NTNU – Trondheim
Norwegian University of
Science and Technology

The Intelligent Use of Multiple Interfaces

Niyaz Adigozalov

Master in Security and Mobile Computing
Submission date: June 2013
Supervisor: Øivind Kure, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem description

Mobile user equipment has two or more network interfaces with different cost functions. The effective delivery of the traffic to one (or more) destinations on the Internet is desirable. Two types of traffic are sent - voice and data. In case of the Long-Term Evolution (LTE), there is a high overhead when sending voice traffic alone. Multiplexing voice and data traffic increases the efficiency of the LTE interface by lowering the relative overhead.

The questions are:

- Where the demultiplexing should be done both in the case of one packet flow and in the case of multiplexing each several flows sent via separate network interfaces?
- How to send the traffic with two interfaces and two codecs used simultaneously?
- What should be done with the traffic in the case of vertical handovers?
- What should be done if there are multiple destinations for the traffic?
- In the case of using the Virtual Private Network (VPN) tunneling to secure traffic on transmission, where should be the other end of the tunnel?

Abstract

Long-Term Evolution (LTE) is the latest development in wide area cellular mobile network technology. In contrast with the earlier generations of circuit-switched mobile networks, LTE is all-IP packet-switched network. Both voice and data are sent inside IP packets. Voice over IP (VoIP) is used to provide voice service to LTE users. The speech frames are encapsulated into real-time protocol (RTP) packets and sent over the network. The underlying UDP and IP layers prepend their headers to this small RTP packet resulting in a relatively high overhead. The small size of the RTP packets containing voice/audio leads to an overhead problem as the protocol overhead is in addition to the large LTE frame overhead, thus wasting network resources. This master's thesis project proposes to multiplex RTP and data packets at the user's device as a solution to reduce the overhead. Moreover, the capability of modern user devices to switch between several interfaces (such as LTE and WLAN), is taken into account and the multiplexing of multiple traffic flows or a single traffic flow are studied in the case of a vertical handover. Performance and cost metrics are used to evaluate different potential demultiplexing points, and then the best possible demultiplexing point is identified. The results of this evaluation show that several demultiplexing points can be used based on the operator's needs. The increased packet payload size increases the energy efficiency of LTE and may avoid the need of the UE to switch to WLAN to save power. In addition, to ensure high quality of service for VoIP traffic, the simultaneous use of multiple interfaces is efficient if the multiplexer is enabled. The multiplexing solution proposed by this thesis is also fully compatible with any virtual private network encapsulation protocol.

Keywords: Long-Term Evolution, LTE, multiplexing, VoIP, overhead, RTP, VPN, WLAN

Sammanfattning

Long-Term Evolution (LTE) är den senaste tekniken inom mobil långdistanskommunikation. Jämfört med tidigare generationer av kretskopplade mobila nätverk, är LTE IP paketförmedlande nätverk. Både röstsamtal och datapaket skickas enkapsulerade i IP paket. Voice over IP (VoIP) används för att transportera röstsamtal över IP nätverket. Röstsekvenser enkapsuleras i Real Time Protocol (RTP) paket och skickas över nätverket. De underliggande lagerna som UDP och IP infogar sin huvudinformation i de små RTP paketen vilket gör att kommunikationen blir ooptimerad. De små RTP paketen som innehåller ljudinformation leder till att det blir ooptimerat tillsammans med LTE i och med att man lägger på huvudinformation för varje lager. I det här examensarbetet förslår vi att multiplexa RTP och datapaket tillsammans direkt i användarens enhet för att minska huvudinformationen. Dessutom diskuterar vi möjligheten att byta mellan olika kopplingar (som LTE och WLAN) samt att multiplexa flerfaldig eller singel trafik under en vertikal överlämning. Prestanda och kostnadsmätningar används för att evaluera olika potentiella sammankopplingspunkter, för att kunna ta reda på den bästa sammankopplingspunkten. Resultatet av detta examensarbete visar på att flera sammankopplingspunkter kan användas beroende på operatörens behov. Den ökade storleken på nyttolasten ökar effektiviteten av LTE nätverken och minskar risken för att behöva byta UE:n till WLAN för att spara energi. Utöver det ovannämnda kan simultan användning av olika kopplingar användas för att öka kvaliteten på VoIP trafik. Multplexlösningen som föreslås i det här examensarbete är dessutom fullt kompatibel med virtuella privata nätverksenkapsulerande protokoll.

Nyckelord: Long-Term Evolution, LTE, multiplexa, VoIP, ooptimerad, RTP, VPN, WLAN

Acknowledgements

First of all I want to express my sincere gratitude to Professor Gerald Q. Maguire Jr. for his advice, comments about my report, and his willingness to share his seemingly unlimited knowledge. His encouragement and support were very helpful during my work.

Thank you to Professor Øivind Kure for agreeing to be my co-supervisor from NTNU. I also extend my gratitude to Muhammad Naeem Adil for his opposition and to Konstantinos Vaggelakos for the Swedish translation.

I want to say many thanks to my family who always supported me during my studies and tried to be nearby even if they were so far away. Especially I would like to highlight my beloved grandfather who has always done everything he could to help me get a good education. He has been waiting for my graduation from this master's program, but passed away peacefully in May 2013. "Я сделал это, деда!"

Last but not the least, huge thanks to all my friends from Baku, Trondheim and Stockholm. Thank you very much for being with me. You made these 2 years unforgettable!

Table of contents

Abstract i
Sammanfattning iii
Acknowledgements v
Table of contents vii
List of Figures ix
List of Tables xi
List of acronyms and abbreviations xiii
1 Introduction 1
1.1 Overview 1
1.2 Problem definition 3
1.3 Goals 4
1.4 Structure of the thesis 5
2 Background 7
2.1 Long-Term Evolution (LTE) / System Architecture Evolution (SAE) 7
2.1.1 Network Architecture 7
2.1.2 LTE's Link Layer architecture 8
2.2 Voice in LTE 12
2.2.1 IMS 12
2.2.2 Real-Time Transport Protocol (RTP) 15
2.2.3 CODECs 16
2.3 Multiplexing 17
2.4 Virtual Private Network (VPN) 18
2.4.1 IPsec 18
2.4.2 SSL/TLS 20
2.4.3 DTLS 20
2.4.4 SRTP 20
3 Method 23
3.1 Metrics 23
3.2 Multiplexing 24
3.3 Demultiplexing 28
3.4 FEC for RTP packets 29
3.5 VPN 30
3.6 Limitations 32
4 Analysis 33
4.1 Latency and Jitter 33
4.2 Throughput 36
4.3 Packet Loss 38
4.4 Energy 41
4.5 Price 43
4.6 Summary 44
4.7 Results 46

5 Conclusions and Future work 49
5.1 Conclusions 49
5.2 Future work 50
5.3 Required reflections 50
References 53

List of Figures

Figure 1.1: Possible demultiplexing points (Mn) 2
Figure 1.2: Downward/Upward multiplexing/demultiplexing 3
Figure 2.1: LTE/SAE architecture 7
Figure 2.2: Air interface protocol stack 9
Figure 2.3: PDCP header for data PDUs with a 7 bit SN (left), a 12 bit SN (center), and a 15 bit SN (right) 9
Figure 2.4: Downlink MAC layer [19] 11
Figure 2.5: Uplink MAC layer [19] 12
Figure 2.6: Establishing a call using SIP 13
Figure 2.7: IMS Architecture (Adapted from figure 5.2.2.1 on page 88 of [25]) 14
Figure 2.8: RTP Header [26] 16
Figure 2.9: MAC frame 17
Figure 2.10: IPsec AH header in tunnel and transport modes [36] 19
Figure 2.11: IPsec ESP header in tunnel and transport modes [37] 19
Figure 2.12: SRTP packet format [43] 21
Figure 3.1: Possible demultiplexing points (Mn) 23
Figure 3.2: The jitter effect 24
Figure 3.3: The multiplexer 28
Figure 3.4: RTP packet structure for FEC using two interfaces 30
Figure 3.5: Application of the ESP IPsec in transport mode at the multiplexer 31
Figure 4.1: Peak and Average LTE latency (Adapted from figure 6 on page 13 of [54]) 34
Figure 4.2: LTE upstream packet loss rate (Adapted from figure 17 on page 21 of [54]) 39
Figure 4.3: Energy per bit for LTE and WLAN uplink (Adapted from figure 12 on page 233 of [60]), μJ = 10^{-6} Joule. 41
Figure 4.4: Energy per payload bit for LTE (Adapted from figure 33 on page 76 of [6]), J = 1 Joule. 42

List of Tables

Table 4.1: Latency and jitter from LTE and WLAN to M1-M4 demultiplexing points 36
Table 4.2: LTE and WLAN uplink throughput 38
Table 4.3: Mobile subscriptions pricing 43
Table 4.4: ADSL and broadband pricing 43
Table 4.5: Cloud operator's prices 44

List of acronyms and abbreviations

2G	Second Generation of Mobile Telecommunications Systems
3G	Third Generation of Mobile Telecommunications Systems
3GPP	3rd Generation Partnership Project
4G	Fourth Generation of Mobile Telecommunications Systems
ACK	Acknowledgement
ADSL	Asymmetric digital subscriber line
AH	Authentication Header
AMR	Adaptive Multi-Rate
AMR-WB	AMR WideBand
AP	Access Point
ARQ	Automatic Repeat reQuest
AS	Application Server
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSCF	Call Session Control Function
CSFB	Circuit-Switched Fallback
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DCCP	Datagram Congestion Control Protocol
DIFS	Distributed InterFrame Space
DTLS	Datagram Transport Layer Security
eNodeB	Evolved NodeB
EPC	Evolved Packet Core
EPS-AKA	Evolved Packet System Authentication and Key Agreement
ESP	Encapsulating Security Payload
eUTRAN	Evolved UTRAN
FEC	Forward Error Correction
GSM	Global System for Mobile
GSM-EFR	GSM Enhanced Full-Rate

GSM-FR	GSM Full-Rate
GSM-HR	GSM Half-Rate
HARQ	Hybrid Automatic Repeat reQuest
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
I-CSCF	Interrogating Call Session Control Function
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	IP Security
IT	Information Technology
ITU-T	ITU Telecommunication Standardization Sector
LAN	Local Area Network
LTE	3GPP's Long-Term Evolution
MAC	Media Access and Control
MBMS	Multimedia Broadcast/Multicast Service
MCCH	Multicast Control Channel
MCH	Multicast Channel
MGW	Media Gateway
MKI	Master Key Identifier
MME	Mobile Management Entity
MMTel	Multimedia Telephony
MTCH	Multicast Transport Channel
NACK	Negative Acknowledgement
NAS	Non-Access Stratum
PaaS	Platform as a Service
PCM	Pulse Code Modulation
PCRF	Policy and Charging Roles Function
P-CSCF	Proxy Call Session Control Function
PDCP	Packet Data Convergence Protocol

PDG	Packet Data Gateway
PDN	Packet Data Network
PDU	Packet Data Unit
P-GW	Packet Data Network Gateway
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RLC	Radio Link Control
RLC-AM	Radio Link Control Acknowledged Mode
RLC-TM	Radio Link Control Transparent Mode
RLC-UM	Radio Link Control Unacknowledged Mode
ROHC	Robust Header Compression
RRC	Radio Resource Control
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Protocol
RTS	Ready to Send
RTT	Round-trip time
SA	Security Association
SaaS	Software as a Service
SAE	System Architecture Evolution
SBC	Session Border Control
S-CSCF	Serving Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDU	Service Data Unit
S-GW	Serving Gateway
SIFS	Short InterFrame Space
SMTP	Simple Mail Transfer Protocol
SN	Sequence Number
SNR	Signal-to-Noise Ratio
SRTP	Secure Real-Time Protocol
SRVCC	Single-Radio Voice Call Continuity
SSL	Secure Socket Layer

TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
UDP-Lite	Lightweight User Datagram Protocol
UE	User Equipment
UID	Unique Identifier
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
UTRAN	Universal Terrestrial Radio Access Network
VHO	Vertical Handover
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless LAN

1 Introduction

This chapter gives a general introduction to the area discussed in this thesis. This master's thesis project aims to provide a solution to the problem caused by the overhead of small packets in a LTE network. The details of the problem are given in section 1.2. The research goals are described in section 1.3. The chapter ends with a summary of the structure of the thesis.

1.1 Overview

Mobile communication technologies are becoming more and more important in our daily lives. The number of mobile broadband subscribers in the world is greater than 1.5 billion and this number will only increase. The 4th quarter of 2012 brought 125 million new mobile subscribers, with 80% of all subscriptions using second generation (2G) or third generation (3G) networks [1]. This growth in numbers of subscribers and their behaviour lead to mobile traffic growing by 70% in 2012 [2]. Almost all of this traffic was generated by smartphones. These smartphones are able to use multiple interfaces for communication, and a very large amount of this traffic was sent using the device's WLAN interface rather than via a wide area mobile network interface. Cisco states that 33% of the total mobile traffic is sent/received by the WLAN interface and they expect this percentage to grow by 2017 to approximately 67% [2].

Long-Term Evolution (LTE) is the latest step in the Third Generation Partnership's (3GPP's) evolution of the GSM networks towards fourth generation (4G) mobile networks. LTE was first initiated in 2004. Unlike the circuit-switched 2G/3G networks, LTE is purely packet-switched. LTE supports a wide variety of services, including packet based voice service. The first LTE services were launched in 2009 and LTE is still being deployed. Today LTE carries only 0.9% of all mobile connections, but already accounts for 14% of the total mobile traffic and it is predicted that LTE will be responsible for 10% of connections and 45% of total traffic by 2017 [2]. This anticipated growth makes the efficiency of transporting traffic over the air a major goal of mobile operators. Real-time and high data rate applications may use more than one access network technology and it is necessary to ensure continuous connectivity despite handovers. A vertical handover (VHO) occurs when the user equipment (UE) switches between radio interfaces, specifically in this thesis we will consider VHOs between cellular and wireless local area network (WLAN) interfaces. Research has shown that in most cases the use of a WLAN interface is preferable to using the LTE interface in terms of energy saving [3] and performance [4, 5]. In LTE, which is an IP based network, voice is sent using voice over IP (VoIP). The real-time protocol (RTP) packets containing encoded voice samples are small comparing to the data packets sent when doing file transfers and web page downloading, as the voice stream typically requires less bandwidth. As a result of the

characteristics of the current network interfaces, VoIP calls sent via WLAN always save energy as compared to sending this traffic via a LTE interface. In the case of data traffic, the energy gain due to VHOs from WLAN to LTE or vice versa varies with different services such as downloads, uploads, or simple web browsing [5].

Unfortunately, the small size of RTP packets containing voice leads to a high overhead for these packets when they are sent over the wireless network. This overhead is due to all of the headers that are appended to the packet as it passes down through layers. The details of this problem are further explained in Section 1.2.

One means of solving this problem is to multiplex small RTP packets with bigger data packets on uplink (i.e., being sent from the UE) in order to reduce the relative overhead by increasing the wireless network frame's payload size. This multiplexing will help to avoid wasting the UE's resources when sending RTP packets. While it is clear that there will be multiplexing and demultiplexing taking place at the UE, there must also be demultiplexing and multiplexing at the other end of this multiplexed tunnel. This thesis aims to find the best possible demultiplexing point. Taking into account that UEs are capable of using several interfaces (although only the wide area mobile network and WLAN interfaces are considered in this thesis), the multiplexed data can flow through any or all of the UE's interfaces. Figure 1.1 shows possible demultiplexing points (denoted by M1, M2 …) on an overview of the combined network infrastructure (where we have combined an LTE network and WLAN access points connected to both public and private networks). M1 performs demultiplexing in an additional entity within the EPC that is connected to a Packet Data Network Gateway (PDN-GW) or perhaps implemented inside the PDN-GW. M2 is an external provider of a demultiplexing/multiplexing service. M3 performs demultiplexing before the multiplexed packets enter the LTE core network and multiplexes them after they leave the LTE core network. M4 is an application server (AS) within the IP Multimedia Subsystem (IMS). The details of the other entities shown in this figure are explained in sections 2.1.1 and 2.2.1.

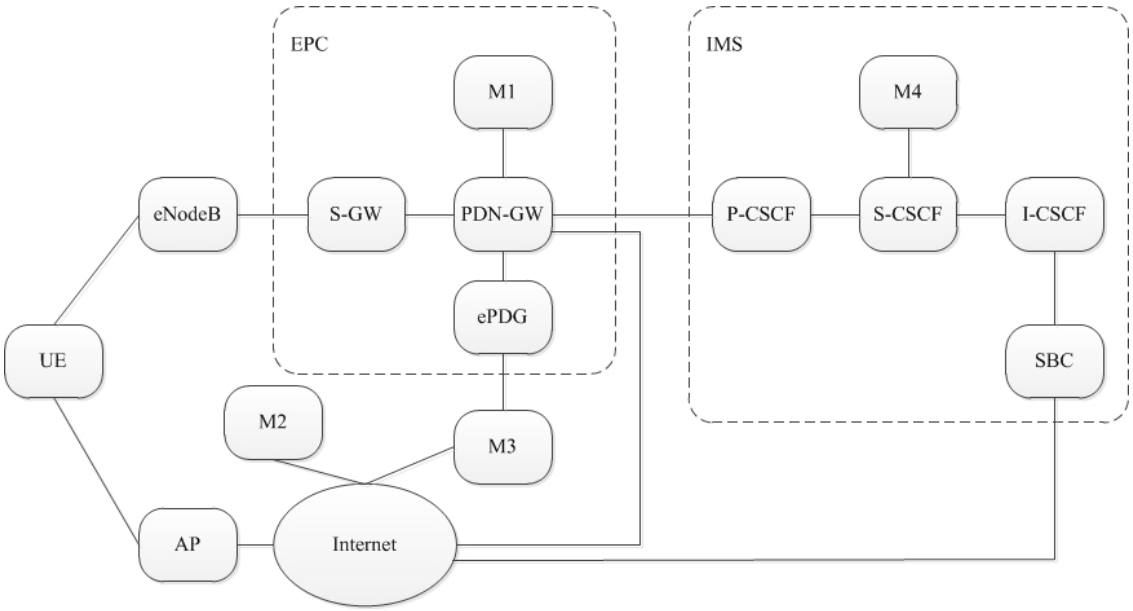

Figure 1.1: Possible demultiplexing points (Mn)

At the multiplexing/demultiplexing endpoints packets are processed as follows: on the sender side, several protocol data units (PDUs) can be combined into one service data unit (SDU) on any layer of the TCP/IP protocol stack. This process is called downward multiplexing. Another possible procedure is to split a PDU into several lower layer SDUs. This is called downward demultiplexing. On the receiver side the inverse of these procedures occurs resulting in upward multiplexing/de-multiplexing. Note, that the layer on which the upward multiplexing/de-multiplexing is performed should be the same layer where the downward operation was done. This is illustrated in Figure 1.2.

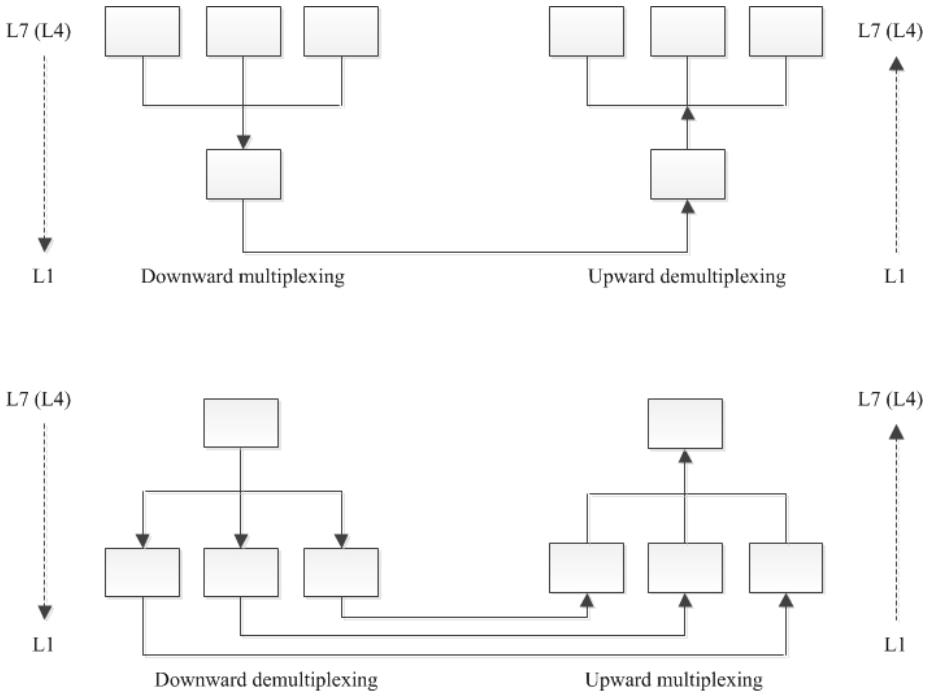

Figure 1.2: Downward/Upward multiplexing/demultiplexing

1.2 Problem definition

As we described earlier, LTE is an IP network, therefore the layered TCP/IP architecture applies. As packets go down through the layers, each layer adds its header or trailer information, which results in overhead. As was noted earlier, the ratio of this overhead relative to the payload is especially large for voice traffic, as the size of the encoded voice payload is quite small [6]. LTE uses robust header compression (ROHC) at the first sublayer of the link layer in order to reduce the relative overhead for small packets (<1kB), but the effect of ROHC is negligible for large packets. ROHC compresses the upper layer headers, but the lower protocol headers and the cyclic redundancy check (CRC) (where applicable) still make up a large part of the total overhead [6]. This large overhead leads to higher power consumption (per bit of user payload) and wastes bandwidth. One solution which reduces the relative overhead by combining multiple VoIP packets was given by Knertser and Adigozalov

[7]. This method is explained in Section 2.3. With this multiplexing solution, the relative overhead is reduced, because of the larger payload. Edström [6] showed that the larger the packet, the less energy per payload bit a transmission consumes, but for the packets >1kB there is not a huge difference in energy consumption. Considering that the largest fraction of the traffic in a mobile network is now data traffic, it is obvious that multiplexing voice packets with data packets will be more effective than directly transmitting voice packets (assuming that there is data traffic that a RTP packet can be multiplexed with). However, a key question is where the demultiplexing should be done. A further challenge is to determine what should be done with the traffic if there are multiple IP destinations for the traffic that is multiplexed together. Note that this later challenge is much easier for the downlink - when the mobile device is the destination for all of the different higher layer packets.

Today it is quite common that the UE is equipped with two or more network interfaces. These interfaces have different cost functions (in terms of energy consumption, available bandwidth, and possibly traffic charges). If two different encodings for voice are used together with forward error correction (FEC) [8], how should the traffic be sent? FEC provides the ability for the receiver to perform error recovery. FEC is implemented by adding information about the previous packet into the next one. As a result the voice frame that was encoded in a packet will be lost only if two sequential packets are lost during transmission. If we are using two interfaces which utilize *different* paths to send packets, then if something goes wrong on one path, packets sent over both paths may still reach the destination successfully via the other path. A question is: How efficient it is to use both interfaces to send packets in order to decouple the probability of sequential packets loss? Recalling the overhead problem above, voice packets can be multiplexed with data streams in order to make more efficient use of energy and bandwidth. Therefore in the case when multiple interfaces are used to send multiplexed traffic, where should the demultiplexing be done?

Moreover, when multiple interfaces are used, VHOs are still possible. The UE can switch between interfaces on-the-go with on-going packet streams. How should the traffic behaviour change and should it change at all? This also concerns the demultiplexing point, which might or might not change when vertical handovers occur.

The final issue is security. Sometimes traffic has to be secured when sent in an untrusted environment. For this purpose, a virtual private network (VPN) is used to send the traffic inside an encrypted tunnel. A question is where the endpoints of this tunnel should be.

1.3 Goals

The main goal of this thesis is to design and evaluate a multiplexing solution that helps to reduce the overhead in RTP packets sent over LTE. Other goals are:

- Define the other end of the multiplexed tunnel, i.e., the demultiplexing point. Then based on various metrics, figure out the advantages and disadvantages of each demultiplexing point and recommend which one to use in practice.

- Identify the advantage of using both LTE and WLAN interface with FEC to ensure high quality for the voice traffic even when there are very bad conditions experienced by the traffic being sent over one interface.
- Describe how vertical handovers affect the multiplexing solution, whether the demultiplexing point should change or not.
- Examine potential VPN protocols that can be used with the proposed multiplexing solution and evaluate the alternative endpoints of the VPN tunnel.

1.4 Structure of the thesis

This thesis is organized as follows:

- Chapter 1 introduces the project, defines the scope of the work and explains the problems and questions that needed to be solved.
- Chapter 2 presents the background needed to understand this thesis. It digs into the architecture and link layer protocol of LTE, and then explains various aspects of voice transmission via LTE. Related work regarding multiplexing solutions is reviewed in this chapter. Security issues, more specifically the use of VPNs are also explained in this chapter.
- The proposed multiplexing solution is discussed in detail in Chapter 3. The application of VPNs to the multiplexed tunnel is explained. The metrics that we base our analysis on are presented and specified.
- The analysis of our solution in terms of these metrics is given in Chapter 4. The discussions of all metrics' values and the answers to the problems and questions introduced in chapter 1 are given in this chapter.
- Chapter 5 concludes the work and presents some suggested directions for the future work. Some of the relevant social, environmental, and economic issues are also discussed in this chapter.

2 Background

This chapter gives the reader the necessary technical background about the technologies used in this thesis project. The overall network architecture and the details of LTE's link layer are described. The implementation of voice in LTE is explained, together with a description of IMS. Finally, a number of protocols used to provide VPNs are covered.

2.1 Long-Term Evolution (LTE) / System Architecture Evolution (SAE)

This section describes the parts of the LTE/SAE architecture that are necessary to understand this thesis. Components of this network architecture are explained in section 2.1.1. The architecture of the link layer and protocols operating at this layer are described in section 2.1.2.

2.1.1 Network Architecture

LTE was designed as a completely packet-switched network, but it needs to ensure compatibility with the circuit-switched networks of prior generations of wide area cellular networks. LTE introduced a new radio access network called Evolved-UTRAN (E-UTRAN). In contrast with the earlier UTRAN radio access network of 3G/UMTS, E-UTRAN has integrated all of the radio-related functions into a single node called an eNodeB [9] The eNodeB connects the UE to the core network. The eNodeB is also responsible for ensuring different levels of quality of service (QoS), for example by prioritizing voice packets over bulk data. To provide mobility and low latency for data transfers, eNodeBs are logically connected to each other via the X2 interface. The non-radio access part of the SAE architecture is the Evolved Packet Core (EPC) network. The EPC is the packet-switched core network for LTE. EPC uses the S1 interface to communicate with eNodeBs. This architecture is illustrated in Figure 2.1.

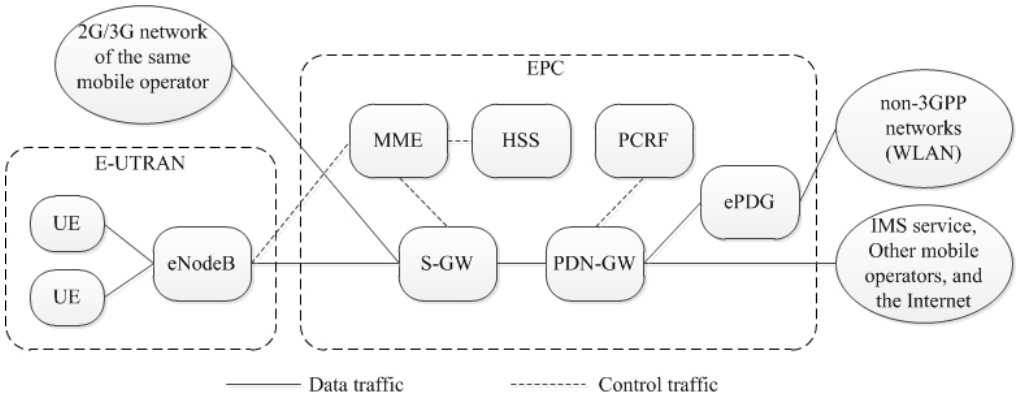

Figure 2.1: LTE/SAE architecture

The components of the EPC are:

- **Mobility Management Entity** (MME) – the main control node of the core network. The MME manages the signalling between the E-UTRAN and EPC, provides user authentication by communicating with the HSS, and is responsible for handover operations between eNodeBs. The MME also handles all functions related to the establishment of traffic bearers and provides all the security key management functions.
- **Serving gateway** (S-GW) – processes and routes packets sent from or to the radio access network. The S-GW can be directly connected to 2G/3G networks of the same network provider, thereby allowing data to flow to and from these networks. The S-GW also manages handovers when the UE moves from one eNodeB to another within the same network and for handovers between LTE and other 3GPP networks. The appropriate S-GW for the handover procedures is chosen by MME.
- **Packet Data Network Gateway** (PDN-GW) – the gateway for data packets between the UE and external packet data networks, such as the Internet.
- **Evolved Packet Data Gateway** (ePDG) – the gateway responsible for providing interworking between LTE and non-3GPP untrusted networks, such as WLAN, femtocells, etc.
- **Home Subscriber Service (HSS)** – the database containing the subscription data of all subscribers in this mobile network. It also contains information about the visited network when a subscriber roams to another network. The HSS generates the security data needed for authentication and encryption functions implemented by the MME.
- **Policy and Charging Roles Function (PCRF)** – manages the collection of data for billing and limits the UE's possible service level according to each subscriber's subscription.

2.1.2 LTE's Link Layer architecture

As previously stated, LTE is a packet-switched network and utilizes a layered TCP/IP architecture. On the transport layer, transmission control protocol (TCP) is normally used for data traffic and user datagram protocol (UDP) is used to carry multimedia traffic (such as RTP). On the network layer the user plane transports IP packets. The radio resource control (RRC) protocol [10] manages signalling messages in the control plane. This is illustrated in Figure 2.2, where the term Non-Access Stratum (NAS) is used to describe the communication between the UE and MME. As the control plane is used only for signalling purposes; only the user plane is relevant for this thesis. For the goals of this thesis, the architecture and design of the link layer are important - as they affect the overhead of carrying the user payload in link layer frames and the maximum amount of data that can be transported in such a frame.

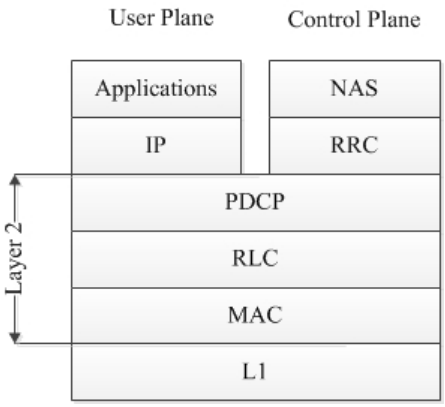

Figure 2.2: Air interface protocol stack

The link layer consists of three sublayers – Packet Data Convergence Protocol (PDCP) layer, Radio Link Control (RLC) layer, and Medium Access and Control (MAC) layer. Packet Data Units (PDUs) from a higher sublayer are passed to the next sublayer, from whose point of view the PDU is a Service Data Unit (SDU). For example, when the PDCP sublayer passes its PDU to the RLC sublayer, from RLC's point of view the PDCP's PDU is a RLC SDU, and so on. At the receiving side this process is reversed.

2.1.2.1 Packet Data Convergence Protocol (PDCP) layer

The PDCP [11] layer provides the data transfer service for both the user plane and the control plane. Other important functions are ciphering, integrity protection, and header compression service for the SDUs received from the network layer. The maximum supported size of a PDCP SDU is 8188 bytes. For the user plane, the SDU is an IP packet. When an IP packet arrives at the PDCP layer, the UE assigns a sequence number (SN) to the packet, applies a header compression mechanism, encrypts the SDU, and performs integrity protection (if needed). When the SN reaches its maximum value, the SN is reset to 0 (i.e., the SN simply wraps around). Figure 2.3 shows the PCDP header with different length SNs. The resulting PDCP PDU is then forwarded to the lower layer (i.e., the RLC layer).

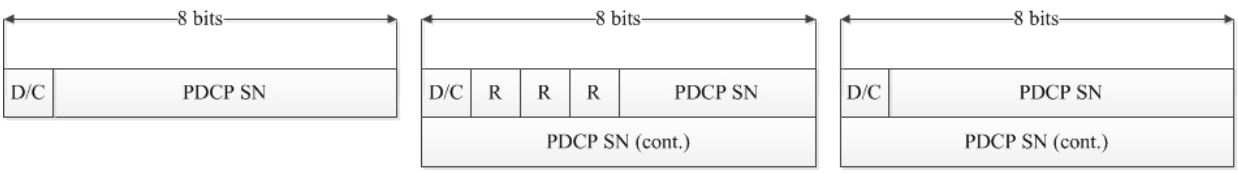

Figure 2.3: PDCP header for data PDUs with a 7 bit SN (left), a 12 bit SN (center), and a 15 bit SN (right)

Two types of PDCP PDUs are used: data PDUs and control PDUs. Data PDUs are used to transport user plane and control plane data. Control PDUs are used for PDCP status reports and for the header compression control information. The type of PDU is indicated by the D/C bit field in the header.

The sequence number (SN) allows the PDCP layer to provide in-sequence delivery and duplicate detection services. The size of SN is configured by the RRC protocol [10]. If not set explicitly, a 12 bit long SN is used [11].

The encryption of the PDCP layer is done to secure both the user data and the signalling traffic over the air interface. Integrity protection is provided only for signalling traffic. The security keys used for these security mechanisms are generated by the Evolved Packet System (EPS) Authentication and Key Agreement (EPS-AKA) procedure [12].

An important function of the PDCP layer is the compression of upper layer headers in order to reduce the amount of overhead. The robust header compression (ROHC) framework [13] uses certain “profiles” (i.e. algorithms), that are specific for a combination of protocols from different layers, e.g. RTP/UDP/IP [14], ESP/IP [14], and TCP/IP [15]. Header compression takes advantage of the redundancy in the headers, particularly in packets that are part of the same flow. Static information is stored at the receiver side and need not be sent until this information changes. For the dynamically changing information only the difference from the last transfer needs to be sent.

The most important use of ROHC is for VoIP traffic [16]. For a packet containing encoded voice samples the header includes the RTP, UDP, and IP headers. The resulting header is 12+8+20=40 bytes for the IPv4 and 60 bytes for IPv6 before compression. After compression the header size is reduced to as little as 3-4 bytes. This overhead will increase further as the packet is forwarded to the next sublayers and the physical layer, as each of them prepends its header (and possibly a trailer). The total protocol overhead on the link layer and the physical layer is 10 bytes if RLC-AM mode is used and 6 bytes when RLC-UM mode is used [17]. These modes are explained below.

The resulting PDCP PDU containing the PDCP header, the ROHC header, and the payload is forwarded to the RLC layer.

2.1.2.2 Radio Link Control (RLC) layer

The RLC [18] layer is responsible for the concatenation, segmentation, and reassembly of RLC SDUs. For the uplink, incoming PDCP PDUs are reconstructed in order to satisfy the requirements of the MAC layer. The RLC layer also handles error correction, error detection, duplicate detection, and reordering. All functions are implemented by RLC entities that operate in one of the following modes: transparent mode (TM), unacknowledged mode (UM), and acknowledged mode (AM).

In TM mode, the RLC SDU is simply mapped to an RLC PDU without adding a RLC header.

In UM mode (which is one-way, i.e. simplex) concatenation and/or segmentation of the incoming SDUs is done, and then an RLC header is added. This header also includes a SN to support reordering and duplicate detection, but the SN is not applicable to multicast traffic. UM mode is primarily used for the error-tolerant and delay-sensitive real-time applications, such as VoIP.

AM mode (which is two-way, i.e. full-duplex), is mainly used for non-real-time services, such as file download and web browsing. This mode ensures reliable transmission by performing Automatic Repeat reQuest (ARQ) operations as necessary. Missing packets can be re-transmitted if they are not correctly delivered to the destination (in this case either the eNodeB or UE). The receiver sends an acknowledgement (ACK) or negative acknowledgement (NACK) back to the sender (either the eNodeB or UE) for every RLC PDU. It is important to note that the RLC ARQ only operates over the UE to eNodeB link.

2.1.2.3 Medium Access Control (MAC) layer

The MAC layer [19] is the lowest of the link layer sublayers. It transfers packets directly to the physical layer. This is performed by mapping logical channels to physical transport channels. Data transfer between the RLC layer and the MAC layer passes through these logical channels. The MAC layer and physical layer are connected by transport channels. Multiplexing and demultiplexing is performed between these channels, hence data from several logical channels can be multiplexed or de-multiplexed into/from one transport channel. The multiplexing of the downlink logical channels and uplink logical channels is shown in Figure 2.4 and Figure 2.5 (respectively). The list of the channels with their descriptions is given in 3GPP TS 36.321 [19].

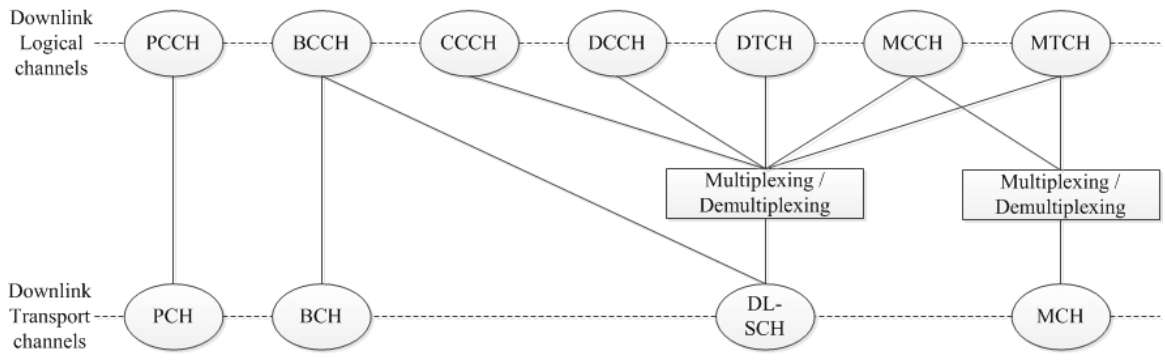

Figure 2.4: Downlink MAC layer [19]

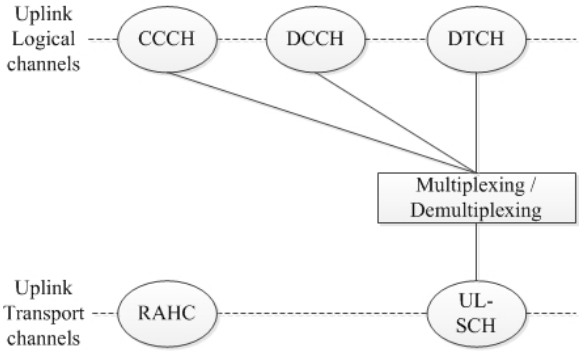

Figure 2.5: Uplink MAC layer [19]

Another important function of the MAC layer is error correction using the lightweight hybrid ARQ (HARQ) protocol. HARQ detects and corrects most errors without propagating them to the upper layers; hence HARQ provides fast retransmissions. This error correction takes places at the UE or eNodeB.

2.2 Voice in LTE

Since LTE was designed to be a purely packet-switched all-IP network, LTE does not transport a voice call as was done in 2G/3G circuit-switched networks. Therefore new methods for sending voice content and interoperating with earlier networks had to be standardized. Three different technologies were developed to provide voice service in LTE:

- IP Multimedia Subsystem (IMS) [20],
- Single-Radio Voice Call Continuity (SRVCC) [21] – to handle handovers between an IMS-based packet-switched network and a circuit-switched network, and
- Circuit-Switched Fallback (CSFB) [22] – provides voice services outside of the LTE network. In CSFB a circuit-switched network is used for voice.

Of these three technologies, we will only consider IMS in this thesis – as SRVCC and CSFB are really designed to be transition technologies until an operator has implemented an IMS system. Additionally, in IMS the voice traffic is sent as packets, hence we can consider multiplexing them with other data traffic.

2.2.1 IMS

IMS is the signalling framework for supporting IP-based multimedia services. It is a logically separate network that communicates with the EPC and controls IP multimedia services, such as VoIP. IMS is based on the Session Initiation Protocol (SIP) [23] and is used

in conjunction with the Session Description Protocol (SDP). SDP assists in negotiating media coders/decoders (CODECs), specifying IP addresses and port numbers to be used, and establishing the desired QoS [24].

SIP is an application layer signalling protocol for managing and establishing multimedia sessions. SIP is text-based and inherited features of the Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) protocols. Users in SIP are identified by public user identities in form of SIP or TEL uniform resource identifiers (URIs). SIP defines a set of messages that are exchanged to initiate a session (call). The calling procedure is shown in Figure 2.6.

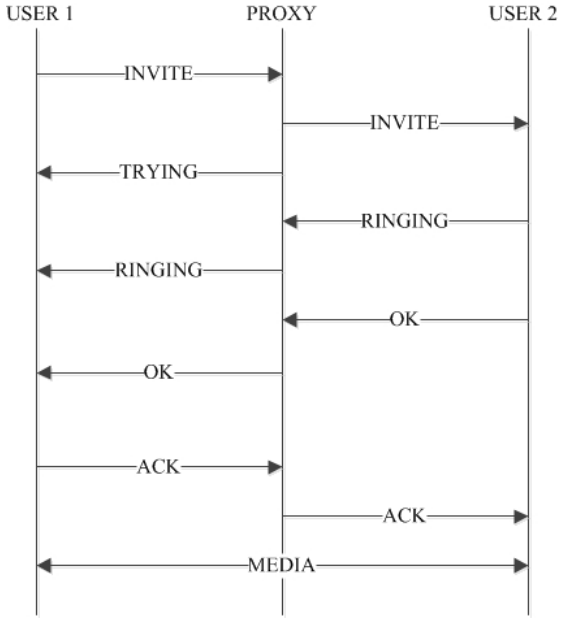

Figure 2.6: Establishing a call using SIP

In a SIP-based network the following entities are implemented:

User agent (UA)	Requests are created by User Agent Client (UAC) and responses are created by User Agent Servers (UAS)
Registrar	Database containing information about UAs
Proxy	Redirects messages either directly or through another proxy to reach the caller

After a successful session establishment, the media flows directly between callers. Note that a session may contain other media components in addition to or instead of voice.

The IMS architecture is shown in Figure 2.7.

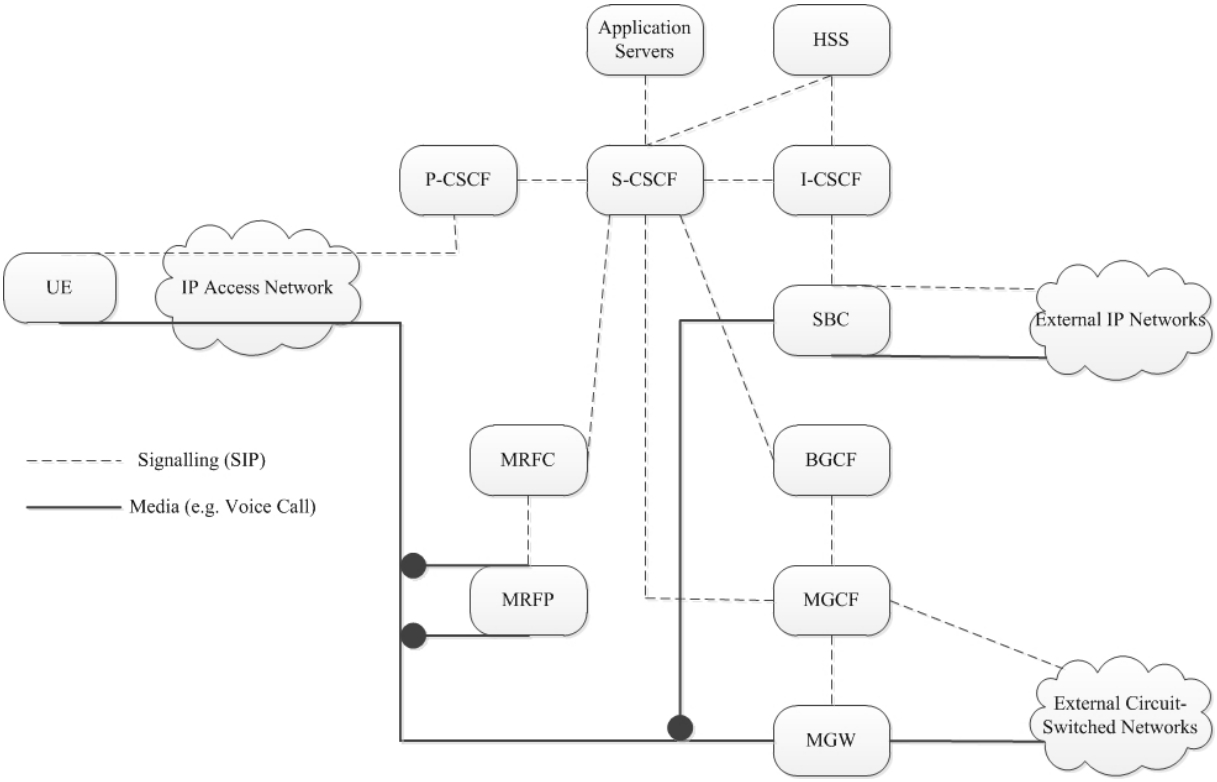

Figure 2.7: IMS Architecture (Adapted from figure 5.2.2.1 on page 88 of [25])

The main new element introduced by IMS is the various Call Session Control Functions (CSCFs). These CSCF functions are logically divided between three entities:

- The Proxy-CSCF (P-CSCF) – is the first entity between the UE and the IMS. It acts as a SIP proxy. All signalling traffic going in or out of the IMS to the IP access network passes through a P-CSCF. The P-CSCF authenticates users and provides this authentication information to other entities within the IMS. Authentication takes place when establishing an IPsec security association between the P-CSCF and the UE. Hence, the P-CSCF is the termination point of an IPsec tunnel for traffic between the UE and the IMS. An IPsec security association is used to provide confidentiality and integrity for SIP signalling traffic [12].
- The Serving-CSCF (S-CSCF) – is the central node in the signalling plane of the IMS architecture. The S-CSCF acts as a SIP registrar, hence it maintains information about the current IP address of an UA and its corresponding SIP address(es). The assigned S-CSCF controls SIP sessions. The S-CSCF contacts the Home Subscriber Server (HSS) in order to access the subscriber's data.
- The Interrogating-CSCF (I-CSCF) – communicates with other IMS domains. An I-CSCF is located at the edge of an IMS administrative domain.

Other relevant parts of the IMS architecture are:

- HSS – contains subscriber-related information for handling multimedia sessions (this HSS can be shared with the HSS of the LTE system or it can be independent).
- Application Servers implement various services and deliver them to end-users. One such service is Multimedia Telephony (MMTel) – the standardized service for voice calls.
- Session Border Control (SBC) – a gateway between IMS and other IP networks.
- Media Gateway (MGW) – converts and transcodes media formats used within the IMS packet-switched network to/from a circuit-switched network.

2.2.2 Real-Time Transport Protocol (RTP)

Voice traffic is transported using RTP [26] over unreliable transport protocols, such as UDP or Datagram Congestion Control Protocol (DCCP)[*]. IMS uses RTP over UDP. Media traffic is generally able to maintain reasonable quality despite some fraction of packets being lost, hence, reliable transport protocols, such as TCP or the stream control transmission protocol (SCTP) are not used. But as UDP does not retransmit or acknowledge packets, application layer protocols must deal with packets failing to arrive or being delayed. The application that receives a RTP stream ensures the proper playback of the stream by buffering packets, and then uses RTP's sequence numbers and timestamps to provide the correct placement of packets into a playback buffer. When packets arrive at their destination out-of-order or delayed, the playback algorithm (and its playback buffer) attempts to ensure that these impairments do not affect the playback quality (or at least tries to minimize the effects). If a packet arrives after its playback time has passed, then the packet is simply dropped by the playback algorithm.

The user's speech is sampled by the UE and encoded for transmission using a CODEC. The encoded audio samples are placed in the RTP packet after the RTP header. Depending upon the CODEC, the length of the RTP payload varies (for example, in G.711 with a 20 ms audio frame the RTP payload is 160 octets). If many packets are lost during transmission, the UE may change the CODEC used to the one with better redundancy (i.e. which provides better quality in the face of a higher packet loss rate) [27]. The CODEC is either statically defined or dynamically negotiated by peers. The CODEC used of a specific RTP packet is indicated using the payload type field in RTP packet's header. The sequence number field in the RTP header is used to detect packet loss and to reorder packets upon arrival. The RTP header is shown in Figure 2.8.

[*] DCCP introduces congestion control which UDP lacks. Without congestion control, a source may send a large amount of traffic using the UDP protocol despite the other traffic passing over a link, hence other TCP flows will back-off (i.e., to avoid congestion all of the TCP connections will reduce their sending rate)

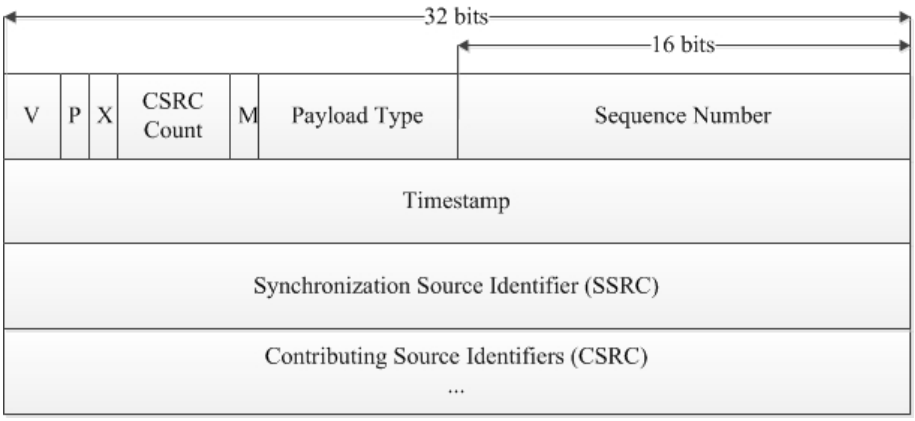

Figure 2.8: RTP Header [26]

2.2.3 CODECs

A CODEC is an algorithm for encoding and decoding a signal. An analogue signal is represented as sequence of digital samples. In the case of voice, CODECs convert the sampled speech into digital data. Two main characteristics of a CODEC are its bandwidth and speech quality. Some well-known CODECs used in VoIP are:

1. G.711 codec [28], also known as the Pulse Code Modulation (PCM), was first introduced in 1972 and widely used in the fixed Public Switched Telephone Network (PSTN). G.711 is supported by all VoIP phones. Its encoding rate is 8 000 Hz, in other words, 8 000 samples per second are encoded. Each sample is compressed to 8 bits. As 8 000 samples of 8 bits are produces per second, i.e. 64 kbit/s bandwidth. This data rate is high compared to modern CODECs with similar or better speech quality. Typically 20 ms worth of samples are placed into an RTP payload.
2. GSM Full-Rate (GSM-FR) [29] compresses 20 ms long audio frames instead of individual samples. The audio frame contains a number of consecutive samples. A 20 ms GSM-FR frame consists of 160 samples. GSM-FR encoding results in 13 kbit/s bandwidth. A similar CODEC is GSM Half-Rate (GSM-HR) [30], which generates 6.5 kbit/s.
3. Adaptive Multi-Rate (AMR) [31] is a mandatory CODEC for IMS, i.e. every UE must support AMR. Eight different CODECs are included in AMR with bandwidths ranging from 12.2 to 4.75 kbit/s. The first is known as the GSM-EFR (Enhanced Full-Rate). As opposed to 8 000 samples per second used in AMR, the AMR-WideBand (AMR-WB) [32] uses 16 000 samples per second. AMR-WB provides higher speech quality than AMR. The bandwidths of AMR-WB range from 23.85 to 6.60 kbit/s.

2.3 Multiplexing

Multiplexing is the procedure of combining several PDU from upper layers into one SDU at a lower layer. The header and possibly a CRC are added to fewer larger SDUs instead of many small ones. This makes the sending of these PDUs more efficient.

One solution which reduces the overhead by using downward multiplexing of VoIP packets was given by Knertser and Adigozalov [7]. The multiplexer is positioned at the eNodeB and combines multiple VoIP flows in the cell into a single multicast frame. This processing occurs between the PDCP and RLC sublayers and marks incoming PDCP PDUs as multicast to ensure their concatenation at the RLC sublayer so that they are sent through a MTCH channel to multiple recipients. The resulting MAC frame is shown in Figure 2.9, where UID is a 1-byte unique identifier of a recipient. This UID is sent to a recipient by the VoIP signalling protocol (e.g. SIP) before the multiplexing procedure is initiated for this receiver.

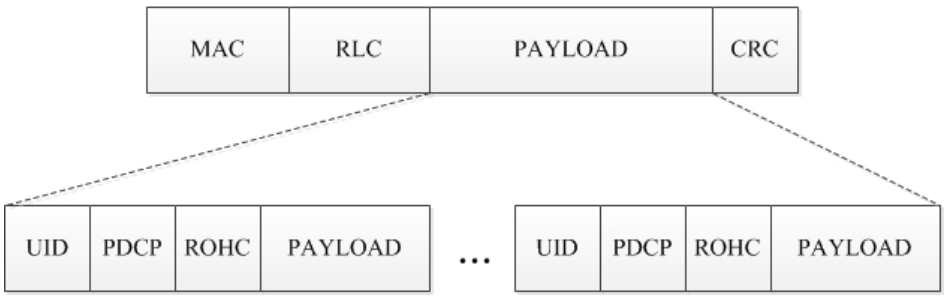

Figure 2.9: MAC frame

A demultiplexer resides in each of the recipient UEs. When this demultiplexer receives the multicast frame, it demultiplexes the RTP packets based upon their UIDs, extracts the RTP packet(s) destined to this UE and forwards the PDCP frame to the PDCP sublayer.

Knertser and Adigozalov showed that this multiplexing is an efficient solution for the purpose of overhead reduction for multiple VoIP sessions in a cell. The relative overhead of RTP packets is reduced from 21.4% in unicast mode to 17.5% in the case of 10 multiplexed flows [7]. Collin and Chazalet showed a similar use of multiplexing multiple RTP packets into a multicast frame in the case of a WLAN cell. They grouped RTP packets arriving at the access point within the same 20ms and sent the resulting packets as broadcast. This use of multiplexing showed that a substantial increase in the number of users per cell was possible [33].

Another multiplexing method for VoIP packets was proposed by Drozdy, et al. [34]. They state that multiplexing can be implemented either in the transport (UDP) or network (IP) layers with the only difference being the difference in gain. A performance evaluation of this multiplexing was performed on the UDP transport layer – between a S-GW and an eNodeB.

The results showed that the bandwidth usage of VoIP calls was reduced significantly and with an increasing number of calls, the gain could exceed 50%. Also, multiplexing allows the network to increase the number of served VoIP sessions by 250%.

In this thesis, the multiplexing of data traffic with RTP traffic is considered. Therefore the multiplexing solutions described above have to be modified and improved to support data traffic as well. The advantage is that the data PDUs are often large and thus the lower layer header overheads are already amortized over a large payload. Adding a small VoIP payload to a large packet will slightly increase the packet's size - but enables the VoIP payload to share the existing overhead - while adding only a small amount of additional overhead. Note that in this thesis the data packets and voice traffic are going to have the same UE as either their source or their destination, hence we will not utilize multicasting. This also means that in all cases one end of the multiplexing and demultiplexing tunnel is at the UE. In this thesis we will explore where the other end of this tunnel should be.

2.4 Virtual Private Network (VPN)

One of the problems which this thesis explores is to define the endpoints for encapsulating voice and data traffic in a multiplexed tunnel. Additionally the multiplexed tunnel may be combined with a VPN tunnel. Therefore, a description of VPNs and general tunnelling protocols is necessary.

A VPN allows sensitive data to be sent over an insecure network, e.g. Internet. The idea is to create a virtual point-to-point connection, called a “tunnel”, and all data transported inside this tunnel is encrypted.

Two tunnelling scenarios are possible for the purpose of this thesis. In the first scenario the data and RTP traffic are first multiplexed and the multiplexed frame is encapsulated into a tunnel. In the second scenario the data and RTP traffic are first separately encapsulated into VPN tunnels, and then the resulting frames are multiplexed into one frame. In either case Internet Protocol Security (IPsec), Secure Sockets Layer / Transport Layer Security (SSL/TLS), or Datagram Transport Layer Security (DTLS) can be used as the VPN encapsulation protocols for data and RTP packets. In the second scenario the Secure Real-Time Transport Protocol (SRTP) might be used for RTP.

2.4.1 IPsec

IPsec [35] is a protocol suite operating at the network layer. It secures all of the data in a flow (i.e., packets with a common protocol, source IP address, and destination IP address) by encryption and/or integrity protection. The protocols that are used to provide these services are:

- Authentication Header (AH) [36] provides integrity protection and data origin authentication. Anti-replay features are optional.
- Encapsulating Security Payload (ESP) [37] provides encryption and/or integrity protection. However as stated in [35], the use of encryption without integrity protection is not recommended. Data origin authentication and anti-replay features are also supported.

IPsec operates in two modes – tunnel and transport. In transport mode, the IPsec header is placed between the IP header and the payload. This mode is used to provide an end-to-end secure connection between two nodes. In tunnel mode, the IPsec header is placed before the IP header, thus protecting the whole packet. A new IP header is placed before the IPsec header and includes the addresses of the IPsec peers [36, 37]. This mode is typically used to protect the packet over specific parts of the network, e.g. between two gateways or between a node and a gateway. The format of packets in both modes is shown in Figure 2.10 for AH and in Figure 2.11 for ESP.

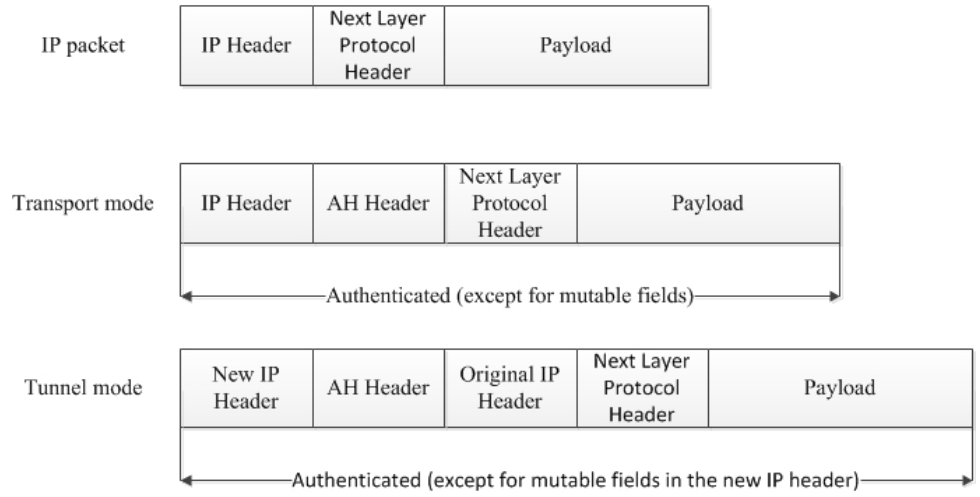

Figure 2.10: IPsec AH header in tunnel and transport modes [36]

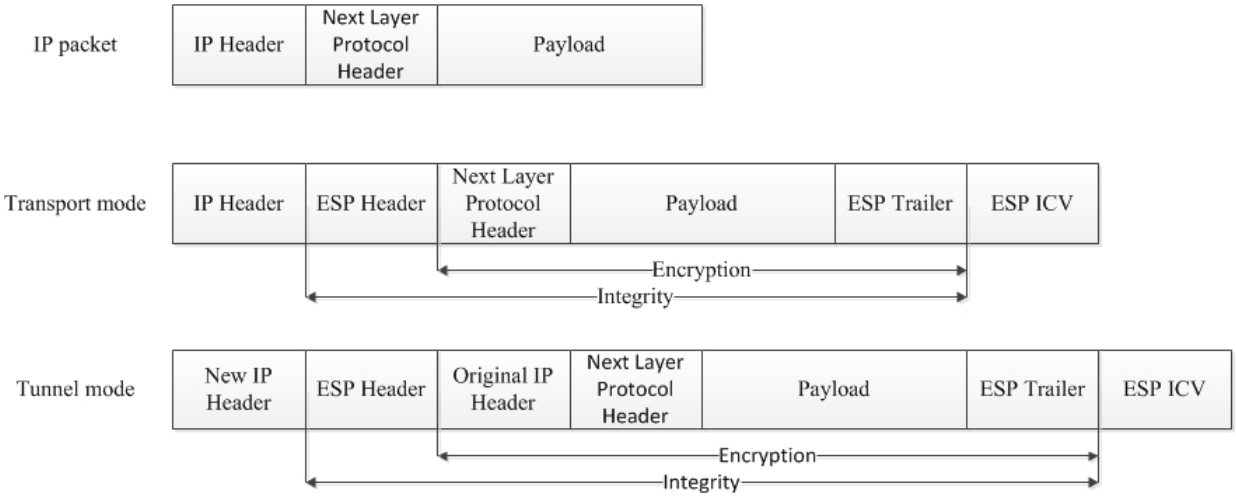

Figure 2.11: IPsec ESP header in tunnel and transport modes [37]

Another protocol involved in IPsec is Internet key exchange (IKE) protocol. IKE is a negotiation protocol for mutual authentication and for establishing security associations (SA). SAs define the set of cryptographic algorithms and shared keys for use with ESP or AH. The initial version of IKE (IKEv1) had two phases. These two phases do not exist in the recent IKEv2 – see RFC 5996 [38].

2.4.2 SSL/TLS

The Secure Socket Layer (SSL) protocol [39] was the basis for TLS [40]. These protocols have two layers. The lower layer operates on top of a reliable transport protocol, such as TCP. This lower layer provides a secure and reliable connection by using symmetric cryptography and hash functions. Higher level protocols provide client-server authentication and negotiation of secret keys and encryption algorithms, by means of asymmetric cryptography. Placing SSL/TLS between the application and transport layers makes it transparent to the application protocols; hence it is easy to secure application layer traffic. SSL/TLS is widely used by web client to access web servers and it also used as the basis for the OpenVPN software [41].

2.4.3 DTLS

SSL/TLS only supports reliable transport protocols. However, some application layer protocols utilize unreliable UDP transport. Examples of such protocols are SIP and RTP. DTLS was designed to be as similar to TLS as possible [42], but to support UDP as a transport protocol. DTLS can be used by delay-sensitive real-time applications such as media streaming, VoIP, etc. DTLS fixes a problem with TLS, as TLS does not have a mechanism to deal with lost or out-of-order packets. The details of DTLS are given in RFC 6347 [42].

2.4.4 SRTP

SRTP is defined as “a profile of the RTP, which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, RTCP (the Real-Time Transport Control Protocol)” [43]. The SRTP packet format is shown in Figure 2.12.

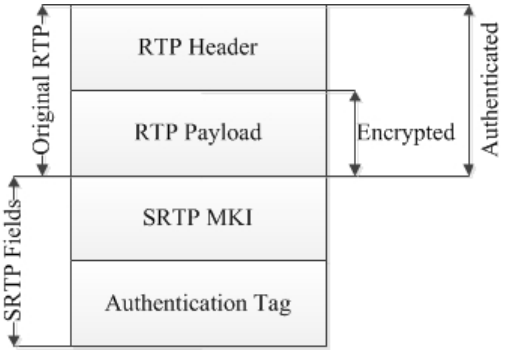

Figure 2.12: SRTP packet format [43]

SRTP provides for the confidentiality of RTP and real-time transport control protocol (RTCP) payloads, and integrity protects the whole RTP or RTCP packet. SRTP preserves the header compression efficiency of RTP and has a low computational cost. These properties and the high tolerance of RTP for lost packets and out-of-order delivery make it very suitable for use in a mobile environment, specifically in a UE.

SRTP fields:

- Master Key Identifier (MKI) is an optional field. The MKI is used for key management and it identifies the key used for authentication and/or encryption.
- Authentication Tag is a recommended field. The authentication tag carries message authentication data.

3 Method

This chapter presents the design of a multiplexing solution that is proposed to solve the problems described in section 1.2 on page 3 and to reach the goals of this master's thesis as described in section 1.3. Section 3.1 introduces the metrics that will be used to compare the different potential demultiplexing points. Section 3.2 describes the operation and details of the multiplexer, while the demultiplexer is described in section 3.3. Section 3.4 specifies the FEC mechanism for RTP packets when used on a UE with two active network interfaces. Section 3.5 discusses how VPN works when utilized with the proposed multiplexing solution. The limitations of the proposed solution are described in section 3.6.

3.1 Metrics

LTE has implemented a QoS mechanism to ensure high performance of the network [44]. All entities of the network architecture must support the recommendations of this QoS mechanism in order to realize high QoS. Moreover, various services place requirements on the network to ensure the best QoS. Various metrics are defined to measure QoS. Some of these metrics are: latency, jitter, etc. Therefore the multiplexing procedure that is proposed in this thesis project has to support QoS.

The source for the multiplexing is always the UE. The choice is obvious, because the voice and data traffic are generated on the UE and without an appropriate multiplexing solution the UE will waste network resources by sending redundant information. Figure 3.1 (repeats Figure 1.1) shows the different potential demultiplexing points: M1...M4.

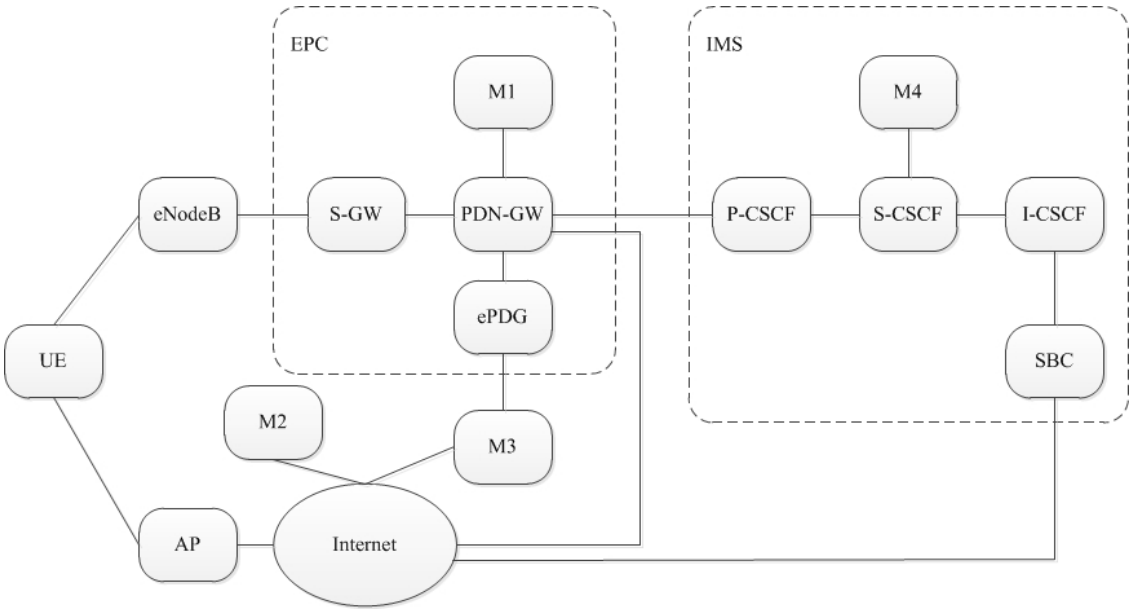

Figure 3.1: Possible demultiplexing points (Mn)

The introduction of different demultiplexing points will have different impacts on the network's performance. This impact will be compared for different UE-Mn pairs to propose the best possible demultiplexing point. To do this comparison, various metrics will be used to define the network characteristics. These metrics are:

- *Latency* – the end-to-end delay. In other words – the time it takes a packet to be transmitted from source to destination.
- *Jitter* – the fluctuation of latency as seen at the destination. Jitter occurs because of varying queuing and processing delays at routers. For example, RTP packets are normally sent every 20 ms, but due to jitter they might not be delivered to the receiver stably every 20 ms. The effects of the jitter are illustrated in Figure 3.2.
- *Packet loss* – the fraction of packets lost during transmission.
- *Throughput (Bandwidth)* – the actual data rate (this is sometimes referred to as goodput – successfully delivered bits per second). For voice traffic the bandwidth differs depending upon the CODEC used to encode and decode the speech.

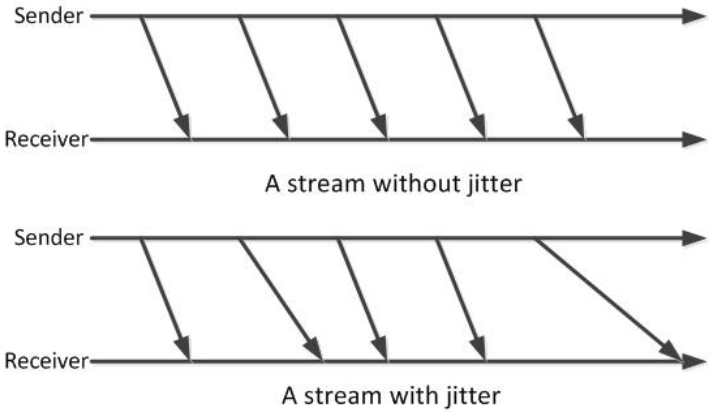

Figure 3.2: The jitter effect

Also, as the UE may send traffic via two interfaces (LTE and WLAN), two additional metrics will be used – *energy* and *price* costs. The energy efficiency of LTE and WLAN interfaces varies with the amount of data sent and/or received, the pattern of transfers, the pattern of low power operations, and with the type of service [5].

3.2 Multiplexing

As stated above, one of the multiplexing points is assumed to always be the UE. This project focuses on multiplexing the uplink traffic and does not consider the downlink traffic. For multiplexing of the uplink traffic at the UE the traffic passes down from the application to the transport, network, link, and physical layers. For the purpose of this thesis, the multiplexing of RTP and data traffic is proposed to be done between the network layer and the link layer. This placement allows the multiplexer to work independently of the physical network interface and allows all upper layer protocols to be used. Moreover, with this

placement, fewer headers are applied after the multiplexing procedure, thus only a small amount of redundant information is added. The multiplexer can process incoming IPsec packets and also can apply IPsec headers to the resulting multiplexed datagrams in order to create a secure tunnel to a demultiplexing point. In section 3.5 we will look at how multiplexing works together with a VPN.

The multiplexer has to be designed to make full use of the native LTE mechanisms and to have minimum impact on the UE's hardware and software. This should allow the easy deployment of this multiplexing solution together with LTE. To make the multiplexing procedure transparent to the original packet processing, a virtual network interface is introduced. The multiplexer is implemented in a virtual network interface driver; hence this driver can process packets at the IP layer, modify them, and put them back into the network layer, which forwards them to the link layer of one of the physical network interfaces. This implementation is useful with any type of packet and with any physical interfaces that packets are sent to, because the multiplexer neither interacts with the routing table (which determines to which physical interface packets should be sent) nor with the physical interface. This multiplexer supports both IPv4 [45] and IPv6 [46].

The multiplexer operates as follows:

1. Packets arrive at the network layer. These are either small RTP packets or bulk data packets. The application decides which source IP address and which destination IP address to put into each outgoing IP packet. The routing table determines to which interface an IP packet is to be forwarded based upon the packet's destination (and possibly also upon its source IP address, protocol, and source & destination ports). We assume that the multiplexer captures IP packets from the outgoing IP queue (i.e., at the network layer). Note that the multiplexer may have to wait for at least one RTP packet to be available before it can multiplex this RTP packet with an outgoing data packet. We will assume that we avoid multiplexing unless there is at least one RTP packet available, thus if there are no active VoIP sessions we need not delay data packets, while if there are active VoIP sessions then we delay the packet for up to 10 ms to wait for an RTP packet[*]. Once an RTP packet is available, multiplexing begins.

   Note, that the multiplexing will not work if IPsec in ESP mode is used at the network layer. As in ESP mode, everything after the ESP header is encrypted (see Figure 2.11), hence the multiplexer will be able to determine whether an incoming packet is RTP or not only by the packet size. Therefore if the multiplexer encounters a packet with ESP header, this packet is either multiplexed immediately (if the packet size is similar to RTP) or not considered for multiplexing.

2. Packets can be multiplexed until the size reaches the maximum MTU size (65535 bytes) to avoid creating jumbograms [47]. The more RTP packets we manage to multiplex with bulk data packets, the larger the overhead reduction we achieve. The

[*] This assumes that we are using a CODEC that emits RTP packets every 20 ms, hence the average waiting time for a packet should be half this amount of time. We do not wait for the full 20 ms as this would increase the delay and if voice activity detection is active we might still not receive an RTP packet.

maximum size for the resulting multiplexed datagram differs depending upon the outer transport layer headers used. Possible headers are UDP (8 bytes), UDP-Lite (8 bytes), or SCTP (12 bytes). Therefore the minimum possible maximum size is 65523 bytes, while the maximum possible maximum is 65527 bytes (65535 – header size).

3. Packets with the same source IP address in the IP header are multiplexed. Normally all packets generated by the UE have the same source address, but when multiple interfaces are used, this solution allows easy segregation of packets associated with different physical interfaces. Note that this means that the multiplexing tunnels for the different interfaces are separate; hence they can have different endpoints. This also means that the source IP address is redundant across the IP packets that are being multiplexed; hence only one copy of this address is needed.

4. The new outer headers are appended to the multiplexed packet. We will assume that this header is a UDP [48], UDP-Lite [49], or SCTP [50] header. A TCP [51] header may **not** be used as we do **not** want to suffer from head-of-line (HOL) blocking if a segment is dropped.

    - **UDP** – Simple, stateless, unreliable transport protocol. The UDP header size is 8 bytes with source port, destination port, length, and checksum fields. Packets are not acknowledged, therefore the delivery is not guaranteed. UDP is useful for multimedia applications.

    - **UDP-Lite** – This lightweight UDP protocol may be used with applications that can tolerate partially damaged payloads, instead of simply discarding them. These applications include multimedia services, such as voice or video streaming, where some CODECs (e.g. AMR for voice) operate better with damaged packets than dealing with lost or discarded packets. The UDP-Lite header is similar to the UDP header with a difference in the checksum field. In UDP-Lite, the checksum field covers only the sensitive parts of the payload. Insensitive parts are not covered by the checksum. For the multiplexed packet, the payload of RTP packets may be marked as insensitive, therefore leaving it up to the CODEC to cope with possible errors. Note, that this concerns only the transmission between the UE and a demultiplexing point. After packets are demultiplexed, the inner transport layer header determines the characteristics of the delivery. If an inner RTP packet was encapsulated with a UDP header (rather than UDP-Lite), then the use of UDP-Lite by the multiplexer is useless, because with the original UDP header the packet would be discarded if an error occurs.

    - **TCP** – TCP is the major reliable transport protocol used in today's IP networks. TCP provides ordered delivery of bytes. TCP may not be used in multiplexer because of the HOL blocking problem [52]. This problem occurs when IP packets are delayed because of the waiting time for previous lost IP packets to be retransmitted. Scharf and Kiesel [52] compare solutions for this

problem with TCP and SCTP transport protocols and say that SCTP provides better performance.

- **SCTP** – SCTP is a comparatively new protocol for reliable or unreliable delivery of messages. It is message-oriented, instead of stream-oriented as was TCP. SCTP allows ordered, partially-ordered and unordered delivery of messages. The latter completely avoids HOL blocking. To eliminate the HOL blocking problem for ordered delivery, the multi-streaming feature of SCTP can be used to create separate independent logical streams, thus a packet loss in one stream does not delay the messages of other streams [53]. Another feature of SCTP is multi-homing, which allows several interfaces to be used within the same SCTP association.

The destination port number in a transport layer header is used to process the packet at the demultiplexer in a demultiplexing point. In the description below we assume that the outer transport layer header will be a UDP header. Finally, an outer IP header is prepended to the packet. The source address field in this outer IP header is the same source IP address as in all the IP headers of the packets that have been combined. The destination address is an IP address of a demultiplexing point.

The multiplexer may use IPsec to create a secure tunnel between a UE and a demultiplexing point. AH and ESP may be used only in transport mode. In this case an additional ESP (or AH) header is placed between the outer IP header and outer UDP header together with the ESP trailer and ESP ICV at the end (note that a trailer and ICV are not used with AH).

5. The resulting datagram is sent to the link layer of a physical interface. Further processing of the outer IP, ESP (AH) if applicable, and UDP headers can be done together with processing of the portions of the headers and bytes of the multiplexed payload.

The procedure described above is shown in Figure 3.3 (without showing the IPsec headers).

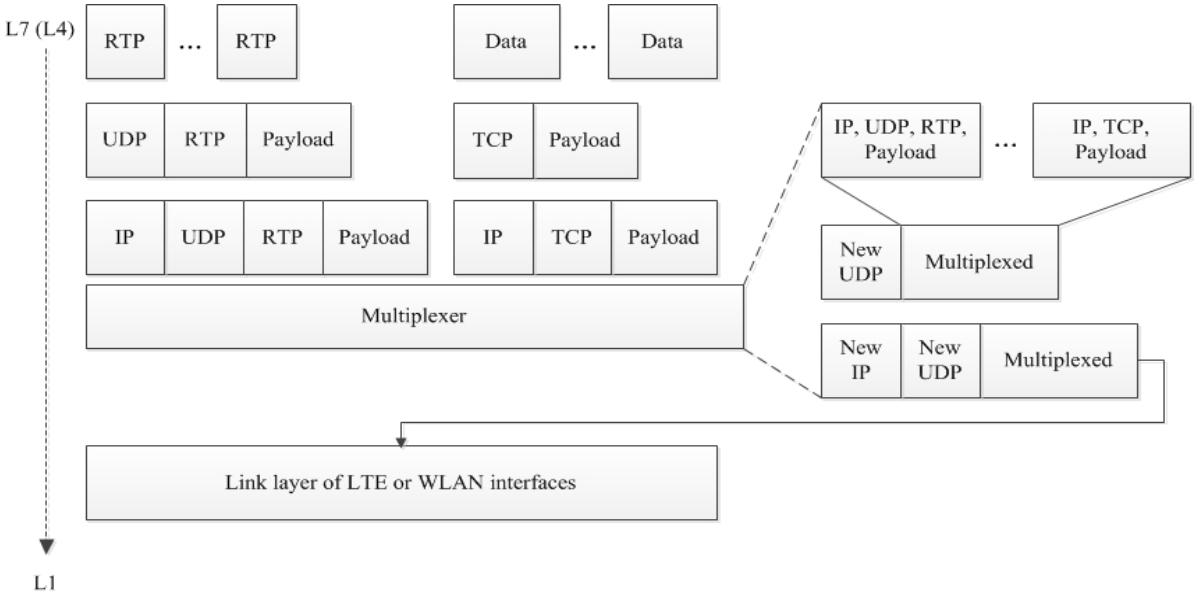

Figure 3.3: The multiplexer

When the LTE interface is used to send data, the resulting multiplexed datagram is forwarded to the PDCP layer. ROHC is applied to the outer IP and UDP headers. The resulting PDU is sent to the RLC layer. Normally voice data is sent using RLC-UM mode to skip the error recovery and packet retransmission functions of ARQ on the RLC layer, while bulk data is sent by RLC-AM to allow fast recovery without propagating errors to higher layers. When data and voice packets are multiplexed, we might think that we are limited to UM mode, because otherwise if errors occur, the whole multiplexed packet would be retransmitted and this would seem to be unacceptable for delay-sensitive voice packets; hence the RLC PDU of the multiplexed datagram would be sent by UM. However, this is not necessarily the case, since the retransmission that is taking place is only happening between the UE and the eNodeB and this is a very fast retransmission mechanism. Additionally, the number of attempted retransmissions is limited; hence it may be possible to consider using AM. Note that it is always possible to consider using TM – especially if we do our own ROHC processing before passing the PDU to the MAC layer

3.3 Demultiplexing

Demultiplexing is the procedure of separating the packets that were combined by the multiplexer at UE into the original separate packets. No matter where in the network (see Figure 3.1) the demultiplexer resides, it shall perform the following operations:

1. When a packet arrives at a demultiplexing point, it first passes through the link layer.
2. At the network layer the outer IP header is processed. If IPsec was used by the multiplexer to securely tunnel the traffic to the demultiplexing point, then the packet

is first checked to see if it is authentic (or a repeat) if authentication is being performed, next it is decrypted and the ESP (AH) header is removed. The resulting packet is passed to the transport layer, where the outer UDP header indicates the destination port of the demultiplexer.

3. The packet without the outer IP and UDP headers is processed by the demultiplexer. The combined packets are separated and sent back to the network layer to be forwarded to their original destinations.

3.4 FEC for RTP packets

The quality of the voice service in LTE varies with the packet loss rate. As more packets are lost during transmission, longer gaps may occur in the recipient's playout buffer leading to interrupted speech. Packet loss may occur due to various factors, one of these is bad communication channel conditions. As UEs communicate with eNodeBs via a wireless channel, conditions may worsen because of a long distance to a base station, because of obstacles between an UE and a base station, or because of some other factor. Normally CODECs are designed to deal with a small percentage of loss. However, when the packet loss becomes higher than 4% or many packets are lost in a row (a burst loss), then the CODEC is unable to provide high voice quality [54]. To address this issue and allow peers to maintain satisfactory call quality, Forward Error Correction (FEC) [8], specifically FEC for RTP [55] is proposed to be used with several network interfaces on a UE. Here we consider a UE with LTE and WLAN interfaces. FEC is an error recovery technique that places information about the packet (N-1) in packet N. Therefore each packet contains redundant information about the previous packet in order to recover this information if the previous packet is lost. Moreover, these packets can contain RTP data generated with different CODECs and these packets can be sent over separate interfaces (and hence potentially separate paths). As was described in section 2.2.3, different CODECs require various network bandwidths. If we add sufficient redundancy – which increases the bandwidth actually used, we can overcome random packet loss. Hence, when we use RTP packets with different CODECs and send them over separate interfaces (LTE and WLAN), we decouple the probability of packet loss, ensuring that it is likely that a call is perceived by the receiver as continuous. The structure of an RTP packet and FEC procedures are shown in Figure 3.4, where payload contains audio data for two different CODECs. In this figure we have highlighted the difference in the RTP timestamps by writing "t=n", where n is the n^{th} timestamp.

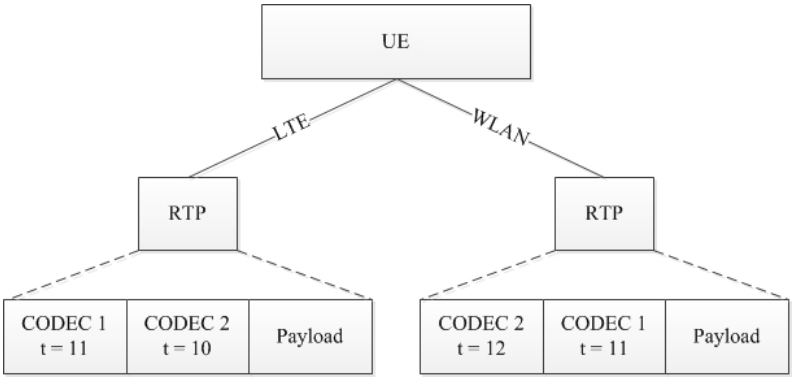

Figure 3.4: RTP packet structure for FEC using two interfaces

The overhead problem is also relevant to this type of RTP packets as even though we are putting two CODEC's payloads into each RTP datagram – the datagram is still relatively small for audio data. Therefore to reduce the overhead of small RTP packets, these packets can be multiplexed with bulk data being sent via both interfaces. The multiplexer takes care of this by combining packets with same source IP and thus RTP streams that are sent to the separate interfaces remain in separate flows (hence preserving their independence). The multiplexed packets are sent to the link layers of corresponding interfaces.

3.5 VPN

To protect data during transmission, users may create a secure VPN tunnel to a destination. As mentioned in section 2.4, two scenarios are possible in this thesis – placing a VPN before the multiplexing procedure or placing the VPN after the multiplexing procedure.

The possibility to apply IPsec to the resulting multiplexed datagram was described in section 3.2. After applying an outer UDP header, the multiplexer can then encapsulate the packet using ESP/AH in transport mode. Note that IPsec tunnel mode is not needed, because this tunnel will always be an end-to-end connection with a demultiplexer as the destination. The application of IPsec after the multiplexing procedure is useful when a user does not trust the path to a demultiplexing point, but trusts the network after a demultiplexing point and therefore does not need to secure packet at higher layers. This solution can also be applied if the user has secured the traffic at higher layers. If packets were secured before multiplexing, then the VPN to the demultiplexer may be omitted. The application of IPsec in the multiplexer is shown in Figure 3.5.

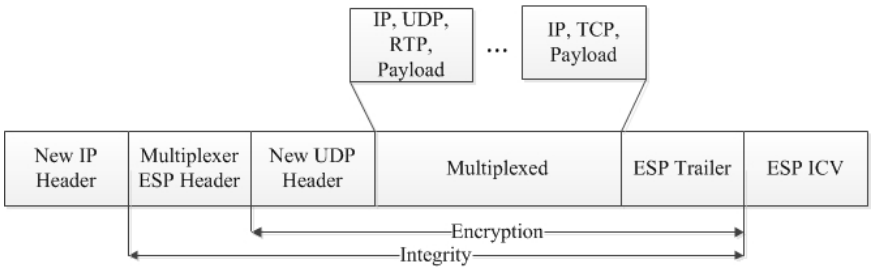

Figure 3.5: Application of the ESP IPsec in transport mode at the multiplexer

A VPN can also be setup **before** multiplexing begins. Different types of VPNs can be used. As the multiplexer can cope with any type of IP packet, securing the IP packet's contents at higher layers does not affect the multiplexing. In this project we consider two types of packets: RTP and other types of data (for example, TCP packets being used for web browsing or TCP/SCTP file transfers).

IPsec is a common solution for both RTP and other types of data packets. IPsec can be applied on the network layer *before* the multiplexer. There is no difference in IPsec's operation in terms of what type of packet is being encapsulated – the ESP/AH header is prepended and the payload is encrypted (in ESP) and authenticated (see section 2.4.1 for details). The multiplexer processes the IPsec packets as if they were any other type of IP packet. For example, when voice is sent in RTP packets that are secured with IPsec, the termination point of this IPsec tunnel is generally the P-CSCF in the subscriber's IMS system (assuming that they are an IMS subscriber).

The secure VPN tunnel can be initiated at the application layer. For example, when web browsing a user's data may be encrypted using the SSL/TLS protocol. For delay-sensitive multimedia data, DTLS can be used, because it enables the use of the UDP protocol that is impossible with SSL/TLS. Moreover, specific for RTP packets is the SRTP protocol, which puts two additional fields at the end of the RTP packet and encrypts its payload.

At the demultiplexing point packets secured before the multiplexer are not affected by the demultiplexing procedure. All VPNs setup by higher layers are terminated at the original destination of each packet. There is no difference whether it is SSL/TLS, DTLS, SRTP or IPsec that was used to encrypt a packet, after these packets are separated at a demultiplexing point; they are forwarded just as any other packet would be. All cryptographic operations are performed at the packet's final destination, regardless of where this destination is. The application of security protocols before the multiplexer allows the traffic to be protected over the whole path to its final destination. The application of IPsec by the multiplexer protects data only until the demultiplexer. Hence, the introduction of the multiplexing solution and choice of a demultiplexing point does not affect the destination of the original packets nor does it affect their security (other than a possible denial of service if the tunnel endpoint is not operating correctly).

3.6 Limitations

We know that on the LTE interface the RLC layer has three modes of operations: TM, UM, and AM. They were described in section 2.1.2.2. Voice traffic is usually sent using UM mode, because the ARQ error recovery procedure of the AM mode will add delay to the delay-sensitive RTP packet flow. RTP packet loss is taken care by CODECs and the playout algorithm. Therefore no additional mechanism is needed for RTP packet recovery. Bulk data traffic, in turn, requires the link layer level error recovery procedures. Therefore, RLC AM mode is used and when the MAC layer HARQ does not recover an error, the ARQ on RLC layer acts. This significantly reduces the number of errors propagated to higher layers. When we multiplex RTP packets with bulk data, if we do not use AM mode for the resulting multiplexed datagram, then if the multiplexed datagram is lost on the link between the UE and eNodeB it would not be recovered by the lower layer procedures at the eNodeB. While this lack of HARQ would be acceptable for RTP packets, the failed delivery of data packets will result in propagating errors to the transport layer and repeated sending of the IP packets generated by the transport layer. Hence we should use AM mode. Later in the thesis we will look at the delay and jitter that will be added as a result of this decision.

Another limitation is related to the LTE QoS mechanism for VoIP. LTE prioritizes VoIP traffic over other types of traffic to ensure high call quality. With the multiplexing solution, voice is sent together with bulk data, therefore either (1) it cannot be prioritized until the multiplexed packet reaches a demultiplexing point or (2) we have to prioritize the resulting multiplexed packet containing both voice and data. Later when packets are separated, RTP packets can be prioritized over data packets on the path to their destination (if there is some type of QoS support over this path such as DiffServ or IntServ).

4 Analysis

This chapter analyses the proposed solution using the metrics listed in section 3.1 for our multiplexing solution and different demultiplexing points. Sections 4.1 to 4.5 show the values of various metrics and how they change with the proposed multiplexing solution. First the average values or their range measured by other researchers are discussed, and then the impact of the proposed multiplexing solution on the metric's value is evaluated. Note that as mentioned in section 3.2 this thesis only considers the uplink. Section 4.6 sums up all values and compares the alternative demultiplexing points. Section 4.7 discusses the results of this master's thesis and answers the questions from section 1.2.

4.1 Latency and Jitter

Latency in a packet-switched network can be measured either one-way (the time it takes the packet to reach the destination), or round-trip (RTT) (the time it takes the packet to reach the destination and a response delivered back to the source, excluding the processing time at the destination). For the purpose of this thesis, we are mostly interested in the one-way delay. Therefore, for easier understanding, when we have utilized RTT measurements done by other researchers, then we divide these values by 2 to estimate the one-way delay. Note that in LTE it is **not** always true that RTT is exactly twice as long as the one-way delay, as the uplink delay is usually a little longer than the downlink delay – as the uplink channel can only be used by one UE at a time while the downlink contains multiplexed that is sent to one or more UEs, so some error may be introduced by our assumption of a symmetric link delay. Jitter is the fluctuation of latency due to various reasons, such as contention to get the uplink channel, retransmission times, queuing delays at routers, etc.

The quality of a VoIP session depends upon the latency, jitter, and packet loss experienced by the RTP traffic. Before examining the latency of LTE and WLAN, it is important to clarify the bounded delay expected in order to provide a high level of QoS. This bounded delay is defined in terms of the one-way transmission time in the International Telecommunication Union's (ITU-T's) G.114 recommendations [56]. It is recommended that regardless of the application, the maximum one-way delay should not be longer than 400 ms in general, but for delay-sensitive applications (VoIP, for example) the delay should not be longer than 250 ms. The target value for the highest QoS and high user satisfaction level of the VoIP service, the latency should be less than 150 ms and this delay is expected in intra-regional routes (less than 5000km). A 200–250 ms mouth-to-ear delay value is acceptable. According to these values, the delay budget for the one-way transmission in LTE is expected to be around 80 ms (acceptable maximum delay minus the known delays, such as speech encoding, delay between eNodeB and EPC (6 ms [57]), processing in the core network, etc.) [58]. Therefore whatever services we add (multiplexer, VPN over multiplexer, or others), the resulting delay should not exceed 50-80 ms in order to support a high QoS.

LTE provides much better performance, including smaller latency (5–100 ms) [59], than previous generations of mobile networks, and is supposed to provide high quality VoIP service and video-conferencing. The RTT and RTT jitter of LTE and WLAN were compared by Huang et al. in [60], resulting in an LTE average RTT value of 69.5 ms (35 ms one-way) and RTT jitter of 5.6 ms (2.8 ms one-way). The WLAN average values are 64.5 ms for RTT (32.5 ms one-way) and 7.9 ms for RTT jitter (4 ms one-way). Moreover, the results of their tests reveal the uplink one-way delay in LTE is sensitive to the packet size. While the WLAN uplink delay was stable at 30 ms, the LTE uplink delay grew from 40 ms to 56 ms as the packet payload size grew from 0 bytes to 1400 bytes (see figure 8 in [60]). This puts some restrictions on the resulting multiplexed payload size and a discussion of this is given in section 4.3. Measurements of a somewhat higher delay are given by Marwat et al. in [61], where the transmission of a pure VoIP packet encoded with the GSM-EFR CODEC, resulting in a 32 byte payload [62], resulted in a delay of 69–74 ms. Figure 4.1 shows the measurement results of TeliaSonera's LTE network done by Epitiro Ltd. [54]. The average latency was stable at 22–23 ms, with the peak delay not exceeding 38 ms.

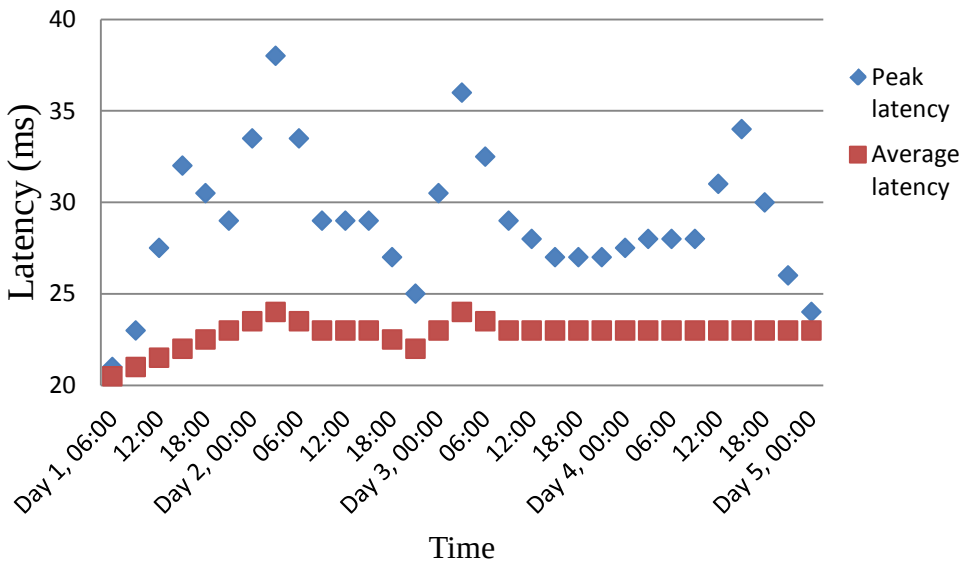

Figure 4.1: Peak and Average LTE latency (Adapted from figure 6 on page 13 of [54])

The user plane RTT was measured by Wiley-Green and Svensson [63] with Near, Mid, and Far located eNodeBs, two payload sizes 32 and 1400 bytes, and with a 50% load and unloaded (0%) network conditions. With no HARQ retransmissions, the average RTT for a 32 byte payload was 23 ms, while the RTT was 40 ms for a 1400 byte payload. HARQ retransmissions add 8 ms to the delay [57], and 1-2 retransmissions are likely to occur [64]. Thus, the resulting average user plane one-way delay for 1400 bytes (this size is close to the resulting multiplexed payload) is 40 (RTT) / 2 + 8 (HARQ) = 28 ms. RTT is divided by 2 to

get the one-way latency. Note that in our analysis we do not consider ARQ retransmission, because very few HARQ errors require ARQ retransmissions.

As mentioned above, the result of measurements of the WLAN uplink delay is 30 ms. The same result was also obtained by Zhai et al. [65]. With the packet size of 1 kB and the probability of collision less than 0.1, the mean delay is less than 30 ms. Collisions add additional delay since WLAN employs the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism to access the channel. If the channel is idle, the sender waits for a Distributed InterFrame Space (DIFS) time (50 µs) and then starts transmitting. If the channel is busy (immediately or becomes busy during the DIFS), then to avoid collisions the sender starts a random backoff timer and waits for the channel to become idle. While the channel is idle, the timer counts down. Another attempt at transmission begins once the timer reaches zero. After receiving data, the receiver waits for a Short InterFrame Space (SIFS) time (10 µs) and sends an ACK. CSMA/CA also includes the optional use of small Ready to Send / Clear to Send (RTS/CTS) packets which WLAN entities can exchange to ensure the channel is available. Although the added time is very low (microseconds), a congested channel can add a delay of a few milliseconds. Longer delays are added if there are packets losses. The correlation of the packet loss rate and the resulting theoretical one-way latency can be obtained from Korhonen and Ye Wang's equation 7 in [66]. According to this equation the higher the loss rate is the greater the additional delay.

The multiplexer proposed in this thesis adds the same latency regardless of the interface used, because the multiplexer operates between the network and link layers. The time it takes to encapsulate packets is insignificant; therefore this time is relevant to our analysis. To meet its goal of reducing the overhead for RTP traffic, the multiplexer has to capture as many RTP packets as possible. But due to delay-sensitive nature of these packets, the capture time is purposely limited. If we assume that RTP packets are sent every 20 ms plus encoding and there is an additional processing time of 1-5 ms, then the multiplexer should wait for up to 10 ms and if no packet arrives, then it encapsulates the already captured packets and sends the resulting packet for further processing. Additional delay will be added if a VPN is used. The encryption for the VPN at the multiplexer side and decryption at the receiver adds an additional 2–10 ms [67].

The demultiplexing points (see Figure 3.1) differ from each other in terms of one-way delay and jitter. The demultiplexing point **M1** resides in the core network, therefore the usage of this point does not add additional delay, as packets without the multiplexer are normally forwarded to the same point in the EPC regardless of the interface used at UE. The demultiplexing point **M2** is a cloud [68] service provider, this should add very low additional access latency. Also the more the operator pays to the cloud service provider the better service it gets. More information about cloud providers and their pricing is given in section 4.5. If **M2** is reached from LTE network, then the delay to send demultiplexed RTP packets or other packets not destined to the Internet back to EPC is added (in contrast bulk data can be forwarded directly to the Internet). The demultiplexing point **M3** is an entity between the external network and ePDG, which is the entry point from external network to the EPC. Packets sent via WLAN interface at UE need to pass this point to be processed in the EPC.

The latency needed to get to the **M3** demultiplexing point is the ordinary one-way latency of the WLAN. The demultiplexing point **M4** is located at the application server within IMS. The usage of this demultiplexing point adds some amount of latency, consisting of the time needed to tunnel from EPC to IMS, to process packets at P-CSCF, S-CSCF, and forward them to the AS, and the time it takes to send the demultiplexed packets to the point where they are forwarded to their destinations (bulk data packets, such as of web browsing, can be sent directly to the Internet, whereas RTP or other packets should be returned to EPC). Also jitter is possible at every hop on the path to **M4**.

Table 4.1 shows the estimated, but very approximate latency, including jitter for all demultiplexing points when sending packets via either the LTE or WLAN interfaces.

Table 4.1: Latency and jitter from LTE and WLAN to M1-M4 demultiplexing points

	M1	M2	M3	M4
LTE	LTE User plane latency + eNodeB-EPC latency = **30-40 ms**	Latency of M1 + EPC latency + route EPC–M2, including jitter + delay at the Cloud + latency back to EPC, including jitter = **55-65 ms**	Latency of M1 + EPC latency = **35-45 ms**	Latency of M3 + latency for processes described above for M4 point + possible jitter at every hop = **55-65 ms**
WLAN	WLAN latency + jitter to EPC + EPC latency = **45-55 ms**	WLAN latency + delay at the Cloud = **35-45 ms**	WLAN latency **30-40 ms**	Latency of M1 + latency for processes described above for M4 point + possible jitter at every hop = **65-75 ms**

4.2 Throughput

LTE's targeted throughput is 100 Mbps for the downlink and 50 Mbps for the uplink [59]. These are the theoretical maximums and operators offer download data rates ranging, for example, from 5 Mbps to 80 Mbps at TELE2 [69] and 40 Mbps to less than 100 Mbps at Telia [70]. The offered upload speed for LTE is 1-20 Mbps [71]. These are much higher peak data rates than in previous generations of wide area cellular networks. These high peak data rates,

as already mentioned in section 4.1 were necessary as LTE is supposed to provide high quality VoIP service and possibly video-conferencing.

There are many versions of the IEEE 802.11 (WLAN) standards [72], of which the most popular and widely used versions in modern smartphones are IEEE 802.11a, 802.11b, 802.11g, and 802.11n. The newest version, IEEE 802.11ac, is already supported by the latest smartphones [73, 74] and allows for a throughput up to 2400 Mbps [75]. However, the IEEE 802.11ac standard is still young and the first products have only recently been certified. A more mature version is IEEE 802.11n which is widely deployed and supports an average throughput between 150 Mbps–250 Mbps (see table 2.1 in [76]). Therefore we will assume that in practice a WLAN is limited to these speeds. Furthermore, we will assume that although broadband access network data rates can reach up to 1 Gbps for the backhaul from an IEEE 802.11 network access point, the normal downlink values are typically a peak of 100 Mbps for broadband and 8-10 Mbps for Asymmetric Digital Subscriber Line (ADSL) [77, 78]. The uplink backhaul broadband access network link is much slower with an average speed ranging from 1 Mbps to 10 Mbps [77, 78]. This means that in practice LTE upload data rates are higher than available via WLAN. Real world tests also have established the higher throughput of LTE. Throughput test of public WLANs showed that the AP throughput is *rarely* greater than 2 Mbps [79]. The LTE test of Swedish operator TeliaSonera done by Epitiro Ltd. revealed an average upload data rate of 1.7 Mbps is rather consistent during the 4 days of measurements [54], and this consistency is important to provide a high quality VoIP service. This data rate was most likely explicitly limited by TeliaSonera. As described below, other tests have shown higher data rates. A comparison by Balasubramanian, Mahajan, and Venkatarami of 3G and WLAN showed that WLAN throughput is much lower than 3G with an upstream UDP throughput being 850 kbps for 3G and 400 kbps for WLAN [80]. Knowing that LTE has a much higher throughput than 3G, the conclusion is obvious.

The test of AT&T and Verizon LTE performance in USA done by RootMetrics showed an upload data rate of up to 8 Mbps [81]. A field trial of LTE throughput was done Wylie-Green and Svensson [63] with Near, Mid, and Far located eNodeBs, two scenarios with 0% and 50% loading, and with TCP and UDP data. Their uplink test revealed that the throughput does not change much between loaded and unloaded scenarios. Moreover, for near and mid distance eNodeBs the throughput was 18.50 Mbps – 18.80 Mbps. For far located eNodeB, the throughput dropped to 2.18 Mbps – 3.70 Mbps for TCP and to 3.70 Mbps – 4.07 Mbps for UDP.

Another test done by Huang et al. [60] was performed using the Android application 4GTest (now known as MobiPerf [82]). The throughput measurements of WLAN were limited to their ISP's advertised peak data rate 6 Mbps and the observed uplink throughput was less than 1 Mbps. The measured LTE uplink was in range around 1.5 Mbps – 10.1 Mbps with a median value of 5.64 Mbps [60].

As a result, the average LTE uplink speed was between 3 Mbps – 6 Mbps with the peak data rate being up to 18 Mbps – 19 Mbps. These values are high enough to support all kinds of high bandwidth services and to perform smoothly with the multiplexing solution regardless

of how large the resulting multiplexed packet would be. Also the various CODEC's required bandwidths (see section 2.2.3) are well below both the LTE and WLAN uplink throughputs. More bandwidth requirements of CODECs are given in [83], but these bandwidth requirements are for voice packets only, whereas the multiplexer combines all types of data. If the high bandwidth demanding services are used (for example, video conferencing), then we can say that in terms of throughput the LTE interface is preferred over the WLAN interface. Moreover, as mentioned earlier, the LTE throughput was consistent during the test, which is important for providing a consistently high QoS. Table 4.2 shows a summary of the LTE and WLAN uplink data rates (in terms of user data throughput).

Table 4.2: LTE and WLAN uplink throughput

	LTE	WLAN
Throughput	**3 Mbps – 18 Mbps**	**1 Mbps – 10 Mbps**

The demultiplexing points (Figure 3.1) **M1** and **M4** do not differ in terms of throughput. They can be accessed via both the LTE interface and the WLAN interface. In case of the LTE interface they both utilize the high LTE throughput of the user plane and are connected to the operator's core network. If **M1** and **M4** demultiplexing points are accessed via an external network, thus they are limited to WLANs throughput or the throughput of the backhaul from the WLAN access point to the core network, but more importantly the delay of these connections which is higher than for LTE. The **M2** demultiplexing point can be accessed from both networks equally. The usage of a cloud service provider does not result in a bottleneck in the operator's network, because the cloud service is generally connected to the Internet by links with much higher data rates than either LTE or WLAN support. Therefore the throughput of the **M2** demultiplexing point is only limited by the LTE or WLAN data rates. The demultiplexing point **M3** is also limited only by the LTE or WLAN data rates.

4.3 Packet Loss

The LTE data rates analysed in previous section are meaningless without the low packet loss rates. If packets are frequently lost in transmission, then despite the high packet throughput the system will not be able to maintain a high QoS. If the received RTP packet is late packet, it will be dropped (see section 2.2.2). If a packet is lost, then the high throughput could be used to rapidly resend the missing packet, but with sufficiently a high loss rate and non-zero RTT it would be impossible to avoid gaps in the receiver's buffer. There are many possible reasons for packet loss. Normally the CODEC and playout buffer & algorithm can deal with most isolated losses, but as mentioned in section 3.4, a packet loss rate of more than 4% or a burst loss will result in degraded voice quality, even if the best CODEC is used. For

the best voice quality the packet loss rate less than 1.5% is required [84]. Figure 4.2 shows the result of LTE upstream loss rate measurements done by Epitiro Ltd. [54]. The data was collected over 4 days and a packet loss exceeding 9% was observed only during one short period of time, the rest of the observed packet loss rate was below 0.5%. The downstream loss rate never exceeded 1.2%. The test done by RootMetrics for AT&T and Verizon resulted in a bit higher packet loss rates, namely 4.1% for AT&T and 2.7% for Verizon in the upstream direction and 3.1% for AT&T and 1.9% for Verizon in downstream direction [81]. All of these results are acceptable and would provide a high QoS for VoIP. LTE's low packet loss rate is due to the introduction of HARQ at the MAC layer which performs fast retransmissions.

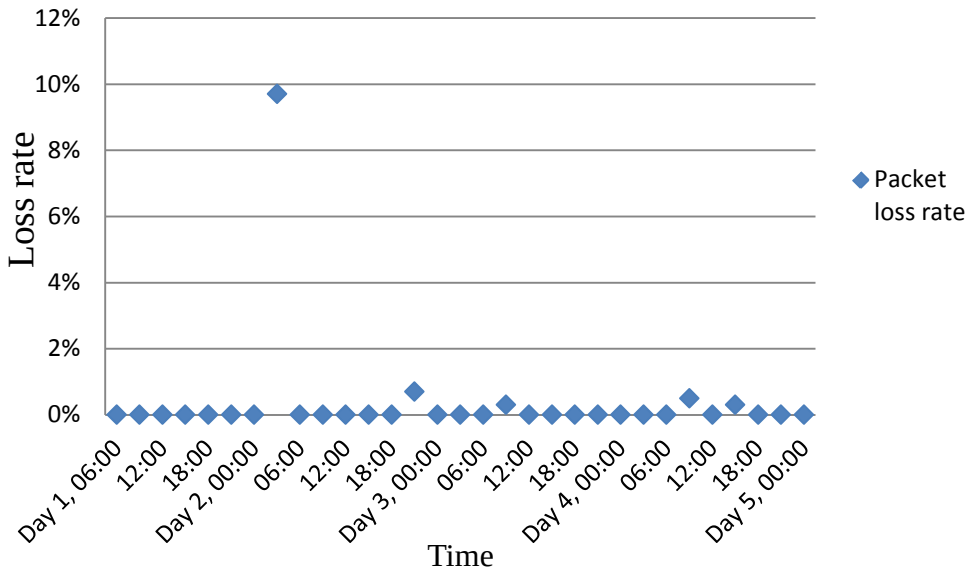

Figure 4.2: LTE upstream packet loss rate (Adapted from figure 17 on page 21 of [54])

WLAN performs worse than LTE in terms of the packet loss rate. Overall it seems that WLAN can support the QoS requirements of real-time applications, such as VoIP (with less than a 3% packet loss rate) and video conferencing (with less than a 1% packet loss rate), and the packet loss rate during silent conditions of 10^{-7}. However, when a WLAN cell is saturated, the packet loss rate is much higher due to the increased probability of collisions and growing queue lengths [65]. Also WLAN losses are bursty, especially when the Signal-to-Noise Ratio (SNR) is low [80, 85]. The dependency of the loss rate on the specific WLAN hardware was measured by Salvers, Striegel, and Poellabauer who reported in [86] that the packet loss rate varied between 0.15% - 3.8%.

Balachandran et al. [79] made real-world measurements of a public-area wireless network for three days with 195 active users. The packet error rate was evaluated based upon the total number of sent and received packets. Once the burst error rate reached 28%, and thrice the burst error rate was over 10%. Overall the mean error rate was 2.41%, but the peaks in the

loss rate were not rare, therefore if there had been an active session, it would have experienced bad quality. On the other hand, WLAN showed low packet loss rate in an indoor environment, where there was low interference and no obstacles. The average packet loss rate was 0.02% [87]. As indoor access points are normally further connected to the Internet by wired links, the whole path to a destination is very reliable.

The WLAN packet loss rate is dependent on the packet size. For a given throughput, the larger a packet is the higher loss rate, but with a throughput of 1-2 Mbps the difference is noticeable, but not significant [88]. Whereas with higher throughputs the difference in packet loss rate between the smallest and largest packets can reach 30% [89]. This dependency was also observed by Korhonen and Ye Wang in [66] who reported a packet loss rate of 0.1054 for 30 byte payloads, and a packet loss rate of 0.4860 for 1400 byte payloads.

It is obvious that large packets are more likely to experience losses than small packets, as their data frame occupies the radio channel for longer. A high packet error rate increases the end-to-end delay due to the time required for retransmissions [66]. Therefore the multiplexer should use an optimal size for payloads (given the link conditions). Our multiplexer uses RLC AM mode to take advantage of the fast retransmissions provided by HARQ at the MAC layer, however despite these fast retransmissions, a burst loss may degrade the session's quality. The dependency or independency of the packet loss rate on the size of a packet being sent over an LTE link has not yet been established. We know that the RLC layer in LTE performs segmentation and concatenation to fit a RLC SDU into the required MAC SDU size, which can be up to 32767 bytes [19]. We will see in the next section that a payload size of greater than 1 kB does not give any advantage in terms of energy per bit in LTE. In WLAN the MAC layer frame length is an Ethernet maximum of 1500 bytes. Thus, the multiplexed packet's size should not exceed 1400 bytes in order to avoid an excessive packet loss rate over the WLAN interface and to make the LTE interface energy efficient. Also this size is sufficient for the purposes of overhead reduction. The RTP payload size is 160 bytes with a G.711 CODEC and 20 bytes with a G.729 CODEC [83]. To avoid causing too long delay, we can limit ourselves to multiplexing 1 to 2 RTP packets with data, therefore 1180-1340 bytes will be left for bulk data (the maximum amount of space that is available will be 1400 – (20 [*] + 40 (RTP+UDP+IPv4)) and a minimum of 1400 – (160[†] + 60 (RTP+UDP+IPv6))). These values are theoretical and therefore are a subject to verification in future measurements.

In terms of the packet loss rate, the differences in the alternative demultiplexing points (see Figure 3.1) only depend upon the interface by which the demultiplexing point is accessed. The effects of errors occurring while packets are being transmitted within the EPC are not considered, because (1) they are unlikely, and (2) they are very rare (as the packet loss rate within this network is very low). Even the external **M2** does not increase the probability of packet loss, because the cloud service operators normally provide high QoS for their services as they utilize high speed fibre optic links to connect to the Internet backbone. Therefore, the QoS effects due to the packet loss rate will only depend on the interface which

[*] In the case of G.729
[†] In the case of G.711

is used. As we could see above, LTE performs much better and it provides a lower packet loss rate than the WLAN interface.

4.4 Energy

The energy consumption of LTE and WLAN interfaces was extensively evaluated by Rodríguez Castillo [5] and some information was already presented in section 1.1. The key result was that for VoIP calls and uploads the LTE interface always consumed more power than the WLAN interface.

For wireless interfaces sending data requires more energy than receiving data. Moreover, the LTE interface becomes a lot more energy efficient when fully utilized. This was proved in measurements of the power consumption of LTE and WLAN interfaces done by Huang et al. [60]. They measured LTE power consumption to be 1.62 times the energy consumption of the WLAN interface for the downlink and 2.53 times the energy consumption for the uplink when 10 MB of *bulk data* was transferred. This energy consumption was a substantial reduction compared to transferring a smaller amount of bulk data, but there is not a huge reduction in the amount of energy per bulk data bit for larger sized transfers. Edström [6] stated that if the TCP *payload size* is greater than 1 kB, then the energy per bit decreases insignificantly for LTE. The significant decrease in energy per bit with an increase in the size of a bulk data transfer for LTE and WLAN over the uplink is shown in Figure 4.3. The LTE energy per bit decreases with increasing amounts of data being transferred in the payload during a TCP connection (as shown in Figure 4.4). According to these graphs, we can see that to achieve the best energy efficiency for LTE, more than 1 MB of data should be sent in a session and this data should consist of packets with payload size greater than 1 kB.

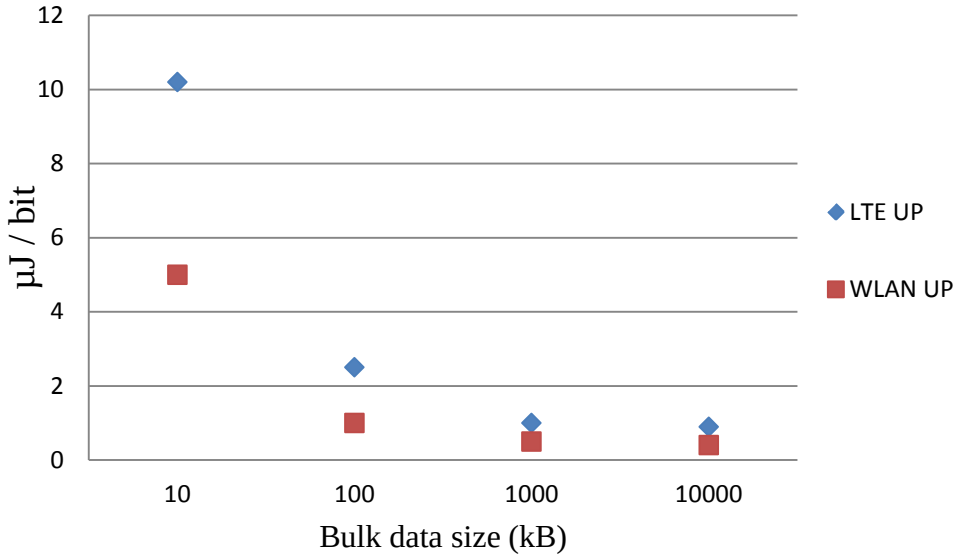

Figure 4.3: Energy per bit for LTE and WLAN uplink (Adapted from figure 12 on page 233 of [60]), µJ = 10^{-6} Joule.

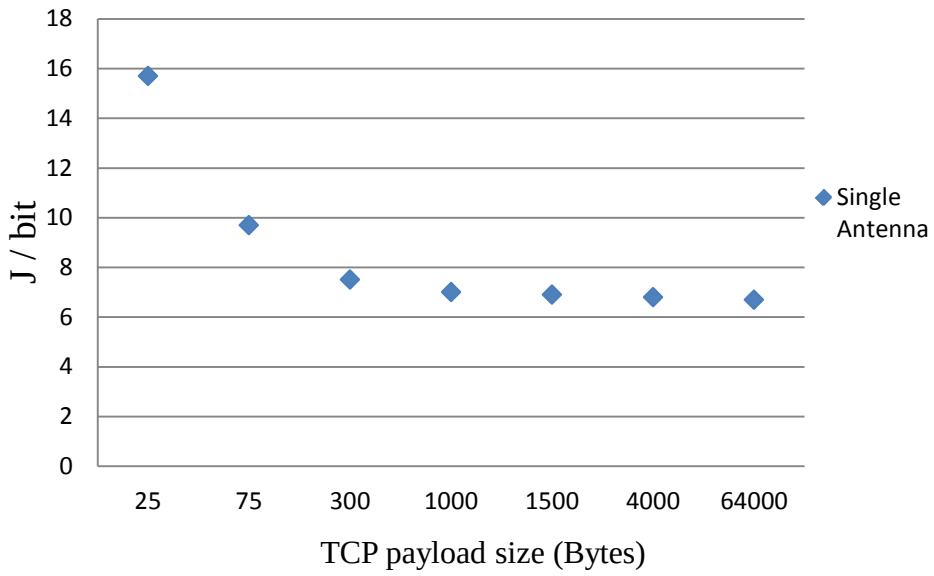

Figure 4.4: Energy per payload bit for LTE (Adapted from figure 33 on page 76 of [6]), J = 1 Joule.

The multiplexer proposed by this thesis project does not depend on the interface chosen due to its placement between the network and link layers. Therefore the multiplexer incurs the same amount of energy consumption regardless of which interface will handle the actual data transmission. It is important that the size of the multiplexed packet should be large enough to best use of the LTE interface in light of energy consumption, especially as LTE is *more* effective with a larger packet; otherwise it is preferable to use the WLAN interface to save power.

From a network operator's point of view, the fewer the number of servers and other entities added to the network, the less power consumption is added when implementing the multiplexer. Comparing the demultiplexing points (see Figure 3.1), **M1** and **M3** add the same amount of potential power consumption if implemented as an additional entity, excluding the additional power needed for the CPU to perform a task if the demultiplexing is implemented inside the PDN-GW or ePDG (respectively). The **M2** demultiplexing point eliminates the need for the mobile operator to worry about energy, because all of the servers reside at the external cloud service provider. Using this **M2** demultiplexing point is beneficial in terms of power, but it adds additional expenses due to the need for reserving virtual instances at the external cloud service provider (see section 4.5). **M4** appears to be the most power consuming alternative; even if IMS has already been implemented, **M4** would still require a new application server (AS), which would be the **M4** demultiplexing point. A new server introduces an additional power consuming entity. The additional power required for the **M4** demultiplexing point is the sum of the P-CSCF + S-CSCF + AS power consumption.

4.5 Price

The proposed multiplexing solution may reduce the subscribers' cost for their mobile data. This is due to the overhead reduction as the amount of data that needs to be transferred is reduced. Table 4.3 shows the current pricing for 4G monthly subscriptions of two Swedish operators, one USA operator, and the average European pricing. All prices are converted to US Dollars (**US$**) and rounded. The average cost per byte is also presented as we can use this to help to understand the impact of the multiplexing solution on the cost difference for a user. However, the byte price turns out to be extremely low; hence the cost difference from a user's point of view will not be a decisive factor when choosing the demultiplexing point.

Table 4.3: Mobile subscriptions pricing

	Average European [90]	TELE2 [69]	Telia [70]	AT&T [91]
Monthly subscription	**US$40** for 10GB	**US$65** for 15GB	**US$60** for 10GB	**US$50** for 5GB
Price per byte	Extremely low with average of **US$3.72 * 10^{-9}**			

In this thesis we assume that data traffic can be offloaded to WLAN networks and that multiplexing can optionally be applied. While a reduction in the amount of redundant information in packets may result in some savings if the LTE interface is used, the present extremely low pricing for ADSL or broadband Internet access makes it unreasonable to count every byte transferred via the WLAN interface and then via the fixed access network. Most subscriptions have no traffic limit and a peak data rate ranging from 3 to 1000 Mbit/s for the donwlink and 0.5-100 Mbit/s for the uplink, therefore the price is fixed regardless of whether the multiplexer being used or not. Table 4.4 shows the monthly subscription prices ranges for two Swedish and one USA providers.

Table 4.4: ADSL and broadband pricing

	Bredbandbolaget [77]	AT&T [92]	TELE2 [78]
Monthly subscription	**US$40 – US$135**	**US$30 – US$55**	**US$40 – US$120**

The demultiplexing point **M2** (see Figure 3.1) is an external provider for the demultiplexing service. Using this demultiplexing point might be useful for mobile operators whom could outsource all processing and tasks related to operating the demultiplexing point.

Nowadays the use of cloud services is growing and almost every task can be moved to the cloud. The main types of services that Cloud infrastructure can provide are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [68]. For example, small or medium size businesses can deploy their IT infrastructure in a cloud using one of many IaaS providers, such as Amazon Web Services [93] or Rackspace [94], hence avoiding the need to purchase servers or maintain an IT department. This same approach is applicable to mobile operators and could be used to realize the multiplexing/demultiplexing service. Even when mobile operators are huge companies with strong IT departments, the additional demultiplexing service might still be operated in the cloud to reduce expenses. When the load is low, the service may be used and paid for on-demand, thus reducing the operating costs, as there is no need to maintain and pay for the power of a mostly idle server. It is infeasible now to estimate how much mobile operates will benefit from moving a highly loaded demultiplexing point to the cloud, as the actual operator's expenses for maintaining a highly loaded demultiplexing server should first be evaluated. Then the possible maximum load of the demultiplexing point should be estimated and the required server configuration determined. Finally, the cost for a cloud server with such a configuration should be compared to the operating costs of a physical server located at and owned & operated by the mobile network operator. These steps are part of the suggested future work and are outside the scope of this thesis project.

The prices for using a Cloud provider to operate a lightly loaded demultiplexing point are given in Table 4.5.

Table 4.5: Cloud operator's prices

	Amazon EC2 [95]	Rackspace [96]
Hourly cost	**US$0.065** for on-demand small Linux instance	**US$0.06** for pay-as-you-go small Linux server or **US$0.18** for small managed Linux server
Monthly cost	**US$61** for reserved small Linux instance + **US$3.50** for CloudWatch detailed monitoring	**US$43.80** for pay-as-you-go small Linux server or **US$131.40** for small managed Linux server

4.6 Summary

The values for all of the metrics have been overviewed above. This section sums up all of these values and comes to conclusion about the preferred demultiplexing point (with reference to the alternatives shown in Figure 3.1).

As was noted in Table 4.1, in terms of *latency* and *jitter*, the **M3** demultiplexing point is the best choice if both LTE and WLAN interfaces are used. But **M1** shows slightly better performance for LTE, because compared to **M3**, it does not include the time that is needed for

a packet to pass through EPC. **M4** adds the most latency; moreover, if a WLAN interface is used, then the latency for accessing the **M4** demultiplexing point almost surpasses the total delay budget of 80 ms. **M2** is an average solution. Accessing it via the LTE interface has a high latency for VoIP packets; while accessing **M2** via the WLAN interface only adds delays due to the normal WLAN latency. However, the **M2** demultiplexing point has other advantages over the other alternatives, as will be explained below.

The *throughput* of the LTE interface is higher than for the WLAN interface. As the multiplexer increases the packet size, this higher throughput can be exploited. Therefore accessing any demultiplexing point via the LTE interface is preferable.

The *packet loss rate* is an important QoS metric. The overall packet loss rate has been observed by others to be much lower via the LTE interface than for via the WLAN interface. With the growth in the packet's size (as when multiplexing multiple packets we increase the resulting size of the payload to be transmitted), the loss rate increases slightly. Every packet loss leads to additional delays, such as retransmission delay and queuing delay for the next packets that may need to wait for erroneous packet to be retransmitted. As in our multiplexing solution we use RLC AM mode, LTE will perform fast retransmission, thus adding mostly smaller delays. Therefore accessing any demultiplexing point via LTE is preferable due to the smaller risk of congestion, reduced probability of collisions, and lower additional delays. The exception is when the WLAN is used indoors with almost no obstacles and low channel load, as in this case a very low packet loss rate was observed by others, hence the usage of WLAN indoors is preferable. The choice of a demultiplexing point does not significantly affect the packet loss rate.

With regard to *energy consumption*, LTE consumes more power than WLAN for a given amount of bytes of user payload transferred. However, with the optimal packet size (greater than 1 kB), the LTE energy per payload bit is close to that of WLAN. Approximate calculations of the resulting multiplexed payload size are given in section 4.3. The LTE interface can consume even less power than WLAN interface if a large amount of data (greater than 1 MB) is transmitted. So, from a user's perspective, the LTE interface is preferable over the WLAN interface if the multiplexer's operation results in an optimal payload size or if there is large amount of data to be transmitted [*]. Handover from LTE to WLAN is only suggested in case of bad LTE channel conditions. The choice of a demultiplexing point from an *energy consumption* point of view only affects the operator. The **M1** and **M3** points if used with the corresponding EPC entities do not add significant power consumption, except for the power required for the devices central processing unit (CPU). **M4** is the worst from a power consumption perspective as it requires additional power as explained in section 4.4. **M2** is the best choice for the operator, as the external cloud service provider not only takes care of all the power consumed by the demultiplexing point's operations, but use of the cloud service provider also reduces the number of human-hours the operator would have needed to maintain the demultiplexing point.

[*] A RTP stream of 160 bytes packets being set at 50 packets per second will take 125 seconds to send 1 MB of users traffic (i.e., ignoring all headers).

The *price* of maintaining a demultiplexing point varies. The **M1** and **M3** demultiplexing points do not require additional expenses if used with their respective EPC entities, or if used separately, a new server (which could be a virtual instance), energy costs, and human-hours for maintenance need to be considered. **M4** adds the most cost due to the number of additional entities, or if an IMS has already been implemented, then the cost is simply an additional application server[*]. The minimum prices for **M2** operations are listed in Table 4.5. They will be higher if there is a high load at the demultiplexing point. These prices are not high for huge mobile operators, especially considering that using the external provider reduces the human-hours costs needed to maintain the demultiplexing point as compared to an internal demultiplexing point. From the user's point of view, the price difference caused by the specific placement of the multiplexer is insignificant between the LTE and WLAN connected alternatives, although with a very high amount of traffic (mostly due to the amount of bulk data), an unlimited subscription via a WLAN access network is preferable.

To sum up, **M2** is the best choice for an initial implementation for testing purposes. The only constraint that makes it **not** the ideal choice for major implementations is the latency via the LTE interface. **M3** is suggested to be used for highly loaded instance of an operator's demultiplexing point accessed either via LTE or WLAN. Also with the introduction of the multiplexer and the use of an optimal payload size, the LTE interface becomes preferable to the WLAN interface when used to transmit data.

4.7 Results

This section answers the questions asked in section 1.2 based on the results of this thesis.

The choice of the demultiplexing point was suggested in previous section. The placement of the multiplexer between the network and link layers eliminates the problem of the multiple IP destinations, as the original packets are multiplexed together with their IP headers. When these packets are demultiplexed at a demultiplexing point, they can be forwarded to their destinations based on the information from their IP headers.

The possibility of the sequential packet loss is low in LTE, but very possible in WLAN, as packets are usually lost in bursts in WLANs. Therefore if RTP packets are sent via the WLAN interface, then the simultaneous use of the LTE interface and the FEC mechanism for RTP packets is advised to ensure high QoS for VoIP. Note, that the LTE interface is very inefficient in terms of energy if small packets are sent; therefore multiplexing of these RTP packets is important to increase the efficiency of using the LTE interface. The usage of WLAN to help LTE maintain high QoS is suggested only in the case of very bad LTE channel conditions. The demultiplexing point for both cases is suggested to be the same as in case of a single data flow. If the provider has both internal and external demultiplexing point available, then the **M2** demultiplexing point is suggested for WLAN and the **M3** demultiplexing point is suggested for LTE, because the latency of LTE to **M2** is above average.

[*] The number of such servers will of course depend upon the amount of traffic to multiplex and demultiplex.

The operation of the multiplexer is independent from the interface used. Therefore VHOs do not affect the traffic's behavior or the multiplexing procedures. The choice of the demultiplexing point is the same as in a non-VHO case, while if multiple demultiplexing points are available, and then the choice is the same as in the two-flow case.

The multiplexing solution supports all types of VPN protocols. Either SRTP, DTLS, SSL/TLS on application layer, or IPsec on network layer may be used. The multiplexer can encrypt the resulting multiplexed packet using IPsec. The details of this are given in section 3.5. The endpoints of the VPN tunnel depend on the protocol used and more specifically for the IPsec is the VPN placed before or after the multiplexer? For the application layer protocols the answer is obvious – as the other end of the VPN tunnel is the destination of the packet and the multiplexer does not affect this at all. If IPsec is used before the multiplexer, then the original packets are first encapsulated by IPsec and then multiplexed intact with other packets. The other end of this VPN tunnel is the original destination of the packet. If IPsec is used by the multiplexer itself, then this VPN tunnel is terminated at a demultiplexing point. The choice of the encapsulation protocols and their application phase depends on the security requirements of the mobile operator or the user.

5 Conclusions and Future work

5.1 Conclusions

The multiplexing solution proposed in this master's thesis allows reducing the overhead of small RTP packets in LTE network. The design of the solution does not have a major impact on the network architecture and involves only minor additional expenses. This solution fully supports the requirements for maintaining the high QoS in LTE and in conjunction with FEC for RTP allows maintaining the high QoS even in bad network condition. Moreover if the resulting multiplexed packet's size is large enough, the good energy efficiency of the LTE network interface is achieved.

The goals of this thesis as defined in section 1.3 were successfully met.

- A multiplexing solution was designed and possible demultiplexing points identified. The values of different metrics were collected from various researchers' publications and based on these metrics recommendations of using one or another demultiplexing point were given in section 4.6.
- The collected metrics helped to identify the efficiency of the simultaneous usage of LTE and WLAN interfaces to send RTP packets of the same session to ensure high QoS even in bad LTE channel conditions. The result was explained in section 4.7 together with an explanation of the impact of VHO on the multiplexing solution, where we found that VHO does not affect the multiplexing at all.
- The security aspect of the solution, specifically the compatibility of different VPN encapsulation methods with the multiplexer, was discussed in section 3.5. The easy application of any VPN encapsulation protocol has been considered during the design of the multiplexer. As a result, any encapsulation protocol can be used without constraints.

The work reported in this thesis allowed me to deeply understand LTE procedures. While reading about the architecture and performance of the LTE, I also learned a lot about the physical layer of LTE and how these channels operate, although these details were out of the scope of my thesis project. It was also noticeable that there is a lack of good performance tests that could give better understanding of what to expect from the wide deployment of LTE. The results of this master's thesis project could have been better if I had been able to make precise measurements using real LTE equipment. In spite of this, the results obtained by the theoretical analysis can be taken as a basis for future work.

If I had to do this project again, I would have considered placing the multiplexer between upper layers in order to reduce the number of headers. This would have required rethinking the demultiplexer's operation and how the original packets would get to their destination after they were reconstituted at a demultiplexing point.

5.2 Future work

Some suggested future work based upon the work reported in this thesis project includes:

- Using a real or virtual LTE implementation and various traffic generators to measure the latency, jitter and packet loss metrics. Moreover, in a real world situation, the actual LTE throughput may differ from the values used in this thesis. A WLAN's throughput might be used to estimate each of the metrics' values. The precise measurement of the optimal resulting multiplexed payload size and hence the amount of the reduced overhead is also important.
- The intra- or inter-cell mobility of an UE should be considered when measuring the metrics' values.
- The performance of the multiplexing solution in the case of roaming is also of importance. Most importantly is the choice of a demultiplexing point, which might be different for visiting UEs. If an external provider is used for the demultiplexing service, then which operator should take care of the multiplexed packet from the UE – the home operator or the visited one?
- A more complex question for future work is whether the multiplexer can be moved to higher layers and how this will impact its performance?

5.3 Required reflections

This master's thesis project deals with the overhead problem of RTP packets in an LTE network. This overhead leads to decreased throughput and increased cost due to a larger amount of redundant information in packets. Longer packets also result in higher energy consumption, which is undesirable especially with the energy demanding LTE interface. The **economic** impact of the proposed solution is twofold. From the user's perspective, the price decreases slightly due to elimination of redundant bytes, but this effect is so insignificant, that we can say there is no financial advantage to do some for users. Most importantly, the proposed multiplexing solution itself does not add any expenses. From the wide area cellular network operator's point of view, the **economic** impact of the multiplexing solution can be negative if an external cloud service provider is used, but this expense can recoup due to the reduced energy consumption due to the reduced overhead and avoidance of processing packets destined to the Internet in the EPC (for example, web browsing traffic).

The **environmental** impact is an important part of almost all research. In this project the energy consumption is reduced due to the reduction in overhead by multiplexing multiple packets and optimization of the packet size for the high power consuming LTE interface to achieve its best energy efficiency. From the wide area cellular network operator's point of view, the use of **M4** demultiplexing point would have a negative effect **environmental** impact, whereas the usage of **M2** demultiplexing point would save power that would

otherwise be consumed by the wide area cellular network operator due to eliminating the need for processing all packets (i.e., due to processing the non-RTP packets) within the EPC.

The **social** aspect of this work is affected by the potentially of always maintaining good VoIP session quality. When we use FEC to send RTP packets redundantly across the two interfaces and when we multiplex thee packets with data packets, we also ensure the continuity of a session even in the face of bad network conditions, thus improving user's perception and satisfaction with the VoIP service.

References

[1] Ericsson, 'Ericsson Mobility Report', Available at http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-february-2013.pdf, February 2013.

[2] Cisco Systems White Paper, 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017'. 06-February-2013, Available at http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

[3] S. Seo and J. Song, 'An energy-efficient interface selection for multi-mode terminals by utilizing out-of-band paging channels', *Telecommunication Systems*, vol. 42, no. 1–2, pp. 151–161, June 2009, DOI:10.1007/s11235-009-9175-8.

[4] R. Tawil, G. Pujolle, and O. Salazar, 'A Vertical Handoff Decision Scheme in Heterogeneous Wireless Systems', in *VTC Spring 2008*, Singapore, 2008, pp. 2626–2630, DOI:10.1109/VETECS.2008.576, Available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4526132.

[5] J. M. Rodríguez Castillo, 'Energy-Efficient Vertical Handovers', Master of Science Thesis, KTH Royal Institute of Technology, ICT School, Communication Systems, Stockholm, Sweden, 2013, Available at http://kth.diva-portal.org/smash/record.jsf?pid=diva2:608059.

[6] P. Edström, 'Overhead Impacts on Long-Term Evolution Radio Networks', Master of Science Thesis, KTH Royal Institute of Technology, Communication Systems, CoS, Stockholm, 2007, Available at http://kth.diva-portal.org/smash/record.jsf?pid=diva2:511755.

[7] D. Knertser and N. Adigozalov, 'VoIP downward multiplexing in LTE', KTH Royal Institute of Technology, Stockholm, Sweden, Course report, May 2012.

[8] M. Watson, A. Begen, and V. Roca, 'Forward Error Correction (FEC) Framework', *Internet Request for Comments*, vol. RFC 6363 (Proposed Standard), October 2011, Available at http://www.rfc-editor.org/rfc/rfc6363.txt.

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

[10] 3GPP, 'Radio Resource Control (RRC) Protocol specification', TS TS 36.331 Available at http://www.3gpp.org/ftp/Specs/html-info/36331.htm, March 2013.

[11] 3GPP, 'Packet Data Convergence Protocol (PDCP) specification', TS TS 36.323 Available at http://www.3gpp.org/ftp/Specs/html-info/36323.htm, March 2013.

[12] *LTE security*. Hoboken, N.J: John Wiley and Sons, Ltd, 2011, ISBN: 9780470661031.

[13] K. Sandlund, G. Pelletier, and L.-E. Jonsson, 'The RObust Header Compression (ROHC) Framework', *Internet Request for Comments*, vol. RFC 5795 (Proposed Standard), March 2010, Available at http://www.rfc-editor.org/rfc/rfc5795.txt.

[14] G. Pelletier and K. Sandlund, 'RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite', *Internet Request for Comments*, vol.

RFC 5225 (Proposed Standard), April 2008, Available at http://www.rfc-editor.org/rfc/rfc5225.txt.
[15] G. Pelletier, K. Sandlund, L.-E. Jonsson, and M. West, 'RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)', *Internet Request for Comments*, vol. RFC 4996 (Proposed Standard), July 2007, Available at http://www.rfc-editor.org/rfc/rfc4996.txt.
[16] S. Sesia, *LTE--the UMTS long term evolution: from theory to practice*. Chichester, West Sussex, United Kingdom; Hoboken, NJ: John Wiley and Sons, Ltd, 2009, ISBN: 9780470697160.
[17] A. Larmo, M. Lindstrom, M. Meyer, G. Pelletier, J. Torsner, and H. Wiemann, 'The LTE link-layer design', *IEEE Communications Magazine*, vol. 47, no. 4, pp. 52–59, April 2009, DOI:10.1109/MCOM.2009.4907407.
[18] 3GPP, 'Radio Link Control (RLC) protocol specification', TS TS 36.322 Available at http://www.3gpp.org/ftp/Specs/html-info/36322.htm, September 2012.
[19] 3GPP, 'Medium Access Control (MAC) protocol specification', TS TS 36.321 Available at http://www.3gpp.org/ftp/Specs/html-info/36321.htm, March 2013.
[20] 3GPP, 'IP Multimedia Subsystem (IMS); Stage 2', TS TS 23.228 Available at http://www.3gpp.org/ftp/Specs/html-info/23228.htm, March 2013.
[21] 3GPP, 'Single Radio Voice Call Continuity (SRVCC); Stage 2', TS TS 23.216 Available at http://www.3gpp.org/ftp/Specs/html-info/23216.htm, March 2013.
[22] 3GPP, 'Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2', TS TS 23.272 Available at http://www.3gpp.org/ftp/Specs/html-info/23272.htm, March 2013.
[23] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, 'SIP: Session Initiation Protocol', *Internet Request for Comments*, vol. RFC 3261 (Proposed Standard), June 2002, Available at http://www.rfc-editor.org/rfc/rfc3261.txt.
[24] G. Camarillo, *The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds*, 2nd ed. Chichester, England; Hoboken, NJ: John Wiley and Sons, Ltd, 2006, ISBN: 0470018186.
[25] M. Olsson, S. Sultana, S. Rommer, L. Frid, and C. Mulligan, *SAE and the evolved packet core: driving the mobile broadband revolution*. Amsterdam: Boston: Academic Press, 2009, ISBN: 9780123748263.
[26] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, 'RTP: A Transport Protocol for Real-Time Applications', *Internet Request for Comments*, vol. RFC 3550 (Standard), July 2003, Available at http://www.rfc-editor.org/rfc/rfc3550.txt.
[27] X. Yi, 'Adaptive Wireless Multimedia Services', Master of Science Thesis, KTH Royal Institute of Technology, Communication Systems, CoS, Stockholm, Sweden, 2006, Available at http://kth.diva-portal.org/smash/record.jsf?pid=diva2:512696.
[28] ITU-T, 'Pulce Code Modulation (PCM) of Voice Frequencies', Available at http://www.itu.int/rec/T-REC-G.711-198811-I/en, November 1988.
[29] 3GPP, 'Full Rate Speech Transcoding', TS TS 06.10 Available at http://www.3gpp.org/ftp/Specs/html-info/0610.htm, June 2001.

[30] 3GPP, ‘Half Rate Speech Transcoding’, TS TS 06.20 Available at http://www.3gpp.org/ftp/Specs/html-info/0620.htm, November 2000.
[31] 3GPP, ‘Adaptive Multi-Rate (AMR) speech codec; Transcoding functions’, TS TS 26.090 Available at http://www.3gpp.org/ftp/Specs/html-info/26090.htm, September 2012.
[32] 3GPP, ‘Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; Transcoding functions’, TS TS 26.190 Available at http://www.3gpp.org/ftp/Specs/html-info/26190.htm, September 2012.
[33] G. Collin and B. Chazalet, ‘Exploiting cooperative behaviors for VoIP communication nodes in a wireless local area network’, KTH Royal Institute of Technology, Communication Systems, CoS, Stockholm, Sweden, Project Available at http://kth.diva-portal.org/smash/record.jsf?pid=diva2:511682, March 2007.
[34] A. Drozdy, A. Rakos, Z. Vincze, and C. Vulkan, ‘Adaptive VoIP Multiplexing in LTE Backhaul’, in *VTC Spring*, Yokohama, 2011, pp. 1–6, DOI:10.1109/VETECS.2011.5956718, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5956718.
[35] S. Kent and K. Seo, ‘Security Architecture for the Internet Protocol’, *Internet Request for Comments*, vol. RFC 4301 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4301.txt.
[36] S. Kent, ‘IP Authentication Header’, *Internet Request for Comments*, vol. RFC 4302 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4302.txt.
[37] S. Kent, ‘IP Encapsulating Security Payload (ESP)’, *Internet Request for Comments*, vol. RFC 4303 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4303.txt.
[38] 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), September 2010, Available at http://www.rfc-editor.org/rfc/rfc5996.txt.
[39] A. Freier, P. Karlton, and P. Kocher, ‘The Secure Sockets Layer (SSL) Protocol Version 3.0’, *Internet Request for Comments*, vol. RFC 6101 (Historic), August 2011, Available at http://www.rfc-editor.org/rfc/rfc6101.txt.
[40] T. Dierks and E. Rescorla, ‘The Transport Layer Security (TLS) Protocol Version 1.2’, *Internet Request for Comments*, vol. RFC 5246 (Proposed Standard), August 2008, Available at http://www.rfc-editor.org/rfc/rfc5246.txt.
[41] OpenVPN Technologies, Inc, *OpenVPN*. [Online]: , Available at www.openvpn.net, [accessed April 22, 2013].
[42] E. Rescorla and N. Modadugu, ‘Datagram Transport Layer Security Version 1.2’, *Internet Request for Comments*, vol. RFC 6347 (Proposed Standard), January 2012, Available at http://www.rfc-editor.org/rfc/rfc6347.txt.
[43] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, ‘The Secure Real-time Transport Protocol (SRTP)’, *Internet Request for Comments*, vol. RFC 3711 (Proposed Standard), March 2004, Available at http://www.rfc-editor.org/rfc/rfc3711.txt.
[44] T. Ali-Yahiya, *Understanding LTE and its performance*. New York: Springer, 2011, ISBN: 9781441964564.

[45] J. Postel, 'Internet Protocol', *Internet Request for Comments*, vol. RFC 791 (Standard), September 1981, Available at http://www.rfc-editor.org/rfc/rfc791.txt.
[46] S. Deering and R. Hinden, 'Internet Protocol, Version 6 (IPv6) Specification', *Internet Request for Comments*, vol. RFC 2460, December 1998, Available at http://www.rfc-editor.org/rfc/rfc2460.txt.
[47] D. Borman, S. Deering, and R. Hinden, 'IPv6 Jumbograms', *Internet Request for Comments*, vol. RFC 2675 (Proposed Standard), August 1999, Available at http://www.rfc-editor.org/rfc/rfc2675.txt.
[48] J. Postel, 'User Datagram Protocol', *Internet Request for Comments*, vol. RFC 768 (Standard), August 1980, Available at http://www.rfc-editor.org/rfc/rfc768.txt.
[49] L.-A. Larzon, M. Degermark, S. Pink, L.-E. Jonsson, and G. Fairhurst, 'The Lightweight User Datagram Protocol (UDP-Lite)', *Internet Request for Comments*, vol. RFC 3828 (Proposed Standard), July 2004, Available at http://www.rfc-editor.org/rfc/rfc3828.txt.
[50] R. Stewart, 'Stream Control Transmission Protocol', *Internet Request for Comments*, vol. RFC 4960 (Proposed Standard), September 2007, Available at http://www.rfc-editor.org/rfc/rfc4960.txt.
[51] J. Postel, 'Transmission Control Protocol', *Internet Request for Comments*, vol. RFC 793 (Standard), September 1981, Available at http://www.rfc-editor.org/rfc/rfc793.txt.
[52] M. Scharf and S. Kiesel, 'NXG03-5: Head-of-line Blocking in TCP and SCTP: Analysis and Measurements', in *GLOBECOM '06*, San Francisco, CA, USA, 2006, pp. 1–5, DOI:10.1109/GLOCOM.2006.333, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4150963.
[53] Shaojian Fu and M. Atiquzzaman, 'SCTP: state of the art in research, products, and technical challenges', *IEEE Communications Magazine*, vol. 42, no. 4, pp. 64–76, April 2004, DOI:10.1109/MCOM.2004.1284931.
[54] Epitiro Ltd., 'LTE "Real World" Performance Study'. 2011, Available at http://www.epitiro.com/assets/files/LTE%20Real%20World%20Performance%20Report-Finland.pdf.
[55] A. Li, 'RTP Payload Format for Generic Forward Error Correction', *Internet Request for Comments*, vol. RFC 5109 (Proposed Standard), December 2007, Available at http://www.rfc-editor.org/rfc/rfc5109.txt.
[56] International Telecommunication Union (ITU-T), 'One-way transmission time', Recommendation G.114 Available at http://www.itu.int/rec/T-REC-G.114/en, May 2003.
[57] L. Zhang, T. Okamawari, and T. Fujii, 'Performance Evaluation of End-to-End Communication Quality of LTE', in *VTC Spring*, Yokohama, 2012, pp. 1–5, DOI:10.1109/VETECS.2012.6240243, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6240243.
[58] K. Aho, I. Repo, J. Puttonen, T. Henttonen, M. Moisio, J. Kurjenniemi, and K. Chang, 'Benchmarking of VoIP over HSDPA and LTE performance with realistic network data', presented at the 5th IEEE International Symposium on Wireless Pervasive Computing (ISWPC), Modena, Italy, 2010, pp. 401–406,

DOI:10.1109/ISWPC.2010.5483803, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5483803.

[59] 3GPP, 'Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN)', TR TR 25.913 Available at http://www.3gpp.org/ftp/Specs/html-info/25913.htm, February 2010.

[60] J. Huang, F. Qian, A. Gerber, Z. M. Mao, S. Sen, and O. Spatscheck, 'A close examination of performance and power characteristics of 4G LTE networks', in *MobiSys '12*, Low Wood Bay, Lake District, UK, 2012, pp. 225–238, DOI:10.1145/2307636.2307658, Available at http://dl.acm.org/citation.cfm?doid=2307636.2307658.

[61] S. N. K. Marwat, Y. Zaki, C. Goerg, T. Weerawardane, and A. Timm-Giel, 'Design and performance analysis of bandwidth and QoS aware LTE uplink scheduler in heterogeneous traffic environment', presented at the 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, 2012, pp. 499–504, DOI:10.1109/IWCMC.2012.6314254, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6314254.

[62] ETSI, 'Enhanced Full Rate (EFR) Speech Transcoding', EN EN 300 726 Available at http://www.etsi.org/deliver/etsi_en/300700_300799/300726/08.00.01_60/en_300726v080001p.pdf, November 2000.

[63] M. P. Wylie-Green and T. Svensson, 'Throughput, Capacity, Handover and Latency Performance in a 3GPP LTE FDD Field Trial', in *GLOBECOM 2010*, Miami, FL, 2010, pp. 1–6, DOI:10.1109/GLOCOM.2010.5683398, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5683398.

[64] D. Jiang, H. Wang, and X. Che, 'Uplink VoIP Performance in E-UTRAN TDD Mode', in *VTC Spring 2008*, Singapore, 2008, pp. 2482–2486, DOI:10.1109/VETECS.2008.547, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4526103.

[65] Hongqiang Zhai, Xiang Chen, and Yuguang Fang, 'How well can the IEEE 802.11 wireless LAN support quality of service?', *IEEE Transactions on Wireless Communications*, vol. 4, no. 6, pp. 3084–3094, November 2005, DOI:10.1109/TWC.2005.857994.

[66] J. Korhonen and Ye Wang, 'Effect of packet size on loss rate and delay in wireless links', presented at the IEEE Wireless Communications and Networking Conference, New Orleans, USA, 2005, vol. 3, pp. 1608–1613, DOI:10.1109/WCNC.2005.1424754, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1424754.

[67] Cisco Systems Inc., 'Voice and Video Enabled IPSec VPN (V3PN)', Solution Reference Network Design (SRND) Available at http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRND/V3PN.pdf, 2007.

[68] P. Mell and T. Grance, 'The NIST Definition of Cloud Computing', National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-145 Available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, September 2011.

[69] TELE2, ‘Subscriptions comparison’. Available at http://www.tele2.se/con_module_compare_subscription.aspx?from=subscription&subscriptionName=volym-hog, [accessed June 2, 2013].
[70] Telia, ‘Telia Mobile Broadband Pricelist’. Available at http://www.telia.se/docs/prislista/mobiltbredband/tellia-mobilt-bredband-prislista_TSP-1067.pdf, [accessed June 2, 2013].
[71] Bredbandsbolaget, ‘Broadband via 4G Prices Comparison’. Available at http://www.bredbandsbolaget.se/bredband/jamforelse/index.html#T24929_3, [accessed June 2, 2013].
[72] Wikipedia, ‘IEEE 802.11’. Available at http://en.wikipedia.org/wiki/IEEE_802.11, [accessed June 4, 2013].
[73] HTC, ‘HTC One Specifications’. Available at http://www.htc.com/www/smartphones/htc-one/#specs, [accessed June 4, 2013].
[74] Samsung, ‘Samsung Galaxy S4 Specifications’. Available at http://www.samsung.com/global/microsite/galaxys4/, [accessed June 4, 2013].
[75] Cisco Systems Inc., ‘802.11ac: The Fifth Generation of Wi-Fi’, Technical White Paper Available at http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/white_paper_c11-713103.pdf, August 2012.
[76] P. Legonkov and V. Prokopov, ‘Small Cell Wireless Backhaul in Mobile Heterogeneous Networks’, Master of Science Thesis, KTH Royal Institute of Technology, ICT School, Communication Systems, Stockholm, Sweden, 2012, Available at http://kth.diva-portal.org/smash/record.jsf?pid=diva2:540129.
[77] Bredbandsbolaget, ‘Broadband Prices Comparison’. Available at http://www.bredbandsbolaget.se/bredband/jamforelse/index.html, [accessed June 2, 2013].
[78] TELE2, ‘All Broadband Speeds’. Available at http://www.tele2.se/bredband/alla-bredbandshastigheter.aspx, [accessed June 2, 2013].
[79] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan, ‘Characterizing user behavior and network performance in a public wireless LAN’, in *SIGMETRICS ’02*, Marina Del Rey, California, 2002, pp. 195–205, DOI:10.1145/511334.511359, Available at http://portal.acm.org/citation.cfm?doid=511334.511359.
[80] A. Balasubramanian, R. Mahajan, and A. Venkataramani, ‘Augmenting mobile 3G using WiFi’, in *MobiSys ’10*, San Francisco, California, USA, 2010, pp. 209–222, DOI:10.1145/1814433.1814456, Available at http://portal.acm.org/citation.cfm?doid=1814433.1814456.
[81] RootMetrics, ‘Solving the LTE Puzzle: Comparing LTE Performance’. 14-April-2012, Available at http://gigaom.com/2012/04/14/solving-the-lte-puzzle-comparing-lte-performance/.
[82] University of Michigan, Univesity of Washington, M-Lab, *MobiPerf*. 2013, Available at www.mobiperf.com.
[83] Cisco Systems Inc., ‘Voice Over IP - Per Call Bandwidth Consumption’. 02-February-2006, Available at

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml.

[84] A. Ahmed, H. Madani, and T. Siddiqui, *VoIP Performance Management and Optimization*, 1st ed. Indianapolis, Ind: Cisco Press, 2011, ISBN: 9781587055287.

[85] J.-H. Jo and N. Jayant, 'Measurement and Analysis of the Channel Characteristics of an In-Building Wireless Network', presented at the 54th ARFTG Conference Digest-Spring, Atlanta, GA, USA, 2000, vol. 36, pp. 1–6, DOI:10.1109/ARFTG.1999.327382, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4120061.

[86] D. C. Salyers, A. D. Striegel, and C. Poellabauer, 'Wireless reliability: Rethinking 802.11 packet loss', in *WoWMoM 2008*, Newport Beach, CA, 2008, pp. 1–4, DOI:10.1109/WOWMOM.2008.4594875, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4594875.

[87] D. Eckhardt and P. Steenkiste, 'Measurement and analysis of the error characteristics of an in-building wireless network', in *SIGCOMM '96*, Palo Alto, California, United States, 1996, pp. 243–254, DOI:10.1145/248156.248178, Available at http://portal.acm.org/citation.cfm?doid=248156.248178.

[88] K. Chebrolu, B. Raman, and S. Sen, 'Long-distance 802.11b links: performance measurements and experience', in *MobiCom '06*, Los Angeles, CA, USA, 2006, pp. 74–85, DOI:10.1145/1161089.1161099, Available at http://portal.acm.org/citation.cfm?doid=1161089.1161099.

[89] M. G. Arranz, R. Aguero, L. Munoz, and P. Mahonen, 'Behavior of UDP-based applications over IEEE 802.11 wireless networks', presented at the 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, San Diego, CA, 2001, vol. 2, p. F–72–F–77, DOI:10.1109/PIMRC.2001.965298, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=965298.

[90] Wireless Intelligence, 'LTE operators adopt next-generation pricing models', White Paper Available at https://wirelessintelligence.com/analysis/2012/08/lte-operators-adopt-next-generation-pricing-models/344/, July 2012.

[91] AT&T, 'DataPro 5GB for Smartphone 4G LTE'. 2013, Available at http://www.att.com/shop/wireless/services/datapro5gb-smartphone4glte-sku5480228.html?source=IC95ATPLP00PSP00L&wtExtndSource=spfamdata5gb#fbid=oZaEPvApYlN.

[92] AT&T, 'U-verse Internet Offers'. Available at http://www.att.com/u-verse/shop/index.jsp?shopFilterId=500001&ref_from=shop&address_id=&ref_from=shop&zip=94931#fbid=S5R-uTYAdVV, [accessed June 2, 2013].

[93] Amazon, 'Amazon Web Services'. Available at http://aws.amazon.com/, [accessed June 2, 2013].

[94] Rackspace, 'Rackspace Cloud Servers'. Available at http://www.rackspace.com/cloud/servers/, [accessed June 2, 2013].

[95] Amazon, 'Amazon EC2 Pricing'. Available at http://aws.amazon.com/ec2/pricing/, [accessed June 2, 2013].

[96] Rackspace, 'Cloud Servers Pricing'. Available at http://www.rackspace.com/cloud/servers/pricing/, [accessed June 2, 2013].