the collected data is analyzed and evaluated against the stated requirements in order to provide an answer for the posed research question.

The second part of this master's thesis is based on a qualitative research methodology. We use a design-based research approach in which new knowledge is obtained through the process of designing and building an artifact. In our case the artifact refers to a proposed algorithm or mechanism for securely integrating a picocell into a modern mobile network. First, a set of problems associated with a particular deployment case is defined. Then a literature study regarding the identified deployment case and the relevant issues was conducted. Finally, a conceptual solution in form of step-by-step procedure is proposed. The actual implementation of these steps is outside the scope of this thesis and will be the topic of a product development effort within the company.

Chapter 2

Background

This chapter provides the background knowledge required to understand the research that was conducted. A reader is introduced to the concept of heterogeneous networks, then a brief description of several wireless architectures is provided. Finally, related research performed in the area is presented.

2.1 Mobile heterogeneous networks

A mobile heterogeneous network is a wireless access network that consists of different types of access nodes (base stations or access points). These nodes differ in their size, power, coverage, and capacity. Specifically in a wide area cellular network a homogeneous network refers to use of a standard RAN consisting only of macro base stations. If the RAN is complemented by low power nodes, such as femtocell access points, picocell base stations, and/or Wi-Fi access points, then we refer to this as a small cell heterogeneous network.

Depending on the type of low power nodes deployed, we can differentiate between three major alternative implementations of heterogeneous networks:

- 3G/LTE data offload using Wi-Fi access points,
- Home or enterprise femtocell implementation, and
- Picocell deployment.

Wi-Fi data offloading corresponds to deployment of Wi-Fi hotspots and integrating this wireless LAN (WLAN) into the mobile operator's network. Note that it may be possible to incorporate this WLAN into multiple operators' networks, but we will not consider this possibility further in this thesis. Depending on the provider's configuration specific types of traffic can be offloaded to this WLAN via a terminal's Wi-Fi interface. In most current implementations Wi-Fi data offloading is used to offload traffic for Internet services (as opposed to real-time services such as voice).

A femtocell targets home and enterprise deployments using cable TV or digital subscriber line (DSL) Internet access as a backhaul transport network to connect the femtocell with the mobile operator's network. The key characteristics of a femtocell access point are relatively small coverage area, support of 3 to 16 simultaneous subscribers, and auto-configuration [7]. Femtocell deployment provides data offload from the macro layer of the operator's mobile network, improving the macro cellular network's effective capacity, and providing better indoor coverage.

A picocell is mainly targeted for deployment in densely populated areas, such as shopping malls and transportation terminals. Compared to femtocells, picocells cover a larger area and support more subscribers. However, this comes at a cost of manual installation and configuration by the network operator (or a contractor working for them).

2.2 Wireless technologies

Since small cells are targeted for deployment together with modern mobile networks, some basic aspects of UMTS, LTE, and Wi-Fi will be described. The architecture of these three mobile technologies, as well as their main functional components, is described in this section.

2.2.1 UMTS and LTE

According to Sauter [8], from a technical standpoint the improvements that UMTS brings to legacy mobile systems are a redesigned RAN - the Universal Terrestrial Radio Access Network (UTRAN), Bearer-Independent Core Network (BICN), and IP Multimedia Subsystem (IMS).

LTE introduces multicarrier and multi-antenna technologies to the RAN, which is now referred to as the evolved UTRAN (eUTRAN). Additionally, packet switching is now applied to the radio interface. The core network is now completely based upon a packet-switched network (i.e., there is no longer any circuit switched domain within the core network). This core network is referred to as the Evolved Packet Core (EPC). According to Sesia *et al.*, LTE is the first completely packet-oriented multiservice mobile system [9].

In order to highlight the architectural differences and similarities between UMTS and LTE consider the interworking architecture of these two technologies as shown in Figure 2.1.

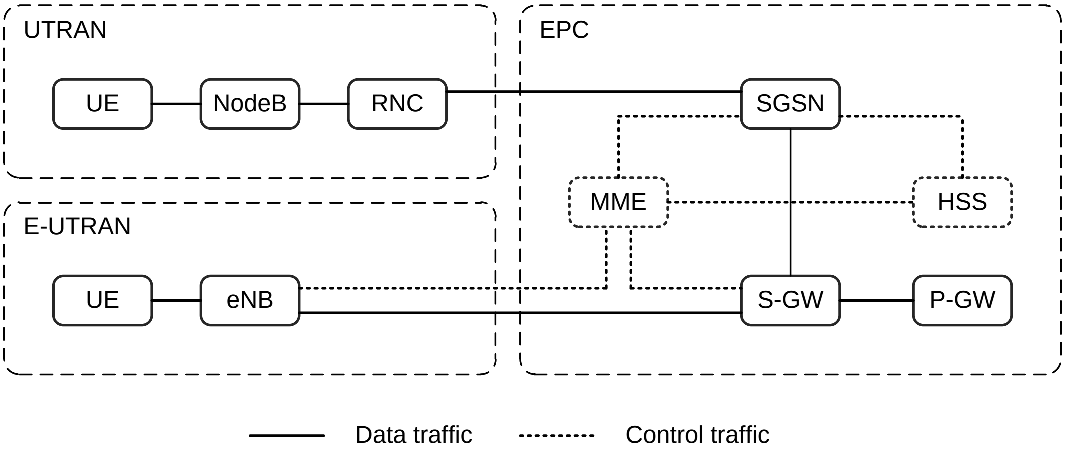


Figure 2.1: The interworking architecture of UMTS and LTE

Let us focus first on the UMTS radio access network - UTRAN. UTRAN has the following functional components:

- NodeB, a UMTS radio base station, which is responsible for sending and receiving data over the air interface.
- Radio Network Controller (RNC), which aggregates NodeBs, terminates radio network interfaces and provides backhaul to the core network.

In comparison the eUTRAN, the radio network of LTE, has only one architectural component besides the User Equipment (UE). This is a base station, referred to as an evolved NodeB (eNB). Unlike UMTS, where the NodeB operates under the control of a RNC, the eNB is an autonomous unit. Hence, the eNB handles not only the radio interface, but also insures Quality of Service (QoS) and performs mobility and interference management. To support such autonomy LTE base stations have an X2 interface to directly communicate with each other. Two of the main purposes of this X2 interface are UE handover and interference management.

This thesis project will not separately consider the core networks of UMTS and LTE, but rather will consider the combined interworking architecture as shown in Figure 2.1.

The functional components of the combined UMTS/LTE interworking core network are:

- Mobile Management Entity (MME), which from the core network's perspective controls the eUTRAN;
- Serving GPRS Support Node (SGSN), which controls the UTRAN;
- Serving Gateway (S-GW), which forwards end-user data flows;
- PDN Gateway (P-GW) acting as a gateway to external networks; and
- Home Subscriber Server (HSS), which manages user data and subscription information.

Further details of the core network components will be given later. Note that the above discussion does not consider the UMTS Gateway GPRS Support Node (GGSN) and its connection to the SGSNs or to external networks as we will focus on a modern mobile network that has implemented EPC.

It is worth mentioning here that the MME performs several important functions, as described in [10]:

- S-GW and P-GW selection for an UE during initial attach and handover;
- Authentication of the UEs through interaction with the HSS;
- Access policy enforcement for an UE, such as authorization to use the operator's Public Land Mobile Network (PLMN) and enforcement of roaming restrictions; and
- Tracking and paging for UEs that are currently in idle mode.

The SGSN node is somewhat similar in its functions to the MME, but it serves subscribers attached through the UTRAN [10]. As stated above, the S-GW is responsible for end-user data packet forwarding. Additionally, the S-GW acts as a local anchor point when UE performs inter-eNB handover. The S-GW also tears down the data downlink path when the UE is in the idle state. The P-GW plays the role of a gateway and provides several services, such as connectivity to external Packet Data Networks (PDNs), IP address allocation for UEs, and packet filtering and QoS enforcement on a per context per UE basis.

Understanding the overall mobile network architecture is of importance because this architecture lays the foundation for understanding how low power nodes can be integrated into this architecture.

Another important issue of commercial networks is security. Since wireless communications could easily be eavesdropped by anyone within the range of the transmitter, the air interface should be secured. Both UMTS and LTE encipher the over the air communication. In general, the security architectures of these two are very similar. Both assume mutual authentication of the user to the network and the network to the user.

The user is represented by a UMTS Subscriber Identity Module (USIM) which securely stores an International Mobile Subscriber Number (IMSI) and a secret 128-bit long key. These two numbers are used during user authentication [11]. On behalf of the network the main node involved in authentication is the HSS, which generates a session cipher key and distributes it to all the involved parties in order to encrypt user traffic over the air.

Apart from the air interface enciphering, sometimes there is a need to secure the data flowing within the core network. While this issue was not addressed in GSM, it attracted attention during the development process of UMTS and LTE. The threat to the communication within the operator's network comes from two directions.

Firstly, situations where core network traffic has to traverse unsecured third-party IP networks are becoming more and more likely, for example in a remote low power node deployment scenario the low power node will need to communicate with the rest of the core network via an insecure network, thus making security of this communication a key-issue.

Secondly, migration to all-IP signaling and user plane transport makes the core network interfaces more open and accessible, and hence more vulnerable to eavesdropping in comparison to the circuit-switched traffic within GSM networks [11].

To address these security issues the 3rd Generation Partnership Project (3GPP) has developed specifications for securing intra-core and inter-core traffic. The relevant 3GPP security architectures are described in Section 2.3.4.

2.2.2 IEEE 802.11n

IEEE 802.11n is a member of the IEEE 802.11 family of standards. It amends the IEEE 802.11-2007 standard describing ways to improve performance and to secure wireless networks. The performance improvements were driven by the introduction of multiple-input and multiple-output (MIMO), the use of wider radio channels, utilization of more efficient modulation and coding schemes (MCSs), and support for frame aggregation [12]. A brief description of the enhancements introduced in IEEE 802.11n that are relevant to the investigation covered in this master's thesis is provided below.

2.2.2.1 MIMO

The main physical layer enhancement introduced in the IEEE 802.11n standard is the use of multiple transmit and receive antennas simultaneously. Such behavior is known as MIMO. IEEE 802.11n incorporates two forms of MIMO: spatial diversity and spatial multiplexing [13]. Using spatial diversity a single radio stream is transmitted from each transmitting antenna. The same single stream is received by the each of the receiving antennas. This makes it possible for the receiver to choose the signal with the best quality, thus spatial diversity improves data reliability, but does not provide any performance benefits.

Spatial multiplexing involves transmitting several independent radio streams concurrently, thus enabling the performance of a wireless channel to be improved. In this thesis the term MIMO will be used in relation to this spatial multiplexing to gain increased performance for a given channel bandwidth.

The peak theoretical throughput of an IEEE 802.11n system strictly depends on the MIMO mode and order. With spatial diversity the the peak data rate is 150 Mbps. With 2x2 spatial multiplexing (referred to as 2x2 MIMO) the peak theoretical throughput is twice as much: 300 Mbps. With 3x3 and 4x4 spatial multiplexing MIMO the data rates are 450 and 600 Mbps respectively.

2.2.2.2 MCS

MCS is value that represents the modulation, coding rate, and number of spatial streams. Depending on the link quality metrics (LQMs) an access point (AP) will choose an appropriate MCS in order to provide the best possible performance [14]. Table 2.1 lists the MCS values defined in the IEEE 802.11n standard and gives their corresponding modulation schemes, coding, and data rates. Different guard intervals are taken into account as well: a long guard interval (LGI) is 800 ns, while a short guard interval (SGI) is 400 ns.

2.2.2.3 Channel width

IEEE 802.11n allows operating within a 40 MHz channel. In theory, a 40 MHz channel can support twice as high data throughput as compared to the 20 MHz channel used by legacy Wi-Fi standards. In practice, as it will be empirically proven in Section 3.3, the data rate benefit is not so significant. Additionally, 40 MHz channels may be utilized in both: the 2.4 and 5 GHz frequency bands.

Table 2.1: Data rates for different MCSs used in IEEE 802.11n

MCS index	MIMO mode	Modulation	Coding rate	Data rate, Mbps			
				20 MHz		40 MHz	
				LGI	SGI	LGI	SGI
0	1x1	BPSK	1/2	6.5	7.2	13.5	15.0
1	1x1	QPSK	1/2	13.0	14.4	27.0	30.0
2	1x1	QPSK	3/4	19.5	21.7	40.5	45.0
3	1x1	QAM 16	1/2	26.0	28.9	54.0	60.0
4	1x1	QAM 16	3/4	39.0	43.3	81.0	90.0
5	1x1	QAM 64	2/3	52.0	57.8	108.0	120.0
6	1x1	QAM 64	3/4	58.5	65.0	121.5	135.0
7	1x1	QAM 64	5/6	65.0	72.2	135.0	150.0
8	2x2	BPSK	1/2	13.0	14.4	27.0	30.0
9	2x2	QPSK	1/2	26.0	28.9	54.0	60.0
10	2x2	QPSK	3/4	39.0	43.3	81.0	90.0
11	2x2	QAM 16	1/2	52.0	57.8	108.0	120.0
12	2x2	QAM 16	3/4	78.0	86.7	162.0	180.0
13	2x2	QAM 64	2/3	104.0	115.6	216.0	240.0
14	2x2	QAM 64	3/4	117.0	130.0	243.0	270.0
15	2x2	QAM 64	5/6	130.0	144.4	270.0	300.0
16	3x3	BPSK	1/2	19.5	21.7	40.5	45.0
17	3x3	QPSK	1/2	39.0	43.3	81.0	90.0
18	3x3	QPSK	3/4	58.5	65.0	121.5	135.0
19	3x3	QAM 16	1/2	78.0	86.7	162.0	180.0
20	3x3	QAM 16	3/4	117.0	130.0	243.0	270.0
21	3x3	QAM 64	2/3	156.0	173.3	324.0	360.0
22	3x3	QAM 64	3/4	175.5	195.0	364.5	405.0
23	3x3	QAM 64	5/6	195.0	216.7	405.0	450.0
24	4x4	BPSK	1/2	26.0	28.8	54.0	60.0
25	4x4	QPSK	1/2	52.0	57.6	108.0	120.0
26	4x4	QPSK	3/4	78.0	86.8	162.0	180.0
27	4x4	QAM 16	1/2	104.0	115.6	216.0	240.0
28	4x4	QAM 16	3/4	156.0	173.2	324.0	360.0
29	4x4	QAM 64	2/3	208.0	231.2	432.0	480.0
30	4x4	QAM 64	3/4	234.0	260.0	486.0	540.0
31	4x4	QAM 64	5/6	260.0	288.8	540.0	600.0

2.2.3 IEEE 802.11s

Wi-Fi is a widely used and well-documented technology with the goal of facilitating the interoperability of IEEE 802.11 based equipment. The basics of Wi-Fi and IEEE 802.11 can be found in any modern textbook on data communications. Here we will give an overview of the advanced amendment to the IEEE 802.11 family of standards, specifically: IEEE 802.11s, which deals with a Wi-Fi mesh.

IEEE 802.11s was created to elaborate a wireless mesh based upon Wi-Fi [15]. In the basic IEEE 802.11 standard it was possible to connect several Wi-Fi Basic Service Sets (BSSs) through another network to form an Extended Service Set (ESS). IEEE 802.11s makes it possible to connect together several BSSs wirelesly to construct a Mesh BSS (MBSS). In other terms, the wireless domain architecture shifts from a one-hop to a multi-hop forwarding paradigm. To support this shift IEEE 802.11s extends the data-plane and the control-plane frames with an additional mesh control field [16].

IEEE 802.11s proposes a new security architecture for wireless mesh networks. Instead of using traditional IEEE 802.11 encryption, a distributed approach based on pairwise key negotiation is imposed. This overcomes the IPsec scalability issue which requires establishing n(n-1)/2 tunnels in a mesh network. In a IEEE 802.11s mesh network it is required to establish merely (n-1) tunnels since only neighboring mesh stations negotiate pairwise keys. As a consequence, IEEE 802.11s mesh network does **not** provide end-to-end security, instead each link is independently secured. Broadcast traffic is encrypted using a separate key shared by all stations within a mesh domain. It should be noted that this is similar to the over-the-air encryption in GSM, UMTS, and LTE - where there is no end-to-end encryption - hence all of the traffic is in clear text in each of the network nodes. End points and applications that desire end-to-end have to implement this themselves.

2.3 Security

This section provides a brief background description of the security technologies that are part of the security architecture for integrating a small cell, as will be described in Section 4.2. The subsections give a brief explanation of protocols such as IPsec, IKEv2, Control And Provisioning of Wireless Access Points (CAPWAP), and Datagram Transport Layer Security (DTLS). Following this the 3GPP security architectures related to low power nodes are described.

2.3.1 IPsec protocol suite

IPsec is a protocol suite for providing security services on the IP level. Since an IPsec tunnel will be used for securing the picocell's backhaul connection, a short description of the IPsec architecture's building blocks is given in this subsection.

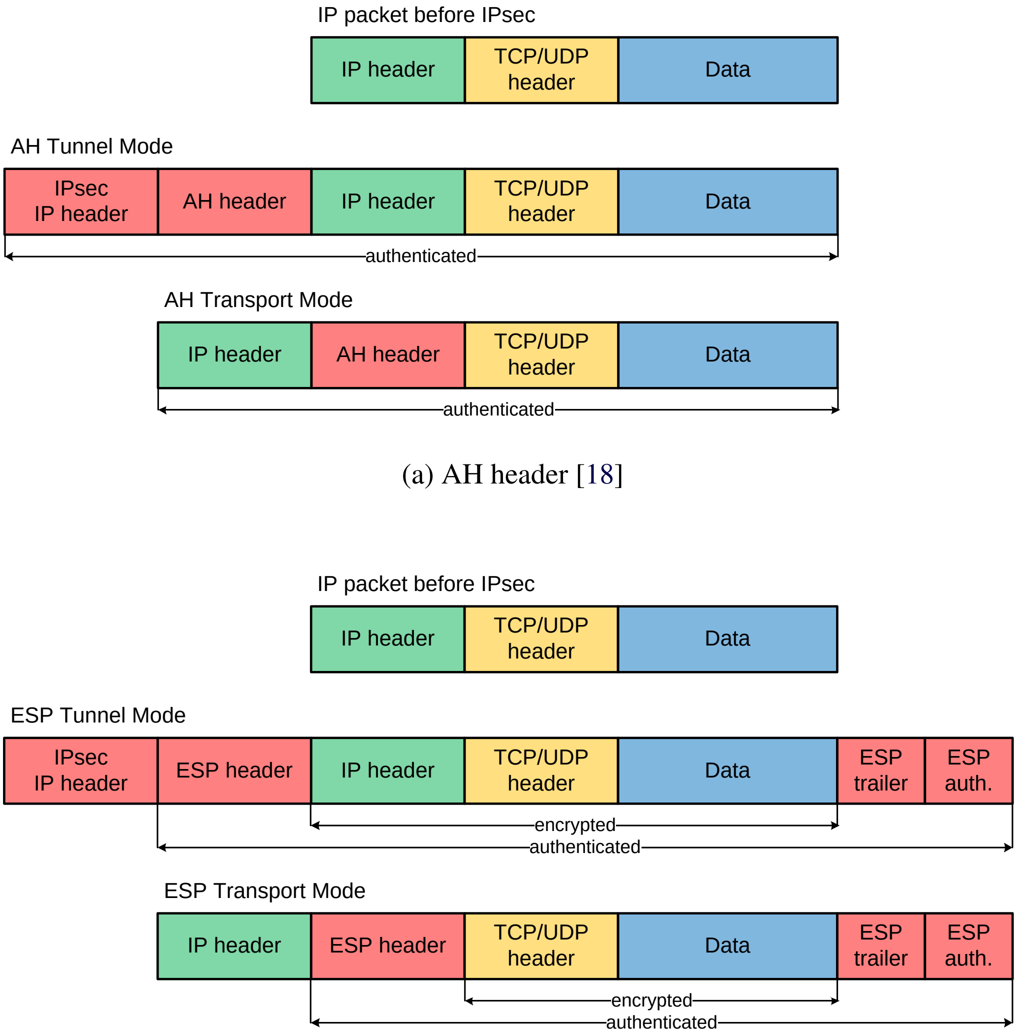
The IPsec protocol suite, as described in RFC 4301, consists of the following protocols [17]:

- Authentication Header (AH), which provides data integrity and data origin authentication services as well as anti-replay attack protection (see Figure 2.2a).

- Encapsulating Security Payload (ESP), which provides data confidentiality service in addition to the set of services provided by AH protocol (see Figure 2.2b).

- Internet Key Exchange (IKE) version 2, which is responsible for key exchange, security policy negotiation, and Security Association (SA) establishment.

An IPsec connection can be established in two modes: transport and tunnel. The main difference between these modes is the position of security protocol header with respect to the original IP packet header. In transport mode the ESP or AH header is inserted right after the IP header. However, in tunnel mode the ESP/AH header is inserted before IP header, thus providing security services for the whole original IP packet. In tunnel mode a new IP header is constructed. Typically, tunnel mode is used between two security gateways and transport mode is used between two end-hosts.



(a) AH header [18]

(b) ESP header [19]

Figure 2.2: IPsec headers for tunnel and transport modes of operation

2.3.2 IKEv2

One important aspect of the IPsec technology is understanding the process of secure connection establishment. An essential element in automating this process is the Internet Key Exchange (IKE) protocol. The current version of IKE is 2. IKE exchanges pairs of request/response messages [20]: IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA, and INFORMATIONAL. IKEv1 specified two phases of secure tunnel establishment, which IKEv2 does not refer to any more. However, IKEv2 exchanges can be mapped to the phases of IKEv1 to ease comprehension. Phase 1, which is also named the Internet Security Association and Key Management Protocol (ISAKMP) SA or IKE SA, includes the first two exchanges: IKE_SA_INIT and IKE_AUTH. The following processes happen during these exchanges [20]:

- Negotiation of a cryptographic suite for the use by the IKE security association,
- Exchange of nonces,
- Diffie-Hellman secret key exchange,
- Mutual authentication, and
- Establishment of the Child SA.

Phase 2 of IKEv1 (sometimes referred to as IPsec SA, ESP/AH SA, or Child SA) is mapped to the CREATE_CHILD_SA exchange. In this step new Child SAs are created if needed or previously created Child SAs and IKE SAs can be re-keyed. The last INFORMATIONAL exchange is mainly responsible for deleting existing SAs and reporting errors. Figure 2.3 depicts an example of the full IKEv2 process.

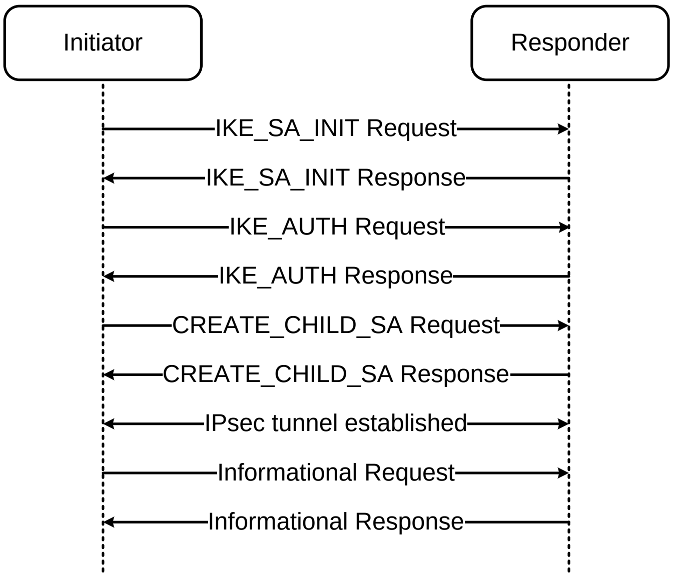


Figure 2.3: IKEv2 operation

2.3.3 CAPWAP over DTLS

Control And Provisioning of Wireless Access Points (CAPWAP) is defined in RFC 5415 [21]. CAPWAP is a protocol that allows an access controller (AC) to remotely configure and control a pool of wireless termination points (WTPs). The CAPWAP protocol does not depend on the underlying layer 2 technology, hence it can be used for various wireless technologies. Specific requirements for a particular wireless technology are defined in the wireless binding standards. The CAPWAP binding for IEEE 802.11 is described in RFC 5416 [22].

Communication between the AC and WTP is based on a typical client-server model. The User Datagram Protocol (UDP) is used as a transport protocol for CAPWAP messages. There are two types of CAPWAP messages. First is the CAPWAP Data message that encapsulates wireless frames for transport between the AC and WTPs. Second is the CAPWAP Control message which is used for management and monitoring of WTPs. On an AC, UDP port 5246 is used for control messages and UDP port 5247 for data messages. Any UDP port can be used by CAPWAP on the WTP's side. The process of CAPWAP connection establishment starts with a discovery phase which is based on a request-response mechanism. Each WTP sends a Discovery Request message in order to locate an AC. Every AC, that receives this request, responds with a Discovery Response message. Subsequently the WTP chooses from the available set of responses one AC in order to establish a secure connection.

The CAPWAP protocol does not provide built-in security mechanisms, rather to provide secure communication it relies on DTLS protocol [23]. DTLS was designed to provide security services, such as confidentiality and integrity for communications over datagram protocols. DTLS is based on the Transport Layer Security (TLS) protocol [24] that provides security services for Transmission Control Protocol (TCP) based connections. It is not possible to use TLS over UDP due to UDP's unreliable nature. For this reason DTLS was designed to overcome unreliability of UDP communication due to packet loss and packet reordering.

After a secure DTLS session is established, a configuration exchange process occurs between the AC and WTP. During this stage the AC supplies each WTP with its configuration settings and, if required, provides updated software. Once this phase is completed, wireless data frames between AC and WTP are encapsulated using the CAPWAP protocol. Figure 2.4 depicts the CAPWAP over DTLS session establishment process.

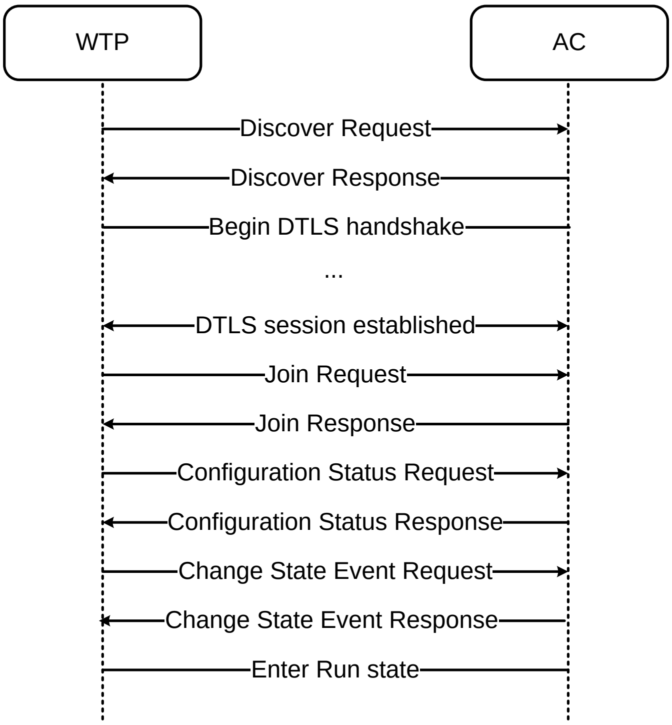


Figure 2.4: CAPWAP session establishment

2.3.4 3GPP security architectures

There are two 3GPP specifications related to a small cell security architecture. First specification *Security of Home NodeB (HNB) / Home evolved NodeB (HeNB)* [25], describes the deployment of a Home NodeB or Home eNodeB (H(e)NB) over an insecure network. This security architecture corresponds to the picocell deployment case, where an insecure transport path, such as the Internet, is used to backhaul the traffic. Figure 2.5 depicts a simplified system architecture of H(e)NB as mandated by 3GPP.

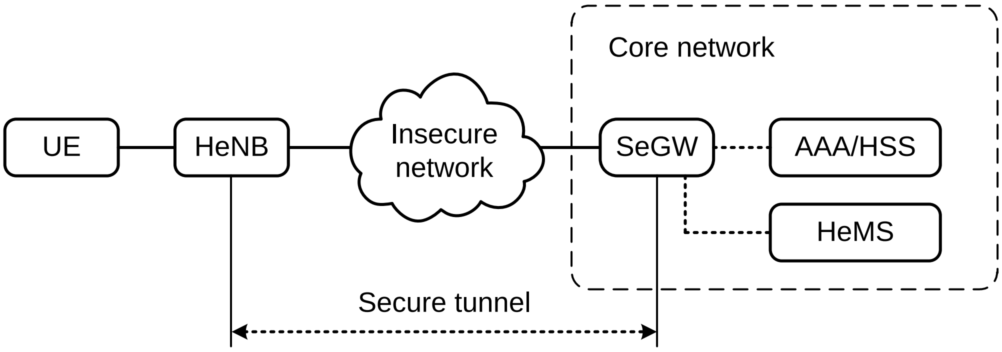


Figure 2.5: System architecture of HeNB

The key aspects of this security architecture that are relevant to our discussion are the following:

- The Security Gateway (SeGW) is the entry point into a mobile network's security domain, so the H(e)NB accesses the core network via the SeGW.
- The H(e)NB and SeGW must be mutually authenticated using their respective certificates.
- A Authentication, Authorization and Accounting (AAA) server is responsible for the authentication process based on information retrieved from a HSS.
- A secure tunnel is established over an insecure link between the H(e)NB and SeGW, so all communications between the H(e)NB and the core network are tunneled through the SeGW.
- Connections between the H(e)NB and its management system must also go through SeGW.
- The H(e)NB and H(e)NB Management System (H(e)MS) must be mutually authenticated.

3GPP recommends the use of the IPsec protocol in ESP tunnel mode for secure communication between the H(e)NB and SeGW. This tunnel should be established by using the IKEv2 protocol, as described in Section 2.3.2. The H(e)NB initiates the connection establishment process. If there is a network address translation (NAT) device in use, then a NAT traversal (NAT-T) mechanism should be configured. According to 3GPP [25], if based on the operator's security policy it is not possible to use the IPsec protocol for securing backhaul link, then appropriate layer 2 security protocols should be used instead. However, DTLS protocol can be used to secure the backhaul link as well.

The second specification that is related to a small cell security is *3G security; wireless LAN (WLAN) interworking security* [26]. This document describes the secure integration of WLANs into a mobile network. Modern picocells incorporate radio interfaces of both 3GPP access technologies, such as LTE and Wideband Code Division Multiple Access (WCDMA), and untrusted non-3GPP access technologies, such as the IEEE 802.11n standard. A small cell network has to comply with the 3GPP's WLAN interworking security architecture. Figure 2.6 presents a simplified view of 3GPP's WLAN interworking system architecture.

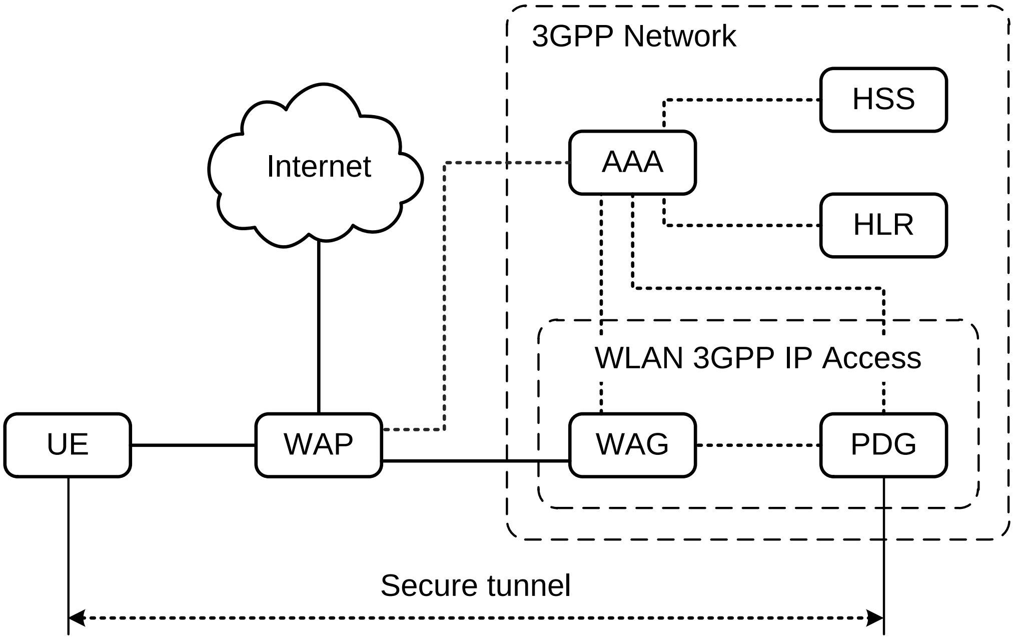


Figure 2.6: 3GPP WLAN interworking

This architecture introduces three new entities into the mobile core network:

- A 3GPP AAA server, either a Remote Authentication Dial In User Service (RADIUS) or Diameter server, is used to authenticate UEs to their 3GPP home network. Decisions are made based on the authentication information retrieved from Home Location Register (HLR) or HSS.

- A Packet Data Gateway (PDG) is responsible for authorization and secure tunnel establishment based on information obtained from a 3GPP AAA server.

- A WLAN Access Gateway (WAG) is commonly used as a firewall that filters the IP access of WLAN users.

3GPP WLAN interworking allows direct access to the Internet as well as an access to a mobile operator's IP services. Network access control in this architecture is based on the IEEE 802.1x standard [27], where the UE is a supplicant, the AP is an authenticator, and the 3GPP AAA server is an authentication server. 3GPP mandates support for the Extensible Authentication Protocol Method for GSM Subscriber Identity Module (EAP-SIM) and Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) by both the UE and AAA server. EAP-SIM and EAP-AKA are methods using the Extensible Authentication Protocol (EAP) framework to use information stored in the GSM Subscriber Identity Module (SIM) and UMTS USIM for the authentication and key agreement processes.

3GPP requires the use of IKEv2 and IPsec protocols for establishing tunnels and securing communication. In contrast with the security architecture for H(e)NB, IPsec tunnels must be established between every UE and a PDG device. There is no specific recommendations by 3GPP on the implementation of security mechanisms between the WAG and WLAN. The common practice is to use CAPWAP over DTLS as described in the previous section.

2.4 Related work

Similar work in terms of IEEE 802.11n performance assessment was done by Shrivastava *et al.* in [28]. However, the main emphasis of their work was to evaluate the performance benefits that each of the new mechanisms of IEEE 802.11n provide. According to Shrivastava *et al.*, the mechanisms that they have been reviewing are MIMO, frame aggregation, and channel bonding.

The performance of an IEEE 802.11n link was also measured in the presence of interference. A IEEE 802.11g link and a IEEE 802.11n link were separately used to disturb the wireless connection whose performance was being measured. A decrease in throughput was observed in both cases. In our work, in addition to measuring the performance of a wireless link in the presence of interference, a comparison of two implementations of IEEE 802.11n hardware produced by different vendors was made. We observe the implementation specifics influence the operation of an AP in an environment with interference. In addition to measuring throughput we also measured the latency and jitter of the link.

Research carried out by Pelechrinis *et al.* [29] focused on peak performance measurements of an IEEE 802.11n system, in contrast to previous research by Shrivastava *et al.*, who obtained throughput results that were far below the maximum theoretical throughput. Performance evaluation started by activating an interface in IEEE 802.11a mode and continued with enabling additional features of IEEE 802.11n in order to see how much performance boost each of these features provide. No performance parameters other than throughput were measured. No interference tests were performed. In our work we address these flaws and, in addition, provide an analysis how suitable the IEEE 802.11n standard is for small cell backhaul.

Wireless backhaul was investigated also by Sheriff *et al.* in [30]. In their work Sheriff *et al.* proposed a mechanism of admission control in wireless networks. The admission control mechanism takes action based upon real-time evaluation of a wireless channel. Specifically, bandwidth allocation, delay, and jitter are used to characterize the state of a wireless channel. The measurements that preceded the development of the admission control mechanism were not so diverse as in our case and included measuring the busy-time fraction and packet reception rate depending on Received Signal Strength Indicator (RSSI). Gathered data allowed to develop an efficient measurement-driven admission control framework.

Another research of IEEE 802.11n wireless backhaul was done by Mohamed *et al.* [31]. In this research wireless backhaul refers to a wireless multihop network. Mohamed *et al.* suggest to use IEEE 802.11n in conjunction with Dual Channel Intermittent Periodic Transmit (DCH-IPT) relaying protocol for wireless backhaul. It is claimed that this technique can provide higher throughput, lower average delay and lower packet dropping rate.

The DCH-IPT protocol incorporates two mechanisms. The first one is the Intermittent Periodic Transmit (IPT) packet forwarding protocol where the source node intermittently and periodically sends source packets with some transmit period. In this way, interference between concurrently transmitting nodes is eliminated which leads to higher throughput. The second mechanism is Duall Channel (DCH) relaying protocol where to different transmission channels are used: one as an uplink and another as a downlink. The result is a relay system with lower interference and better performance.

In order to benchmark the performance of IEEE 802.11n with DCH-IPT a

MATLAB program linked with network simulator was used by Mohamed *et al.*. During the simulation aggregate throughput, average delay and packet loss rate were measured. In the beginning Single Channel (SCH)-Conventional relaying method was compared with DCH-Conventional relaying method under IEEE 802.11a and IEEE 802.11n standards. The simulation tests proved that DCH-Conventional relay method provides higher throughput, lower latency, and lower packet loss rate.

Afterwards, the comparison between DCH-IPT and DCH-Conventional relaying protocols using IEEE 802.11n was done. The results showed that DCH-IPT outperforms DCH-Conventional, especially in terms of average delay and packet loss rate. Mohamed *et al.* conclude that utilization of DCH-IPT in IEEE 802.11n based wireless backahul will facilitate introduction of small cells into conventional mobile networks.

Chapter 3

IEEE 802.11n as backhaul for a small cell

This chapter establishes some performance requirements for a small cell's backhaul link. A description of an IEEE 802.11n Wi-Fi experimental study is provided. Result analysis and conclusions drawn from the experimental study complete the chapter.

3.1 Constrains and limitations

Since this master's thesis project was conducted in a company, the set of wireless technologies supported by a small cell was explicitly specified. Figure 3.1 summarizes the set of available technologies that were to be considered. On the client side the small cell could have a WCDMA, LTE, and IEEE 802.11n (2.4 GHz) radio interfaces. These three interfaces are considered as they represent the most likely wireless interfaces for a small cell to be deployed by a network operator. On the network side we have assumed that there is a IEEE 802.11n radio interface operating within the 5 GHz band.

Note that in this work the term "picocell" is used to refer to a physical device, not a mobile network cell. That is since a picocell has different mobile technologies, i.e. WCDMA and LTE, each forming its own cell.

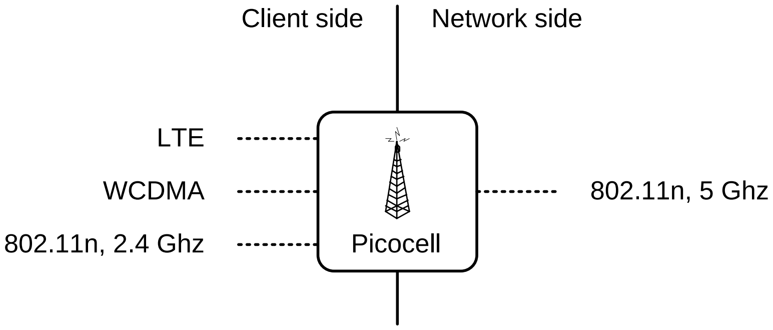


Figure 3.1: Wireless technologies supported by a picocell

3.2 Performance requirements

Performance requirements are expressed in terms of desired network characteristics with regard to throughput, latency, and jitter. In the case of a small cell's backhaul there are no strict limits imposed on these network metrics by 3GPP or other telecommunication standards bodies. Instead, the recommendations come from a number of different mobile operators and communication equipment vendors.

Performance requirements for a small cell's backhaul vary depending on the mobile technologies that a given small cell has on its client access side. Since in this research a picocell with a WCDMA, LTE, and IEEE 802.11n radio interfaces is considered, the backhaul performance requirements are aligned with the specifics of these technologies.

3.2.1 Throughput requirements

Ideally, a backhaul link should provide the same or better throughput as the fastest wireless technology on the client side. However, it is hard to define precisely the performance provided by a particular wireless technology. There is a discrepancy between the theoretically possible and practically achievable values.

As an example, Table 3.1 shows the theoretical peak throughput rates for LTE and IEEE 802.11n. The asymmetric data rates are listed in the form of downlink (DL)/uplink (UL) data rate.

Table 3.1: Peak theoretical throughput of LTE and IEEE 802.11n

	LTE [32]		**IEEE 802.11n** [33]		
MIMO mode	2x2	4x4	2x2	3x3	4x4
Channel width, MHz	20	20	40	40	40
Peak data rate, Mbps	173/58	327/86	300	450	600

In practice, the throughput rates that can be achieved in real deployments are significantly lower than those presented in the above table. For a small cell this means that it is acceptable if the performance of a backhaul link is somewhat less than the theoretical performance of the mobile technologies on its user side. But how much less is "reasonable"? In order to answer this question we have to estimate the amount of traffic sent through the backhaul interface of a small cell. The amount of this traffic depends on the wireless access technology enabled in the small cell and the number of users in the cell and their individual simultaneous data rates. In keeping with the constrains described in the previous section it is assumed that there are three wireless technologies on the access side of a small cell: WCDMA, LTE, and IEEE 802.11n (2.4 GHz). They will each be investigated separately.

The backhaul traffic estimate for LTE could be done based on a study preformed by the Next Generation Mobile Networks (NGMN) alliance [34]. This study, which is based on a theoretical modeling approach, provides some guidelines for an LTE backhaul traffic estimate. The study considers several components that comprise LTE backhaul traffic:

- S1 interface traffic - user data traffic between a base station and a core network,
- X2 interface traffic - user handover traffic between cells,
- Control plane traffic - S1 and X2 interfaces control traffic,
- Synchronization signaling and Operation, Administration and Maintenance (OAM) traffic,
- Transport protocol overhead, and
- IPsec protocol overhead.

Obviously, the user plane data dominates the other types of traffic. X2 interface traffic constitutes 4% of S1 user plane traffic. S1 and X2 control plane, synchronization signaling, and OAM traffic can be ignored as the amount of traffic is extremely low comparing to the user plane traffic. In general, the overhead added by a transport protocol without IPsec is considered to be around 10%. With IPsec in ESP tunnel mode the overhead is around 25%.

In the study an LTE cell's backhaul throughput was estimated for two separate cases: busy time and quiet time. Busy time refers to the case with many UEs are operating within the cell. Quiet time refers to the case when there is only one UE served by the base station. Table 3.2 provides the average and peak throughput figures estimated on the access side of an LTE macro cell operating in 2x2 MIMO mode [34].

Table 3.2: Average and peak LTE macro cell throughput rates

	20 MHz channel	**10 MHz channel**
Average throughput, DL/UL, Mbps	21/16	11/8
Peak throughput, DL/UL, Mbps	117.7/47.8	58.5/20.8

According to NGMN [35] throughput requirement for a small cell backhaul link is 1.25 times higher than for a macro cell backhaul link in busy time case. There are two reasons that lead to higher average small cell throughput:

- In a small cell mobile users are concentrated closer to the center of the cell where the signal quality is good, and

- Small cells are deployed in more isolated locations where inter-cell interference is very low or does not exist at all, which improves the signal quality.

The scaling factor is not applied to the peak throughput since it is limited by the mobile technology.

Taking into consideration additional components (X2 traffic and IPsec tunnel overhead) it is possible to calculate backhaul throughput requirements (see Table 3.3). Note that X2 traffic is not considered in the peak throughput case since this case assumes ideal signal conditions without handover and interference.

Table 3.3: Calculated throughput rates for an LTE small cell backhaul

	20 MHz channel	**10 MHz channel**
Average throughput, DL/UL, Mbps	34.1/26	17.9/13
Peak throughput, DL/UL, Mbps	147.1/59.7	73.2/26

Still, the calculated throughput values are quite optimistic since the study states:

> "The backhaul traffic figures produced by this study represent mature LTE networks with a sufficient number of subscribers to fully load eNBs during busy times. In practice, it may take several years after roll out to reach this state, and even then, only some of the eNBs in the network will be fully loaded."

After studying these calculations, in order to come even closer to reality, it was decided to study several current LTE performance measurement reports. In March 2011, a real deployment performance test of TeliaSonera's LTE network was made in Finland [36]. Measurements were made at locations with a strong signal availability over a 5 day period at 30 minute intervals. Tests revealed that the average download rate was 36.1 Mbps and peak download rate was 48.8 Mbps.

In September 2011, a measurement of AT&T's LTE service was performed [37]. Average and peak DL/UL data rates of 23.6/15.2 Mbps and 61.1/23.6 Mbps respectively were achieved.

Another interesting report comparing the performance of LTE networks of AT&T and Verizon was recently published [38]. These measurements, conducted during the first quarter of 2012, revealed that AT&T's LTE service provides 17/8 Mbps average DL/UL rates and Verizon's - 15/8 Mbps.

As it is seen from these reports, today mobile operators are not able to actually provide high data rates in their LTE networks. Even if it would be possible to obtain a peak throughput close to theoretical maximum, the average LTE data rates are still far below the 100 Mbps figure. This means that a small cell's backhaul performance of even 100/50 Mbps DL/UL should be more than sufficient for backhauling traffic from current **mobile** services. We make such a generalization as GSM and UMTS are slower than LTE, which was taken as a reference point for the above calculation performance requirements.

A similar discrepancy between theory and reality is observed with the performance of the IEEE 802.11n standard. An extensive test of the IEEE 802.11n was conducted in 2011 [39]. The test environment comprised sixty laptops and nine tablet computers. Six Wi-Fi access points manufactured by different vendors were used during the performance tests. In a 30 meter NLOS deployment in the 2.4 GHz frequency band the peak throughput was 76/89 Mbps DL/UL with no interference, and 29/32 Mbps with sixty interfering clients with bi-directional traffic.

To conclude, after estimating the backhaul traffic generated by different access side wireless technologies, we find it reasonable to set a 100/50 Mbps DL/UL value as a throughput requirement for a small cell's backhaul link.

3.2.2 Latency and jitter requirements

If throughput requirements are mainly dictated by the access side technologies of a picocell, then latency and jitter requirements primarily depend on the network services in use. Therefore, in order to specify latency and jitter requirements for a small cell's backhaul it is necessary to identify the types of services utilized by mobile clients these days.

As mobile access technologies evolve, and mobile devices such as smartphones and tablet computers become more ubiquitous, the mobile traffic pattern is becoming similar to the traffic pattern of a fixed network. Services such as file sharing, video streaming, and voice over IP (VoIP) generate a major part of today's mobile traffic. According to Allot Communications' "MobileTrends Report" [40], which is based on the statistics concerning 250 million subscribers all over the world, the most bandwidth consuming mobile services are video streaming and file sharing.

Video streaming traffic, with YouTube as a major driving force (52% of total mobile streaming), increased by 93% during the first half of 2011 and today represents 39% of global mobile data usage. File sharing traffic increased by 33% in the same period and accounts for 29% of global mobile data. This report states that VoIP and Instant Messaging (IM) applications generate only 4% of global mobile traffic. However, these services are the fastest growing with 101% of growth in the same period. Finally, Web traffic has increased by 55% in the same period and it constitutes 25% of a global mobile traffic.

IDATE's "Mobile traffic forecasts 2010-2020" report forecasts mobile traffic growth up to year the 2020 [41]. According to this forecast, VoIP and video traffic will continue growing. Their second prediction is that global data consumption will still be dominated by video streaming applications during the next decade.

As these studies suggest, the mobile traffic patterns will mainly be defined by video, voice, Web, and file sharing applications. Since Web browsing and file sharing traditionally represent a best effort type of service, they can tolerate substantial latency and jitter. However, the same cannot be said for video and voice traffic. Thus, a network that meets the latency and jitter demands for voice and video applications will certainly fulfill the best effort traffic demands.

Once again, as was in case of throughput, there are no strict requirements for delay and jitter in regard to voice and video traffic. However, there are **recommendations** from various standardization bodies and companies. For instance, ITU Telecommunication Standardization Sector (ITU-T) recommends keeping the "mouth-to-ear" voice delay below 150 ms [42]. A delay of between 150 and 400 ms is still considered to be acceptable for voice traffic, however the the user may experience a low quality voice call. A one-way delay of above 400 ms is considered unacceptable for voice traffic.

Jitter of up to 20 ms is considered perfect. Jitter in the range from 20 to 50 ms is considered acceptable, while jitter above 50 ms is unacceptable for real-time traffic [43]. These recommendations are taken as a reference for establishing a small cell's backhaul link requirements.

Note that acceptable one-way voice delay below 150 ms comprises the sum of all delays in the network path. Hence, when estimating acceptable delay for the small cell's backhaul link, the delay added by the rest of the network path must be considered. Delay requirements for a small cell's backhaul link can vary depending on a specific network topology. This makes the establishment of precise delay requirements difficult. In case of simplified small cell network topology shown in Figure 3.2 the following network segments are considered:

- Radio access segment - a path between the user equipment and the picocell,
- Small cell's backhaul segment - a path between the picocell and the point of presence (POP), that aggregates backhaul links from several small cells,
- Core access segment - a path between the POP and the mobile network's core, and
- Public access segment - a path between the mobile network's core and a public service in the Internet, i. e. video streaming server or Skype node.

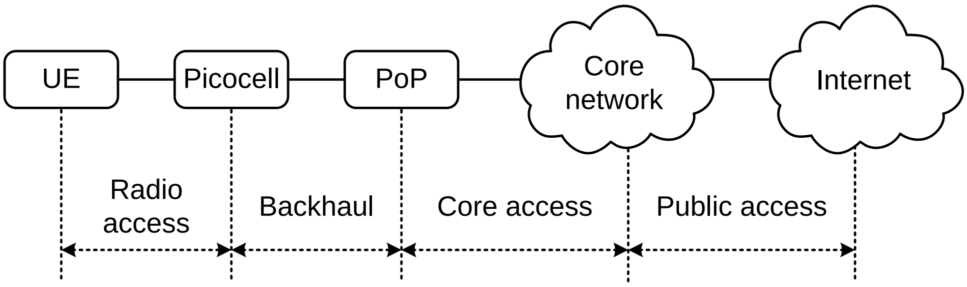


Figure 3.2: Simplified small cell network topology

Delay for the radio access segment depends on the mobile access technology in use. The requirement for LTE user-plane one-way delay (delay between user equipment and radio base station) posed by 3GPP is below 5 ms [44]. However, this delay corresponds to the **quiet time** case described in Subsection 3.2.1. It is obvious that in reality one-way delay for LTE radio access segment will be higher than 5 ms.

Core access segment usually corresponds to the high speed fiber network which provides latency below 1 ms [45]. For the public access segment latency can vary significantly, hence it is difficult to indicate any figures.

According to various real world LTE measurements latency figures looks optimistic. For instance, results from already mentioned performance study of Telia Sonera's LTE network in Finland [36] showed that average one-way delay was 23 ms and peak one-way delay was 38 ms. The delay was measured between the UE and public server in the Internet.

The small cell's network backhaul link can be interpreted as an additional network segment in the macro cell network topology. Considering that today's LTE networks provide one-way delay of 50 ms at maximum, there is still 100 ms left to achieve the limit of recommended latency for real-time traffic.

Taking into consideration everything stated above as well as the constrains described in Section 3.1, the following performance requirements for a small cell's backhaul link are recommended:

- DL/UL rate of 100/50 Mbps,
- One-way delay between the picocell and the POP up to 100 ms, and
- Jitter of 20 ms or less.

3.3 Experimental study

This section describes the experimental study of IEEE 802.11n technology. During the study network performance parameters (specifically bandwidth, latency, and jitter) were measured for a wireless backhaul link established between a pair of APs under various circumstances. This section presents the goals of this experimental study, describes the equipment used for the experiments, and provides information on the measurement scenarios. The section also presents the results of the study as well as an analysis of these results. Conclusions and recommendations complete the section.

3.3.1 Goals

As it was stated before, this master's thesis project investigates a wireless small cell backhaul link. In general, metrics such as performance, ease of deployment, scalability, security, and availability should be taken into consideration when choosing the most suitable technology for a small cell's backhaul. Of these metrics our project initially focuses on performance. In Chapter 4 we will consider some aspects of security.

The aim is to understand if IEEE 802.11n technology is fast enough to be used as a small cell's backhaul. If so, under what specific conditions is the performance adequate. The assessment is done by means of an experimental study of an

IEEE 802.11n wireless link in different deployment scenarios and under various conditions. First, we measured performance metrics such as peak throughput, latency, and jitter. Afterwards, the collected data was analyzed. In this way we aimed to reach a conclusion of if the performance of the IEEE 802.11n wireless link is sufficient to serve as a backhaul link for a small cell.

3.3.2 Equipment

The empirical part of this master's thesis project was conducted during a six week time period. More than 300 separate tests were performed. Some of the measurements were made in a shielded room, which eliminated external radiations and prevented reflections inside the room.

In order to observe how different implementations of IEEE 802.11n standard influence wireless performance, APs manufactured by two vendors were used in these tests. For business reasons, the vendor's names the and APs' model numbers are not disclosed, but rather we use the labels Vendor A and Vendor B in this document. The technical specifications of the APs are provided in Table 3.4.

Table 3.4: Technical specifications of the APs used in the measurements

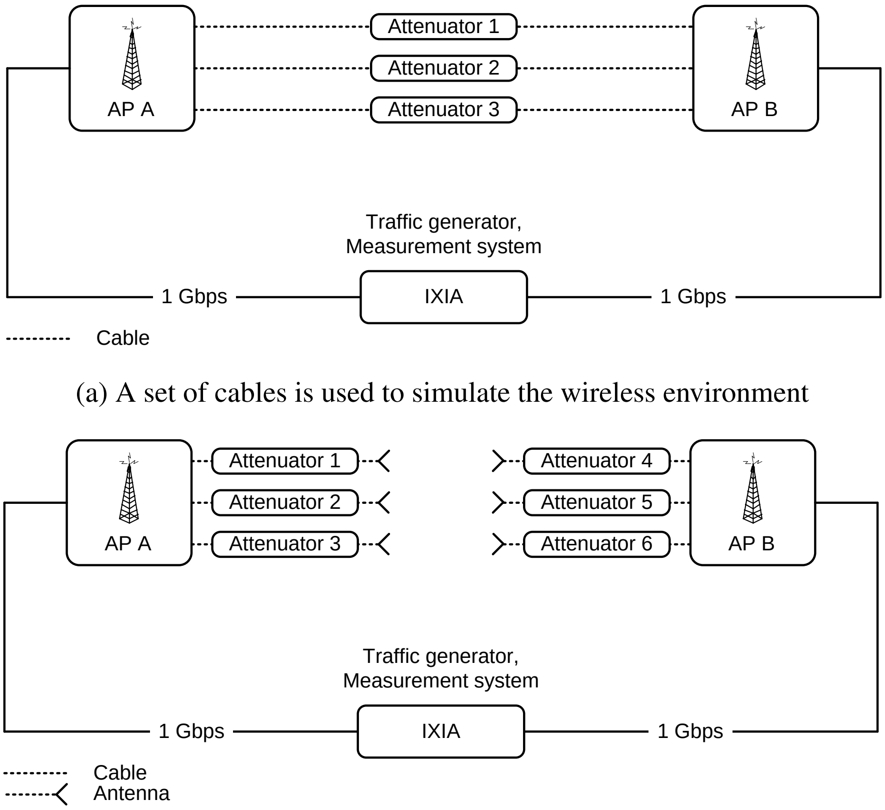
	Vendor A	**Vendor B**
Bands of operation, GHz	2.4 and 5	2.4 and 5
MIMO modes supported	1x1, 2x2, 3x3	1x1, 2x2
Channel width, MHz	20 and 40	20 and 40
Peak theoretical rate, Mbps	450	300
Maximum output power, dBm	25	17

An IXIA XM2 chassis [46] with a 16-port Gigabit Ethernet module [47] was used to generate traffic as well as to measure the performance metrics.

3.3.3 Measurement scenarios

Several measurement scenarios were defined in order to evaluate the performance of the IEEE 802.11n wireless link in different conditions:

1. **Point-to-point scenario**: where two APs were placed in a shielded room. A wireless link between the APs was established and evaluated. The point-to-point scenario has two sub-scenarios. In the first sub-scenario a set of cables was used to simulate the wireless environment (see Figure 3.3a). The second sub-scenario assumed an over the air wireless link establishment (see Figure 3.3b).



(a) A set of cables is used to simulate the wireless environment

(b) Over the air wireless link establishment

Figure 3.3: Point-to-point measurement scenario

2. **Interference scenario**: where the performance of a wireless link is measured under conditions when interference exists. In this scenario an additional pair of APs was installed in the shielded room in order to generate interference (see Figure 3.4). Two sub-scenarios configure the AP pairs to operate within the same radio channel or within adjacent radio channels.

3. **Indoor scenario**: where the performance of a wireless link is measured inside a building without people. The building is organized as an open space office environment. Pairs of APs were installed in four different locations as shown in Figure 3.5.

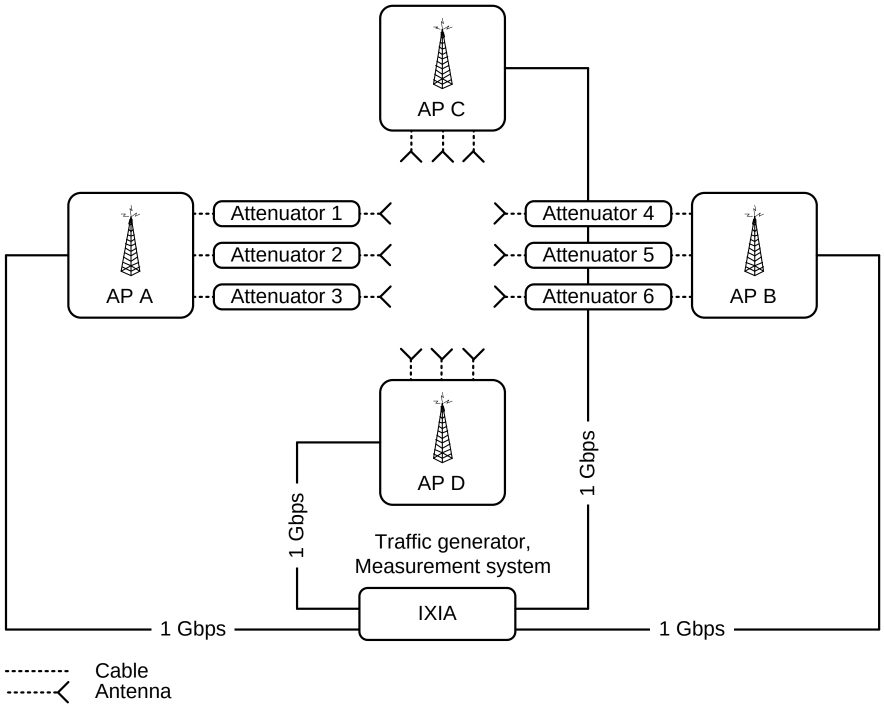


Figure 3.4: Interference measurement scenario

During the tests some variables were changed in order to observe how different settings and conditions influence the performance of the wireless link understudy. The list of variables is summarized in the Table 3.5.

Table 3.5: Variables changed during the measurements

Variable	**Values**
MIMO mode	1x1, 2x2, 3x3
Channel width, MHz	20, 40
Antenna	Small square panel with 14 dBi gain, big square panel with 24 dBi gain, rectangular panel with 22 dBi gain
Traffic pattern	IMIX, ITU-T IMIX, large frame

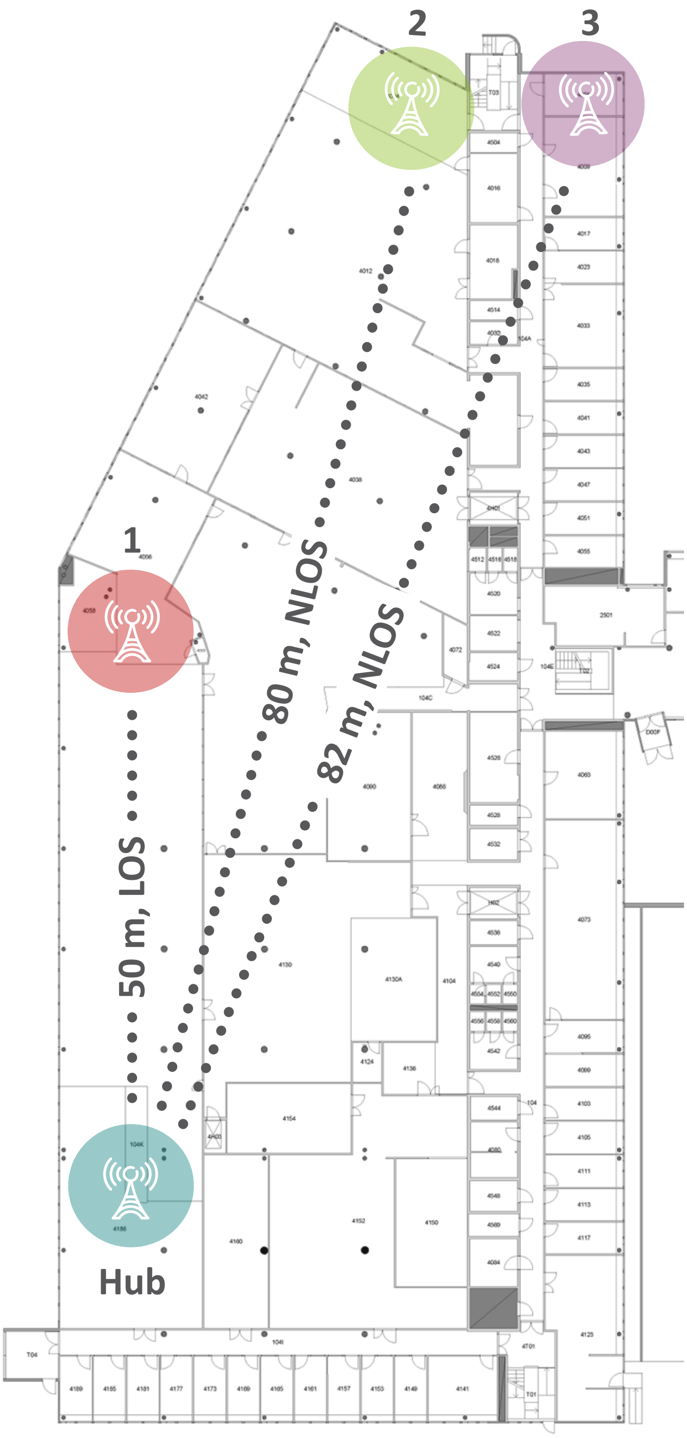


Figure 3.5: Indoor measurement scenario

The traffic patterns generated during the tests were:

- Large frame traffic pattern where the size of the frame is constant and fixed at its maximum possible value of 1518 bytes.

- Internet Mix (IMIX) traffic pattern with small frames dominating to simulate voice traffic. This pattern was preconfigured in the IXIA XM2 measurement system used during the tests (see Section 3.3.2). The frame size/weight scheme is 64:7, 570:4, 1518:1, which means that the ratio among small, middle, and large frames was 7 to 4 to 1.

- ITU-T IMIX traffic pattern [48] with large frames dominating to simulate data transmission. The frame size/weight scheme is 64:3, 576:1, 1518:6.

Initially the measurements were performed using the set of cables between the APs in order to get a baseline which could be used as a reference point for the over the air measurements. Since the shielded room was limited in size attenuation was introduced into the wireless link to simulate increasing the distance between the sender and the receiver. The attenuation step size was 5 dB.

Over the air measurements were made with the antennas integrated into the APs as well as with a set of external antennas, which we assumed put the APs of different vendors to comparable conditions. Dual polarized panel antennas of different sizes and shapes were used during the tests (see Table 3.5).

Another important parameter that had to be kept under control during the measurements is frame loss ratio. In order not to overwhelm the buffers of the AP and to keep latency and jitter values consistent it was decided to keep the frame loss rate under 1% during the measurements.

3.3.4 Results and analysis

The results of the measurements along with a measurement environment description are available in test reports: [49], [50], and [51]. Partial test results are presented in Appendix A. The analysis of obtained results and their assessment from a wireless small cell's backhaul perspective is provided below.

3.3.4.1 Theoretical and practical peak throughput

Since performance is the major requirement for a Wi-Fi backhaul link it has to be mentioned that in reality Wi-Fi does not nearly provide the actual maximum throughput that is specified in the IEEE 802.11n specification. Although the IEEE 802.11n specification mentions 450, 300, and 150 Mbps as a maximal throughput for 3x3, 2x2, and 1x1 MIMO modes respectively. Our the measurements revealed that in close to ideal environmental conditions it was possible to achieve only 66 to 74 percent of the claimed throughput for large packet traffic, and from 27 to 50 percent for IMIX traffic (see Appendix A tests 1, 12, 23, 33, 43, and 53). The peak data rates achieved were 306, 226, and 111 Mbps for 3x3, 2x2, and 1x1 MIMO modes respectively. These values were measured for the APs from Vendor A.

For Vendor B the numbers were in the range of 27 to 56 percent of claimed throughput for large packets and around 14 percent for an IMIX traffic. Peak data rates were 202 and 105 Mbps for 2x2 and 1x1 MIMO modes.

The obtained results (shown in Figure 3.5) were expected. Below is an explanation of why it is unlikely to get the maximum theoretical throughput:

1. High speed modulation schemes are not robust against transmission errors and are able to operate effectively only under ideal conditions without radio interference, reflections, absorptions, etc. Thus, in a real environment it will not be possible to approach the theoretical throughput since there will be one or more of these factors limiting the throughput.

2. High throughput may be achieved only when the transmitter and the receiver are close to each other in terms of distance. In that case the RSSI is normally sufficient on both ends to provide a high data rate. However, in a real deployment as the distance increases the maximum data rate decreases.

3. IEEE 802.11n employs distributed coordination function (DCF) to arbitrate access to the media [52]. DCF is based on the carrier sense multiple access with collision avoidance (CSMA/CA) medium access method. Since CSMA/CA incorporates random backoffs and requires exchange of control messages before sending data over the air, it also reduces the performance of a wireless backhaul link [53].

4. Protocol overheads are also impose a significant performance penalty. Wireless transmission of each data or control frame begins with a preamble and physical layer convergence procedure (PLPC) header, and ends with the other AP sending an acknowledgment. Even though a frame aggregation technique was introduced in the IEEE 802.11n amendment (see Section 2.2.3), the overhead is still significant [53].

5. Weaknesses of the actual implementations can be another reason for the poor performance of a wireless link established between a pair of APs. Switching fabric limitations or lack of a hardware crypto-accelerator can limit the AP's performance.

The conclusion is that even in a shielded laboratory it is infeasible to approach the theoretical peak throughput. Thus, when planning a Wi-Fi backhaul, the actual tested throughput should be taken as a reference point to make any kind of further estimates of performance.

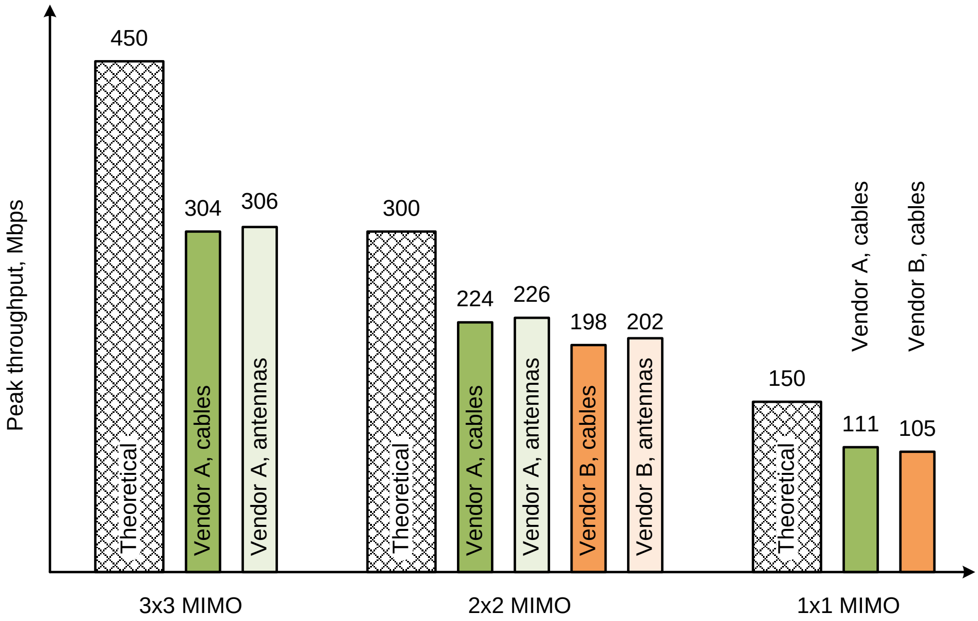


Figure 3.6: Peak data rates obtained on the tested IEEE 802.11n devices

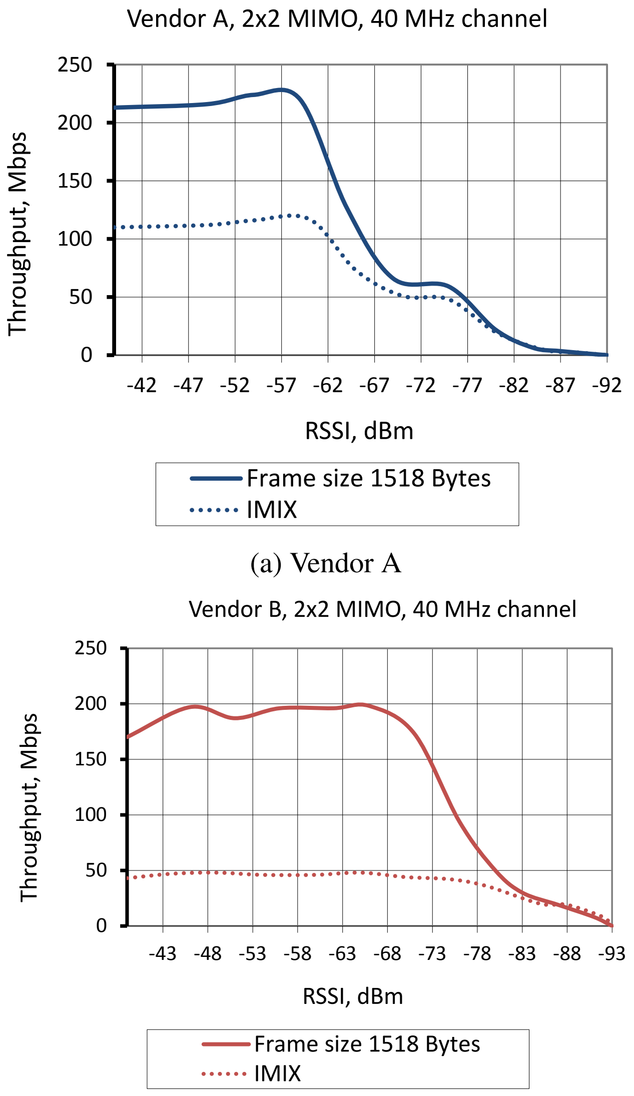
3.3.4.2 Switching fabric limitations

The measurements revealed another limiting factor for the throughput in a Wi-Fi implementations, this limitations is the throughput of switching fabric inside the access point. This performance parameter is measured in packets per second (PPS) or frames per second (FPS). Fixed switching throughput of the chip explains the discrepancy in maximal throughput obtained in the cases of large and small frames.

For Vendor A the maximal throughput measured for large frames, i.e., those 1518 bytes long, is 299 Mbps (see Table A.1 test 1), while for a mixture of small and large frames the throughput was only 123 Mbps (see Table A.1 test 12). The measurement conditions for both of these tests were the same. For Vendor B the respective values are 170 Mbps and 43 Mbps (see Table A.10, tests 158 and 170). Figure 3.7 demonstrates the difference in peak throughput for different types of traffic with large or small frames prevailing as a function of the RSSI.

The difference in rates obtained for different traffic patterns is due to the fact that it is easy to saturate the link with a smaller number of large frames than with a greater number of small frames. In the ideal case the switching fabric within the AP should be fast enough to achieve maximal throughput even with the smallest frames of 64 bytes. For example, the access point should be able to process approximately 880 000 of small frames per second in order to achieve a throughput of 450 Mbps. In realistic scenarios the traffic is usually a mixture of different sized frames, hence vendors avoid putting fast and thus expensive fabrics into consumer devices. Vendor A, for instance, has a fabric that is able to process no more than 34 kFPS. This means that to obtain 450 Mbps of throughput the average size of a frame should be 1654 Bytes.

Switching fabric throughput should be taken into consideration when designing the hardware for a small cell base station. Users connected to a cell may heavily utilize VoIP services which transmit relatively small packets (and hence small frames) over the network. With a poor design the small cell will reach its maximum switching capacity well before the backhaul radio link is saturated in terms of its throughput. Ultimately this fabric bottleneck might lead to client throughput starvation.



(a) Vendor A

(b) Vendor B

Figure 3.7: Large frame against IMIX

3.3.4.3 Maximum distance

The measurements have demonstrated that the signal between two access points fades entirely at an RSSI of approximately -90 dB. There was no significant difference between the two vendors' equipment in this regard. It is possible to estimate the maximum distance that this would corresponding to using the Friis transmission equation:

$$\frac{P_r}{P_t} = G_r G_t \left(\frac{\lambda}{4\pi R} \right)^2$$

where P_t is transmitting power of the sender,
P_r is available power at the receiver,
G_t and G_r are the antenna gains of the sender and the receiver respectively,
λ is a wavelength, and R is the distance between the APs.

For an antenna gain of 0 the maximum distance between APs are calculated with the Friis equation would be **4310** meters if we assume that the transmission power is at its maximum allowed for channel 108, which is 30 dBm in Europe.

The results tables provided in Appendix A list a number of measured metrics such as throughput, latency, and jitter as a function of RSSI. Using the provided equation the distance could be calculated and used as a rough reference for wireless backhaul link deployment and selection of antennas.

3.3.4.4 Modulation and coding schemes

Another predictable outcome from the measurements is that MCSs are chosen for data transmission by the access point depending on the radio channel's characteristics referred to as LQMs. Among the LQMs there are metrics for bit error rate (BER), signal-to-noise ratio (SNR), and RSSI. The RSSI is the most influential parameter. As RSSI gets worse MCSs are gradually changed from high-performance and error intolerant schemes towards low-performance schemes that are more robust against the transmission errors.

When these different schemes are applied to wireless backhaul this means that the backhaul link has some flexibility to counteract transmission errors caused by interference, reflections, and other harmful influences. Using these schemes the backhaul link can provide uninterrupted and smooth transmission under different circumstances at a cost of decreasing link throughput. It was infeasible timewise to observe all the points where the different MCSs change during the measurements. The granularity of attenuation introduced into the wireless backhaul link during the tests was 5 dB. However, the tendency to switch from a higher-rate MCS to a lower-rate MCS with an increase in attenuation can be observed in all test cases. Figure 3.8 illustrates how the different MCSs changed for Vendor A.

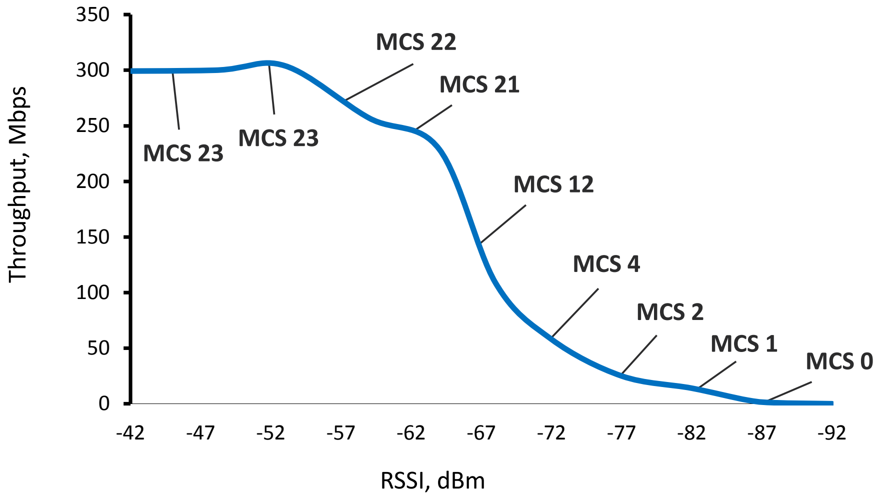


Figure 3.8: MCS scheme as a function of RSSI for Vendor A

As it was mentioned earlier, an IEEE 802.11n AP decides which MCS to use by continuously evaluating the characteristics of the received signal in order to estimate the characteristics of the transmission environment. In some cases these characteristics fluctuate near the point of MCS change. It may happen that the fluctuations are so significant that two or more MCS are being used interchangeably. The measurements have demonstrated that in the cases when there is a persistent switching between several MCSs the performance (in terms of throughput, latency, and jitter) is slightly worse than when using one even less productive MCS continuously. Thus, when deploying a backhaul link one should avoid leaving the installation in a borderline state where the choice of MCS is constantly being switched in order to avoid poor performance.

3.3.4.5 MIMO modes

Predictable results were obtained with regard to how different MIMO modes were used by the APs and how this influences the backhaul link's performance. The more spatial streams used simultaneously, the more throughput is obtained at the same RSSI value, and lower the jitter and latency are. In order to get the maximum performance from a backhaul link the 3x3 MIMO mode is the most beneficial, followed by 2x2, and 1x1 (see Figure 3.9). Our recommendation is to use the highest MIMO mode whenever available to achieve the best performance.

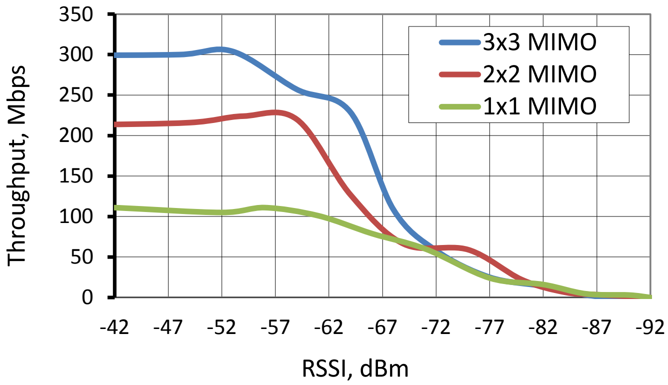


Figure 3.9: Peak throughput for different MIMO modes for Vendor A

3.3.4.6 Channel bandwidth

Channel bandwidth is a configurable parameter on all of the access points utilized in the tests. Measurements have demonstrated that on average it is possible to get up to 50 percent of an increase in throughput by switching from using a 20 MHz channel to using a 40 MHz channel. Therefore, a recommendation would be to enable the 40 MHz channel for the backhaul link whenever the link traffic justifies this increased use of bandwidth by a single AP.

However, channel bandwidth influences not only the performance characteristics of the wireless backhaul, but also affects the scalability of the deployment. Since the spectrum resources are limited, the number of non-overlapping channels that can be utilized is finite. Consequently, there will be fewer non-overlapping channels of 40 MHz and more non-overlapping channels of 20 MHz in a particular spectrum range. More non-overlapping channels means that it is possible to deploy additional picocells to increase the coverage area or to increase capacity. However, the performance of the backhaul link for each of the picocells will decrease since a narrower channel is used to transmit the data.

3.3.4.7 Antenna types

The measurements have shown that there is no significant difference in performance characteristics between different tested antenna types (see Table 3.5 on page 35) within a specified RSSI range. The antennas were dual-polarized with horizontal and vertical polarization. Under laboratory conditions with a neglectable radio noise floor and LOS antenna installations the similarity of results is expected. The antennas did provide additional gain to the signal, but at comparable RSSI levels the measured characteristics were roughly the same as would be expected.

From the perspective of wireless backhaul the performance requirements could be met with any antenna pair when the transmitter and the receiver are within a short range of each other. However, to be able to provide sufficient performance within a longer range, directional antennas may have to be deployed.

3.3.4.8 Interference measurement scenario

Previous analysis presented in this section was based on the results obtained in a point-to-point measurement scenario. This paragraph will provide information on interference tests. The goal of the tests in the interference scenario was to measure the performance parameters of two IEEE 802.11n wireless links operating at the same radio frequency. The channel number selected for the test was 100, which corresponds to a center frequency of 5500 MHz.

The measurements in the environment with interference demonstrated that the throughput dropped significantly for the APs of both vendors as compared to the tests without interference. For Vendor A the drop was 38% (see tests 138 and 299 in Appendix A): from 199 Mbps to 124 Mbps. For Vendor B the drop was more substantial at 63% (see tests 266 and 300), as the throughput rate decreased from 134 Mbps to 50 Mbps. Since the pairs of APs were similarly configured and carefully placed at the tops of the cross (see Figure 3.4 on page 35) the conclusion could be drawn that Vendor A has done a better job preparing its APs to work in an environment with interference. The main results of the interference measurements are summarized in Table 3.6.

Table 3.6: Interference measurements: configurations and results

	Point-to-point		**Interference**	
	Vendor A	**Vendor B**	**Vendor A**	**Vendor B**
Throughout, Mbps	199	134	124	50
MIMO mode	2x2	2x2	2x2	2x2
MCS index	15	15	15	15
RSSI, dBm	-44	-54	-45	-50
Tx. power, dBm	23	17	17	17
Ch. width, MHz	40	40	40	40
Ch. (Freq., MHz)	100 (5500)	100 (5500)	100 (5500)	100 (5500)
Traffic pattern	IMIX	IMIX	IMIX	IMIX
Antenna	Small panel	Small panel	LollyPop	Small panel

Surprisingly, the MCS used by the APs while working in the environment with interference is the highest possible MCS and was the same MCS used in the non interference measurements. This seems illogical since the performance of a the wireless link has decreased considerably. However, the highest MCS is used because the quality of the radio channel is still good and collisions with other traffic in the channel is are the only problem. The interfering sources are both IEEE 802.11n transmitters so the negotiation about the usage of air interface is done by the DCF mechanism.

It would be interesting to observe how the IEEE 802.11n wireless link's performance is changed when the source of interference is something other than Wi-Fi equipment, e.g. a microwave oven or a cordless phone. However, such measurements have not been conducted and are the subject of future work.

3.3.4.9 Indoor measurement scenario

The indoor scenario concerned measurements made inside the building where the APs were located as specified in Figure 3.5 on page 36. One AP from each pair was fixed in a "hub" location. The other AP was mounted on a pole and moved to different spots inside the building.

A general conclusion from the indoor measurements is that it is possible to get decent wireless link performance even when the APs are quite far away from each other but located on the same floor. For example, the peak throughput rate in the 50 meter LOS installation was 123 Mbps for Vendor A and 173 Mbps for Vendor B (see Appendix A, tests 325 and 326).

In a NLOS installation the performance decreased significantly. For Vendor A the throughput was 52 Mbps (test 328), for Vendor B the throughput was 43 Mbps (test 329). Placing the second access point even further away in the corner of the building it was impossible for the equipment of Vendor B to establish a wireless link. Vendor A in a 82 meter NLOS test case demonstrated a poor performance of only 3.5 Mbps when an internal antenna was used. With a rectangular panel external antenna the peak throughput for Vendor A increased to an impressive 57 Mbps with an impressive average latency of less than 6 ms (test 334).

These test results prove that a IEEE 802.11n wireless backhaul link could potentially be deployed inside a building with walls and furniture as an obstacles for the radio waves. Even in the NLOS AP placement the performance of the wireless link should possibly satisfy the backhaul requirements. However, there is a question of why not simply connect the small cells to a fixed Gigabit Ethernet network rather than using a wireless backhaul link. The answer is that the set of small cells could be deployed in a place like shopping mall in form a mesh network. Then it could be impossible to interconnect all of these small cells with a cable, making a wireless link the only available option to provide a backhaul.

3.4 Conclusions

Recall that the goal of the experimental study was to investigate the performance of an IEEE 802.11n wireless link and to assess how well it met the requirements for a small cell backhaul link (see Section 3.3.1). In order to make an assessment we developed a set of requirements. The analysis of data gathered during our experimental study revealed that the IEEE 802.11n wireless link as realized by two different vendor's APs meets these requirements. Under different conditions, including interference from other APs operating in the same channel, the link could provide sufficient throughput, latency, and jitter for backhauling the traffic of a picocell.

It was also found that changing the settings and configuration of the link, e.g. the specific MIMO mode and channel band width, influence the performance. These settings along with the different antenna types should be carefully tuned and selected for each specific wireless backhaul deployment. With careful configuration it is possible to get the maximum performance, decrease interference, and increase the maximum backhaul distance.

Chapter 4

Secure integration of a small cell into a modern cellular system

In this chapter we consider how to securely integrate a small cell into a modern cellular network (specifically the EPC shown in Figure 2.1). The chapter begins with a description of the problems to be solved, then goes on to propose a security mechanism that could be use. The chapter ends by drawing some conclusions.

4.1 Problems

Two distinct scenarios can be defined for small cell deployment. The first scenario is in-house deployment. This refers to a scheme where a backhaul link for a small cell is under the control of the same mobile operator that deploys the small cell. The second scenario is remote deployment. This refers to a scheme where the backhaul link for a small cell has to traverse an insecure network, e.g. the Internet or a third party's network, in order to connect the small cell to the operator's mobile core. The latter case would seem to impose additional security requirements on the integration of a small cell into the operator's mobile network. The intentions of this master's thesis project were to investigate the security aspects of a remote small cell deployment, then to propose a secure mechanism for integrating a picocell into a generic modern mobile network.

Before defining the problems associated with the remote deployment scenario it is important to specify the essential characteristics of a picocell, for which a secure integration mechanism is to be proposed. It is also necessary to describe the major network entities participating in the integration of this picocell.

As it was already mentioned in Section 3.1, the scope of this master's thesis project considers a picocell with LTE, WCDMA, and IEEE 802.11n radio interfaces. In addition, it is assumed that the picocell has a unique serial number and pre-installed digital certificates issued by the vendor who manufactured the picocell. There is no need for any customer specific pre-configuration of the picocell.

Figure 4.1 depicts the major elements of the picocell remote deployment scenario:

- Pico server (Pico srv.) - a globally accessible server operated by the manufacturer that stores a database of picocell serial numbers and correspondent cryptographic public keys. Each picocell is aware of its manufacturer's server's permanent uniform resource identifier (URI), for example "http://vendor.com/picoserver".

- Mobile Network Operator (MNO) server - a globally accessible server operated by the mobile operator. This server is located outside the SeGW (so that it can be globally accessible). The MNO server stores the IP addresses and URIs of different servers in the operator's network.

- Registration Authority (RA) server - a mobile operator's server that issues certificates signed by the operator.

- SeGW - the node that terminates secure tunnels carrying the LTE/WCDMA traffic.

- WAG server, which terminates secure tunnels carrying IEEE 802.11n traffic.

- Configuration (CFG) server, which belongs to the mobile operator. The CFG server provisions a picocell with the operator's specific configuration for this picocell.

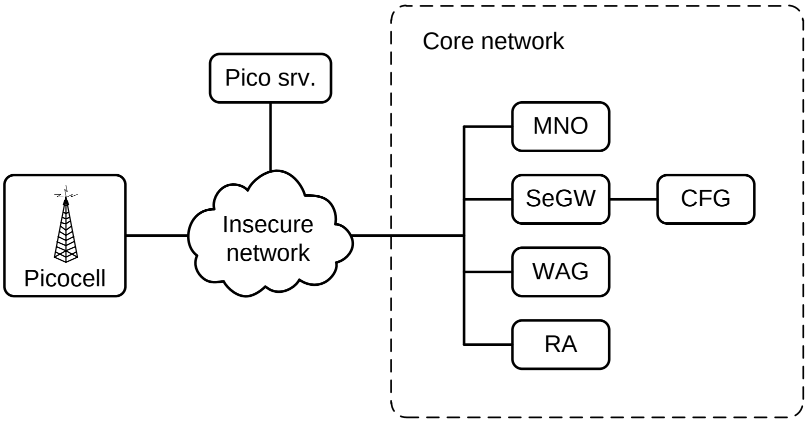


Figure 4.1: Remote picocell deployment network architecture

What technical problems are associated with picocell integration? The essential problem is a secure retrieval of the MNO server's IP address. Initially a picocell does not have information about which mobile operator's network it should be attached to. However, a picocell **needs** to connect and perform mutual authentication with its owner's MNO server in order to obtain the IP addresses of all other servers required for its operation. The mechanism to acquire the MNO server's IP should not allow other mobile operators to impersonate the legitimate MNO - thus it should prevent man-in-the-middle attack using IP spoofing.

Another security aspect of a picocell integration comes from the fact that a picocell is assume to be equipped with both trusted 3GPP LTE/WCDMA radio interfaces and an untrusted non-3GPP IEEE 802.11n interface. According to 3GPP security architectures described in section 2.3.4, traffic from trusted and untrusted air interfaces have to be isolated in two different secure tunnels. Thus, appropriate secure authentication, key distribution, and tunnel establishment mechanisms need to be specified.

4.2 Proposed security mechanism

The proposed mechanism for secure integration of a picocell is aimed to be compatible with a generic modern mobile network. The picocell should be deployed in a plug-and-play manner with as little user intervention as possible.

The call-flow describing the establishment of a secure connection between a picocell and a mobile network is presented in Figure 4.2.

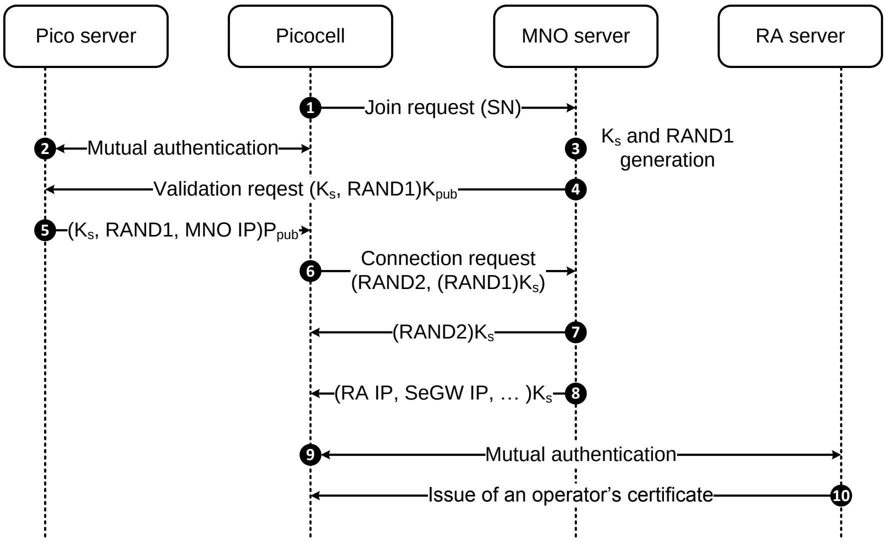

Pico server
Picocell
MNO server
RA server
1 Join request (SN)
2 Mutual authentication
3 K_s and RAND1 generation
4 Validation reqest (K_s, RAND1)K_{pub}
5 (K_s, RAND1, MNO IP)P_{pub}
6 Connection request (RAND2, (RAND1)K_s)
7 (RAND2)K_s
8 (RA IP, SeGW IP, ...)K_s
9 Mutual authentication
10 Issue of an operator's certificate

Figure 4.2: Call-flow of a secure connection establishment

1. A person deploying the cell sends its serial number to the MNO server of a specific mobile operator in a secure fashion. The serial number can be entered manually or a Quick Response (QR) code reader could be used to scan the label on picocell. The message containing the serial number is regarded as a request for a picocell to join a mobile operator's network.

2. After the picocell boots up, it obtains an IP address via Dynamic Host Configuration Protocol (DHCP) and locates a Pico server using its built-in permanent URI to its manufacturer's Pico server. A mutual authentication between the picocell and the Pico server occurs using a built-in certificate.

3. The "Join Request" message that was generated during the step one is processed by the MNO server. A random challenge RAND1 along with a 256-bit long symmetric key K_s is generated by the server for the picocell.

4. The MNO server provides the Pico server with a "Validation Request" message that contains the picocell's serial number, RAND1, and K_s, all encrypted with the manufacturer's public key K_{pub}.

5. The Pico server forwards K_s and the MNO server's IP address, both encrypted with the picocell's public key P_{pub}, to the picocell.

6. The picocell generates a random challenge RAND2 and sends a "Connection Request" message, containing the challenge RAND2 and the challenge RAND1 encrypted with K_s to the MNO server.

7. The MNO server decrypts RAND1 challenge with K_s, then compares the received RAND1 with the one it has stored, and sends challenge RAND2 encrypted with the same K_s back to the picocell.

8. The picocell compares received RAND2 challenge with its own copy of RAND2. If they match then the mutual authentication process is finalized.

9. The MNO server sends the Domain Name System (DNS) names of all required servers to the picocell. The Domain Name System Security Extensions (DNSSEC) [54] must be used for data origin authentication and integrity check of supplied DNS names.

10. The picocell contacts the RA server and performs mutual authentication using the installed certificate.

11. The RA server issues a local certificate to a picocell.

12. From this point on all key exchange processes and the secure tunnel establishment process can be performed using the operator's local certificate stored in the picocell.

Once a picocell has obtained an operator's certificate, all other information exchange with the operator can be performed securely. In accordance with 3GPP's security architectures two secure tunnels should be established after a picocell has obtained a local certificate. The first is an IPsec tunnel between a SeGW and the picocell for tunneling WCDMA/LTE traffic. The second tunnel is for CAPWAP over a DTLS tunnel between the WAG and the picocell for tunneling the IEEE 802.11n traffic.

4.3 Conclusions

The process described in the previous section allows the picocell to securely locate and communicate with the MNO server eliminating any possibility of a man-in-the-middle attack. Note that we do not require that a picocell's manufacturer have any of operator's specific configuration in advance only that the manufacturer's server securely introduce the picocell to its new owner who then securely configures the picocell for operation within its network.

The developed algorithm of secure picocell integration was not implemented and tested. The design of the algorithm will be used as an input for product development activities in the company hosting the project.

Chapter 5

General conclusions and future work

The chapter describes the conclusions reached based upon the work done during this master's thesis project and provides suggestions for related investigations in the future.

5.1 General conclusions

In accordance with the goals defined in Section 1.3 the main research question of this project was if the IEEE 802.11n technology is able to provide sufficient performance in a real environment to be used as a small cell's backhaul link. Several consequent activities were undertaken to answer this question:

- The performance requirements for the small cell backhaul were established (see Section 3.2),
- The performance of a IEEE 802.11n wireless link was as implemented by two different AP vendors measured under various conditions (see Section 3.3.3),
- The results of these measurements were analyzed (see Section 3.3.4).

Taking into account the constrains described in Section 3.1, the conclusion was that IEEE 802.11n is in fact capable of providing sufficient performance to be deployed as a backhaul link for a small cell. The conditions when the performance would be acceptable were defined based on an extensive experimental study. The expertise of the authors in the domain of radio measurements grew exponentially during this project. Thus, as the work was approaching its ending, we began noticing slight inconsistencies and minor inaccuracies allowed during the initial stage of our measurements. If there was a way to travel back in time, we would have paid more attention to the following things:

- Packet loss should be kept under 1% during the measurements to make the results accurate (initially in our cable based interconnections of the APs the packet loss value exceeded the 1% threshold),
- Identical antennas should be used on all devices operating simultaneously in the interference tests, and
- The average latency is more reliable for making a performance assessment than the minimum and maximum values that we measured.

Another goal of the investigation was fulfilled by proposing a secure mechanism for initial picocell integration into a generic mobile network. Only a fraction of the security related issues were analyzed during the project due to time required to study the whole range of security topics that have arisen with the advent of the small cell paradigm.

5.2 Future work

The concept of a small cell being incorporate into a operator's mobile network is a relatively new topic in the area of mobile networks. There are still many problems to solve in order to fully adopt these small cells. At the same time the evolution of mobile technologies poses additional issues.

This master's thesis project considered only IEEE 802.11n standard as a wireless technology for a small cell's backhaul link. In addition, performance of Worldwide Interoperability for Microwave Access (WiMAX) and LTE could be evaluated and compared to IEEE 802.11n. During the project some initial measurements of a proprietary IEEE 802.11n-based time division multiple access (TDMA) implementation were done. The results of those measurements are available in Appendix B. These results could be used as a foundation in the future investigations.

In the future work it is also suggested to investigate even more recently developed wireless technologies that support data rates close to 1 Gbps, as these are expected to eventually replace the current standards. The case of a picocell with LTE-Advanced and IEEE 802.11n 5 GHz access interfaces should consider the feasibility of using the IEEE 802.11ac standard as a backhaul.

Another vector is to continue the measurements of IEEE 802.11n, but the focus should be on closer-to-reality tests. In particular:

- Build a topology with a RAN and core network elements where the base station backhauls the traffic over the IEEE 802.11n link and interconnects to the EPC. Tests of how different kinds of services behave depending on the wireless backhaul link's load and interference should be made.

- Measure the IEEE 802.11n link's performance in a real outdoor environment. For instance, in a shopping mall or transportation terminal.

- Perform field trials of a real LTE/WCDMA base station having a IEEE 802.11n wireless backhaul with real clients attached to it.

Additionally, tests and measurements should be made to observe how real services behave, in addition to the lower layer measurements that were made in this study.

Regarding the security aspects of small cell networks, the current study does not cover the deployment case where several picocells form a mesh network. In this topology one picocell takes a role of a root node that interconnects all the other small cells within the mobile core network. This deployment scenario raises several additional security concerns. The essential ones are the need for an access control mechanism, key exchange and distribution process, secure tunnel establishment and scalability, and operation of non-root picocells behind a NAT.

5.3 Social, economic, ethical, and environmental issues

This master's thesis project facilitates the deployment of small cells by making use of a wireless backhaul link. Deploying small cells increases the capacity and extends the coverage of a mobile network. This improves the quality of services provided by a mobile network, as well as extending the area where these services are available. These two effect should lead to increased client satisfaction with the provided mobile services, which is a desirable **social** effect of this master's thesis project.

Moreover, a wireless backhaul link makes it possible to deploy a small cell in places where it was economically infeasible to deploy a small cell before. That is mostly due to the high expense in providing wired connectivity at that specific place. Being a less expensive alternative to a wired backhaul link, a wireless backhaul link makes an **economic** contribution to the mobile operator's business.

In addition, the extended coverage and higher peak data rate provided by small cells are seen by the customers as an advantage of a mobile network. Better coverage and capacity of a mobile network distinguishes a given network from the competitors' networks and attracts new customers, which is another **economic** benefit of this work.

Because of business and **ethical** reasons the names of the APs' vendors benchmarked during this master's thesis project were not disclosed.

The deployment of small cells with wireless backhaul also has a positive **environmental** aspect in reducing the power consumption of the terminals (since they need less power to transmit to the small base station). However, there is a negative effect in the fact that the information has to be transmitted over a radio link twice - once to the base station and a second time to the mobile (and similarly for the reverse path). Despite this extra transmission, when directional antennas are used for the backhaul link the net transmission power over the whole coverage area is reduced. The issues raised by the interaction of the radio waves with tissue is outside the scope of this thesis project.

Bibliography

[1] Ericsson, "Differentiated mobile broadband," Jan. 2011. [Online]. Available: www.ericsson.com/res/docs/whitepapers/differentiated_mobile_broadband.pdf [Accessed: June 14, 2012].

[2] Ericsson, "Ericsson predicts mobile data traffic to grow 10-fold by 2016," Nov. 2011. [Online]. Available: www.ericsson.com/news/1561267 [Accessed: June 14, 2012].

[3] Cisco White Paper, "Cisco visual networking index: Global mobile data traffic forecast update, 2011-2016," Feb. 2012. [Online]. Available: cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf [Accessed: February 14, 2012].

[4] M. Donegan, "2011 Rewind: Where in the World Is LTE?" Dec. 2011. [Online]. Available: www.lightreading.com/document.asp?doc_id=215741 [Accessed: June 14, 2012].

[5] S. Landström, A. Furuskär, K. Johansson, L. Falconetti, and F. Kronestedt, "Heterogeneous networks – increasing cellular capacity," *Ericsson Review*, no. 1, Feb. 2011. [Online]. Available: www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2011/heterogeneous_networks.pdf [Accessed: June 14, 2012].

[6] G. K. Chesterton and J. Graham, *The Scandal of Father Brown: 7 Unabridged Stories*, unabridged ed. Audio Partners, Aug. 2001, ISBN 1572701811.

[7] J. Zhang and G. De la Roche, *Femtocells: technologies and deployment*. Chichester, West Susssex, U.K.; Hoboken, NJ: Wiley, 2010, ISBN 9780470742983.

[8] M. Sauter, *From GSM to LTE: an introduction to mobile networks and mobile broadband*. Chichester, West Sussex, U.K.; Hoboken, N.J.: Wiley, 2011, ISBN 9780470667118.

[9] S. Sesia, M. Baker, and I. Toufik, *LTE, the UMTS long term evolution : from theory to practice*. Chichester, U.K: Wiley, 2009, ISBN 9780470697160.

[10] M. Olsson, *SAE and the evolved packet core driving the mobile broadband revolution*. Amsterdam; Boston: Elsevier/Academic Press, 2009, ISBN 9780123748263.

[11] D. Wisely, *IP for 4G*. Chichester, U.K.: J. Wiley & Sons, 2009, ISBN 9780470510162.

[12] A. Behzad, *Wireless LAN radios system definition to transistor design*. New York Chichester: Wiley-IEEE, 2007, ISBN 9780470209301.

[13] J. Chen, H. Li, F. Zhang, and J. Wu, "MIMO Mode Switching Scheme for Rate Adaptation in 802.11n Wireless Networks," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, dec. 2011, pp. 1 –6.

[14] T. Jensen, S. Kant, J. Wehinger, and B. Fleury, "Fast Link Adaptation for MIMO OFDM," *Vehicular Technology, IEEE Transactions*, vol. 59, no. 8, pp. 3766 –3778, oct. 2010.

[15] IEEE Computer Society, *IEEE standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements. Part 11, Amendment 10, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. Mesh networking*. New York: Institute of Electrical and Electronics Engineers, 2011, ISBN 9780738167312. [Online]. Available: ieeexplore.ieee.org/servlet/opac?punumber=6018234

[16] G. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "IEEE 802.11s: The WLAN mesh standard," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 104–111, Feb. 2010. [Online]. Available: ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5416357 [Accessed: July 4, 2012].

[17] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," *Internet Request for Comments*, vol. RFC 4301 (Proposed Standard), Dec. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4301.txt Updated by RFC 6040.

[18] S. Kent, “IP Authentication Header,” *Internet Request for Comments*, vol. RFC 4302 (Proposed Standard), Dec. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4302.txt

[19] S. Kent, “IP Encapsulating Security Payload (ESP),” *Internet Request for Comments*, vol. RFC 4303 (Proposed Standard), Dec. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4303.txt

[20] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, “Internet Key Exchange Protocol Version 2 (IKEv2),” *Internet Request for Comments*, vol. RFC 5996 (Proposed Standard), Sep. 2010. [Online]. Available: http://www.ietf.org/rfc/rfc5996.txt Updated by RFC 5998.

[21] P. Calhoun, M. Montemurro, and D. Stanley, “Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification,” *Internet Request for Comments*, vol. RFC 5415 (Proposed Standard), Mar. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5415.txt

[22] P. Calhoun, M. Montemurro, and D. Stanley, “Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11,” *Internet Request for Comments*, vol. RFC 5416 (Proposed Standard), Mar. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5416.txt

[23] E. Rescorla and N. Modadugu, “Datagram Transport Layer Security,” *Internet Request for Comments*, vol. RFC 4347 (Proposed Standard), Apr. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4347.txt Obsoleted by RFC 6347, updated by RFC 5746.

[24] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” *Internet Request for Comments*, vol. RFC 5246 (Proposed Standard), Aug. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5246.txt Updated by RFCs 5746, 5878, 6176.

[25] 3GPP, *Security of Home Node B (HNB) / Home evolved Node B (HeNB)*, ser. TS, Jun. 2011, no. TS33.320, Rel-9 v9.6.0. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33320.htm

[26] 3GPP, *3G security; Wireless Local Area Network (WLAN) interworking security*, ser. TS, Jun. 2010, no. TS33.234, Rel-9 v9.2.0. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33234.htm

[27] “IEEE standard for local and metropolitan area networks - port-based network access control,” *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)*, pp. C1 –205, May 2010.

[28] V. Shrivastava, S. Rayanchu, J. Yoonj, and S. Banerjee, “802.11n under the microscope,” in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, ser. IMC ’08. New York, NY, USA: ACM, 2008, pp. 105–110, ISBN 9781605583341. [Online]. Available: doi.acm.org/10.1145/1452520.1452533

[29] K. Pelechrinis, H. Lundgren, N. Vaidya, and T. Salonidis, “Analyzing 802.11n performance gains,” in *Proceedings of the ACM MobiCom (poster session)*, Beijing, China, 2009. [Online]. Available: www.cs.ucr.edu/~kpele/mobipost-paper16.pdf

[30] I. Sheriff, P. A. K. Acharya, and E. M. Belding, “Resource estimation on wireless backhaul networks,” in *Proceedings of the 3rd international conference on Wireless internet*, ser. WICON ’07. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2007, pp. 11:1–11:10. [Online]. Available: dl.acm.org/citation.cfm?id=1460047.1460061

[31] E. M. Mohamed, D. Kinoshita, K. Mitsunaga, and Y. Higaand H. Furukawa, “IEEE 802.11n based wireless backhaul enabled by dual channel IPT (DCH-IPT) relaying protocol.” Moscow, Russia: IEEE, Oct. 2010, pp. 525–530. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5676587

[32] 3GPP, *Feasibility study for evolved Universal Terrestrial Radio Access (UTRA) and Universal Terrestrial Radio Access Network (UTRAN)*, ser. TR, Oct. 2009, no. TR25.912, Rel-9 v9.0.0. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/25912.htm

[33] “IEEE standard for information technology– local and metropolitan area networks– specific requirements–part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: Enhancements for higher throughput,” *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009)*, pp. 1 –565, 29 2009.

[34] Julius Robson, “Guidelines for LTE Backhaul Traffic Estimation,” Next Generation Mobile Networks Alliance, Tech. Rep., 2011. [Online]. Available: www.ngmn.org/uploads/media/NGMN_Whitepaper_Guideline_for_LTE_Backhaul_Traffic_Estimation.pdf

[35] Next Generation Mobile Networks Alliance, “Small Cell Backhaul Requirements,” Tech. Rep., 2011, Internal Draft.

[36] Epitiro Company, “LTE "real world" performance study,” 2011. [Online]. Available: www.epitiro.com/assets/files/LTE%20Real%20World%20Performance%20Report-Finland.pdf [Accessed: June 14, 2012].

[37] Signals Research Group, “AT&T goes live with LTE,” Sep. 2011. [Online]. Available: www.signalsresearch.com/NewDetails.aspx?id=43 [Accessed: June 14, 2012].

[38] Bill Moore, “Solving the LTE puzzle: comparing LTE performance,” Apr. 2012. [Online]. Available: gigaom.com/2012/04/14/solving-the-lte-puzzle-comparing-lte-performance/ [Accessed: June 14, 2012].

[39] William Van Winkle, “Why Your Wi-Fi Sucks And How It Can Be Helped, Part 2,” Tom’s Hardware, Tech. Rep., Jul. 2011, [Accessed: April 26, 2012]. [Online]. Available: www.tomshardware.com/reviews/wi-fi-performance,2985.html

[40] Allot Communications, “MobileTrends Report H1, 2011,” 2011. [Online]. Available: www.allot.com/MobileTrends_Report_H1_2011.html [Accessed: April 28, 2012].

[41] IDATE, “Mobile traffic forecasts 2010-2020,” *UMTS Forum Report*, no. 44, Jan. 2011. [Online]. Available: www.umts-forum.org/component/option,com_docman/task,cat_view/gid,485/Itemid,213/ [Accessed: June 12, 2012].

[42] ITU-T Recommendation G.114, “One-way transmission time,” International Telecommunication Union, Tech. Rep., 2003. [Online]. Available: www.itu.int/rec/T-REC-G.114-200305-I

[43] P. Calyam, M. Sridharan, W. M, and P. Schopis, “Performance measurement and analysis of H.323 traffic,” in *Proc. of Passive and Active Measurement Workshop*. Springer, 2004.

[44] 3GPP, *Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN)*, ser. TR, Dec. 2009, no. TR25.913, Rel-9 v9.0.0. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/25913.htm

[45] Kevin Miller, “Calculating Optical Fiber Latency,” Jan. 2012. [Online]. Available:

www.m2optics.com/blog/bid/70587/Calculating-Optical-Fiber-Latency [Accessed: June 21, 2012].

[46] "XM2 Portable Chassis," Oct. 2009. [Online]. Available: www.ixiacom.com/products/chassis/display?skey=ch_optixia_xm2 [Accessed: June 16, 2012].

[47] "XMVR LAN Services Modules," Nov. 2010. [Online]. Available: www.ixiacom.com/products/interfaces/display?skey=in_gigabit_ethernet_xmv_lan_modules [Accessed: June 16, 2012].

[48] ITU-T Recommendation G.8261, "Timing and synchronization aspects in packet networks," International Telecommunication Union, Tech. Rep., 2008. [Online]. Available: www.itu.int/rec/T-REC-G.8261-200804-I

[49] V. Prokopov and P. Legonkov, "Detailed test report for measurements of IEEE 802.11n link. Point-to-point scenario. Vendor A." May 2012. [Online]. Available: dl.dropbox.com/u/1117969/thesis/TestSpec1.pdf [Accessed: June 14, 2012].

[50] V. Prokopov and P. Legonkov, "Detailed test report for measurements of IEEE 802.11n link. Point-to-point scenario. Vendor B." May 2012. [Online]. Available: dl.dropbox.com/u/1117969/thesis/TestSpec2.pdf [Accessed: June 14, 2012].

[51] V. Prokopov and P. Legonkov, "Detailed test report for measurements of IEEE 802.11n link. Interference scenario." May 2012. [Online]. Available: dl.dropbox.com/u/1117969/thesis/TestSpec3.pdf [Accessed: June 14, 2012].

[52] A. Ashtaiwi and H. Hassanein, "Enhancements to IEEE 802.11 DCF collision avoidance based on MIMO Adaptive Spatial Channels Sharing," in *Computers and Communications, 2009. ISCC 2009. IEEE Symposium on*, july 2009, pp. 564 –569.

[53] S. Abraham, A. Meylan, and S. Nanda, "802.11n MAC design and system performance," in *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, vol. 5, may 2005, pp. 2957 – 2961 Vol. 5.

[54] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," *Internet Request for Comments*, vol. RFC 4033 (Proposed Standard), Mar. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4033.txt Updated by RFC 6014.

Appendix A

Experimental study results

The major part of the results obtained during the experimental study (see Section 3.3) is provided below in form of tables. Full test specifications arranged by a measurement scenario are available at [49], [50] and [51].

Table A.1: Measurement results for Vendor A, point-to-point scenario, cables, 3x3 MIMO, 40 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Tx. pwr., dBm	MCS index	Throughput, Mbps			Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern
						A-B	B-A	Agg.				
1	3x3	40	0	25	23	150	149	299	67	115	-38	Large frame
2	3x3	40	10	25	23	148	152	300	63	115	-48	Large frame
3	3x3	40	15	25	23	150	154	304	59	112	-53	Large frame
4	3x3	40	20	25	23/22	128	129	257	85	128	-59	Large frame
5	3x3	40	25	25	21	114	115	229	128	138	-64	Large frame
6	3x3	40	30	25	12	54	55	109	250	207	-68	Large frame
7	3x3	40	35	25	4	28	30	58	8205	325	-72	Large frame
8	3x3	40	40	25	2	12	13	25	537	700	-77	Large frame
9	3x3	40	45	25	1	7	7	14	998	1580	-82	Large frame
10	3x3	40	50	25	0	1.7	1.5	3.2	5380	3800	-86	Large frame
11	3x3	40	55	25	0	0.4	0.5	0.9	15000	10000	-88	Large frame
			60			0	0	0			-92	
12	3x3	40	0	25	23	60	63	123	40	76	-39	Cust. IMIX
13	3x3	40	10	25	23	61	61	122	40	81	-48	Cust. IMIX
14	3x3	40	15	25	23	63	64	127	40	79	-52	Cust. IMIX
15	3x3	40	20	25	23	62	63	125	38	79	-57	Cust. IMIX
16	3x3	40	25	25	22	50	50	100	65	90	-62	Cust. IMIX
17	3x3	40	30	25	12	36	36	72	160	103	-68	Cust. IMIX
18	3x3	40	35	25	4	26	25	51	112	150	-73	Cust. IMIX
19	3x3	40	40	25	2	11	12	23	250	260	-77	Cust. IMIX
20	3x3	40	45	25	1	8	8	16	250	350	-82	Cust. IMIX
21	3x3	40	50	25	0	2	2	4	7500	1400	-85	Cust. IMIX
22	3x3	40	55	25	0	1.1	0.9	2	5500	2200	-88	Cust. IMIX
			60			0	0	0			-92	

Table A.2: Measurement results for Vendor A, point-to-point scenario, cables, 2x2 MIMO, 40 MHz channel

#	**MIMO mode**	**Chan. width, MHz**	**Att., dB**	**Tx. pwr., dBm**	**MCS index**	**Throughput, Mbps**			**Max. latency, ms**	**Jitter, µs**	**RSSI, dBm**	**Traffic pattern**
						A-B	**B-A**	**Agg.**				
23	2x2	40	0	23	15	107	106	213	97	150	-39	Large frame
24	2x2	40	10	23	15	108	108	216	87	145	-49	Large frame
25	2x2	40	15	23	15	112	112	224	80	138	-54	Large frame
26	2x2	40	20	23	15	110	110	220	82	144	-59	Large frame
27	2x2	40	25	23	14/13	63	64	127	280	203	-64	Large frame
28	2x2	40	30	23	5	33	33	66	279	450	-69	Large frame
29	2x2	40	35	23	4	29	30	59	271	400	-75	Large frame
30	2x2	40	40	23	2	11	11	22	1150	672	-80	Large frame
31	2x2	40	45	23	0	3	3.5	6.5	4400	2500	-84	Large frame
32	2x2	40	50	23	0	1.7	1.8	3.5	3500	5900	-87	Large frame
			55			0	0	0			-92	
33	2x2	40	0	23	15	55	55	110	50	82	-39	Cust. IMIX
34	2x2	40	10	23	15	55	57	112	53	83	-49	Cust. IMIX
35	2x2	40	15	23	15	58	58	116	48	81	-54	Cust. IMIX
36	2x2	40	20	23	15	58	59	117	101	82	-60	Cust. IMIX
37	2x2	40	25	23	15	36	37	73	107	117	-65	Cust. IMIX
38	2x2	40	30	23	5	25	26	51	120	160	-70	Cust. IMIX
39	2x2	40	35	23	4	24	24	48	108	173	-75	Cust. IMIX
40	2x2	40	40	23	2	10	10	20	199	320	-80	Cust. IMIX
41	2x2	40	45	23	0	2.5	2.5	5	986	1100	-85	Cust. IMIX
42	2x2	40	50	23	0	1.1	1.1	2.2	1163	1180	-89	Cust. IMIX
			55			0	0	0			-92	

Table A.3: Measurement results for Vendor A, point-to-point scenario, cables, 1x1 MIMO, 40 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Tx. pwr., dBm	MCS index	Throughput, Mbps			Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern
						A-B	B-A	Agg.				
43	1x1	40	0	20	7	55	56	111	167/161	200/197	-42	Large frame
44	1x1	40	10	20	7	49	56	105	183/151	230/190	-52	Large frame
45	1x1	40	15	20	7	54	57	111	146/153	225/195	-56	Large frame
46	1x1	40	20	20	7	44	57	101	195/160	330/227	-61	Large frame
47	1x1	40	25	20	5	39	40	79	227/217	245/261	-66	Large frame
48	1x1	40	30	20	4	29	31	60	264/250	313/313	-71	Large frame
49	1x1	40	35	20	2	12	12	24	550/570	815/801	-77	Large frame
50	1x1	40	40	20	1	8	8	16	699/758	1100/1200	-82	Large frame
51	1x1	40	45	20	0	2.3	2.2	4.5	2000/2200	2900/2900	-86	Large frame
52	1x1	40	50	20	0	1.4	1.6	3	5400/5500	2700/3100	-90	Large frame
			55			0	0	0			-92	
53	1x1	40	0	20	7	37	39	76	69/71	108/110	-42	Cust. IMIX
54	1x1	40	10	20	7	38	38	76	61/75	116/118	-52	Cust. IMIX
55	1x1	40	15	20	7	37	39	76	68/66	117/114	-56	Cust. IMIX
56	1x1	40	20	20	7	31	39	70	78/62	140/113	-61	Cust. IMIX
57	1x1	40	25	20	5	28	27	55	123/137	149/151	-67	Cust. IMIX
58	1x1	40	30	20	4	26	24	50	132/119	161/156	-72	Cust. IMIX
59	1x1	40	35	20	2	10	10	20	233/227	287/291	-77	Cust. IMIX
60	1x1	40	40	20	1	8	8	16	510/512	351/352	-82	Cust. IMIX
61	1x1	40	45	20	0	2.1	2.2	4.3	933/930	1352/1346	-86	Cust. IMIX
62	1x1	40	50	20	0	1.8	1.9	3.7	2186/2177	1523/1537	-90	Cust. IMIX
			55			0	0	0			-92	

Table A.4: Measurement results for Vendor A, point-to-point scenario, cables, 3x3 MIMO, 20 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Tx. pwr., dBm	MCS index	Throughput, Mbps			Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern
						A-B	B-A	Agg.				
63	3x3	20	0	25	23	83	84	167	106/96	160/155	-38	Large frame
64	3x3	20	10	25	23	81	85	166	95/111	171/172	-48	Large frame
65	3x3	20	15	25	23	82	83	165	105/105	173/171	-52	Large frame
66	3x3	20	20	25	23	84	82	166	106/100	170/171	-57	Large frame
67	3x3	20	25	25	23/22	77	71	148	111/143	214/240	-62	Large frame
68	3x3	20	30	25	14/13	39	32	71	275/344	490/450	-67	Large frame
69	3x3	20	35	25	5	14	14	28	618/550	1023/1023	-73	Large frame
70	3x3	20	40	25	4	13	14	27	490/495	640/641	-77	Large frame
71	3x3	20	45	25	2	5	8	13	1300/900	1900/1300	-81	Large frame
72	3x3	20	50	25	1	4.5	4.5	9	2000/1500	2500/2500	-86	Large frame
73	3x3	20	53	25	0	0.2	0.2	0.4	17k/18k	11k/13k	-88	Large frame
			55			0	0	0			-92	
74	3x3	20	0	25	23	50	51	101	53/57	84/84	-39	Cust. IMIX
75	3x3	20	10	25	23	50	49	99	54/58	93/95	-48	Cust. IMIX
76	3x3	20	15	25	23	50	50	100	50/48	93/95	-53	Cust. IMIX
77	3x3	20	20	25	23	51	49	100	47/54	93/96	-58	Cust. IMIX
78	3x3	20	25	25	23/22	47	43	90	69/78	95/100	-63	Cust. IMIX
79	3x3	20	30	25	21/15	26	24	50	127/141	149/161	-68	Cust. IMIX
80	3x3	20	35	25	12	23	19	42	182/193	165/173	-73	Cust. IMIX
81	3x3	20	40	25	4	10	12	22	205/171	367/298	-78	Cust. IMIX
82	3x3	20	45	25	2	6	5	11	394/444	586/810	-83	Cust. IMIX
83	3x3	20	50	25	1	3.6	3.4	7	775/816	1062/1094	-86	Cust. IMIX
84	3x3	20	55	25	0	1.9	1.6	3.5	3332/3770	1665/1776	-88	Cust. IMIX
			55			0	0	0			-92	

Table A.5: Measurement results for Vendor A, point-to-point scenario, cables, 2x2 MIMO, 20 MHz channel

#	**MIMO mode**	**Chan. width, MHz**	**Att., dB**	**Tx. pwr., dBm**	**MCS index**	**Throughput, Mbps**			**Max. latency, ms**	**Jitter, µs**	**RSSI, dBm**	**Traffic pattern**
						A-B	**B-A**	**Agg.**				
85	2x2	20	0	23	15	51	52	103	173/162	232/228	-40	Large frame
86	2x2	20	10	23	15	50	54	104	181/169	229/217	-50	Large frame
87	2x2	20	15	23	15	58	58	116	148/134	226/217	-55	Large frame
88	2x2	20	20	23	15	58	58	116	150/140	208/201	-60	Large frame
89	2x2	20	25	23	15	57	53	110	140/166	227/273	-65	Large frame
90	2x2	20	30	23	13	32	30	62	307/324	442/476	-70	Large frame
91	2x2	20	35	23	4	12	13	25	552/529	758/788	-74	Large frame
92	2x2	20	40	23	4	8.5	13	21.5	1000/500	1900/800	-80	Large frame
93	2x2	20	45	23	2	8	5	13	800/1400	1000/1900	-84	Large frame
94	2x2	20	50	23	0	2.7	2.7	5.4	4200/2900	2600/1800	-88	Large frame
			55			0	0	0			-92	
95	2x2	20	0	23	15	39	36	75	69/65	113/105	-40	Cust. IMIX
96	2x2	20	10	23	15	38	35	73	71/59	112/109	-50	Cust. IMIX
97	2x2	20	15	23	15	40	40	80	61/58	113/113	-55	Cust. IMIX
98	2x2	20	20	23	15	41	40	81	63/59	112/113	-60	Cust. IMIX
99	2x2	20	25	23	15	41	39	80	62/68	113/118	-65	Cust. IMIX
100	2x2	20	30	23	13	26	23	49	118/122	177/196	-70	Cust. IMIX
101	2x2	20	35	23	4	11	12	23	245/191	261/239	-75	Cust. IMIX
102	2x2	20	40	23	4	7	12	19	297/181	411/243	-80	Cust. IMIX
103	2x2	20	45	23	3	6.6	4.5	11.1	327/484	390/439	-84	Cust. IMIX
104	2x2	20	50	23	2	4.4	3.7	8.1	644/529	627/712	-88	Cust. IMIX
			55			0	0	0			-92	

Table A.6: Measurement results for Vendor A, point-to-point scenario, cables, 1x1 MIMO, 20 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Tx. pwr., dBm	MCS index	Throughput, Mbps			Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern
						A-B	B-A	Agg.				
105	1x1	20	0	20	7	27	27	54	290/275	283/297	-43	Large frame
106	1x1	20	10	20	7	27	27	54	262/286	283/308	-53	Large frame
107	1x1	20	15	20	7	26	27	53	273/275	291/290	-58	Large frame
108	1x1	20	20	20	7	27	28	55	265/270	290/290	-63	Large frame
109	1x1	20	25	20	7/6	24	24	48	330/325	680/720	-68	Large frame
110	1x1	20	30	20	5	14	13	27	530/550	1030/1140	-74	Large frame
111	1x1	20	35	20	4	14	14	28	467/480	650/660	-79	Large frame
112	1x1	20	40	20	3	7	8	15	1020/830	1400/1030	-83	Large frame
113	1x1	20	45	20	2	4	6	10	1870/1430	2600/1900	-87	Large frame
114	1x1	20	50	20	0	1.7	1.6	3.3	5000/5020	5100/5400	-91	Large frame
			55			0	0	0			-92	
115	1x1	20	0	20	7	24	23	47	101/111	159/160	-42	Cust. IMIX
116	1x1	20	10	20	7	23	24	47	97/101	160/159	-52	Cust. IMIX
117	1x1	20	15	20	7	24	23	47	98/97	159/160	-57	Cust. IMIX
118	1x1	20	20	20	7	24	23	47	104/107	160/159	-62	Cust. IMIX
119	1x1	20	25	20	7	22	20	42	112/128	192/207	-68	Cust. IMIX
120	1x1	20	30	20	5	14	13	27	192/206	295/320	-74	Cust. IMIX
121	1x1	20	35	20	4	13	12	25	172/162	277/292	-79	Cust. IMIX
122	1x1	20	40	20	3	5.9	5.3	11.2	347/386	657/689	-83	Cust. IMIX
123	1x1	20	45	20	1	2.9	4.4	7.3	818/572	1063/719	-88	Cust. IMIX
124	1x1	20	50	20	0	0.9	0.8	1.7	2108/2503	3119/3125	-91	Cust. IMIX
			55			0	0	0			-92	

Table A.7: Measurement results for Vendor A, point-to-point scenario, small panel antenna, 3x3 MIMO, 40 MHz channel

#	**MIMO mode**	**Att., dB**	**MCS index**	**Throughput, Mbps**			**Min. latency, ms**	**Max. latency, ms**	**Jitter, µs**	**RSSI, dBm**	**Traffic pattern**	**Antenna**
				A-B	**B-A**	**Agg.**						
125	3x3	0	23	153	153	306	0.8/0.55	44/50	112/113	-42	Large frame	Small panel
126	3x3	0	23	125	125	250	1.1/0.6	43/40	97/97	-42	ITU-T IMIX	Small panel
127	3x3	10	23	125	125	250	0.7/0.45	39/39	97/97	-52	ITU-T IMIX	Small panel
128	3x3	15	23/22	98	110	208	0.6/0.35	54/25	130/112	-57	ITU-T IMIX	Small panel
129	3x3	20	21/15	61	61	122	0.45/0.53	40/79	219/201	-62	ITU-T IMIX	Small panel
130	3x3	25	12	47	50	97	0.58/0.53	108/101	223/206	-67	ITU-T IMIX	Small panel
131	3x3	30	4	28	28	56	1/0.5	155/168	335/338	-71	ITU-T IMIX	Small panel
132	3x3	35	4	22	22	44	0.3/0.3	84/79	600/600	-75	ITU-T IMIX	Small panel
133	3x3	40	1	5	8	13	0.2/0.2	52/158	1800/1300	-80	ITU-T IMIX	Small panel
134	3x3	45	0	3	2	5	0.2/0.2	74/122	2500/2200	-83	ITU-T IMIX	Small panel
135	3x3	50	0	1.8	1.8	3.6	0.3/0.3	130/130	4500/4500	-86	ITU-T IMIX	Small panel
136	3x3	55	0	0.6	1	1.6	0.3/0.3	300/100	3800/2500	-88	ITU-T IMIX	Small panel
		60		0	0	0				-92		

Transmit power: 25 dBm.

Table A.8: Measurement results for Vendor A, point-to-point scenario, small panel antenna, 2x2 MIMO, 40 MHz channel

#	MIMO mode	Att., dB	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern	Antenna
				A-B	B-A	Agg.						
137	2x2	0	15	114	112	226	0.7/0.8	63/66	141/144	-44	Large frame	Small panel
138	2x2	0	15	99	100	199	0.7/0.4	50/45	120/119	-44	ITU-T IMIX	Small panel
139	2x2	10	15	99	100	199	0.4/0.7	53/50	120/119	-54	ITU-T IMIX	Small panel
140	2x2	15	15	98	99	197	0.4/0.8	53/49	122/122	-59	ITU-T IMIX	Small panel
141	2x2	20	14	54	56	110	0.7/0.3	100/47	250/235	-64	ITU-T IMIX	Small panel
142	2x2	25	5	33	35	68	0.7/0.7	206/101	401/365	-69	ITU-T IMIX	Small panel
143	2x2	30	4	29	30	59	0.7/0.8	142/147	318/315	-76	ITU-T IMIX	Small panel
144	2x2	35	2	12	13	25	0.2/0.2	118/205	1100/1000	-81	ITU-T IMIX	Small panel
145	2x2	40	0	2	2	4	0.3/0.3	92/95	2300/2700	-86	ITU-T IMIX	Small panel
146	2x2	45	0	1.7	1.7	3.4	0.3/0.3	67/83	2600/2700	-88	ITU-T IMIX	Small panel
		50		0	0	0				-92	ITU-T IMIX	Small panel

Transmit power: 23 dBm.

Table A.9: Measurement results for Vendor A, point-to-point scenario, big panel antenna, 2x2 MIMO, 40 MHz channel

#	MIMO mode	Att., dB	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern	Antenna
				A-B	B-A	Agg.						
147	2x2	0	15	113	113	226	0.6/1	62/64	143/143	-39	Large frame	Big panel
148	2x2	0	15	99	99	198	0.9/0.5	46/36	119/120	-39	ITU-T IMIX	Big panel
149	2x2	10	15	99	99	198	0.7/0.5	45/48	120/120	-49	ITU-T IMIX	Big panel
150	2x2	15	15	94	99	193	0.9/0.5	72/44	213/123	-54	ITU-T IMIX	Big panel
151	2x2	20	13	50	62	112	0.5/0.4	53/97	271/197	-59	ITU-T IMIX	Big panel
152	2x2	25	7	47	50	97	0.7/0.7	109/73	257/211	-64	ITU-T IMIX	Big panel
153	2x2	30	5	34	34	68	0.7/0.4	92/76	350/330	-68	ITU-T IMIX	Big panel
154	2x2	35	4	28	28	56	0.5/0.7	107/89	330/330	-74	ITU-T IMIX	Big panel
155	2x2	40	2	11	11	22	0.3/0.3	74/79	650/650	-79	ITU-T IMIX	Big panel
156	2x2	45	0	4	4	8	0.3/0.3	280/260	1600/1600	-83	ITU-T IMIX	Big panel
157	2x2	50	0	2	2	4	0.3/0.3	173/144	2900/2900	-86	ITU-T IMIX	Big panel
		55		0	0	0				-92	ITU-T IMIX	Big panel

Transmit power: 23 dBm.

Table A.10: Measurement results for Vendor B, point-to-point scenario, cables, 2x2 MIMO, 40 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Tx. pwr., dBm	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern
						A-B	B-A	Agg.					
158	2x2	40	0	17	15	86	84	170	6.3/4.8	48/49	160/154	-39	Large frame
159	2x2	40	10	17	15	99	98	197	5.5/1.6	45/45	150/145	-46	Large frame
160	2x2	40	15	17	15	93	94	187	2.6/0.6	45/46	121/115	-51	Large frame
161	2x2	40	20	17	15	99	97	196	3.3/0.8	28/36	120/117	-56	Large frame
162	2x2	40	25	17	15	98	98	196	1.5/3.0	38/38	97/92	-62	Large frame
163	2x2	40	30	17	15	100	98	198	0.7/1.2	34/38	103/107	-66	Large frame
164	2x2	40	35	17	14	90	83	173	0.5/0.7	242/299	122/150	-71	Large frame
165	2x2	40	40	17	12	45	49	94	7.1/0.7	512/623	250/260	-76	Large frame
166	2x2	40	45	17	12	36	14	50	0.8/8.7	1500/780	492/138	-80	Large frame
167	2x2	40	50	17	11	18	12	30	0.6/0.3	1700/800	750/200	-83	Large frame
168	2x2	40	55	17	10	9	10	19	0.6/0.6	4300/900	1900/1100	-87	Large frame
169	2x2	40	58	17	8	1.5	6.5	8	19.9/2.3	19k/2800	10k/500	-91	Large frame
			60			0	0	0				-93	
170	2x2	40	0	17	15	22	21	43	1.0/0.3	133/128	90/81	-39	Cust. IMIX
171	2x2	40	10	17	15	24	23	47	8.0/7.5	154/130	101/95	-44	Cust. IMIX
172	2x2	40	15	17	15	24	24	48	1.0/0.4	107/81	93/100	-49	Cust. IMIX
173	2x2	40	20	17	15	23	23	46	1.5/2.0	97/115	94/99	-54	Cust. IMIX
174	2x2	40	25	17	15	23	23	46	4.5/9.0	78/107	93/100	-60	Cust. IMIX
175	2x2	40	30	17	15/14	24	24	48	2.5/7.0	103/121	95/102	-65	Cust. IMIX
176	2x2	40	35	17	15/14	22	22	44	6.5/9.0	96/115	99/114	-70	Cust. IMIX
177	2x2	40	40	17	13	21	21	42	5.0/2.5	963/957	104/116	-75	Cust. IMIX
178	2x2	40	45	17	12	17	19	36	0.4/0.3	508/236	190/165	-79	Cust. IMIX
179	2x2	40	50	17	10	6	14	20	0.8/0.4	1069/330	534/185	-85	Cust. IMIX
180	2x2	40	55	17	10	4	15	19	0.5/0.4	2773/517	634/172	-88	Cust. IMIX
181	2x2	40	58	17	8	1	7	8	1.9/0.3	15k/1534	8400/407	-92	Cust. IMIX
			60			0	0	0				-93	

Table A.11: Measurement results for Vendor B, point-to-point scenario, cables, 1x1 MIMO, 40 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Tx. pwr., dBm	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern
						A-B	B-A	Agg.					
182	1x1	40	0	17	4/3	19	22	41	0.4/0.5	630/245	990/580	-37	Large frame
183	1x1	40	10	17	7	51	51	102	0.4/0.5	22/22	267/267	-45	Large frame
184	1x1	40	15	17	7	52	53	105	0.5/0.5	29/37	250/250	-51	Large frame
185	1x1	40	20	17	7	45	45	90	0.4/0.4	18/14	266/264	-55	Large frame
186	1x1	40	25	17	7	44	44	88	0.4/0.4	16/20	300/300	-61	Large frame
187	1x1	40	30	17	7	49	50	99	0.5/0.5	23/21	270/270	-64	Large frame
188	1x1	40	35	17	6	43	42	85	0.5/0.5	34/44	330/340	-70	Large frame
189	1x1	40	40	17	4	23	23	46	0.5/0.5	86/63	470/470	-74	Large frame
190	1x1	40	45	17	4	22	22	44	0.5/0.5	380/140	750/702	-78	Large frame
191	1x1	40	50	17	3	13	13	26	0.6/0.6	705/240	1300/1100	-82	Large frame
192	1x1	40	55	17	2	7	8	15	0.6/0.6	341/204	2200/1700	-87	Large frame
193	1x1	40	58	17	2/1	4	4	8	0.7/0.7	661/211	4000/3600	-89	Large frame
194	1x1	40	0	17	4	11	11	22	0.3/0.3	323/134	404/369	-37	Cust. IMIX
195	1x1	40	10	17	7	23	25	48	0.1/0.1	36/48	127/110	-44	Cust. IMIX
196	1x1	40	15	17	7	24	25	49	0.2/0.7	37/38	119/111	-49	Cust. IMIX
197	1x1	40	20	17	7	24	24	48	0.3/0.8	35/35	117/119	-54	Cust. IMIX
198	1x1	40	25	17	7	24	25	49	0.3/0.9	47/41	119/111	-59	Cust. IMIX
199	1x1	40	30	17	7	24	25	49	0.5/0.7	39/48	119/112	-64	Cust. IMIX
200	1x1	40	35	17	6	24	23	47	0.4/0.3	54/83	130/124	-69	Cust. IMIX
201	1x1	40	40	17	5/4	18	20	38	0.4/0.3	124/63	209/179	-74	Cust. IMIX
202	1x1	40	45	17	4	7	12	19	0.3/0.2	372/62	399/230	-79	Cust. IMIX
203	1x1	40	50	17	2	4	7	11	0.3/0.3	435/131	944/450	-85	Cust. IMIX
204	1x1	40	55	17	2	4	6	10	0.2/0.2	504/242	877/467	-88	Cust. IMIX
205	1x1	40	58	17	2/1	2	4	6	0.2/0.2	585/198	2045/883	-89	Cust. IMIX

Table A.12: Measurement results for Vendor B, point-to-point scenario, cables, 2x2 MIMO, 20 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Tx. pwr., dBm	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern
						A-B	B-A	Agg.					
206	2x2	20	0	17	15	46	46	92	0.5/0.5	186/112	414/419	-38	Large frame
207	2x2	20	10	17	15	55	55	110	0.4/0.5	45/29	255/253	-44	Large frame
208	2x2	20	15	17	15	54	54	108	0.5/0.5	34/31	253/252	-49	Large frame
209	2x2	20	20	17	15	53	54	107	0.5/0.5	37/23	258/252	-55	Large frame
210	2x2	20	25	17	15	53	54	107	0.5/0.5	34/43	260/252	-60	Large frame
211	2x2	20	30	17	15	53	53	106	0.5/0.6	39/41	259/260	-64	Large frame
212	2x2	20	35	17	15	54	53	107	0.5/0.5	41/39	271/277	-70	Large frame
213	2x2	20	40	17	14/13	44	44	88	0.4/0.5	195/200	384/365	-75	Large frame
214	2x2	20	45	17	12	28	29	57	0.5/0.5	412/330	480/455	-79	Large frame
215	2x2	20	50	17	11	12	15	27	0.5/0.6	501/172	1650/890	-82	Large frame
216	2x2	20	55	17	10	9	12	21	0.6/0.7	480/306	1681/1146	-86	Large frame
217	2x2	20	58	17	10	8	12	20	0.7/0.7	395/228	2140/1200	-89	Large frame
			60			0	0	0				-93	
218	2x2	20	0	17	15/12	14	15	29	0.3/0.5	104/99	170/160	-38	Cust. IMIX
219	2x2	20	10	17	15	22	22	44	0.3/0.3	31/26	136/136	-43	Cust. IMIX
220	2x2	20	15	17	15	23	22	45	0.4/0.4	32/30	139/136	-48	Cust. IMIX
221	2x2	20	20	17	15	22	22	44	0.3/0.5	31/28	126/127	-55	Cust. IMIX
222	2x2	20	25	17	15	20	21	41	0.6/0.3	33/30	130/128	-60	Cust. IMIX
223	2x2	20	30	17	15	23	23	46	0.4/0.3	31/31	127/129	-65	Cust. IMIX
224	2x2	20	35	17	15	23	23	46	0.3/0.5	126/126	127/129	-70	Cust. IMIX
225	2x2	20	40	17	14/13	23	23	46	0.3/0.3	141/121	166/166	-75	Cust. IMIX
226	2x2	20	45	17	12	15	18	33	0.3/0.3	690/60	230/170	-80	Cust. IMIX
227	2x2	20	50	17	12	7	7	14	0.3/0.3	430/151	650/630	-83	Cust. IMIX
228	2x2	20	55	17	10	4	6	10	0.3/0.3	877/210	760/460	-86	Cust. IMIX
229	2x2	20	58	17	10/9	2	3	5	0.3/0.3	904/271	1300/770	-90	Cust. IMIX
			60			0	0	0				-93	

Table A.13: Measurement results for Vendor B, point-to-point scenario, cables, 1x1 MIMO, 20 MHz channel

#	**MIMO mode**	**Chan. width, MHz**	**Att., dB**	**Tx. pwr., dBm**	**MCS index**	**Throughput, Mbps**			**Min. latency, ms**	**Max. latency, ms**	**Jitter, µs**	**RSSI, dBm**	**Traffic pattern**
						A-B	**B-A**	**Agg.**					
230	1x1	20	0	17	4	10	13	23	0.7/0.7	273/242	1549/1265	-38	Large frame
231	1x1	20	10	17	7	27	28	55	0.5/0.7	52/71	495/466	-43	Large frame
232	1x1	20	15	17	7	27	28	55	0.5/0.5	43/34	495/469	-48	Large frame
233	1x1	20	20	17	7	27	28	55	0.5/0.5	49/47	500/463	-54	Large frame
234	1x1	20	25	17	7	26	28	54	0.5/0.5	72/32	493/478	-60	Large frame
235	1x1	20	30	17	7	27	27	54	0.6/0.5	36/35	486/485	-65	Large frame
236	1x1	20	35	17	7	27	27	54	0.5/0.5	95/74	544/528	-70	Large frame
237	1x1	20	40	17	6/5	20	22	42	0.6/0.6	126/163	757/658	-75	Large frame
238	1x1	20	45	17	4	14	15	29	0.7/0.7	227/226	948/856	-80	Large frame
239	1x1	20	50	17	2	4	7	11	0.8/0.8	224/152	1130/850	-84	Large frame
240	1x1	20	55	17	2	4	6	10	0.8/0.8	297/234	1150/714	-87	Large frame
241	1x1	20	58	17	2	4	4	8	1.0/0.9	245/294	1100/820	-90	Large frame
242	1x1	20	0	17	4	7	10	17	0.3/0.3	600/112	575/400	-38	Cust. IMIX
243	1x1	20	10	17	7	14	18	32	0.3/0.3	37/48	250/180	-43	Cust. IMIX
244	1x1	20	15	17	7	14	18	32	0.4/0.4	43/50	152/180	-50	Cust. IMIX
245	1x1	20	20	17	7	16	18	34	0.3/0.4	73/120	220/185	-54	Cust. IMIX
246	1x1	20	25	17	7	16	18	34	0.5/0.5	67/97	220/185	-60	Cust. IMIX
247	1x1	20	30	17	7	14	16	30	0.3/0.4	33/45	260/220	-65	Cust. IMIX
248	1x1	20	35	17	7	14	16	30	0.3/0.4	30/26	255/220	-70	Cust. IMIX
249	1x1	20	40	17	6/5	13	16	29	0.3/0.4	100/69	283/230	-75	Cust. IMIX
250	1x1	20	45	17	4	8	10	18	0.3/0.3	160/80	450/350	-81	Cust. IMIX
251	1x1	20	50	17	4/3	4	8	12	0.3/0.3	312/118	1000/500	-83	Cust. IMIX
252	1x1	20	55	17	3	4	2	6	0.3/0.3	1000/580	933/550	-87	Cust. IMIX
253	1x1	20	58	17	2	2	3	5	0.3/0.3	152/85	690/480	-89	Cust. IMIX

Table A.14: Measurement results for Vendor B, point-to-point scenario, small panel antenna, 2x2 MIMO, 40 MHz channel

#	MIMO mode	Att., dB	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern	Antenna
				A-B	B-A	Agg.						
254	2x2	0	15	100	100	200	0.6/0.7	39/36	117/116	-44	Large frame	Small panel
255	2x2	0	15	62	62	124	0.5/0.4	90/71	129/128	-44	ITU-T IMIX	Small panel
256	2x2	10	15	67	67	134	0.3/0.7	22/25	115/115	-54	ITU-T IMIX	Small panel
257	2x2	15	15	67	67	134	0.5/0.3	29/22	116/115	-60	ITU-T IMIX	Small panel
258	2x2	20	14	66	66	132	0.6/0.7	31/36	121/133	-65	ITU-T IMIX	Small panel
259	2x2	25	13	61	57	118	0.4/0.5	62/59	144/158	-70	ITU-T IMIX	Small panel
260	2x2	30	12	35	20	55	0.3/0.3	39/210	224/388	-75	ITU-T IMIX	Small panel
261	2x2	35	11	20	8	28	0.3/0.5	88/584	200/670	-80	ITU-T IMIX	Small panel
262	2x2	40	10	20	8	28	0.3/0.3	171/580	308/1000	-84	ITU-T IMIX	Small panel
263	2x2	45	9	8	1	9	0.3/0.3	607/857	500/6000	-87	ITU-T IMIX	Small panel
		50		0	0	0				-90		

Transmit power: 17 dBm.

Table A.15: Measurement results for Vendor B, point-to-point scenario, big panel antenna, 2x2 MIMO, 40 MHz channel

#	MIMO mode	Att., dB	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Traffic pattern	Antenna
				A-B	B-A	Agg.						
264	2x2	0	15	101	101	202	0.6/0.4	35/35	118/117	-40	Large frame	Big panel
265	2x2	0	15	67	67	134	0.7/0.3	25/34	117/113	-40	ITU-T IMIX	Big panel
266	2x2	10	15	67	67	134	0.6/0.7	18/19	117/117	-48	ITU-T IMIX	Big panel
267	2x2	15	14	63	62	125	0.5/0.7	40/67	142/139	-53	ITU-T IMIX	Big panel
268	2x2	20	14/13	61	60	121	0.5/0.4	80/146	149/156	-59	ITU-T IMIX	Big panel
269	2x2	25	13	59	58	117	0.4/0.6	66/138	161/166	-63	ITU-T IMIX	Big panel
270	2x2	30	12	45	40	85	0.4/0.3	34/127	178/248	-68	ITU-T IMIX	Big panel
271	2x2	35	11	28	18	46	0.3/0.3	50/390	271/479	-73	ITU-T IMIX	Big panel
272	2x2	40	10	23	8	31	0.3/0.3	154/739	270/1300	-78	ITU-T IMIX	Big panel
273	2x2	45	9	15	7	22	0.3/0.3	336/717	557/1600	-84	ITU-T IMIX	Big panel
		50		0	0	0				-88		

Transmit power: 17 dBm.

Table A.16: Measurement results for the interference scenario

#	Vendor	MIMO mode	Chan. num.	Tx. pwr., dBm	MCS index	Throughput, Mbps			Min. latency, ms	Max. latency, ms	Jitter, µs	RSSI, dBm	Antenna
						A-B	B-A	Agg.					
295	A	3x3	100	25	21	51	55	106	0.6/0.6	89/53	250/226	-36	LollyPop
296	B	2x3	100	17	15	30	28	58	0.5/0.5	108/118	390/420	-51	Small panel
297	A	2x2	100	23	15	60	59	119	0.6/0.3	73/82	200/200	-38	LollyPop
298	B	2x2	100	17	15	28	25	53	0.5/0.7	180/170	430/480	-50	Small panel
299	A	2x2	100	17	15	63	61	124	0.7/0.2	70/70	190/190	-45	LollyPop
300	B	2x2	100	17	15	25	25	50	0.2/0.7	230/280	490/490	-50	Small panel
301	A	2x2	100	17	15	93	93	186	0.7/0.6	40/40	125/125	-45	LollyPop
302	B	2x2	108	17	15	64	64	128	0.5/0.4	20/20	125/125	-50	Small panel

Channel width: 40 MHz.
Traffic pattern: ITU-T IMIX.
Frame loss: <0.1%.

Appendix B

TDMA wireless backhaul performance measurements results

Table B.1: Measurement results for Vendor C, point-to-point scenario, cables, 2x2 MIMO, 40 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Aggregate throughput, Mbps			Average latency, ms			RSSI, dBm	
				64 Bytes	512 Bytes	1518 Bytes	64 Bytes	512 Bytes	1518 Bytes	AP 1	AP 2
303	2x2	40	0	152.4	192.5	197.4	2.91	2.81	4.23	-39	-41
304	2x2	40	10	152.4	192.5	197.4	4.62	5.02	4.14	-49	-50
305	2x2	40	15	152.4	192.5	197.4	4.75	3.94	4.12	-55	-56
306	2x2	40	20	152.4	192.5	197.4	5.13	5.03	5.17	-60	-62
307	2x2	40	25	152.4	192.5	197.4	8.48	49.36	38.77	-64	-67
308	2x2	40	30	152.4	162.4	163.5	43.04	109.2	164.76	-69	-72
309	2x2	40	35	133.3	120.3	129.5	90.34	61.23	187.03	-74	-74
310	2x2	40	40	83.3	81.2	74.0	92.95	64.32	230.59	-78	-80
311	2x2	40	45	42.9	36.0	37.0	57.25	97.34	374.23	-83	-85
312	2x2	40	50	17.2	12.0	12.3	9.33	6.78	426.33	-88	-89
			60	0	0	0					

Transmit power: 20 dBm.

Table B.2: Measurement results for Vendor C, point-to-point scenario, internal antenna, 2x2 MIMO, 40 MHz channel

#	MIMO mode	Chan. width, MHz	Att., dB	Aggregate throughput, Mbps			Average latency, ms			RSSI, dBm	
				64 Bytes	512 Bytes	1518 Bytes	64 Bytes	512 Bytes	1518 Bytes	AP 1	AP 2
313	2x2	40	0	152.4	192.5	197.4	6.32	6.41	5.8	-41	-43
314	2x2	40	10	152.4	192.5	197.4	2.87	2.84	3.17	-51	-53
315	2x2	40	15	152.4	192.5	197.4	5.04	5.03	4.57	-58	-58
316	2x2	40	20	152.4	192.5	197.4	6.42	7.56	7.46	-63	-63
317	2x2	40	25	151.2	166.9	168.0	43.5	105.22	154.05	-66	-68
318	2x2	40	30	120.2	120.3	123.4	90.1	143.21	197.56	-71	-71
319	2x2	40	35	90.2	92.2	95.6	85.33	148.21	213.04	-73	-74
320	2x2	40	40	85.7	87.2	87.9	93.3	68.74	231.42	-75	-76
321	2x2	40	45	65.5	63.2	61.7	76.41	77.45	285.86	-80	-81
322	2x2	40	50	19.0	18.0	21.6	63.07	144.53	340.48	-84	-85
			60	0	0	0					

Transmit power: 25 dBm.

TRITA-ICT-EX-2012:129

www.kth.se