Towards a seamless multi-technology access network

Younes Khadraoui

UNIVERSITE
BRETAGNE
LOIRE

THÈSE / Télécom Bretagne
sous le sceau de l'Université Bretagne Loire

pour obtenir le grade de Docteur de Télécom Bretagne
En accréditation conjointe avec l'Ecole Doctorale Matisse
Mention : Informatique

présentée par
Younes Khadraoui
préparée dans le département Réseaux, sécurité et multimédia
Laboratoire Irisa

Towards a seamless multi-technology access network

Thèse soutenue le 27 septembre 2016
Devant le jury composé de :

César Viho
Professeur, Université de Rennes 1/ Président

Raymond Knopp
Professeur, Eurecom - Biot / rapporteur

Philippe Martins
Professeur, Télécom ParisTech / rapporteur

Marcelo Dias De Amorim
Directeur de recherche, Université Pierre et Marie Curie – LIP6 / Examinateur

Stéphane Gosselin
Ingénieur de recherche, Orange Labs - Lannion / Examinateur

Annie Gravey
Directeur d'études, Télécom Bretagne / examinateur

Xavier Lagrange
Professeur, Télécom Bretagne / Directeur de thèse

N° d'ordre : 2016telb0411

Sous le sceau de l'Université Bretagne Loire

Télécom Bretagne

En accréditation conjointe avec L'Ecole Doctorale Matisse

Ecole Doctorale – MATISSE

Towards a seamless multi-technology access network

Thèse de Doctorat

Mention : Informatique

Présentée par **Younes Khadraoui**

Département : Réseaux, Sécurité et Multimédia (RSM)

Laboratoire : IRISA:

Directeur de thèse : Xavier Lagrange

Soutenue le 27 Sept. 2016.

Jury :

M. César Viho, Professeur, Université de Rennes 1 (Président)
M. Raymond Knopp Professeur, Eurecom (Rapporteur)
M. Philippe Martins, Professeur, Télécom ParisTech (Rapporteur)
M. Marcelo Dias De Amorim, Directeur de Recherche CNRS, UPMC (Examinateur)
M. Xavier Lagrange, Professeur, Télécom Bretagne (Directeur de thèse)
Mme Annie Gravey, Professeur, Télécom Bretagne (Encadrant)

To my beloved parents, to my wife...

Acknowledgements

My deepest and infinite gratitude goes first to the Almighty. Without his support, I'm certain that I would never get so far in my life.

I would like to express my sincere gratitude to my supervisor, Professor Xavier Lagrange. Until the last day of this thesis, he was always by my side providing me precious advice and insights, that allowed me getting so far in my work. He was a supervisor, a teacher and a second father during my PhD life. More than an honor, it was a pleasure to work with him. Xavier, I will always remain indebted to you.

My special thanks go to Prof. Annie Gravey that supervised me during this thesis. When I look back now, I can see the problems I had that could be solved only with Annie's help, and I feel that I have learned a lot from her. Thank you Annie.

This thesis has been conducted within the COMBO project. I had the chance to work with experts from different fields and to meet with awesome people. I would thus like to thank partners for their relevant questions during our meetings.

I would also like to express my deepest gratitude to the members of the Jury that accepted to review my work and for their relevant questions and remarks that made my thesis defense an unforgettable moment.

Furthermore, I would like to thank my office collegues, Jialong, Romain and Yangyang. I would also want to especially thank Roberto. The discussions we had togather helped me develop myself at a professional level as well as personnal. Moreover, my gratitude goes to all my collegues in the RSM department for their support, help and good company. I would also want to thank Alberto, Gwendal, Géraldine and Bruno for the days we were teaching togather in Brest and Rennes.

My heartful thanks go to all my friends that were always there to support me: Ahmed, Mohamed, Rabah, Salah, Smail, Yasir and Youcef. Thank

you guys for being always by my side, I always thank God for having the chance to meet you all. You all are more than friends, you are brothers.

My deepest gratitude goes to my beloved wife: Asma. These three years were tiring for you, but you never gave up. You were always by my side, in my best as much as in my worst moments. I feel like you deserve this PhD more than me. I will be forever grateful for this unforgettable moments we had togather, and wish I can one day do the same for you. I will also never forget my parents-in-law: uncle Ali and aunt Zohra. You supported me and helped me all along these years and more than that, you adopted me as one of your children.

Now that comes the moment to thank my beloved parents, I can't find the words to do it right. They were always supporting me, all along my life, whatever the circumstances. Whatever I say, that will never be enough to thank my father that initiated me to computer science, and taught me all the things I need to know to face this world. I will never be able to thank my mother neither, who gave me all the love and support I needed. In summary, if I am where I am now, it is because of you.

I will never forget my two grand-mothers. I gratefully thanks my brothers (Loukman, Chouaib, Yacoub, Ishaak and Youssef) and sisters (Maroua, Safa and Aya), who backed me up my entire life.

Abstract

The mobile data traffic has been continuously increasing. To avoid saturation of cellular network, operators need to use alternative access networks for offloading purpose. WiFi is a good solution as the operator can take advantage of its unlicensed spectrum as well as the large number of deployed WiFi access points.

In this thesis, we first provide a state-of-the-art of the different coupling solutions between LTE and WiFi. We show that most solutions cannot guarantee session continuity or duplicate the security procedures. This leads to propose "Very Tight Coupling" between LTE and WiFi. In this architecture, WiFi access points are connected to the LTE base stations and the security mechanisms of LTE are reused to ensure fast access to WiFi. It allows dual connectivity and to keep control signalling in the LTE network, which gives the possibility to have optimized interface selection procedures.

We study how very tight coupling can be implemented and how WiFi APs that integrated in customer residential gateways can be connected to LTE base stations in a converged fixed/cellular network. We then mathematically evaluate the performance of different deployment schemes and compute how much capacity can be saved on the LTE network. Furthermore, we implement the solution on a platform with a real LTE radio interface based on the Open Air Interface framework as a proof-of-concept. We perform several experiments to find the configuration of the link-layer protocols that gives the highest bit rate. In particular, we show that using WiFi and LTE simultaneously does not always increase the bit rate.

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation

The generalization of mobile devices, i.e. smartphones, tablets and laptops, has led to a significant increase of the number of mobile users. Moreover, mobile operators are always seeking to offer higher bit rate to their users by developing their networks with new technologies, from High Speed Packet Access (HSPA) to the 4th generation (4G) Long Term Evolution (LTE). These changes have opened new possibilities to developers, which can now propose applications that are more powerful, but also more and more demanding in terms of bandwidth. As a direct and expected result, the mobile data traffic has exploded. According to Cisco [5], the global mobile data traffic per year will grow from 6.5 exabytes in 2016 to 30.6 EB to 2020. Ericsson expects on the other hand the data traffic to be multiplied by 11 between 2015 and 2021 [6]. This creates new challenges for cellular operators that need to find efficient solutions to face this increase and to avoid their networks to be overloaded.

Furthermore, fixed networks are still being largely used by mobile users with the massive deployment of WiFi APs in most residential gateways (RGWs) as well as in public and office spaces. Hence, many today mobile devices use both the WiFi and cellular networks without any distinction. This is interesting for both, the fixed and cellular operators. WiFi can be used by the cellular operator to offload its network and to save some capacity, while the fixed operator can use the cellular network as a complement to WiFi. This is known as Heterogeneous Networks (HetNets).

However, even if the user has the impression to use both WiFi and cellular network simultaneously, this is not true from the application or from the network point of view. Today applications (e.g. Voice over IP, video) rely on the Internet Protocol (IP) address of the UE and of the distant server to map the different

ongoing sessions. When the UE moves from one network to another, e.g. from LTE to WiFi, its IP address changes. Although the user is connected the whole time, the session is disrupted and the application is disconnected. Moreover, current protocol stack are not designed to use more than one connection at a time, and multi-path is thus not supported.

1.2 Context of the thesis

This thesis was conducted within the "COnvergence of fixed and Mobile BrOadband access/aggregation networks" (COMBO) project [7]. COMBO is a European project that received funding from the European Union's Seventh Framework Program (FP7). The project groups 15 partners coming from different fields. Large operators are participating: Deutsche Telekom AG (DTAG), Orange and Telefonica. Several industrial companies are also involved: Ericsson, ADVA Optical Networking, AITIA International, Telnet, FON, Argela and JCP-connect. Finally, academic universities and schools contribute to COMBO: Telecom Bretagne, Lund University (ULUND), Centre Tecnologic de Telecomunicacions de Catalunya (CTTC), Politecnico di Milano (POLIMI) and the Budapest University of Technology and Economics.

The objective of COMBO is to propose and design new network architectures allowing the convergence of fixed and cellular accesses, i.e. Fixed Mobile Convergence (FMC). There have been several works regarding FMC networks, but so far the convergence was limited at a service level, i.e. all IP networks. COMBO rather focuses on the convergence of the network architecture itself. This aims at improving the use of the network equipment and infrastructure, which will result in reduced costs, better performance and seamless experience for the user. Our work within COMBO is to propose a novel WiFi/LTE coupling method, and to evaluate it using mathematical and experimental tools.

1.3 Contributions

Several issues are raised when a terminal is using the WiFi network beside the cellular LTE network. As most of the applications rely on the IP address to map the different session, the connection is broken if the address changes. Thus, when the UE moves from one access network to another, e.g. from WiFi to LTE, it obtains

a distinct IP addresses, which causes the disruption of all ongoing sessions on the UE and the application has to make a new connection using the new IP address.

This is due to the fact that the fixed and cellular networks are today separated and only connected through the Internet. In COMBO, new FMC architectures are proposed where the fixed and cellular share parts of the network, for instance the aggregation network. This opens new possibilities to have a fully integrated WiFi and LTE HetNet. In this work, we study a new LTE/WiFi coupling architecture that allows the user to use simultaneously WiFi and LTE in a transparent manner to the application. This architecture is called Very Tight Coupling between LTE and WiFi. In the following, we present our main contributions in the thesis.

Very Tight Coupling between LTE and WiFi

The general idea of very tight coupling was proposed in a paper published in [8], and was not studied in depth. In this thesis, we specify an architecture for Very Tight Coupling. We define the different building blocks such as how this mechanism can be integrated and deployed in COMBO FMC network and the different modifications needed in current LTE protocol stack. We also define the different procedures to connect and use WiFi in parallel to LTE.

Performance analysis of Very Tight Coupling

We mathematically compute how much capacity can be saved when using WiFi in Very Tight Coupling. We consider different scenarios, where a WiFi AP can be connected to only the nearest base stations, the two nearest base stations or all base stations. We first do a mathematical modeling of the problem for a limited number of base stations. Then we perform Monte Carlo computations for an extended number of LTE base stations. We analyze and compare the results obtained through the two methods. This work has been published in CCNC 2016 [9].

Implementation of Very Tight Coupling on a real time testbed

We set up a real-time Very Tight Coupling testbed based on the OpenAir Interface (OAI) framework. We developed several modules that we integrated to OAI. These include a WiFi integration module consisting of several functions that allow OAI to use WiFi in parallel to LTE, and a per-packet interface selection.

We used this proof-of-concept for different experimental studies.

Experimental analysis of Very Tight Coupling

LTE and WiFi have different properties in terms of bit rate, delay and loss rate. When using both simultaneously in Very Tight Coupling, these differences may disturb higher layers causing degradation of the throughput. In the first experiment, we study the impact of the delay diversity of the different paths. We show that using WiFi in parallel to LTE does not always increase the throughput. We then study the link-layer that provides the better performance. We use for the developed testbed for the different experiments.

The results of this part were presented in WD 2016 [10] and Cores 2016 [11].

Network coding for Very Tight Coupling

When using WiFi simultaneously with LTE, delayed packets and losses are the two main parameters that impact the performance. In order to mitigate these issues, we propose to use Network Coding. The idea is to send a redundancy packet on the most reliable link. In case of a late or lost packet on the late link, this redundancy can be used to recover it using already received packets.

We developed an integrated a new module responsible for Network coding operation. The module computes the redundancy packet and transmit it on the most reliable link. At the reception side, it detects and recover when possible a missing packet. We defined different coding schemes corresponding to different redundancy rates, that we experimented. The obtained results were published in VTC fall 2016 [12].

1.4 Structure of the thesis

The rest of this document is organized as follows. In chapter 2, we give a reminder of current fixed and cellular networks, and present the convergence proposed by the COMBO project. Chapter 3 gives a State of the Art of most of multihomming and mobility solutions. We finish the SoA with an analysis of all the presented solutions. This includes the different building blocks of the architecture and the different network configurations and procedure. In Chapter 4, we present in details the proposed architecture for Very Tight Coupling between LTE and WiFi. Then, Chapter 5 gives a performance analysis of Very Tight Coupling. We first use a mathematical model and then with extended Monte Carlo simulations. We study in this part how much capacity can be saved for different deployment scenarios. Chapter 6

deals with implementation aspects of Very Tight Coupling and experiments. It first gives a presentation of the testbed that we used for experiments and details about the modules that we developed. We then present and discuss the obtained results for different studies. Finally, Chapter 7 concludes this document and gives insights and perspective for possible future works.

Chapter 2

Fixed and mobile convergence

2.1 Introduction

Up to now, the development of fixed and cellular networks was done independently, using different technologies and protocols. Hence, today networks are completely separated. However, the continuous increase of the mobile data traffic forces the operators to develop their networks towards new technologies and architectures in order to always provide a satisfying quality or service to their subscriber. Fixed Mobile Convergence (FMC) is a good alternative.

Even if several works on FMC networks have preceded, the convergence was limited to service convergence. All networks are connected to the same IP network, i.e. the Internet, and have access to the same services using different access networks. On the other hand, COMBO focuses on the convergence of the network architecture itself. This will allow to have fewer equipment by sharing the infrastructure between the different accesses and to have a more efficient use of the network resources which will ultimately lead to a reduction of Capital Expenditure (CAPEX) and Operation Expenditure (OPEX). Moreover, FMC gives the possibility to operators to more efficiently distribute the traffic between WiFi and cellular in case of offloading, and allows optimized traffic control procedures which ensures better and seamless experience to users.

In this chapter, we first give an overview of current fixed and cellular network architectures. This will help understand the convergence proposed by COMBO, that we introduce just after. This network architecture will serve as the reference framework for the rest of this thesis.

2.2 Overview on current fixed networks architecture

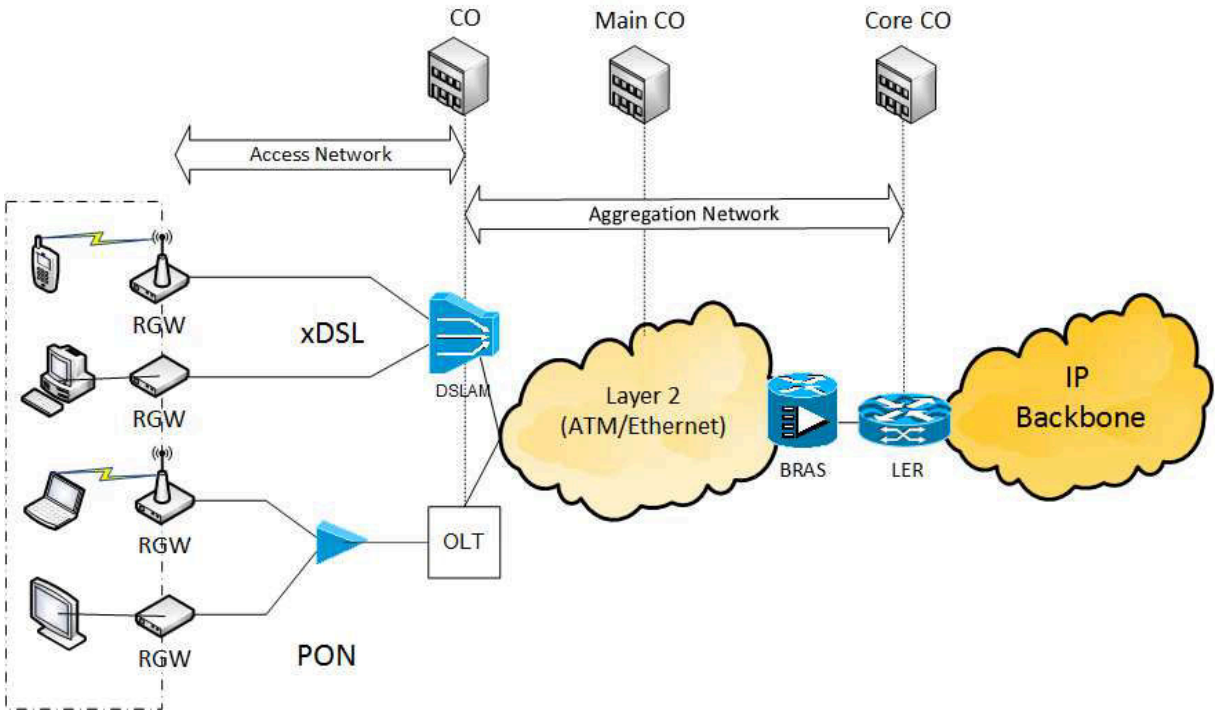


Figure 2.1: Current Fixed Networks architecture

Today fixed networks can be divided into three main segments: the access network, the aggregation network and the core network (see Fig.2.1). Each part covers geographic areas of different sizes and uses different technologies and protocols. Moreover, the network is composed of several network sites: i.e. Central Office (CO), main CO and core CO. In the following we first describe the different segments, and then give the function of each network site.

2.2.1 The home network

The home network is not really a part of the operator network as it is located in the subscriber premise. The main element here is the Customer Premise Equipment (CPE), usually called Residential Gateway (RGW), which connects the end user terminals to the operator network. Legacy RGWs provides only wire technologies (i.e. Ethernet), but with the generalization of wireless networks, WiFi has become more popular and most RGWs are equipped with a WiFi Access Point (AP). Indeed, the number of WiFi APs is continuously increasing according to [13], while there

are more than 267 millions WiFi access points registered by the same website. In addition to Internet access, RGWs are used by some operators to provide additional services, like Television over IP (IPTV) and Voice over IP (VoIP). Most recent RGWs also include some advanced features, such as Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) and Web/mail servers. Fig.2.2 shows a simplified view of an RGW.

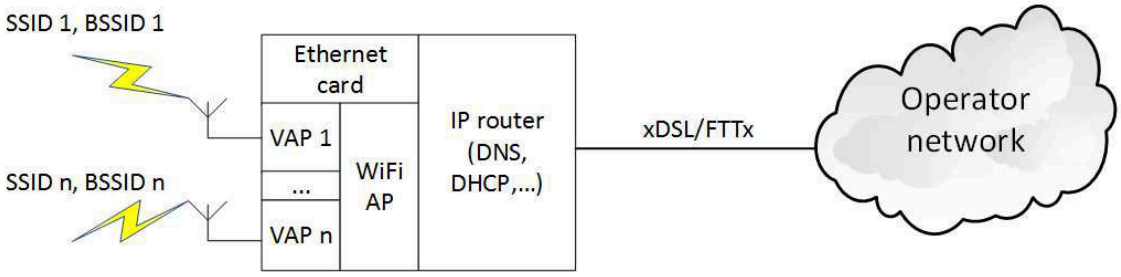


Figure 2.2: Residential Gateway global view

WiFi Access Points

In 802.11 terminology, a WiFi network is called a Basic Service Set (BSS), which consists of a WiFi AP and the different stations associated to that AP. A BSS has a Service Set Identifier (SSID), which can be seen as the name of the WiFi network, and is uniquely identified by a Basic SSID (BSSID). Usually, the SSID is a human readable name, while the BSSID is the MAC address of the WiFi AP serving this BSS. A WiFi AP broadcasts special frames called beacons to advertise its SSID and BSSID, in addition to other parameters such as supported security protocols.

Virtual Access Point

A physical WiFi AP can actually consist of several logical APs, called Virtual AP (VAP) [14]. There are many options for implementing VAPs. One of them is to have a single BSSID for all networks, and different SSIDs. However, the most common option used in current APs is to have a specific BSSID for each VAP (see Fig.2.2). In this case, each VAP broadcasts its own SSID and BSSID, and is seen by users as an independent AP. An example of the utilization of VAPs is the use by operators of RGWs to provide community networks to allow their subscribers to have Internet access when they are away from home. In this case, the WiFi AP in the RGW consists of two VAPs, one is for the residential WiFi network and the other one is for community network.

WiFi layer 2 bridging

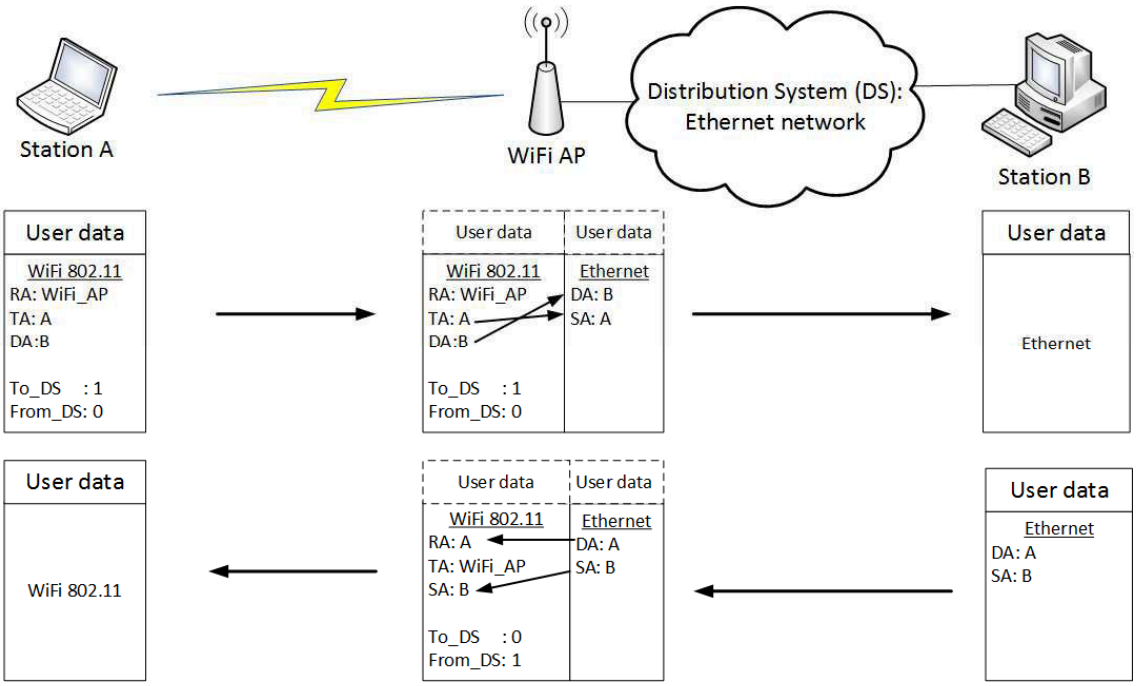


Figure 2.3: WiFi layer 2 bridge operation

A WiFi AP can also act as a layer 2 bridge. This is typically the case of an AP connecting two part of a single layer 2 network. In order to understand the operation of a layer 2 WiFi bridge, let us take the example of an AP connecting a WiFi network and a wire Ethernet network, both belonging to the same layer 2 network. The wired network is called a Distribution System (DS). This architecture allows the stations connected to the AP by WiFi to directly communicate with the stations on the DS, without requiring the AP to include an IP router. Technically, this is achieved using the 802.11 four-address (only three are used in this scenario) frame and to the To_DS and From_DS fields. Fig.2.3 shows how should these fields be set for a communication between station A connected to the WiFi network and station B on the wired Ethernet network. Depending on the combination To_DS and From_DS, the signification of each address field can be different.

For a frame sent from A to B (i.e. over WiFi), the To_DS field is set to 1 to indicate to the AP that it has to forward the frame toward the distribution system. In this case, the Receiver Address (RA) is the WiFi AP address (i.e. its BSSID), the Transmitter Address (TA) is the MAC address of A while the Destination Address (DA) is B MAC address. Upon reception of the frame, the AP encapsulates the user data on a new Ethernet frame and transmits it on the DS. By looking at the To_DS and From_DS fields, it knows exactly what addresses to use. In this case,

the WiFi DA is the Ethernet destination address, and the TA is the source address of the frame.

On the opposite direction, station B sends a standard Ethernet frame with its MAC address as the source address, and station A' MAC as the destination address. Upon reception of the frame, the AP recognizes the destination address as one of its associated stations. It thus creates a new 802.11 frame, with the From_DS field set to 1 and the To_DS field set to 0. The Ethernet source and destination address are copied in the new 802.11 frame, while the TA is the WiFi AP BSSID.

Additional information about WiFi

The 802.11 frame does not include a protocol field like Ethernet to indicate the encapsulated higher layer protocol. Thus, when it transports higher layer traffic, for e.g. IP, a Logical Link Control (LLC) header is added. It includes a *protocol* field that has the same signification as the Ethernet one and can take the same values.

Note that the WiFi beacon frames broadcast by the AP also provide information about the BSS load. It includes the number of stations that are currently associated with the AP as well as the channel utilization.

From a security point of view, 802.11 includes security mechanisms such as Wired Equivalent Privacy (WEP) and WiFi protected Access (WPA). These protocols are based on a pre-shared key system, meaning that both the terminal and the AP share the same key, which is used for authentication and ciphering. Recently, a new security protocol called Extensible Authentication Protocol-Subscriber Identity Module (EAP-SIM) was proposed. It allows a UE equipped with a cellular interface (e.g. LTE) and a WiFi interface to be seamlessly authenticated to the cellular operator WiFi networks using the credentials in its Subscriber Identity Module (SIM) card. Even if security is recommended over WiFi, it is not mandatory. For instance, in case of WiFi community networks, APs are open and the authentication is done at a higher layer, e.g. with a captive portal. In this case, the AP has an "open authentication" system with no pre-shared key required to the terminal to associate to the AP.

2.2.2 The access network

The access network transports subscriber flows to the aggregation network. In legacy architectures, copper was used to connect the customer premise to the Central Office (CO), using point-to-point Digital Subscriber Line (DSL) technologies such as Asynchronous DSL (ADSL) or Very-high-bit-rate DSL (VDSL). In this case, the

DSL line connects CPE equipped with DSL modems to a DSL Access Multiplexer (DSLAM) located in the CO. Historically, the Asynchronous Transfer Mode (ATM) protocol was used between the customer premise and the DSLAM, but Ethernet is more common lately.

Copper is more and more replaced with fiber and operators are deploying FTTx architectures such as Fiber-to-the-Home (FTTH) and Fiber-to-the-Cabinet (FTTC). These architectures are based on Passive Optical Network (PON) topologies, where several subscribers share a single optical fiber using point-to-multipoint connections. The CPE is equipped with an Optical Network Termination (ONT) and is connected through a PON to an Optical Line Termination (OLT) that can be located either in the CO or in the main CO.

2.2.3 The aggregation network

The aggregation network is responsible for transporting the flows of several subscribers attached to different COs to the core network. It is a layer 2 network that can be based either on Ethernet or on the Multi-Protocol Label Switching (MPLS).

The aggregation network is mainly composed of switches that are interconnected, for instance using a ring topology. The main function of a switch is to forward frames according to the destination address and VLAN. If we take the example of Ethernet, a typical switch has a forwarding table that maps each address to an interface and a VLAN. When it receives a frame, it looks up for the destination address in its forwarding table to know on each interface and VLAN it should send it. If the address is unknown, the frame is broadcast on all the interfaces (i.e. flooded). A switch also uses the source address to fill its forwarding table. It thus associates the source address of each incoming frame to the interface from which it was received.

Layer 2 multiplexing in the aggregation network can be performed using Virtual Local Area Networks (VLANs), i.e. QinQ (802.1ad standard [15]). The 802.1ad standard provides a multi-tag frame structure allowing two level of VLAN tagging, i.e. a Customer tag or C_VLAN and a Service Tag or S_VLAN.

There are different ways of multiplexing with VLAN that have been standardized by the broadband forum [16]. The most common one is to use the C_VLAN in order to isolate subscriber in different broadcasting domains while the S_VLAN is used to aggregate different service flows (e.g. VoIP), which allows the application of specific priority policies for each service.

For legacy access networks based on ATM, the Access Node (AN), i.e. DSLAM

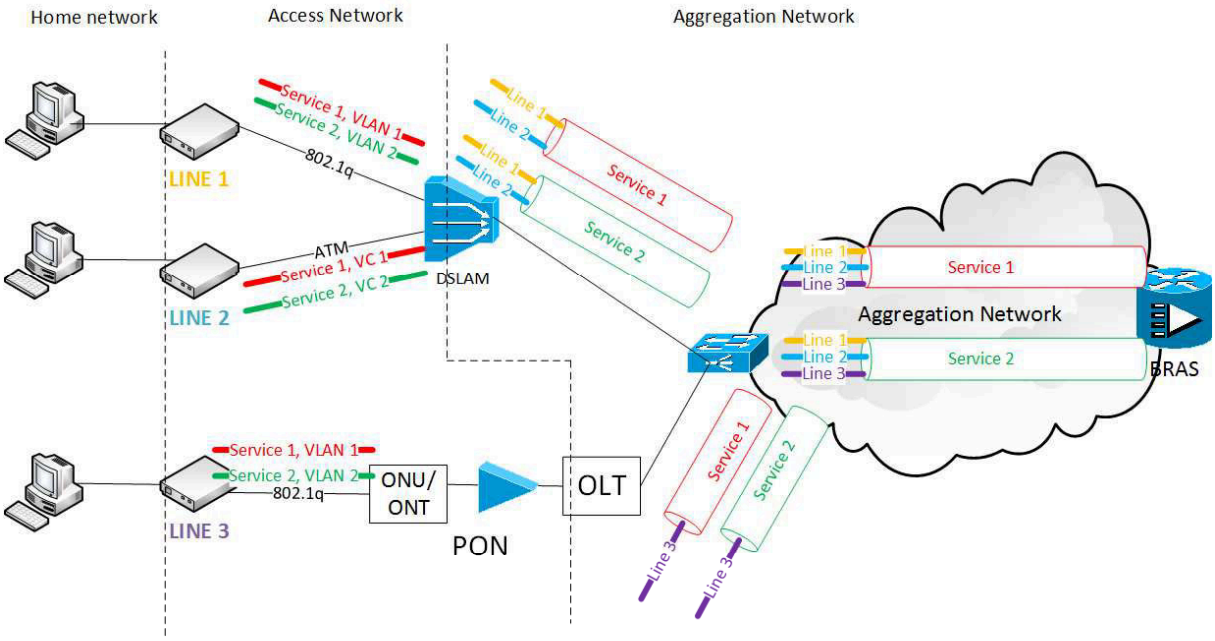


Figure 2.4: VLAN use in operator networks

or OLT, was the one responsible for tagging the frame. The customer RGW had just to send each type of traffic on a different Virtual Circuit (VC). Then the AN sets the S_VLAN tag according to the VC on which it receives the frame, and the C_VLAN associated to the customer.

In new Ethernet-based access networks, 802.1Q [17]VLAN tagging between the CPE and the AN. In this architecture, each service is sent over a VLAN in the access network, instead of an ATM virtual circuit. Then, the AN maps VLANs to S_VLANs in the aggregation network.

At the core CO, the traffic is routed between the BRAS and the Label Edge Router (LER) on the IP part of the aggregation network. The Layer 2 Tunneling Protocol (L2TP) is usually used to transparently transport subscribers IP traffic over the IP network between the BRAS and the LER.

2.2.4 The core network

The core network is responsible for connecting the operator network to the Internet. It is usually implemented in a ring architecture and is based on technologies like IP or MPLS. It also connects aggregation networks to other service networks, e.g. content distribution networks, or to management and control equipment, such as security and billing platforms.

2.2.5 Network sites

Figure 2.5: Network sites and distances

Fixed networks are composed of different network sites located at different levels in the network. These sites are usually operator buildings grouping network equipment. The most important sites and distances are displayed in Fig.2.5. The description of each one and usual distances [18] are given in the following:

- **Office (CO)**: The CO is a network site that terminates cables used to connect the customer premise to the aggregation network. It is thus the limit between the access and aggregation network. It holds the DSLAM in case of copper architecture and OLTs for fiber-based architectures. It is also the first powered site, unlike the legacy cabinet which is lower in the network. For dense urban areas, the CO can be from 1 to 2km away from the customer premise. In urban areas, it can be up to 3km while it can reach 4km in rural zones. It is worth mentioning that COs are currently being removed by operators.

- **main Central Office (main CO)**: The main CO is a building located in the aggregation network that hosts some operator equipment, such as Ethernet switches, ATM switches or even OLTs in some cases. The main CO can be close to the customer premise, i.e. 2km, in dense urban zones, while it can reach 5km and 10km in urban and rural areas respectively.

- **core Central Office (core CO)**: The core CO is the edge between the aggregation and core networks and is thus the IP edge for all subscriber traffic. Its distance to the customer depends on the geotype. It can reach 20, 60 or 100km in case of dense urban, urban and rural ares respectively.

2.3 Reminder on LTE architecture

The LTE network, also called the Evolved Packet System (EPS), is responsible for providing the end user with IP connectivity and and to connect him to the

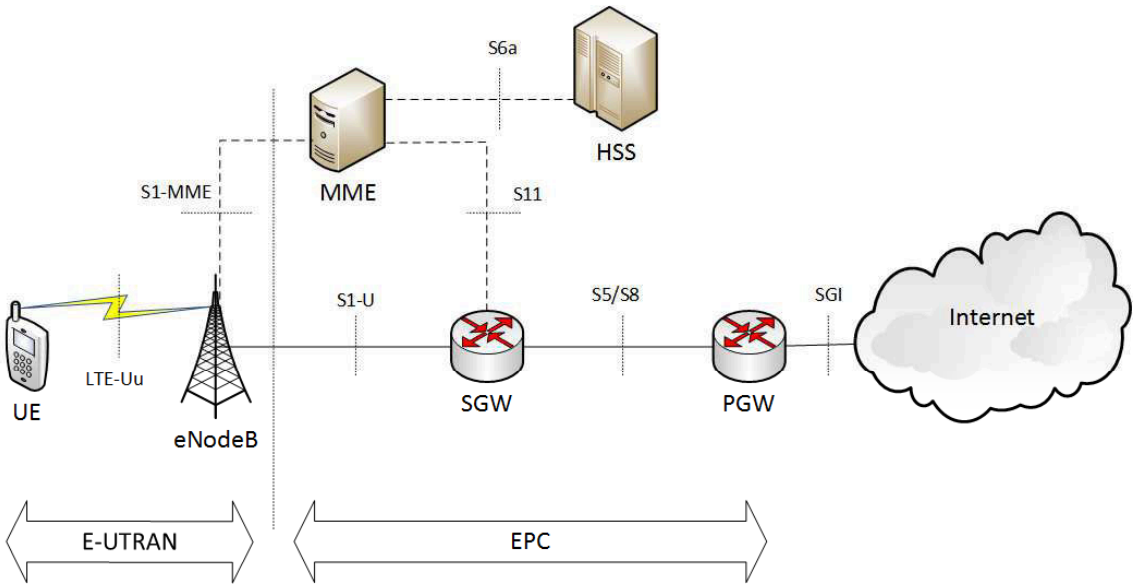


Figure 2.6: LTE network architecture

Internet. The EPS is organized around the concept of bearers. Bearers can be seen as IP data flows defined between the UE and a Packet Data Network (PDN) with a specific Quality of Service (QoS). When the UE connects to the EPS, it obtains a default bearer with a best effort QoS, i.e. non-guaranteed bit rate. Then, it has the possibility to request for dedicated bearers with specific QoS. Note that bearers need to be established in the EPC and in the E-UTRAN as well.

The EPS consists of two main parts: the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC) (see Fig.2.6). In the following, we give a description of each part.

2.3.1 The E-UTRAN

The E-UTRAN [1] is the radio part of the LTE network. It is responsible for connecting the UE to the EPC. It consists of several base stations, also called eNodeBs. Unlike precedent cellular network architectures, there is no controller in LTE and eNodeBs are directly connected to the EPC. The interface connecting the UE to the eNodeB is called LTE-Uu. It is used to transport user traffic as well as signaling traffic through the radio interface from the UE to the eNodeB.

An eNodeB can serve different cells in case of cell sectorization. A cell is identified with a E-UTRAN Cell Global ID (ECGI). An ECGI consists of the combination of the Public Land Mobile Network (PLMN) ID, which is unique for a given operator, and the Cell ID, which is used to identify a cell within a PLMN. Thus, the ECGI can

uniquely identifies a cell among different Public Land Mobile Networks (PLMNs).

A UE can be identified on the E-UTRAN with a Radio Network Temporary Identifier (RNTI), which is assigned by the eNodeB that is serving it. The RNTI is transported by the MAC layer and is used by the UE to identify which radio channel message is destined to it. It is worth mentioning that the RNTI is not actually transported in the MAC header, but it is used to compute the Cyclic Redundancy Check (CRC) of the radio message so that only the UE with the corresponding RNTI can decode the message.

In the E-UTRAN, there are two types of radio bearers: Signal Radio Bearers (SRBs), which are responsible for carrying signaling traffic, and Data Radio Bearers (DRBs) that carry user data traffic. DRBs are associated with a bearer in the EPC network, i.e. S1-bearer. Each bearer is identified with a Logical Channel Identifier (LCID).

The LTE transmission is organized in sub-frames, which last 1 ms. Two duplexing schemes are possible in LTE: the Frequency Division Duplex (FDD) or Time Division Duplex (TDD). In FDD, the frequency band used for downlink is different from the one used for uplink, while TDD uses the same frequency for both. It is worth noting that the duration of the sub-frame means that the latency is at least equal to 1ms.

2.3.2 The Evolved Packet Core

The Evolved Packet Core (EPC) [1] is the LTE core network. It provides IP connectivity to users and is responsible for transporting IP traffic toward the Internet. Unlike previous network architectures, LTE EPC is entirely IP-based. The EPC consists of different gateways and equipment:

- *The Serving Gateway (SGW)*: The SGW is the gateway connecting the eNodeBs to the EPC through the S1-U interface. It is also considered as a mobility anchor when the UE performs handover from one eNodeB to another.

- *The Packet Gateway (PGW)*: This is the IP edge for all LTE user traffic. It allocates IP addresses to users and connects them to external IP networks, i.e. the Internet.

- *The Mobility Management Entity (MME)*: The MME is responsible for mobility and session management in addition to some security functions.

- *The Home Subscriber Service (HSS)*: The HSS is the database that contains all subscriber information. It includes authentications and policy management functions.

2.3.3 LTE protocol architectures

In this section, we present the LTE protocol architectures of the control and the data planes.

Control plane

LTE control plane consists of all traffic used for signaling in the EPS. Typically, it is used for establishment of bearers, mobility management and for security procedures.

In the E-UTRAN, the Radio Resource Control (RRC) [19] is the protocol used for signaling on the LTE-Uu interface between the UE and the eNodeB. It is responsible for radio bearers establishment as well as measurement reporting.

RRC messages are encapsulated into Packet Data Convergence Protocol (PDCP) packets. PDCP is responsible for security in the radio interface (we give more details about PDCP specification in section 2.3.3). Packets are then transported using the Radio Link Control (RLC) and the Medium Access Control (MAC) LTE protocols to the eNodeB.

RLC [20] is responsible for segmentation and reassembly of higher layer Packet Data Units (PDUs), i.e. PDCP PDUs, as well as error correction through the Automatic Repeat reQuest (ARQ) protocol. It also provides reordering and in-sequence delivery of PDUs to PDCP. Three modes are supported by RLC: a Transparent Mode (TM) in which RLC is bypassed, a Unacknowledged Mode (UM) that provides in-sequence delivery but no ARQ and a Acknowledged Mode (AM) that includes all functions.

The main function of the MAC LTE layer [21] is to map different logical channels into physical transport blocks. It is also responsible for error correction through Hybrid ARQ (HARQ).

Within the EPC, the Stream Control Transport Protocol (SCTP) [22] is used for reliable communication between the eNodeB and the MME over the S1-MME interface.

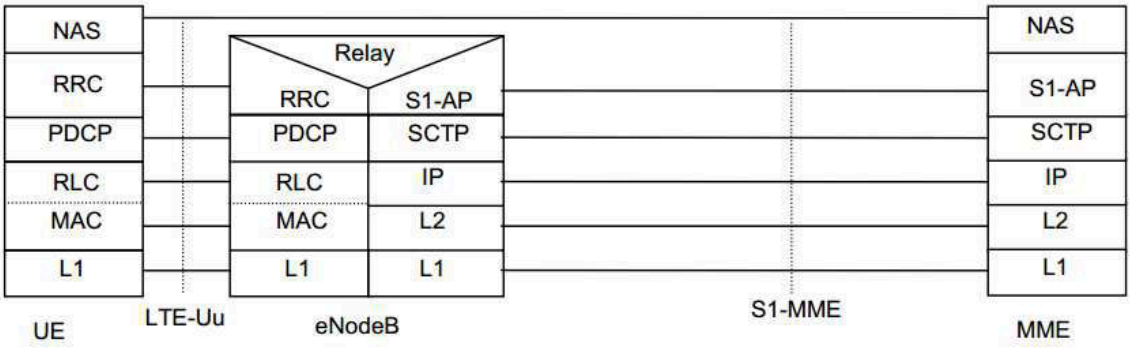


Figure 2.7: LTE Control plane protocol stack, source [1]

User plane

The user plane consists of all the user data traffic generated by UE, typically IP traffic. On the E-UTRAN, user plane IP packets follow the same protocol encapsulation as the control plane, i.e. PDCP/RLC/MAC.

In the EPC, the GPRS Tunneling Protocol (GTP) [23] protocol has been defined by the 3GPP. It allows user IP packets to be transparently transported over an IP network.. It is used in the EPC between the eNodeB and the SGW, i.e. S1-U interface, and between the SGW and PGW, i.e. S5/S6 interface.

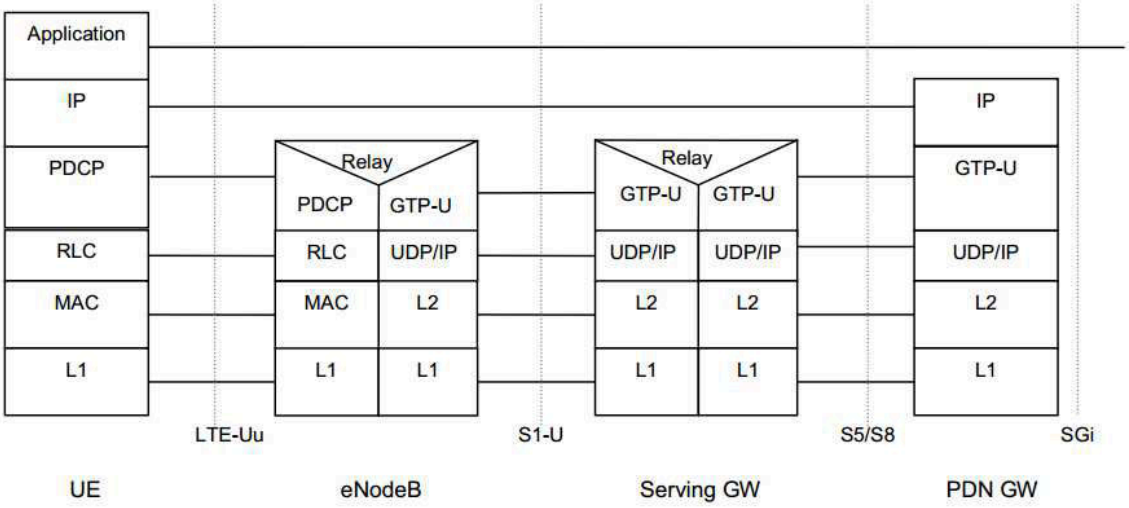


Figure 2.8: LTE User plane protocol stack, source [1]

In the following section, we give some important aspects about the Packet Data Convergence Protocol (PDCP) which is one important element of our work.

The LTE Packet Data Convergence Protocol

The Packet Data Convergence Protocol (PDCP) [2] is used in LTE communications between the UE and the eNodeB for both the data plane and the control plane. Fig.2.9 shows the main function of PDCP. In the user plane, PDCP carries IP packets, while it transports RRC Packet Data Units (PDUs) in case of control plane. The main function of PDCP is to provide security to LTE RAN communications. It

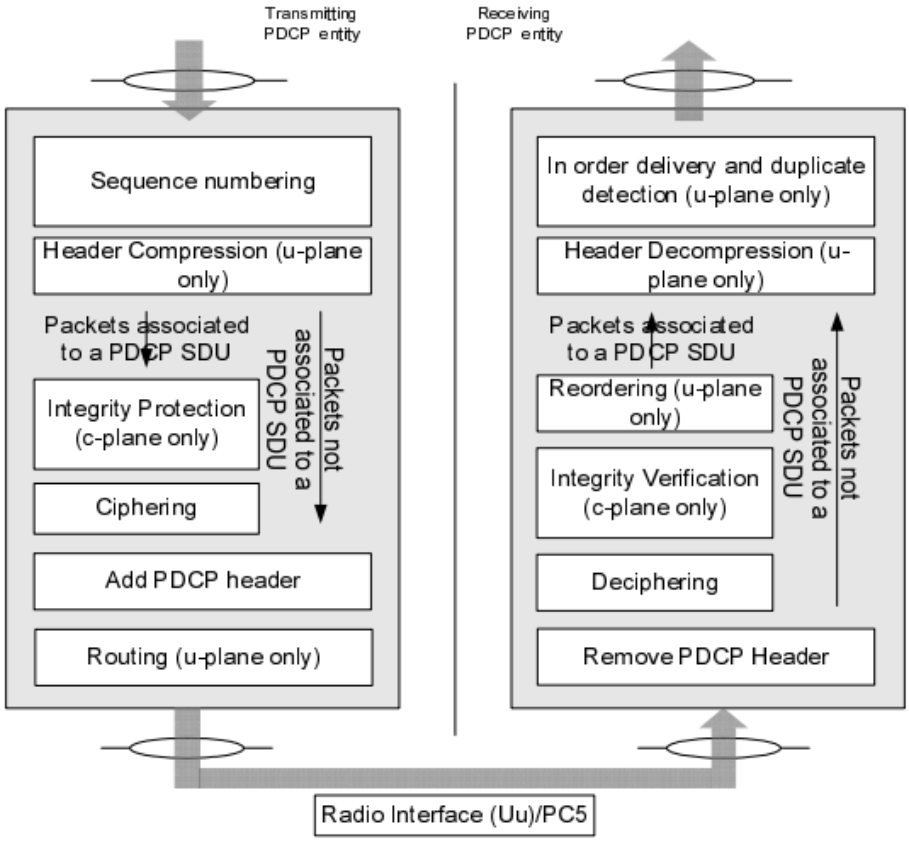


Figure 2.9: PDCP functions, source [2]

is thus responsible for ciphering and integrity checks, in addition to other functions. These functions can be summarized as follows:

- *In-sequence delivery*: PDCP gives a sequence number to each PDU and is responsible for delivering them in the right order to the upper layer.
- *Ciphering*: each upper layer packet is ciphered before transmission, i.e. IP packets in case of user data traffic and RRC for control traffic.
- *Integrity*: integrity checks are only performed for control plane traffic.

- *Header compression*: Header compression and decompression is based on the Robust Header Compression (ROHC)[24].

In release 8 to 11, the in-sequence delivery is used only when re-establishment of lower layers: in the case of handover, the numbering is reset at the Radio Link Control (RLC) layer in the target eNodeB but is kept at the PDCP layer. This allows to guarantee an in-sequence delivery.

In release 12, a reordering function is introduced for bearer split scenario at the PDCP level for small-cells integration. In a bearer split scenario, several RLCs entities are setup corresponding to the different connections the UE is using (i.e. macro BS and small BS), but there is only one PDCP entity. RLC entities are independent and PDUs may arrive in wrong order to the PDCP entity. The reordering function allows these PDUs to be buffered and only delivered to the upper layer if all PDUs before have been received.

2.3.4 BBU/RRH split

The eNodeB can be split into a Remote Radio Head (RRH) [25] and a Baseband Unit (BBU). The RRH is located in the antenna site while the BBU can be several kilometers away. The RRH is responsible for digital/analog conversion (including filtering) and frequency shifting. The rest of the protocol stack operation is performed within the BBU. In the uplink, the received radio signal is transposed to baseband; i.e. sampled, quantified and transmitted in digital over the fiber to the BBU. In the downlink, the baseband signal generated by the BBU is digitized and transmitted to the RRH, which transposes it to the carrier frequency.

With this architecture, it is possible to have several BBUs at the same location and the same cabinet, i.e. a BBU hostel, which are distant from the RRHs. Such an architecture is called centralized-RAN. In this architecture, the delay between the BBU and the RRH should not exceed 0.2ms [26]. This constraint limits the distance between the RRH and the BBU to at most 40km.

2.4 COMBO architectural approach

The objective of COMBO [7] is to propose a unified access and aggregation network to allow the convergence of fixed and cellular networks, i.e. a Fixed/Mobile Converged (FMC) network. This aims at improving the network infrastructure and

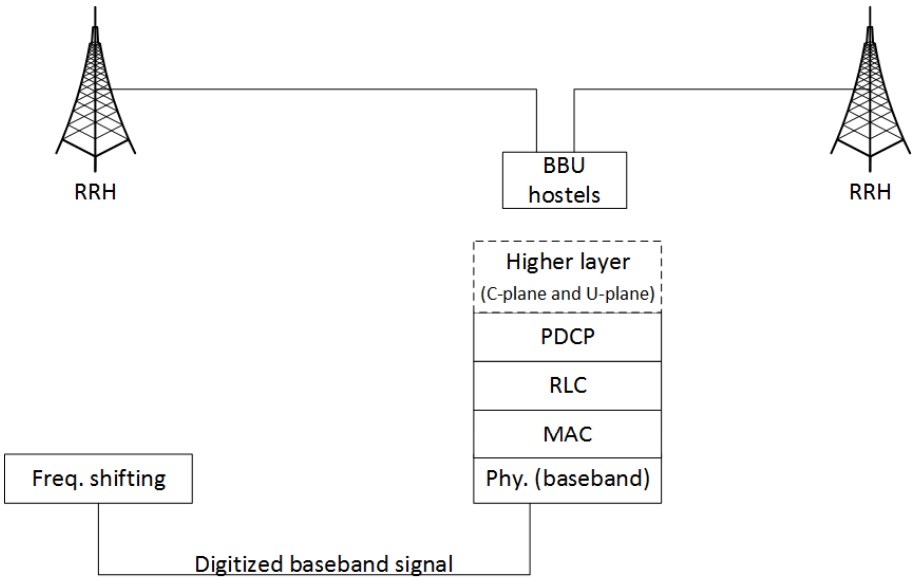


Figure 2.10: BBU/RRH split protocol stack

to enhance the overall performance of the network, by reducing the delay, increasing the end user throughput and providing him with seamless access to broadband networks.

From this perspective, COMBO defines two types of convergence: structural and functional convergence. In functional convergence, the same basic functions (authentication, session establishment,...) are used for both the fixed and cellular networks. Structural convergence focuses on how to efficiently use the infrastructure of fixed and cellular by sharing them as much as possible.

COMBO convergence is organized around the concept of Next Generation Point-of-Presence (NG-POP) and Universal Access Gateway (UAG). The UAG is a functional entity located in the NG-POP that serves as a common IP edge to fixed and cellular access networks. In the following, we give a description of both concepts.

2.4.1 Next-Generation Point-of-Presence

The NG-POP [3] was proposed by COMBO as the evolution of the first aggregation node, i.e. the central office (CO), also called Local PoP. However, unlike the CO, the NG-POP will be higher in the network and will be able to host advanced functions: cellular S-P/GW, BBU hostels and even content distribution network.

The motivation behind NG-POP is to have a better localization of network functions allowing a more optimized utilization of the network, which will reduce infrastructure cost and enhance the overall performance of the network.

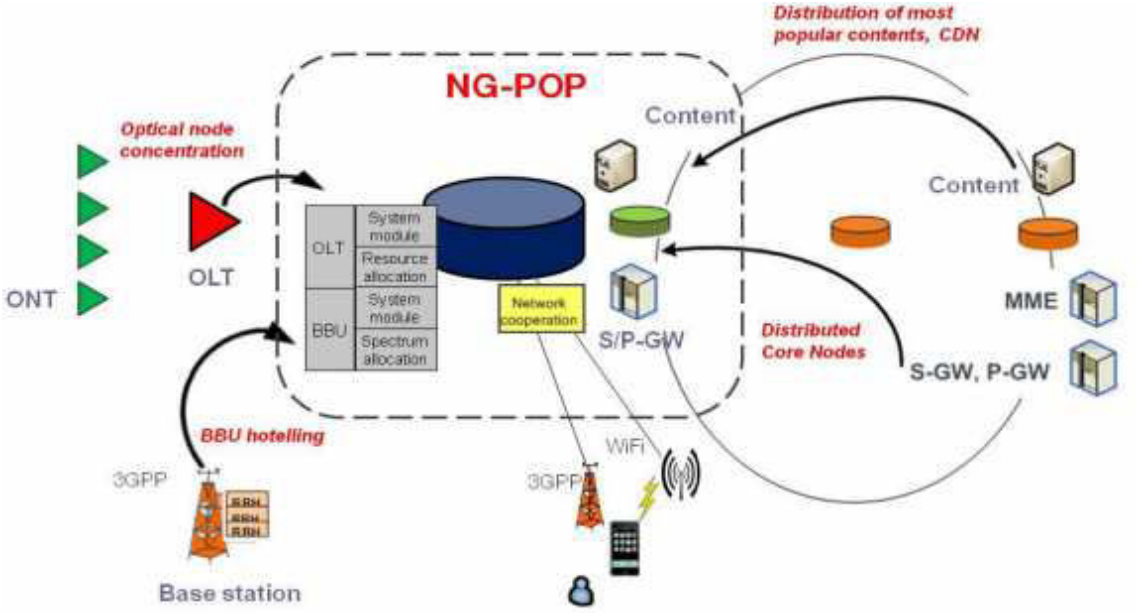


Figure 2.11: NG-POP COMBO concept, source [3]

2.4.2 The Universal Access Gateway

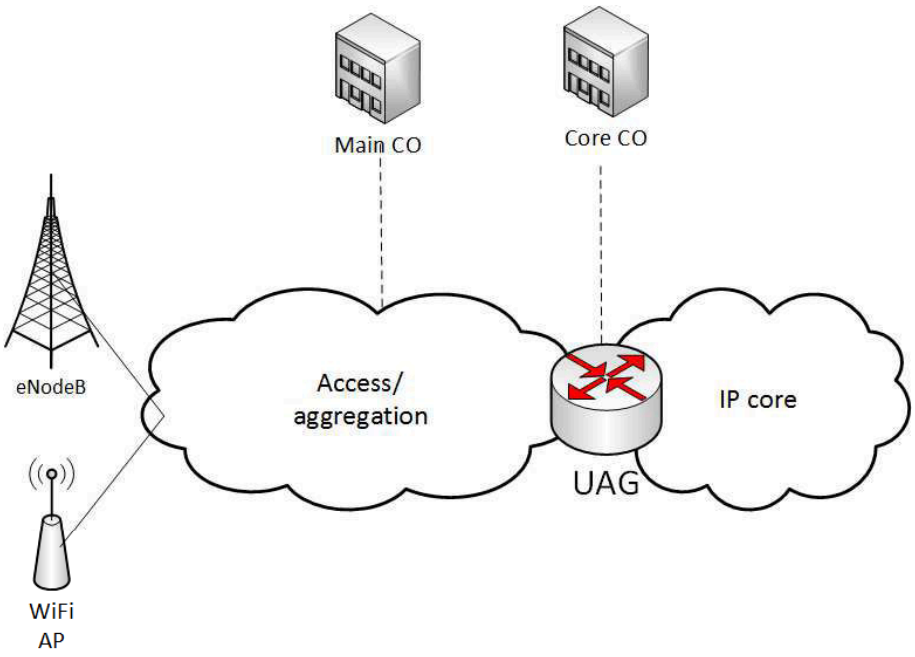
The UAG [27] is a functional entity proposed by COMBO as one of the most important aspects of fixed/cellular convergence, to serve as the common IP edge for all access networks (i.e. fixed, cellular, WiFi). Thus, it should host both cellular SGW and PGW, as well as a BRAS for fixed access. It can also include other functions, such as security, charging and policy management.

COMBO identified two important functions for the convergence that should be included in the UAG: a universal authentication (uAUT) for a unified user authentication and a universal data path management (uDPM).

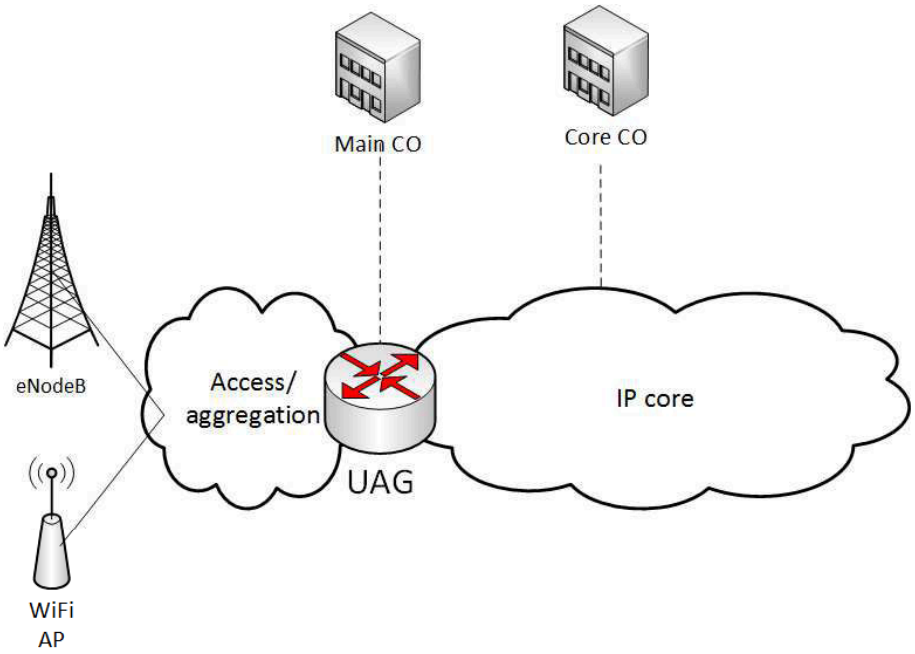
- The uAUT is a functional block within the UAG that serves as a unified subscriber authentication system whatever the type of access network the user is attached to. This allows the user to be authenticated in a transparent way whether it uses LTE or WiFi.

- The uDPM functional block allows the user connections to be mapped on the different available data paths while ensuring session continuity.

The location of the UAG has been largely discussed within COMBO, and it was concluded that it can reside in two locations depending whether the NG-POP is distributed or centralized: in the main CO or in the core CO.



(a) COMBO centralized architecture



(b) COMBO distributed architecture

Figure 2.12: COMBO centralized and distributed options

COMBO distributed architecture

In a distributed architecture (see Fig.2.12b), the UAG is located in the main CO. This induces distributed mobility anchoring and require inter-UAG interfaces. This

also requires the IP network to be extended to the access network, and thus implies reviewing the IP architecture. However, an IP edge located in the main CO reduces latency and thus enables low-latency application without any change of the network architecture. It is also more reliable and requires simple network equipment. Moreover, it gives the possibility to integrate in the same location advanced functions such as caching and BBU hostels.

COMBO centralized architecture

In the centralized architecture (see Fig.2.12a), the UAG is located higher in the network, i.e. in the core CO. In this case, fewer equipment are needed compared to the distributed scenario, which allows an easier operation and deployment and increase the network equipment utilization, thus reducing CapEX and OpEX. Furthermore, this architecture does not require a lot of modification at the IP level, allowing an easier migration compared to the distributed scenario.

The Universal Data Path Management

The uDPM [27] has been proposed by COMBO as a functional block part of the UAG. It allows the operator to manage multiple paths of different technologies per user at the same time, and to map each user session on a given path in an optimized manner. The uDPM is composed of different logical entities as described in Fig.2.13. The *decision engine* block is triggered by a UE *session event*. This event can be either generated by the *monitoring* functional block, e.g. mobility of the UE, or by specific policies saved in the *Subscribers' profiles and network's policies*, for instance the use of WiFi at specific hours. According to these events and following operator specific rules and policies, the *decision engine* takes the decision of mapping one or several sessions to a specific data path. The *data path creation and destruction* functional entity is responsible for creating/destructing data paths when necessary. The *path coordination and control* block manages the different paths when more than one is in use. Typically, it delivers packets to the correct session in case of concurrent path and ensure that session continuity is guaranteed in case of user mobility. The UAG is composed of a Multipath Entity (MPE) that can be located at a different location than the other functions. The MPE includes the *session mapping execution* function that is responsible for applying the policies and the decision taken by the decision engine. Specifically, it forwards the packets on the selected data path in the downlink, and merge the data from the different paths on the uplink.

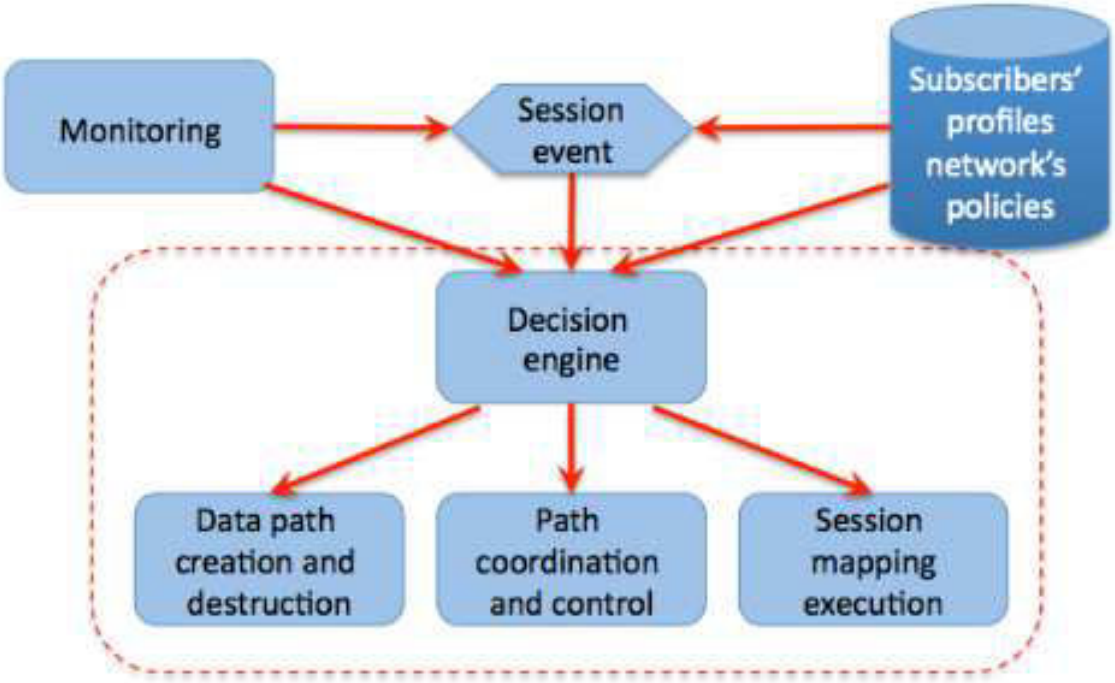


Figure 2.13: uDPM main building blocks, source [4]

2.5 Virtual residential gateways

In COMBO, we aim at having as much functions as possible in the UAG. As seen in the last section, this mainly depends on its location, whether it is in the main CO or the core CO. One proposition of COMBO is to virtualize RGWs. As presented in section 2.2.1, a RGW is composed of different advanced features, which are usually a part of the integrated IP router (e.g. DNS, DHCP). These functions need to be configured by the customer, which has not necessarily the required skills for that. Virtualizing the RGW allows thus to have less complex devices. This reduces configurations for the customer on the one hand, and allows a better resource allocation and management control to the operator on the other hand.

In this section, we present the main architecture of virtualized RGW (vRGW) and evaluate the performance of such architecture.[1]

2.5.1 Description of the architecture

To virtualize an RGW, COMBO proposes to reuse the same idea of BBU/RRH split used in LTE eNodeBs. More specifically, the RGW WiFi AP is divided into

[1]The results were obtained within a master student project

an RRH that stays in the customer premise and a BBU in the operator network, i.e. in the main or the core CO. Note that to be able to transport baseband signals between the BBU and the RRH, a high bit rate is needed, which is only the case of optical links. A special interface is needed between the BBU and the RRH such as the Common Public Radio Interface (CPRI).

To summarize, what remains in the customer premise is only a device with a WiFi RRH, an Ethernet card and a CPRI interface. The rest of the functions are performed in the operator network. For simplicity reasons, we do not represent Virtual WiFi AP as they are a part of the physical AP. The vRGW is described in Fig.2.14.

In the next section, we give a description of how CPRI works.

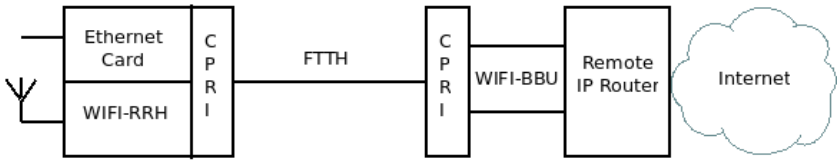


Figure 2.14: Virtual residential gateway (vRGW)

2.5.2 The Common Public Radio Interface

The Common Public Radio Interface (CPRI) [28] is an industry cooperation, which defines the specifications for the interface between the RRH and the BBU. The specification defines only the protocols for layer 1 (physical layer) and layer 2 (data link layer) making it restricted to the link interface.

The transmission in CPRI is organized in frames. A typical CPRI frame (Fig. 2.15) consists of 1 control word (CW) used for control and management, and of 15 data words transporting the IQ user data. A word can be coded in 1 byte, 2,...up to 16 bytes. Each word is always an integer number of bytes but transferred with 8B/10B coding. Consecutive control words produce a channel used for control, management and synchronization. CPRI was initially proposed for the Universal Mobile Telecommunications System (UMTS), and the frame rate is thus equal to the UMTS chip rate: $T_c = 1/3.84$ MHz $\approx$ 260ns. The BBU generates modulation symbols with a sampling frequency f_s. These samples, which consist of M bits per component (I or Q), are then packaged into a so called AxC Container (Axc: antenna carrier). A typical AxC container is composed of a part or several IQ samples depending on the mapping method used. The AxC container size denoted

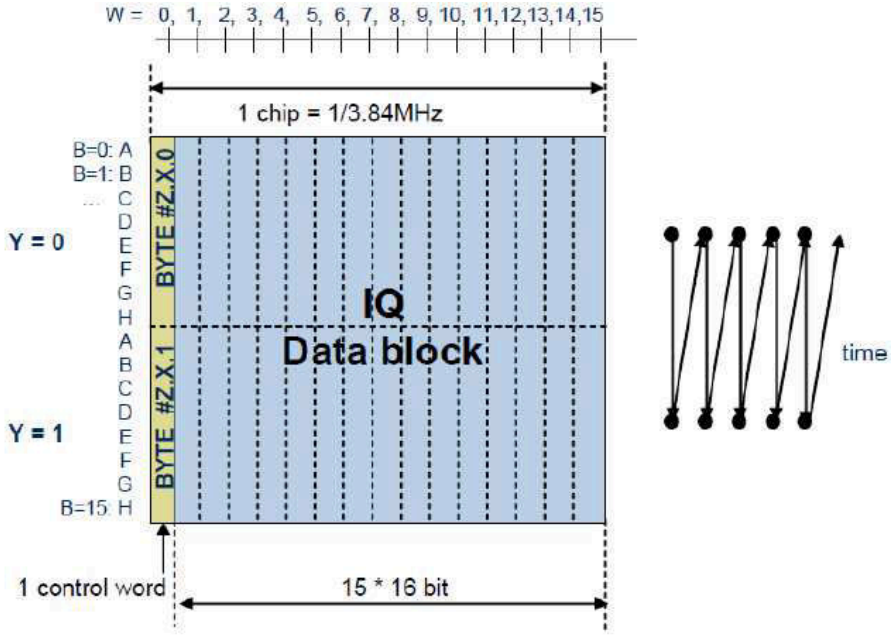


Figure 2.15: One typical CPRI frame composed of two bytes words

by N_{AxC} is required to always be an even number (as many bits on the I and the Q channel). AxC container are then mapped in the IQ data block of the CPRI basic frame according to different possible methods.

IQ mapping method

For systems other than UMTS, the sampling frequency (f_s) is not always equal to the CPRI frame frequency ($f_c = 1/T_c$). The number of bits per frame is thus equal to $2Mf_s/f_c$, which is not always an integer number. To be sure that all AxC containers have the same size, the specification defines the concept of AxC container block which spans over the minimum number of CPRI frames K such that it includes an integer number of samples S (Fig. 2.16). K and S are defined by:

$$K = \frac{\mathrm{LCM}(f_s, f_c)}{f_s} \tag{2.1}$$

$$S = \frac{\mathrm{LCM}(f_s, f_c)}{f_c} \tag{2.2}$$

where LCM stands for Least Common Multiple.

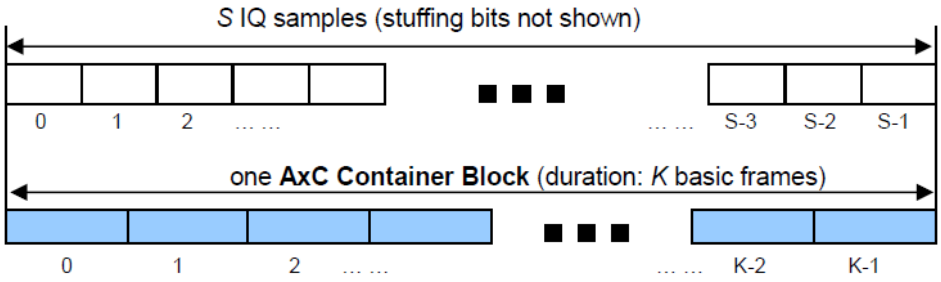


Figure 2.16: Relation between S samples and one AxC container Block

2.5.2.1 Mapping method 1 (IQ sample based)

This mapping method requires that an AxC container contains an even number of bits. N_{AxC} is then given by:

$$N_{AxC} = 2\lceil \frac{Mf_s}{f_c} \rceil. \tag{2.3}$$

Note that it is possible to have several IQ samples or a part of a sample within one AxC container. As the number obtained is rounded up, there is still some unused bits when the AxC container is mapped into the frame. This unused space is filled with stuffing bits that are placed in the beginning of the AxC container block. To know how many stuffing bits are necessary, we use:

$$N_{ST} = KN_{AxC} - 2MS. \tag{2.4}$$

2.5.2.2 Mapping method 2 (Backward compatible)

In this mapping method, an AxC container contains one IQ sample only, its size is thus equal to the sample size: $N_{AxC} = 2M$. However, it is possible to group several antenna carriers (AxC) with the same sampling frequency and the same sample width in a so called AxC Container Group. Let N_A be the number of AxC in one AxC container group. The AxC IQ samples are then multiplexed into a AxC container block consisting of N_C AxC container per basic frame, so $N_A S$ samples. In order to minimize the number of stuffing bits, the number of AxC container per CPRI frame is calculated with:

$$N_C = \lceil \frac{N_A S}{K} \rceil. \tag{2.5}$$

The number of stuffing bits per AxC container block is given by:

$$N_V = N_C K - N_A S. \tag{2.6}$$

In the next section, we show how CPRI can be used in the vRGW and study the different mapping methods.

2.5.3 CPRI interface in virtual residential gateway

As presented in section 2.2.1, a vRGW includes a WiFi and an Ethernet interface. The traffic generated by both of them is transported through the CPRI interface over the fiber toward the operator network. Therefore, we suppose that the CPRI frame is divided into two parts: the first one is allocated to WiFi traffic while the remaining space carries Ethernet frame (Fig. 2.17).

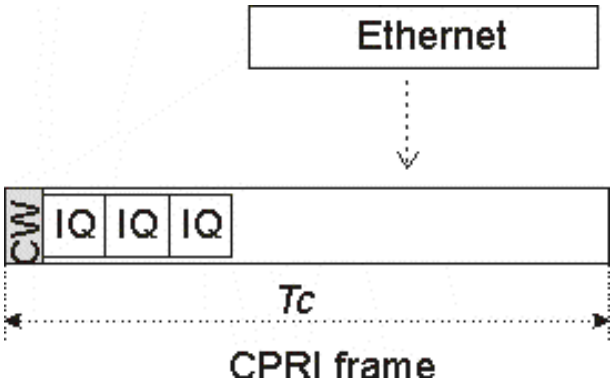


Figure 2.17: Mapping Ethernet frame in the CPRI frame

RGWs Ethernet interface is often a 1Gbps interface, but can be only a 100Mbps interface in some cases. Hence, to be able to transport the Ethernet traffic over CPRI, it is necessary that the remaining capacity is at least equal to the Ethernet interface bit rate.

2.5.4 WiFi over CPRI

As we presented before, CPRI acts as the interface between WiFi-RRH and the BBU. In this section, we show how to transport WiFi over CPRI using methods presented in 2.5.2. Due to its popularity, all our study is about IEEE 802.11g but it can be adapted to other standards.

The 802.11g sampling frequency is 20 MHz [29], which is different from the CPRI frame frequency 3.84 MHz (2.5.2). Therefore, we need to compute the AxC

container block size K and the number of samples S it contains. As $f_s = 20$ MHz and $f_c = 3.84$ MHz, using (2.1) and (2.2) we have: $K = 24$ and $S = 125$.

In order to determine which mapping method is most adapted for WiFi, we calculate the number of RGWs that can be supported by the CPRI link. Indeed, FTTH is based on Passive Optical Networks (PONs). In a PON, several Optical Network Unit (ONUs) (located within the RGW) are sharing the same optical link. Thus, it is important to optimize the link use so it can support as much RGWs as possible.

We also calculate the unused bit rate for each method. As seen before, this unused rate can be used to transport Ethernet traffic.

mapping method 1

We first compute the number of unused bits per CPRI frame, which is equal to the useful bits N (bits allocated to IQ data) per frame minus the number of unused bits:

$$N_b = N - N_{AxC}N_G. \tag{2.7}$$

Thus, the unused bit rate is equal to $3.84N_b$ Mbps.

N_{AxC} is the AxC container size given by (2.3), and N_G is the number of AxC groups. We suppose that an AxC group contains samples from only one AxC, so N_G can be seen as the number of vRGWs. Using the fact that N_b have to be greater than or equal to 0, it is possible to compute the maximum number of vRGWs:

$$N_G \leq \frac{N}{N_{AxC}} \Leftrightarrow N_G = \lfloor \frac{N}{N_{AxC}} \rfloor. \tag{2.8}$$

mapping method 2

Using the same reasoning, we can compute the number of unused bits with:

$$N_b = N - N_{AxC}N_C \tag{2.9}$$

Since an AxC container consists of only one IQ sample, N_{AxC} is equal to the sample size $2M$. N_C is the number of AxC container per CPRI frame and according to (2.5), it is equal to $\lceil \frac{N_A S}{K} \rceil$. As it is possible in this method to have samples from several AxC container, N_A can be seen as the number of vRGWs.

2.5.4.1 Maximum number of supported vRGWs

Tables (2.18) and (2.19) show, for the two mapping methods, the maximum vRGWs that can be supported depending on the line bit rate, and taking into consideration the LAN interface rate. Since the unused bit rate is used to transport Ethernet traffic, it has to be at least equal to the Ethernet interface bit rate.

The first column is the possible word sizes (modes) in the CPRI frame. The second one is the CPRI line bit rate we consider, *IQ bit rate* is the bit rate needed to transport WiFi data and *available bit rate* is the unused bit rate calculated using (2.7) or (2.9). The last column is the bit rate allocated to each vRGW and has to be at least equal to the interface rate (Ethernet min rate). Note that when the unused bit rate is less than 1Gbps, we consider that the Ethernet card is a 100Mbps interface.

CPRI Mode	CPRI Bit Rate (Mbps)	nb AP	IQ bit rate (Mbps)	Available bit rate (Mbps)	Eth min rate (Mbps)	Eth rate / AP (Mbps)
1	614,4	1	322,56	138,24	100	138,24
2	1228,8	2	645,12	276,48	100	138,24
4	2457,6	1	322,56	1520,64	1000	1520,64
5	3072	1	322,56	1981,44	1000	1981,44
8	4915,2	2	645,12	3041,28	1000	1520,64
10	6144	3	967,68	3640,32	1000	1213,44
16	9830,4	5	1612,8	5760	1000	1152

Figure 2.18: Number of possible RGWs for different line bit rate (Mapping method 1)

CPRI Mode	CPRI bit Rate(Mbps)	nb AP	IQ bit rate (Mbps)	Available bit rate (Mbps)	Eth min rate (Mbps)	Eth rate / AP (Mbps)
1	614,4	1	368,64	92,16	100	92,16
2	1228,8	2	675,84	245,76	100	122,88
4	2457,6	1	368,64	1474,56	1000	1474,56
5	3072	1	368,64	1935,36	1000	1935,36
8	4915,2	2	675,84	3010,56	1000	1505,28
10	6144	3	983,04	3624,96	1000	1208,32
16	9830,4	5	1658,88	5713,92	1000	1142,784

Figure 2.19: Number of possible RGWs for different line bit rate (Mapping method 2)

As we can see in Fig. 2.18, it is only possible to have a 100 Mbps interface for mode 1 and 2. However, if we look at Fig. 2.19 we can see that for mode 1, the available bit rate is less than the minimum bit rate required. Thus, it is not possible to have even a 100 Mbps interface for mode 1 when using mapping method 2. For

the two methods, the maximum number of vRGWs is the same whatever the CPRI bit rate. We can see however that method 2 gives a better IQ bit rate than method 1 but in the other side method 1 provides a higher rate for Ethernet interface.

However, we can notice that it is necessary for both methods to have a line bit rate almost equal to 1Gbps to support at most 5 vRGWs.

2.5.4.2 Impact of the propagation delay

IEEE 802.11 MAC layer uses a random access to the medium based on the carrier sense (CSMA/CA) mechanism [29]. This means that a mobile terminal wishing to send data first needs to listen to the medium during a period called Distributed Interframe Space (DIFS), and can begin the transmission only if the carrier is free. However, if the propagation delay between two stations becomes too large they will not be able to sense the transmission of each other. More precisely , if station A is transmitting and the propagation delay to station B is larger than DIFS, B can believe that the medium is free and starts sending, which causes a collision. In other words, the collision probability is proportional to the propagation delay and so to the distance [30].

In our case, the fact that the BBU is moved to the operator network increases considerably the propagation delay between the BBU and mobile terminals (Fig. 2.20). Indeed, the transmission speed depends mainly on the medium. In 802.11, the radio signal speed is approximately equal to 3.0×10^8 m/s, while it is equal in the fiber to 2.0 x 10^8 m/s (supposing that the delay added by intermediary devices is insignificant). The delay in the fiber is then reduced to $\frac{2}{3}$ of the radio propagation delay. To evaluate the performances of Wi-Fi in a such architecture, we use the

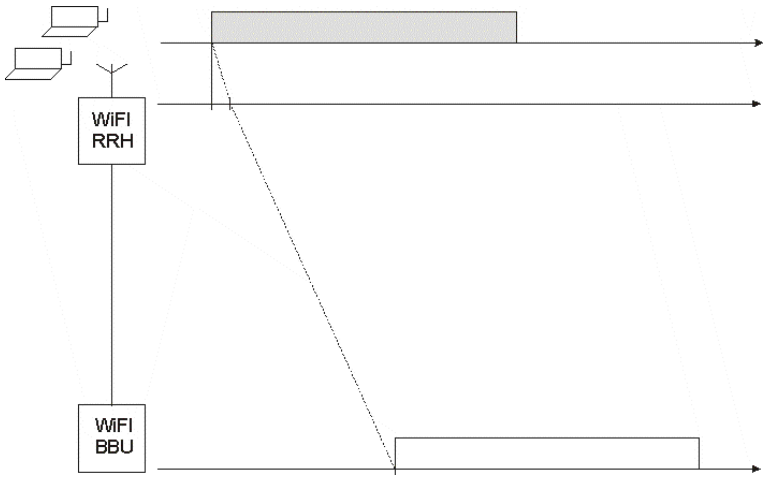


Figure 2.20: Propagation delay in a virtual gateway Architecture

analytic approach developed by Bianchi [31]. Several assumptions have to be made in order to use the model.

We first suppose that there is a limited number of stations N and that the propagation delay between each pair of them is the same. The other key assumption is that each station operates in "saturation" conditions, which means that there are always a frame to be sent. This is a very strong assumption making the obtained performances undervalued. The different parameters we used for simulations are given in Table 2.1 where CW_{min} and CW_{max} are the minimum and maximum contention windows given by:

$$CW_{min} = W \tag{2.10}$$

$$CW_{max} = 2^m W \tag{2.11}$$

where W is equal to one time slot and m is the maximum back-off stage. In order

Table 2.1: Parameters for simulations

Parameters	IEEE 802.11g
Transmission bit rate (Mbps)	54
MAC header (bytes)	34
ACK (bytes)	14
PHY Preamble + Header (bytes)	16+4
Slot time (Âţs)	9
SIFS (Âţs)	10
DIFS (Âţs)	28
CW_{min}	16
CW_{max}	1024

to evaluate the performance, we look at the achieved throughput by a station in different situations. We vary the 3 main factors that can affect the throughput in a WiFi network: the number of stations, the distance between them and the payload.

In the first case, we fixed the propagation delay to 9μs (1.8 km through the fiber) and we varied the payload. We did this for different numbers of stations. In the other test, we fixed the payload to 1500 bytes and varied the propagation delay. Fig. 2.21 represents the results of the first test. It shows the achieved normalized throughput versus the payload when 2, 3 or 20 stations are sharing the medium. As it is expected, the throughput increases with the payload as more useful data are

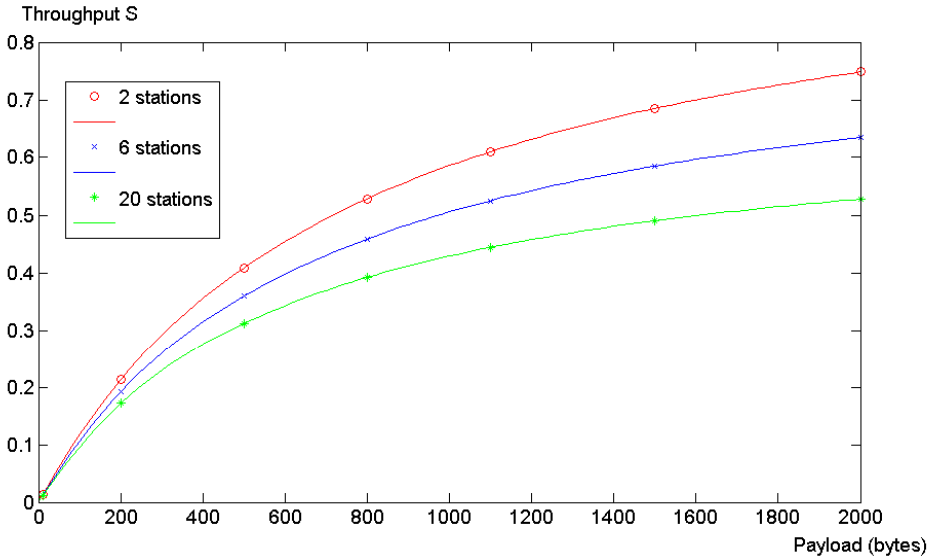


Figure 2.21: Achieved normalized throughput vs. payload

transported within one frame. However, the more the number of stations is the less the throughput is. This is due to the number of collisions which increases with the number of stations.

In Fig. 2.22, we can see the achieved normalized throughput as a function of the distance. Note that the propagation delay can be obtained given that the transmission speed over the fiber is equal to 2.0×10^8m/s. As we can see the throughput decreases as the distance grows which is due to the increase of the number of collisions. Like the first case, the throughput decreases also when the number of stations grows.

2.5.5 Discussion

In the context of COMBO, the RGW would be virtualized either in the main CO or in the Core CO (i.e. COs are currently being completely removed by operators). Virtualization in the core CO can not be considered as the distance is too high, i.e. more than 20km for dense urban and more than 100km for rural areas. So this scenario is definitely not possible as it would induce a very high degradation of the throughput.

Now let us consider the vRGW in the main CO, which is at most at 15km in rural areas. Even if the number of connected stations is limited, i.e. we take the example of 2 stations, the capacity loss is still too high. Indeed, each user can at most obtain 40% of the transmission bit rate, i.e. $0.4 \times 54 = 21.6$Mbps.

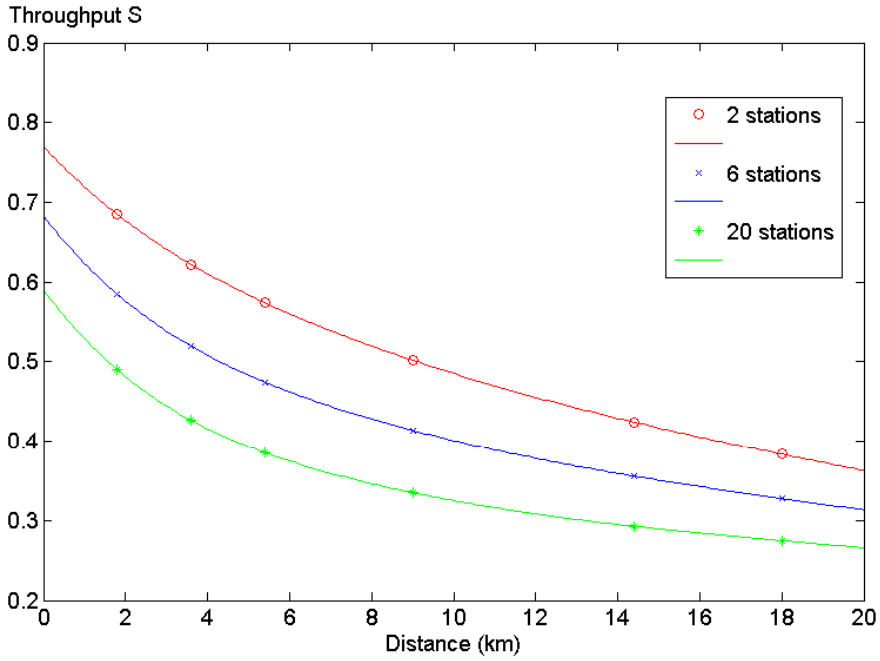


Figure 2.22: Achieved normalized throughput vs. propagation delay (distance)

In dense urban areas, the main CO is not as much far to the customer premise, i.e. at most 5km away. However, the load is much higher in dense areas compared to a rural areas. Thus, users can not achieve more than what they could in a rural area. For instance, if we consider 20 stations, the achieved saturation throughput is limited to 40% of the available transmission bit rate.

Our conclusion from this study is that virtualizing WiFi APs highly impacts the performance as the capacity loss is too high, whatever the type of area (i.e. rural or dense urban). We thus conclude that the WiFi AP should remain in the RGW within the customer premise, and this is what we consider in the rest of the study.

2.6 Conclusion

In this chapter, we gave the main elements needed for the rest of this thesis. We presented the current architecture of both cellular and fixed networks, and described the different elements that need to be remembered. We also briefly presented the convergence proposed by the COMBO project. We also discussed a study that we proposed that consists of virtualizing the WiFi APs higher in the network. We analyzed the performance of the architecture and showed why this is not a good idea.

As seen in this chapter, cellular and fixed access networks have up to now evolved separately. However, the increasing mobile data traffic has led operators to review this philosophy, changing toward the convergence between both networks. This opens the opportunity for new architecture and protocols, that see the network in a different way.

Chapter 3

State of the Art on Multihoming and mobility solutions

3.1 Introduction

Today most terminals have multiple interfaces (WiFi, cellular, sometimes Ethernet). As all applications are IP based, they can transparently use any interface. However, in most cases, mobility is not supported, i.e. a session is generally broken when the terminal switches from a technology to another. This is due to the fact that the transport protocol (typically TCP) binds the different sessions to the IP addresses, which need to remain the same during the whole connection. Furthermore and for the same reason, it is not always possible to use several interfaces at the same time. In the following, we call this feature multi-homing or bonding.

The research community has addressed these issues with different approaches and proposed several protocols at different layers of the OSI protocol stack. An extensive state of the art on the different solutions proposed was published in 2014 [32]. In this work, we update this state of the art and use a similar approach to classify the different architectures and protocols. In addition to [32], we provide an extended qualitative analysis with additional criteria.

In this chapter, we describe the most relevant solutions classified depending on the feature they provide and their location in the TCP/IP protocol stack. We follow a bottom-top approach, i.e. we first present layer 2 solutions and finish with application layer solutions. This allows to go from the most network-dependent solutions to the most application-dependent ones. For each solution, only the considered layer needs modifications. Moreover, the feature provided is transparent to all above lay-

ers. For instance, a layer 3 mobility solution means that any change in layer 2 is transparent to layers higher than layer 4, and thus to the application.

3.2 Definitions

In the rest of this chapter, we use the terms *mobility*, *multi-homming* and *bonding*. Although these terms are quite used in the literature, there signification is not always the same. Thus, we give in this section the definitions that we used in our work.

Mobility

When the terminal moves from one access network to another, its old IP address is replaced with a new one assigned by the new network. Most today applications are based on TCP which uses the pair of destination/local IP addresses to identify the sessions. If the terminal IP address changes, all ongoing sessions are terminated.

In this work, we use the term *mobility* as the ability for a device to move from one access network to another without causing current sessions to be broken and made again.

Multihoming

We define *multi-homing* as the ability to be connected to several access networks at the same time. In our study, we do the distinction between site-multihoming and host multi-homing. In site multi-homing, the different network portions are called sites, for instance the edge network and the core network are two sites. A user can be reached through different sites, for e.g. different core networks. In host multi-homing, the user terminal itself can simultaneously use several interfaces or have several addresses without impacting upper layers.

Bonding or Bundling

Bonding or *Bundling* consists of grouping several physical channels into one logical channel in a complete transparent way to all above layers. Thus, the network layer sees only one network interface. Fig. 3.2 shows the difference between bonding and multi-homing. Bonding is also called trunking or link aggregation in some cases.

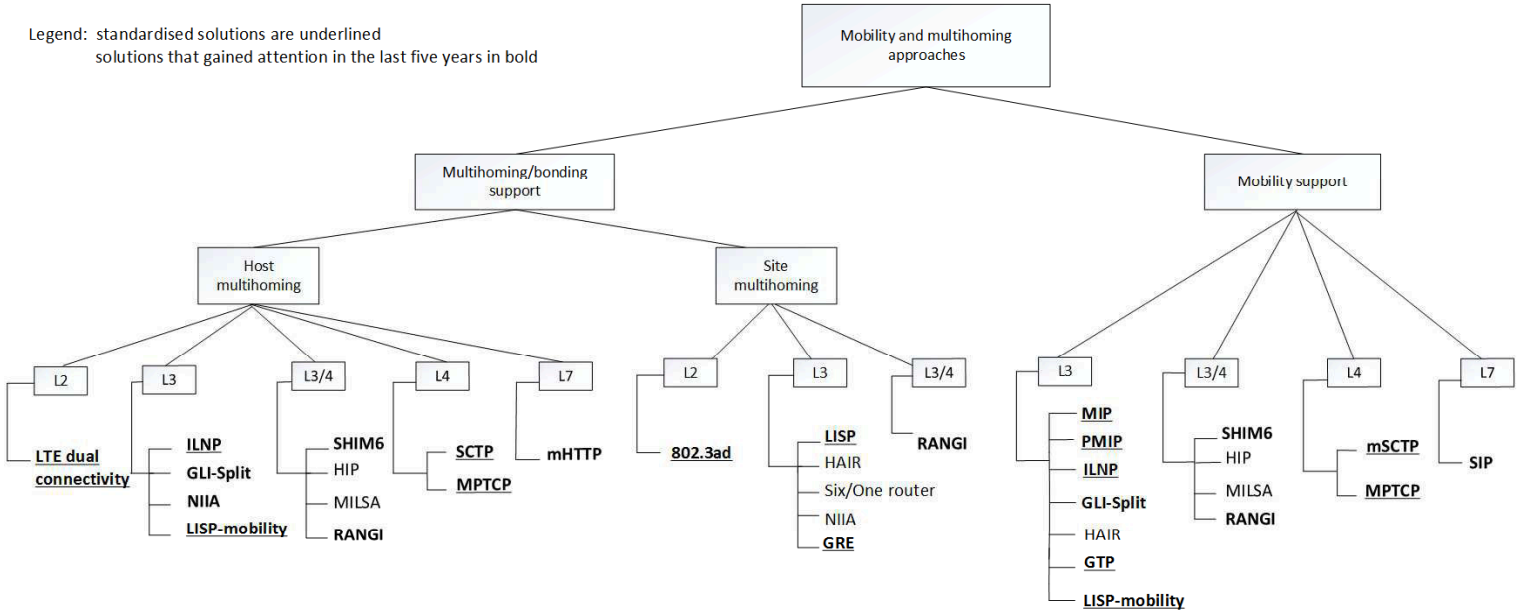


Figure 3.1: Solutions classification

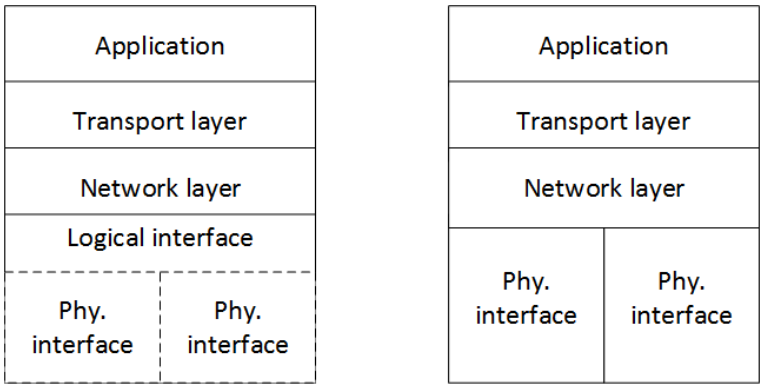


Figure 3.2: Bonding vs Multi-homing

3.3 Bonding and Multi-homing solutions

In this section, we present the most relevant solutions that provide bonding and/or multi-homing.

Layer 2

At layer 2, only bonding is provided. Ethernet 802.3ad bonding proposed by the IEEE [33][34] allows to group several physical links into one logical link in order to increase the capacity. In [33], a definition of 802.3ad link aggregation is given: "Link Aggregation allows one or more links to be aggregated together to form a Link Aggregation Group, such that a MAC client can treat the Link Aggregation Group as if it were a single link".

On the other hand, the ITU-T proposed the Ethernet-based multi-pair bonding [35] to allow bonding of xDSL lines into a single one. The ITU-T also proposed the ATM-based multi-pair bonding [36] that has the same purpose but with ATM transportation instead of Ethernet. It is worth mentioning that in layer 2 bonding, links normally have very similar characteristics which results in that normally scheduling is not an issue.

On the 3GPP side, the LTE dual-connectivity was standardized [37]. It allows the UE to use simultaneously the radio resources proposed by at least two eNodeBs. This typically applies to the case of small-cells. This architecture is called Heterogeneous Networks or HetNets [38] [39]. In a HetNet, new base stations transmitting at low power and with limited coverage are deployed. These base stations are called small-eNodeBs (SeNodeB). The idea is to have legacy eNodeBs, i.e. macro-eNodeBs

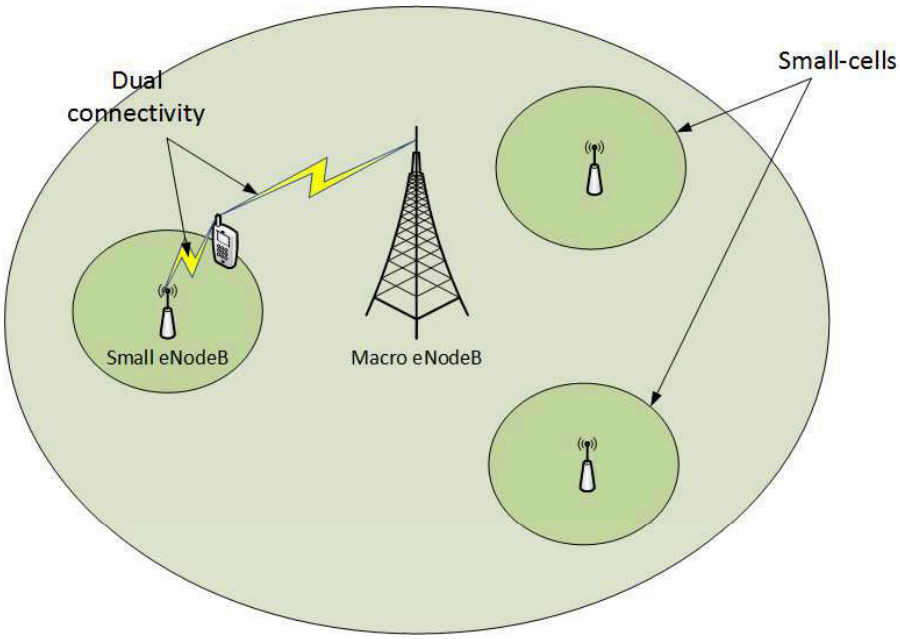


Figure 3.3: Dual connectivity between macro and small eNodeBs in LTE

(MeNodeBs), ensuring a continuous coverage to the user, while SeNodeBs are used to enhance the network capacity (see Fig.3.3). This is particularly interesting to provide connectivity to indoor users that are not well covered by the MeNodeB.

HetNets raise several challenges for the operators, which limit their efficiency as an offload solution. Spectrum allocation between small and macro cells, and SeNodeBs placement are among the issues identified by the community. In most proposed architectures, small-cells operate on the same spectrum as the macro-cell. This requires powerful coordination between the MeNodeB and the SeNodeB in order to reduce the impact of interface [40]. Moreover, the SeNodeB are transmitting at low power, which limits the capacity.

Layer 3

Today, the most used and known layer 3 protocol is IP. The IP protocol is known to mix two different concepts in the address fields: the identifier and the locator. An identifier should be used to uniquely refer to a given host and thus be used by layer 4 to identify a session and a locator should be used for routing purpose. Such confusion between the location and identification causes problems for mobility management and for multi-homing as different addresses are used though there should be only one identifier. Separating identifiers and locators is then a natural way to allow different paths for the same terminal (i.e. different locators and one

identifier). Several studies took interest in the locator/identifier split idea [41]. In the following, we give a description of the most relevant ones.

"Locator and Identifier Separation Protocol" (LISP) [42] considers different sites, e.g. the edge and the core network are two different sites. In the edge network, Endpoint Identifiers are used to address the users. Inside the core network, Routing Locators are used for routing. The different sites are connected through Tunnel Routers. Packets are tunneled between the Tunnel Routers using Routing Locators. LISP allows a TR to be connected to multiple core networks through different Routing Locators and thus to have site-multihoming. However, since Endpoint Identifiers are also used as locators inside the edge network, it is not possible to have host-multihoming. The extension LISP Mobile Node (LISP-MN) [43] was proposed to overcome this issue. A sub-layer is added between layer 2 and layer 3, and all features of Tunnel Routers are implemented in the host protocol stack. Hence, in addition to the Endpoint Identifier, the host also gets a Routing Locator used for routing.

Six/one router [44] uses two different address prefixes in the edge and core network, and uses special routers to tunnel user traffic in the core. The "Hierarchical Architecture for Internet Routing" (HAIR) [45] considers the network as three portions connected using attachment points. A user has an identifier (ID) and a locator. The locator is the combination of the different attachment points addresses the user is attached to. Then, combination of the ID and the locator are used as source and destination addresses in the IP header. Routing is based on the ID part of the address in the edge network while it is based in the attachment points addresses in the other network portions. In "Node Identity Interworking Architecture" (NIIA) [46], the network is divided into different routing domains, i.e. edge and core network and Node Routers are used for interconnection. An additional header is used, namely the Node ID header, which includes the final destination host Node ID and the last router Node ID. Standard IPv4 is used to route packets to the first Node Router. Then, according to the destination Node ID in the Node ID header, the address in the IPv4 header is replaced with the correct one in order to be routed correctly in the core network.

In the "Identifier-Locator Network Protocol" (ILNP) [47], a host may have several locators bound to a unique identifier. The current Domain Name Service (DNS) needs to be enhanced to support the translation between a Fully Qualified Domain Name (FQDN) and an ILNP identifier. Current applications that do not use a FQDN but an IP address instead may not use ILNP.

"Global-Locator, Local locator, and Identifier split" (GLISplit) [48] defines a new IPv6 address structure, namely a GLI-address. This structure consists of two parts: an Identifier on the first part and either a Local Locator or a Global Locator. The Identifier is used to identify a host, the Local Locator is used for routing inside the edge network and the Global Locator is assigned to the router connecting the edge to the core and is used for routing inside the core network. "Routing Architecture for next Generation Internet" (RANGI) [49][50] is also an identifier/locator split solution that allows both site and host multi-homing.

SHIM6 [51][52][53] introduces a shim layer between layer 3 and 4 to ensure identifier/locator split. The transport layer sees only the identifier, i.e. upper-layer identifier (ULID), while locators are used by the transport layer. SHIM6 is responsible for translating the locator to the corresponding identifier and vice-versa. Identifiers and locators are standard IPv6 addresses, which avoids defining a new namespace and allows to stay compatible with current network architecture and applications.

Fig.3.4 shows an example of how SHIM6 works. In this example, the host communicates with a distant server through the Internet. It is connected to different access networks (e.g. WiFi and cellular) using different interfaces and thus obtains two IP addresses, one for each interface. One IP address from the two available is chosen (i.e. IP1) as the ULID. The transport protocol uses the ULID pair (host and destination) to identify the session. For out-going packets, SHIM6 replaces IP1 with one of the available locators, i.e. IP2 or keep IP1 depending on the chosen outer interface. If the locator is different from the ULID, a sub-header is added to the IPv6 header to indicate this to the destination. For in-coming packets, SHIM6 replaces the source locators (IP1 or IP2) with the correct ULID (IP1).

Host Identity Protocol (HIP) [54] and "Mobility and Multihoming Supporting Identifier Locator Split Architecture" (MILSA) [55] [56] have the same principle as SHIM6 by introducing a sub-layer between layer 3 and layer 4 to ensure identifier/locator split. However, instead of reusing IP addresses, HIP uses cryptographic public keys as identifiers while MILSA uses a Uniform Resource Identifier (URI) and hosts are identified with an identifier name assigned hierarchically.

Generic Routing Encapsulation (GRE) [57] is a tunnelling protocol. Its extension "GRE notification" [58] allows to manage several GRE tunnels over multiple physical lines to one home network. For instance , it is possible to have the Customer Premise Equipment (CPE) being connected to different physical lines (e.g. fixed and cellular). The CPE gets different addresses but a Hybrid Access Aggregation Point (HAAP) shows only one to the external world (i.e. the internet). However,

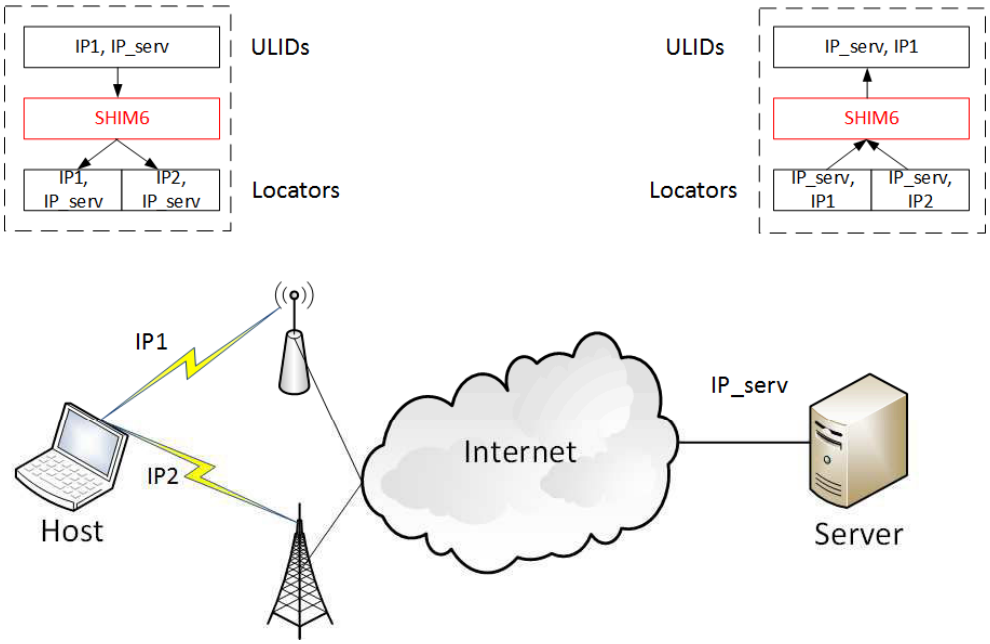


Figure 3.4: SHIM6 operation

the terminal can not be connected to the CPE using different interfaces. It is thus considered as a site multi-homing solution.

Layer 4

In respect to layer 4 solutions, the most notable solutions are the Stream Control Transmission Protocol (SCTP) [59] and the Multi-path Transport Control Protocol (MPTCP) [60] (see Fig.3.5).

SCTP was proposed as a substitute to TCP to allow the use of different access networks. It allows a user to announce several IP addresses when establishing a new connection and to use them simultaneously. However, its adoption is very limited as it was proposed to replace TCP, which would force developers to adapt existing application for using SCTP socket.

In opposite to SCTP, MPTCP comes as an extension to TCP and does not intend to replace it. It allows the user to have several IP addresses in a transparent way to the application. To do this, MPTCP opens regular TCP connections, called subflows, on each path. Only one subflow, i.e. the master subflow, is visible to the application and accessible using standard TCP sockets. From the application point of view, the host has only one IP address whatever the number of subflows established by MPTCP.

In MPTCP, both corresponding hosts need to be MPTCP-aware. MPTCP makes

sure that the distant host supports MPTCP before establishing more than one subflows. If this is not the case, a standard TCP connection is used. To avoid defining new message structures, MPTCP uses options fields in the TCP header to announce MPTCP ability. However, this can cause MPTCP traffic to be blocked by middleboxes [61], which are most of the time configured to drop any TCP traffic with unknown options.

Moreover, MPTCP is known to be not very suited in case of high delay diversity on the different paths due to the head-of-line blocking [62]. This typically occurs when a delayed segment in one slow flow blocks all already received ones on fast flows in the buffer.

Multi-path Multimedia Transport Protocol (MPMTP) [63] was recently proposed to transport multimedia content over multiple paths. All other multipath transport protocols are based on TCP (e.g. MPTCP), which is known to not be appropriate for multimedia traffic because of the delays incurred by re-transmission of lost packets. MPMTP has the same principle of MPTCP but uses UDP for useful data while the control of the connection is based on TCP.

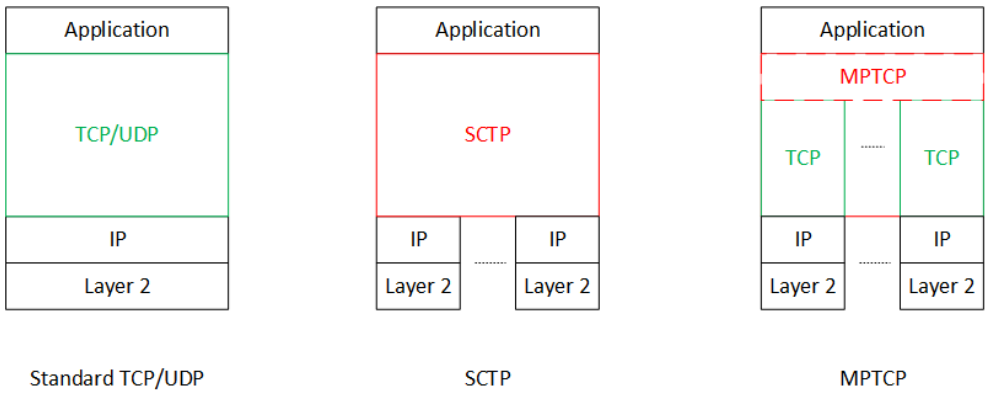


Figure 3.5: Transport layer solutions

Application Layer

The first proposal to do multihomming at the application layer is the Multi-source Multi-path Hypertext Transfer Protocol (mHTTP) [64]. The idea is to use an HTTP feature named HTTP range request in order to fetch for different blocks of content from different servers. The objective is to be able to receive data through individual TCP connections. However, mHTTP is still only a proposal and did not receive much attention from the research community since the first publication in 2014.

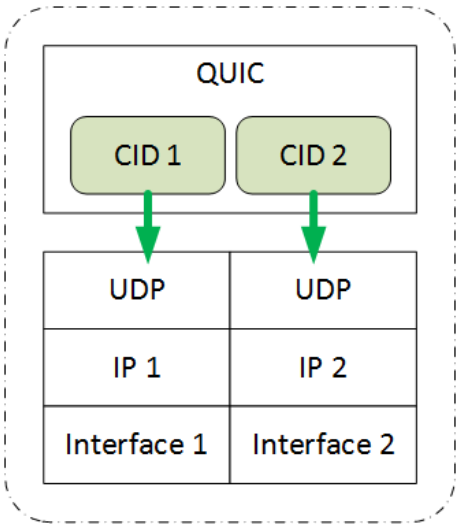


Figure 3.6: Multipath with QUIC

In 2012, Google proposed SPDY [65] as a substitute to HTTP in order to reduce time retrieval of web pages. However, SPDY is built on top of TCP and thus inherits of all its negative points due to congestion control. To overcome this, Google introduced "Quick UDP Internet Connections" (QUIC) [66] [67]. In opposite to SPDY and HTTP, which use TCP as a transport protocol, QUIC uses UDP (see Fig.3.6). This avoids all issues induced by TCP in case of losses and delayed segments. In addition to that, QUIC provides native support for multihomming. Indeed, QUIC identifies a session using a special identifier called Connection IDentifier (CID) independently from the IP addresses. Thus, the terminal can use all the available networks it is connected to for only one CID at the application layer. However, it is worth noting that the multi-path is not yet implemented in the current version of the Chrome Browser.

3.4 Mobility Solution

Among the solutions presented in Section II-A for multihomming, many of them also provide mobility. In GLI-Split, RANGI, ILNP, HIP, MILSA and SHIM6, the identifier is kept unchanged even if the locators change so the mobility is transparent to the transport layer. By including the features of a Tunnel Router in the hosts, LISP-MN can also be considered as a mobility solution.

With the SCTP Dynamic Address Reconfiguration (DAR) extension [68], it is now possible for mobile SCTP (mSCTP) [69] to dynamically add and remove new addresses during an ongoing session. Hence, when a user moves to another access

and obtains a new address, it just announces it to the destination host and can remove the old addresses.

In MPTCP, the application sees only one TCP connection even if there is actually several ones corresponding to different IP addresses. Thus, new TCP connections can be established or removed without the application knowledge, which can be used in a mobility scenario.

Note that in mSCTP and MPTCP the new connection has to be made before breaking the old one.

QUIC allows a user to move from one access network to another as it is built over UDP which is not based on the connection principle. Moreover, QUIC uses the CID to identify a session which is kept the unchanged even it the terminal IP address is changing when moving between access networks.

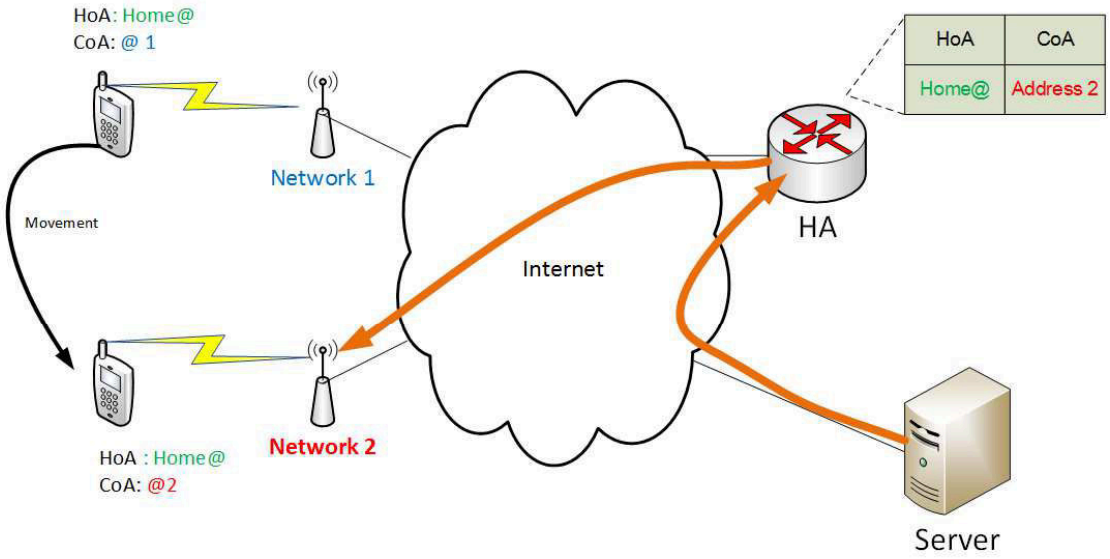


Figure 3.7: Mobile IP architecture

Mobile IP (MIP) [70] [71] is a layer 3 solution that proposes to a user to keep its IP address even if it moves from one access network to another (see Fig.3.7). In MIP, the Home Agent (HA) entity is introduced. It is located in the user home network and is responsible for keeping the binding between its permanent IP address, i.e. the Home Agent Address (HoA), and any address obtained in a foreign network, i.e. a Care of Address (CoA). This HA is thus considered as an anchor point and all the traffic to and from the user has to go through it. When a user visits a foreign network and gets a new IP address, i.e. a CoA, a bidirectionnal tunnel is established from the HA to the visited network. It is worth noting that the user itself needs

to change the binding between its HoA and the new CoA, using defined signaling message. Other extensions were proposed such as MIPv6 [72] to support IPv6 or Dual stack MIP (DMIP) [73] to support both IPv4 and IPv6.

In MIP, the host protocol stack needs to be modified to include mobility signaling procedures. In order to cope with this issue, Proxy MIP (PMIP) [74] was introduced where all signaling procedures are pushed into the network. The two main entities in PMIP are the Local Mobility Anchor (LMA) and the Mobility Access Gateway (MAG). The LMA acts as the MIP-HA while the MAG is responsible for tracking user movements and to inform the LMA of its new position (see Fig.3.8). A network area controlled by an LMA is called a PMIP-domain. In opposite to MIP, the user obtains a unique IP address, i.e. HoA, that can be used whithin the entire PMIP-domain. Thus, from the user point of view, an area covered by an LMA, i.e. a PMIP domain, is considered as one unique link.

The 3GPP proposed an architecture based on DSMIPv6 to allow mobility between cellular and other access networks, e.g. WiFi. This architecture actually proposes a *Tight Coupling* between WiFi and cellular access network such as LTE, in which WiFi APs are directly connected to the EPC network. The user address assigned by the 3GPP access network is the HoA while the address obtained on the WiFi network is considered as the CoA. The PGW keeps the binding between the HoA and the CoA and is thus considered as the HA. The IP flow mobility (IFOM) proposed by the 3GPP [75][76] is based on MIP and allows the operator to offload specific flows over other access networks.

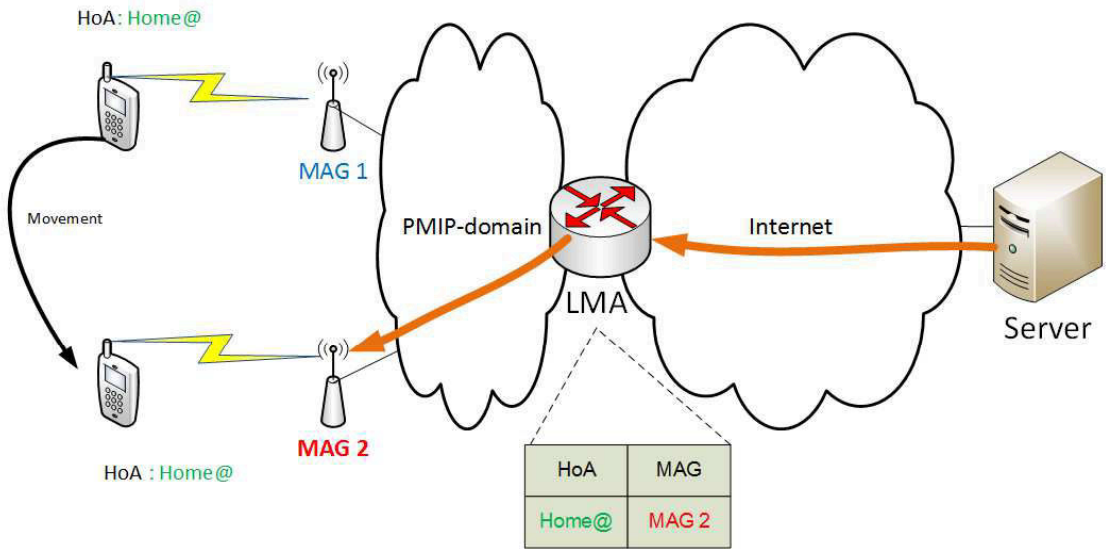


Figure 3.8: Proxy Mobile IP architecture

The General Packet Radio Service Tunnelling Protocol (GTP) [23] is the tunnelling protocol used by the 3GPP in the Evolved Core Network (EPC). With GTP, the user mobile IP address is not used for location purpose inside the EPC. Thus, the user keeps its IP address when it moves from one eNodeB to another.

The Session Initiation Protocol (SIP) [77] is used for signaling and controlling multimedia sessions. A SIP session is bound to a couple of Uniform Resource Identifiers (URIs) instead of IP addresses. The URIs doe not change during a session even if there is a change in the IP address. Hence, session are not broken when a user move to another access network.

3.5 Qualitative Analysis

In Table I, we analyze the solutions described before according to different criteria that we consider important for a deployment.

The first parameter considers the modification of the host protocol stack. Some solutions introduce new protocols or sub-layers. This requires the host protocol stack to be modified and thus modification of the entire terminal operating system in some cases.

One other argument is the introduction of additional agents in the network and modify the network architecture. This can be an excluding argument as it would drive major investments for the operator.

The transparency to current applications and to network elements are also important parameters to take into consideration. Indeed, the deployment can be difficult if the solution requires current applications to be modified or if it introduces new messages that can cause to the user traffic to be blocked by network elements.

Modification of the host protocol stack

Most solutions require the modification of the protocol stack, either by introducing a sub-layer, for e.g. SHIM6, an extension for e.g. MPTCP or to introduce a completely new protocol to one layer such as SCTP. Other solutions like MIP introduce new signaling messages, which also requires the modification of the protocol stack inside host terminals.

Table 3.1: Evaluation of mobility and multihoming/bonding solutions

Logical layer	Solution	Modification of the host protocol stack	Modification of the network architecture	Transparency to current applications	Transparency to network elements	Control entity (host/network)	Mobility area
Layer 2	802.3ad	Yes	No	Yes	Yes	Host	-
Layer 3	MIP	Yes	Yes	Yes	No	Host	Full
	PMIP	No	Yes	Yes	No	Host	Local
	ILNP	Yes	No	No	No	Host	-
	GLI-Split	Yes	Yes	Yes	No	Host	Full (MIP)
	NIIA	Yes	Yes	No	No	Host	Full
	LISP	No	Yes	Yes	No	Host	-
	HAIR	Yes	Yes	Yes	No	Host	Full
	Six/One Router	No	Yes	Yes	No	Host	-
Layer 3/4	SHIM6	Yes	No	Yes	No	Host	Full
	HIP	Yes	Yes	No	No	Host	Full
	MILSA	Yes	Yes	No	No	Host	Full
Layer 4	MPTCP	Yes	No	Yes	No	Host	Full
	SCTP	Yes	No	No	No	Host	-
	mSCTP	Yes	No	No	No	Host	Full
Application	SIP	No	No	-	Yes	Host	Full
	mHTTP	No	No	-	Yes	Host	-
	QUIC	No	No	-	Yes	Host	Full

Modification of the network architecture

Introducing new agents, physical or functional, requires the modification of the network architecture. For instance, all MIP-based solutions use additional agents like the Home Agent and the Mobility Access Gateway in the case of PMIP. Even if the feature is more functional since it can be co-located with already deployed equipment, the residential gateway for instance, it requires modification of the network element anyway.

The modification of the network architecture is mainly the case in layer 3 solutions. This is due to the fact that all mechanisms from layer 4 and above are end-to-end protocols and are by nature built to be independent from the network architecture.

Transparency to current applications

Current applications are developed to use standard sockets to access lower layer. As the most used and known protocols are layer 4 TCP/UDP protocols, the majority of today applications use the TCP/UDP sockets. Proposing a solution that requires to use a specific socket would force developers to modify their applications.

In table I, "Yes" in this field means that the mechanism does not require any modification on current application and is completely transparent. This parameter concerns most layer 4 solutions which are directly accessed by the application. For instance, SCTP was proposed to completely replace TCP and thus to use the SCTP specific socket. MPTCP was proposed to overcome this issue, by proposing only an extension to standard TCP. The application has no knowledge of MPTCP and regular TCP is used and accessed with standard socket.

Transparency to network architecture

The transparency to network architecture considers how much a solution is transparent to network elements and more precisely middleboxes such as firewals, Network Address Translation (NAT) equipment,etc. Such elements are often configured to block any unknown traffic. Almost all solutions presented do not full fill this criteria as they introduce new types of messages such as in MIP or SCTP. MPTCP is a little bit different as it is based on top of standard TCP. However, it defines new options in the TCP option field, which may cause its blocking by middleboxes. Since network elements works most of the time at layer 3 or 4, application solutions are not concerned with this parameter.

Control entity

By control entity, we mean the entity that is responsible for establishing and destroying a new path. As can be seen, all solutions are designed to have control is in the host and not in the network. This means that the terminal is the only one that decides which interface to use. However, the terminal has no knowledge about available resources and the load on the networks it is willing to connect to. This can lead to non-optimized decisions and Quality of Experience degradation if the network is too loaded for instance.

Mobility area

The last criteria concerns mobility solutions only. Most propositions allow mobility without any area restrictions. This is not the case for PMIP, which allows mobility only within the same LMA controlled zone.

3.6 Conclusion

Several solutions for multi-homing and mobility were proposed at layer 3. Most of them are based on the locator/identifier split paradigm, trying to separate between the location and the identifier functions of current IP address. However, in most cases, additional elements need to be deployed in the network. This can stop the deployment because of the extra-cost it induces. Serious propositions were also made at the transport layer, especially MPTCP which is seen as the most relevant one. At the application layer, QUIC seems to be the best choice as it is supported by Google. But it is still very related to the type of the application as it is limited to web pages download.

For both layer 3 and 4 solutions, none of them ensure transparency to network elements, i.e. middleboxes such as firewalls or NATs. This is because most protocols introduce new messages, or in the best case new fields in existing headers, while most middleboxes are configured to block any unknown traffic. Note that middleboxes operate at layer 3 or 4, so this issue does not concern application layer neither layer 2 solutions.

Layer 2 solutions seem to have all qualities for a possible deployment. First, non or limited modification of the network architecture is needed. Indeed, by definition layer 2 networks are very limited geographically and thus does not go further the customer access network. It is by design completely independent to any upper layer

protocol, especially the application, and also to the network element which operate generally at layer 3 or 4. However, most studies focused in layer 3 and 4 while layer 2 propositions are very limited. The 802.3ad is too hardware dependent, i.e. the device needs to be equipped with a specific network card. On the other hand, the LTE dual connectivity requires to be connected to LTE networks and does not allow bonding between different technologies, e.g. between LTE and WiFi.

Chapter 4

Very tight coupling between LTE and WiFi

4.1 Introduction

In this chapter, we introduce a novel WiFi and LTE coupling architecture. We first review the limitations of current mechanisms and identify the requirements for a new low cost and efficient architecture. We then present the proposed architecture that we designed according to the defined requirements. Finally, we give a brief analysis of its impact on networking and security aspects, and give some insights to alleviate these issues.

The general idea of very tight coupling was proposed just before the begining of my PhD thesis [8]. However, the detailed specification of the protocols and interfaces and the qualitative analysis is my specific contribution.

4.2 Motivations

4.2.1 Limitations of legacy solutions

As seen in the last chapter, several architectures and protocols were proposed in order to face the continuous increase of the mobile data traffic on cellular networks. These solutions are centered around the concept of small-cells; that can be either based on LTE technology or WiFi. The idea is to use macro-cells to provide a continuous coverage, and small-cells to carry on the user traffic.

In case of LTE small-cells [37], the terminal can use simultaneously the radio resources proposed by two eNodeBs, i.e. the SeNodeB and the MeNodeB. This is

known as dual connectivity as defined by the 3GPP. However, these small cells are deployed mostly on the same spectrum as the one used macro-cell, which requires strong coordination between the MeNodeB and the SeNodeB in order to mitigate the impact of interference. This necessitates an ideal backhaul link, forcing the operator for costly deployment.

WiFi-based small-cells operate on unlicensed bands and can offer high bit rates (especially at 5GHz). This is very interesting to operators that see an opportunity for an efficient and low cost offload solution. However, this also confronts them to issues resulting from the design nature of today network. On the one hand, the majority of WiFi network are connected to the Internet using the fixed access network, which is today completely independent from the cellular network. On the other hand, the TCP/IP protocol stack was not designed to allow users to move between networks, still less to allow them use these networks simultaneously.

The research community addressed these issues and several proposal have been made to allow multi-homing between WiFi and LTE and to provide session continuity when moving between the two access networks. Most of these solutions propose a *Loose Coupling* between LTE and WiFi, which is based on new protocols and on the modification of the current TCP/IP protocol stack. This may oblige mobile application developers to introduce some major modifications on their products in order to solve a problem that is not directly related to them. Other solutions even require to modify the current network architecture by adding new elements. This may induce extra-costs that an operator is not ready to pay.

From the 3GPP point of view, *Tight Coupling* was the natural way to propose a full integration of WiFi to the LTE cellular network. However, tight coupling requires some major investment from the operator, for e.g. the deployment of new WiFi Access Points and special gateways.

Furthermore, all proposed solutions are not adapted for moving users because of the large time needed by the UE to attach to a given AP. This is due to the security procedures required by each WiFi AP, either through specific protocols (e.g. WPA) or through a login portals. Even if some mechanisms allows an automatic attachment without a physical intervention of the users, these procedures are time consuming. The coverage of a WiFi AP is limited, and a moving users may have only dozen of seconds between the detection of the AP and the time it leaves its vicinity. This is often not enough for a user to authenticate and to start using WiFi. (See Fig.4.3)

The choice to put the control in the UE is also a disadvantage. Today, the user terminal is the only one that takes the decision to make or break a new connection.

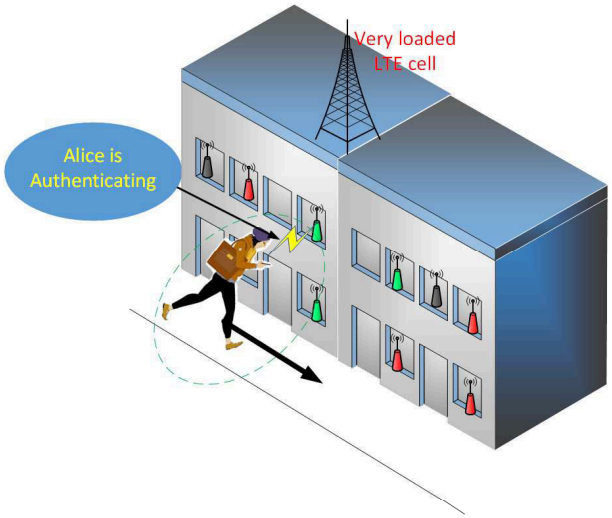


Figure 4.1: Alice tries to use WiFi while moving

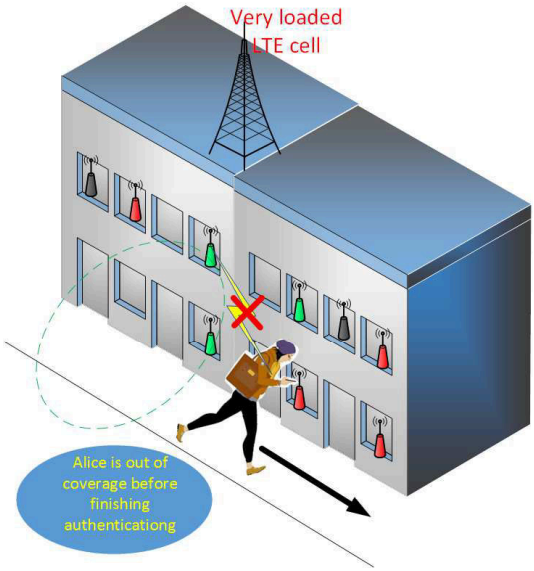


Figure 4.2: Alice is out of the AP coverage before finishing association step

Figure 4.3: WiFi/LTE traditional coupling scenario

It can be the user himself that manually connects to a WiFi network or the terminal can be pre-configured to use certain WiFi networks. In any case, the user and the terminal take the decision based on very limited information. For instance, the user may choose to use WiFi as it is cheaper than LTE. On the other hand, terminals are usually configured to connect to the AP from which they receive the strongest signal. The selected WiFi AP is thus not the best one as it can be very loaded with too much traffic or have too many stations already connected. Some mechanisms have been proposed to overcome this issue, such as the Access Network (ANDSF) [78][79] or Hotspot 2.0 [80], which propose to provide the UE with information about the nearby WiFi networks. However, the choice is still made by the terminal itself depending on specific OS implementation.

Requirements and objectives

From the analysis we performed about current LTE and WiFi coupling mechanisms, we identified the following requirements for a low cost and efficient solution:

- The solution should avoid additional deployment costs by reusing existing WiFi APs that are already deployed. It should also require no modification of the hardware and very limited or no modification of the software.

- The solution should provide a higher offload efficiency compare to previous solutions by allowing the offload of all users, including the moving ones;
- Finally, the solution should always be able to provide a satisfying QoS, which requires optimized data path management mechanisms.

4.2.2 Overview of Very Tight Coupling between LTE and WiFi

Very tight coupling was proposed to overcome current LTE/WiFi coupling mechanisms, and in line with the requirements for an efficient offloading solutions cited in the last section. The main idea is to connect directly WiFi APs to the eNodeBs that cover them (see Fig.4.4). This is possible thanks to the convergence of cellular and fixed networks in which both accesses share a common access/aggregation network. By connecting APs to eNBs, it is possible to reuse the PDCP layer for WiFi communications and thus to have common security procedures between WiFi and LTE. This reduces the attachment time to an AP and allows moving users that stay only few seconds in an AP coverage to use WiFi for this time. Unlike already proposed LTE/WiFi integration mechanisms, very tight coupling proposes to keep the control plane traffic (i.e. RRC traffic), in LTE to allow efficient *Dual Connectivity* (see Fig.4.5). Since the integration of the two access networks is done at a low layer

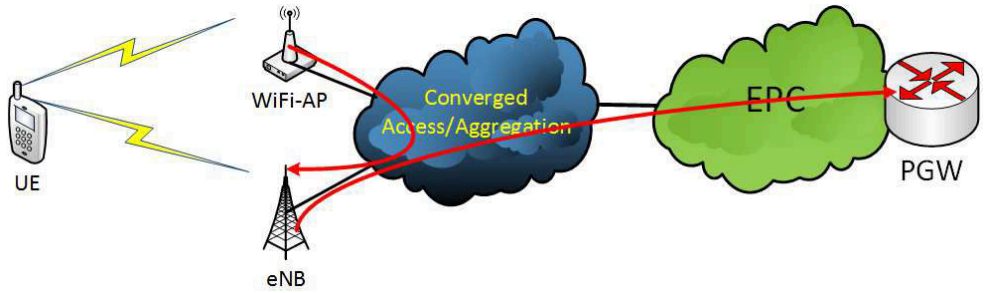


Figure 4.4: Very Tight Coupling main architecture

(i.e. PDCP), WiFi and LTE flows share the same IP layer. Thus, the UE manages only one IP address: this ensures session continuity and seamless experience when moving between the two networks.

Very tight coupling aims to allow all users, including the ones moving fast, to use WiFi when it is available while always ensuring a good QoS to the end user. This requires quick and optimized decisions regarding the establishment/destruction of a new path. In very tight coupling, the path control entity is in the network instead

of the terminal. As the network has a global view of the cellular network, and can even have information about the WiFi networks using specific mechanisms, it can thus take optimized decisions and can decide exactly when to use a WiFi network. Finally, very tight coupling is proposed in a way to avoid additional deployment

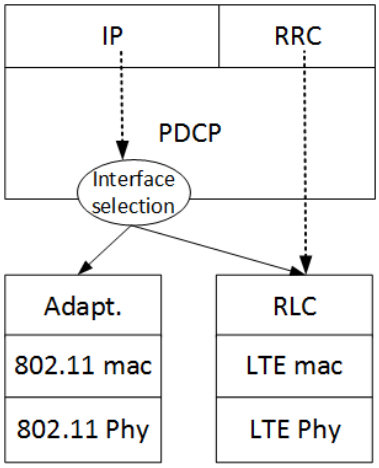


Figure 4.5: Very Tight Coupling stack

of WiFi APs by the operator. The idea is to reuse existing WiFi networks that are already deployed, in customer Residential Gateways (RGW) for instance, with limited modification of the software and no modification of the hardware.

4.3 Description of the proposed architecture

In this section, we describe the proposed architecture for very tight coupling, including the protocol stacks and the different network procedures. We first start by giving the different assumptions we made.

Assumptions

We made several assumptions that can be summarized in the following:

- *FMC network*: the first assumption concerns the network architecture. Since our work is in the scope of COMBO, we propose to use the FMC framework proposed in the project (see chapter 2). Thus, the fixed and cellular access networks share the same layer 2 aggregation network. Even if Very Tight Coupling can be imagined in a non-converged network, the connection between eNodeBs and WiFi APs can be achieved much easier and in an optimized manner in an FMC network.

- *Access and aggregation network* We consider an Ethernet-based access network, which is the leading future technology, replacing ATM. We also consider an Ethernet-based aggregation network, consisting of interconnected Ethernet switches. This means that each equipment connected to the network, i.e. RGWs and eNodeBs, are reachable through a layer 2 MAC address.

- *single operator*: we study the case of a single operator that owns and manages both the cellular and the fixed access network. This includes all equipment, such as RGWs. The study can be extended for a multi-operator scenario.

- *User Equipment*: we consider dual mode UEs; each UE consists of an LTE and a WiFi interface. It can be identified on the WiFi network with a layer 2 MAC address. On the LTE network, it can be identified with an RNTI that is assigned by the eNodeB on the radio access network.

4.3.1 RGW and Cellular Access Point

Very tight coupling aims at allowing the operator to offload their LTE network to WiFi without deployment of new APs and with limited modification of the software and configuration of the network. The idea is to reuse existing APs that already deployed, typically the ones implemented in RGWs.

Hence, RGWs should include a new feature that we call Cellular offload AP (CeAP). A CeAP is a functional entity that acts as a classical WiFi AP. As seen in section 2.2.1, a physical AP can include several virtual APs (VAPs) that broadcast different SSIDs. A CeAP is thus just another VAP, which has its own BSSID and broadcasts a specific SSID that is set by the operator. The operator can choose to configure the same SSID for all CeAPs or to have different ones depending on the area or on other criteria. Moreover, the CeAP is a layer 2 WiFi bridge, connecting the WiFi access to the aggregation network, which is the Distribution System (DS). It thus needs to support four addressing WiFi frame scheme.

Unlike traditional WiFi APs, the CeAP does not include any security mechanism and we thus consider an open authentication system. Very tight coupling already includes a security level provided by PDCP used for both LTE and WiFi. An additional WiFi security level would be redundant and time consuming.

4.3.2 eNodeB

In very tight coupling, the eNodeB is the anchor point for uplink and downlink traffic. This means that the flows from the different access networks, i.e. LTE and WiFi, are aggregated at the eNodeB in the uplink, while the downlink traffic is split between the available networks at the eNodeB as well. Hence, at least the *session mapping execution* function, which is performed in the uDPM Multipath Entity (MPE), should be implemented within the eNodeB.

The eNodeB interacts with other uDPM functions that can be located upper in the networks, i.e. at the main CO for instance. However, it can be more appropriate to have them directly implemented within the eNodeB. For instance, having the *decision engine* in the eNodeB would allow to have dynamic decisions and increase responsiveness to session events.

The eNodeB can be split into a BBU and an RRH (see section 2), which can be at different locations in case of centralized-RAN. We consider both architectures in our study, i.e. with and without centralized-RAN. For the centralized-RAN case, the BBU hostel is located in the main CO. For the other scenario, eNodeBs are connected to the aggregation network. In the following, we identify the different

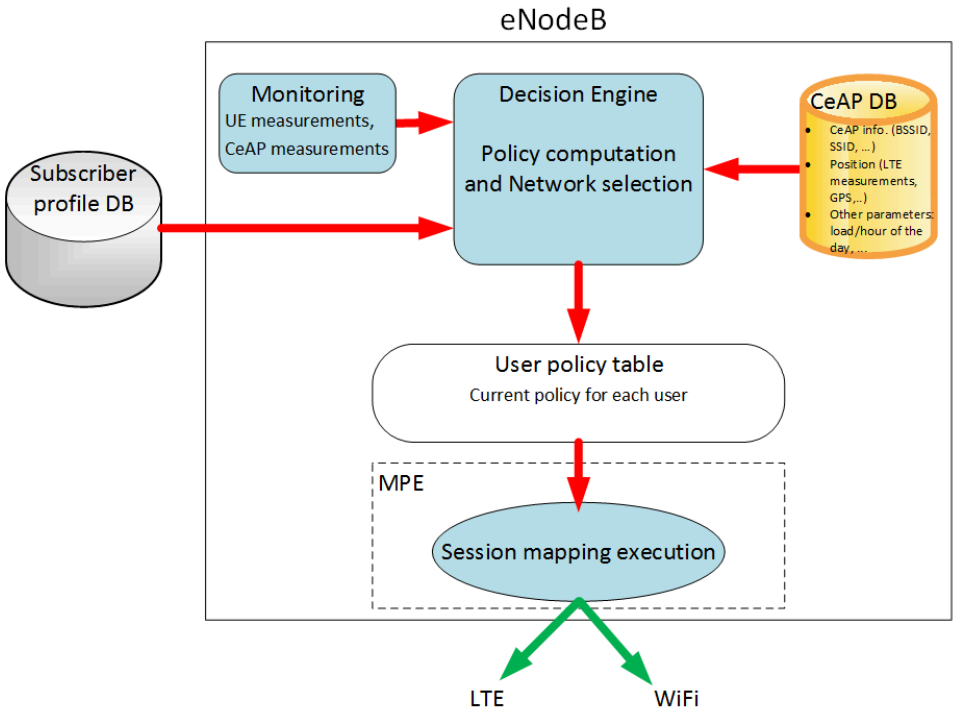


Figure 4.6: eNodeB building blocks

building blocks (see Fig.4.6) that should be within the eNodeB.

User policy table

The user policy table indicates to the eNodeB which policy to apply for a given connected UE. The table should map the following information:

- UE specific information: these include the UE current RNTI and its WiFi MAC address,
- CeAP information: in case the UE is already connected to a CeAP, the eNodeB needs to know its SSID and BSSID;
- Policies: this indicates which policy to apply for each bearer (i.e. identified by an LCID). A policy can be for instance to have 50% of the traffic over WiFi and the rest over LTE. These policies are computed by the *decision engine*.

CeAP database

The CeAP database saves all the CeAPs connected to the operator network. It can be similar to the ANDSF database that contains information about all the WiFi networks. In our architecture, the database should include at least:

- CeAP proper information: These includes all information concerning a WiFi AP such as the CeAP SSID and BSSID, the channel, the supporter bit rates,.... The SSID can be the same for all or for a subset of CeAPs. However, the BSSID is used to uniquely identify the CeAP;
- The RGW MAC address: This is the RGW address on the access/aggregation network side. Even if the CeAP is used as a layer 2 bridge, the RGW MAC address can be used by the eNodeB to directly request information concerning the CeAP;
- Position information: These can be Global Positioning System (GPS) coordinates or LTE radio measurements. The eNodeB uses these information to locate a CeAP, and used to identify nearby CeAP of a terminal;
- Other parameters: the database may also include parameters regarding the state and profile of the CeAP, that can be used in the network selection process. These information can be the BSS load according to the time of the day, or the RSS according to the different estimated positions in the cell;

ANDSF is a high layer IP-based solution used to provide the UE with information that helps for the selection of the access network. The UE is the only one that takes the decision. In Very Tight Coupling, the network and more precisely the *decision engine*, takes the decision. Since we propose to have the *decision engine* in the eNodeB, the *CeAP database* should be at the same location to avoid additional delays between the two entities. Moreover, the database should only contain information related to CeAPs in the eNodeB coverage unlike the ANDSF one that is centralized. This allows to have less entries in the database and a faster lookup process.

4.3.3 eNodeB/RGW Interfaces

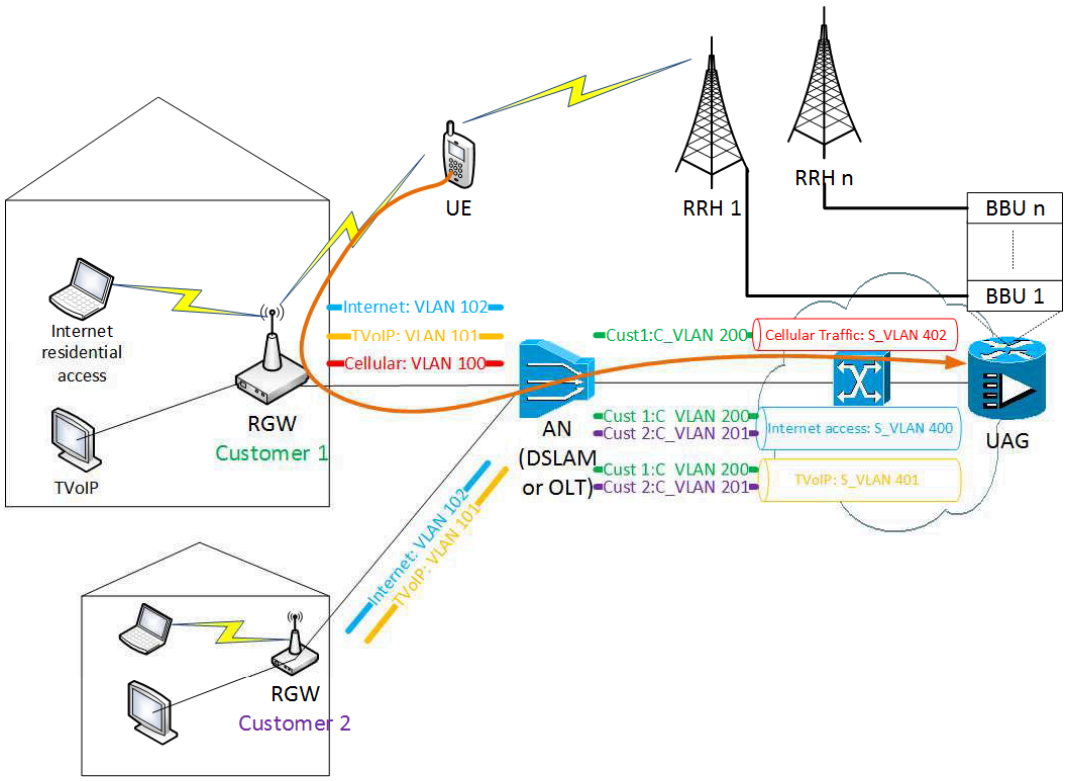
Two new logical interfaces have to be defined between the eNodeBs and the RGWs. The first one is responsible transporting the user plane traffic between the eNodeB and the RGW over the aggregation network. We also proposed to have a signaling interface between the eNodeB and the RGW. This interface is used to allow the eNodeB to request and get measurement reports from the CeAP.

As we consider an Ethernet-based aggregation network, we propose to implement the eNodeB/RGW interface using VLANs. The idea is to consider the *cellular traffic*, i.e. the traffic between UE and eNodeB going through WiFI, as any other service offered by a RGW such as IPTV or VoIP. These services are usually transported over a 802.3q VLAN between the RGW and the AN, i.e. DSLAM or OLT, and a corresponding S_VLAN inside the aggregation network. Thus, we propose to have specific VLAN and S_VLAN values to transport the *cellular traffic* the same way. For eNodeBs to be able to received the *cellular traffic*, they should be configured in the same VLAN. The rational behind carrying the traffic on an S_VLAN is twofold: i) Allow the application of specific prioritization, and ii) Isolate the traffic from the rest of the network.

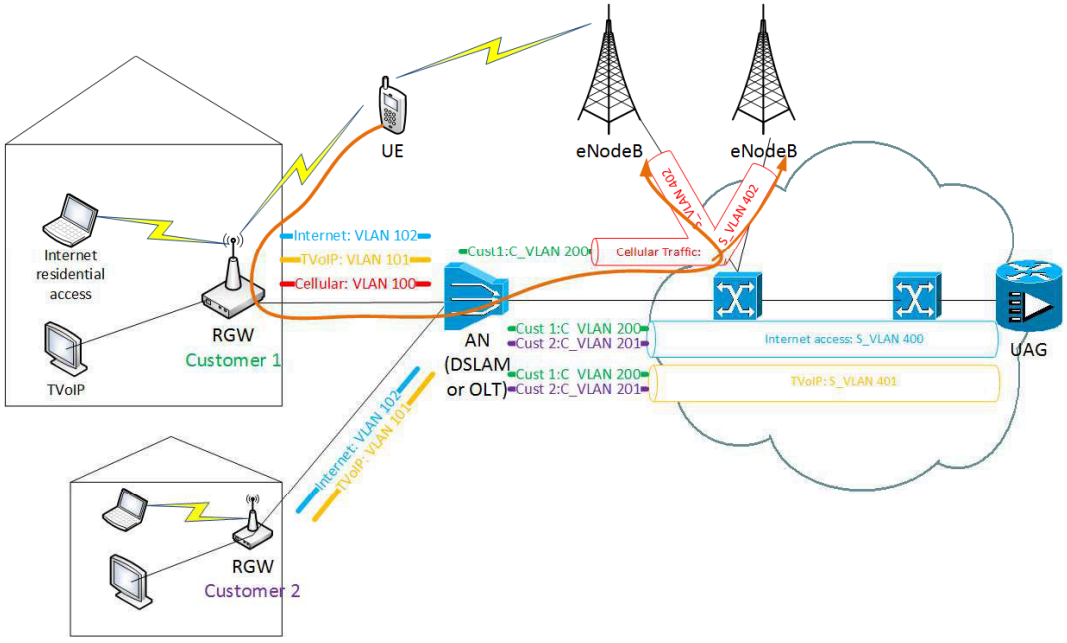
Even if this configuration applies to both centralized and distributed COMBO architecture, some specific considerations need to be taken, as discussed in the following.

Centralized COMBO architecture

In the centralized COMBO architecture, the UAG is located in the core CO. We already saw in chapter 2 that this does not give the possibility of BBU-hosteling in the UAG. In this case, legacy eNodeBs are connected to the aggregation network



(a) Distributed Architecture



(b) Centralized Archicetture

Figure 4.7: VLANs and Very Tight Coupling

and are considered as Ethernet nodes. In the proposed architecture, each eNodeB should be configured in the S_VLAN to be able to received the *cellular traffic* (see.

Fig.4.7b).

Distributed COMBO architecture

In case of distributed architecture, a centralized-RAN can be considered. In this case, eNodeB are split in an RRH that stays in the antenna site, and a BBU located in a BBU-hostel in the UAG at the main CO. In this case, the UAG is the termination point for the *cellular traffic* coming from all CeAPs. This requires less configuration compared to the legacy eNodeB architecture as only the UAG needs to be configured in the S_VLAN (see. Fig.4.7a).

4.3.4 Protocol architecture

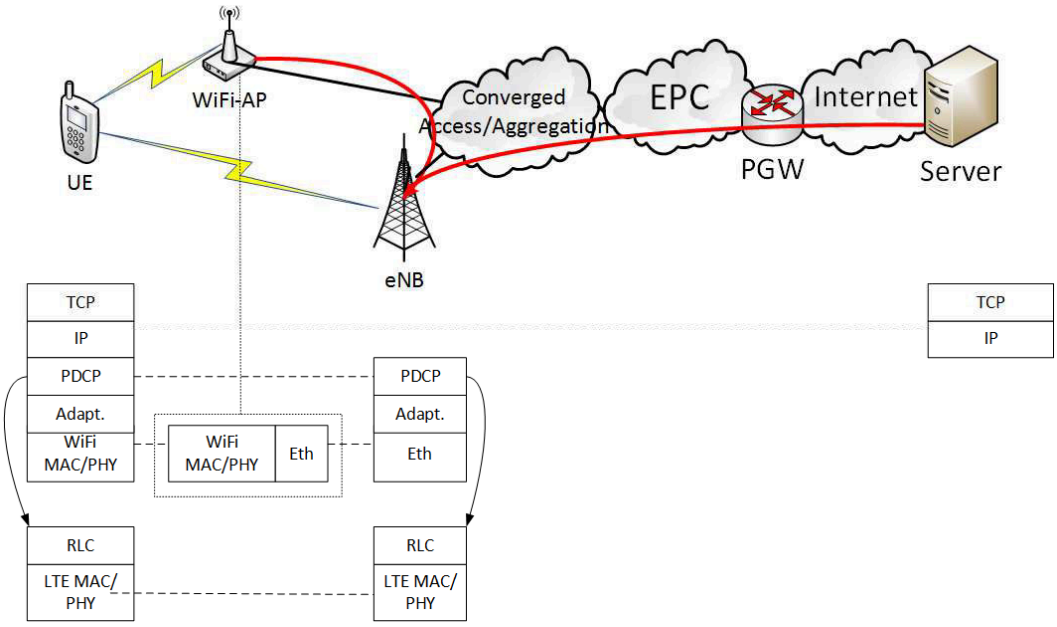


Figure 4.8: Very Tight Coupling protocol stack

Fig.4.8 shows the protocol stack architecture that we propose for Very Tight Coupling. The LTE control plane, i.e. RRC traffic, is sent as usual over LTE. The user plane can be sent either through LTE or WiFi, or both simultaneously. When it is sent over LTE it follows the usual protocol stack with no modifications, i.e. RLC/MAC/PHY.

When WiFi is used, in the uplink, PDCP PDUs are encapsulated by the UE into WiFi frames. We propose to add an adaptation sub-header before the 802.11 header. The user packet, i.e. the PDCP PDU, is then encapsulated in a new Ethernet frame

at the CeAP and sent over the aggregation network to the eNodeB. On the downlink, the eNodeB puts the PDCP PDU in an Ethernet frame and sends it to the CeAP. The PDU is then encapsulated into a 802.11 frame and sent to the UE.

4.4 Operation of Very Tight Coupling

In this section, we describe how Very Tight Coupling works. We first give the specification of the adaptation sub-header and presents the transmission of a frame between the UE and the eNodeB. Then we give the different procedures and use cases that we identified.

4.4.1 UE modes

In the rest of the document, we assume that the UE can be in two different modes:

- *LTE-only*: This mode corresponds to a standard LTE communication and the UE is using exclusively LTE for both control and user plane;
- *Very Tight Coupled (VTCo mode)*: The VTCo mode means that the UE is connected to the LTE network and to WiFi through a CeAP. In this mode, the control plane is sent over LTE while the user plane can be either over WiFi, or both LTE and WiFi.

4.4.2 Adaptation sub-header

The adaptation sub-header is used when PDCP is encapsulated into WiFi frames, in order to transport information that are needed by the eNodeB. These information include the Radio Temporary Network Identifier (RNTI) and the Logical Channel Identifier (LCID), which are usually transported by LTE lower layers (i.e. MAC). It also include the eNodeB E-UTRAN Cell Global Identifier (ECGI). The RNTI allows the eNodeB to identify the user from which the frame is coming, while the LCID allows it to identify the bearer. The ECGI is useful in the case of BBU hosteling when several eNodeBs are located in the same hostel. It allows identifying to which eNodeB the frame is destined.

4.4.3 Transmission in very tight coupling

In Fig.4.10 we show a typical transmission of a frame sent from the UE to the eNodeB following the protocol stack proposed in section 4.3.4. As explained before,

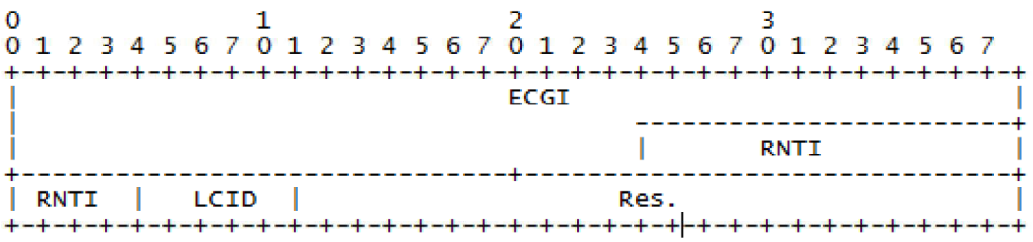


Figure 4.9: Adaptation sub-header specification

the adaptation sub-header is added to the each PDCP PDU to be sent over WiFi. It includes the UE RNTI, the bearer LCID and the eNodeB ECGI. As for standard WiFi frames, an LLC header is added to indicate the carried protocol using the *protocol* field. We define in our case a new value, i.e. 0x99ff, that indicates that the frame is carrying PDCP traffic. The To_DS bit is up to let the CeAP know how to interpret the different address fields. Upon reception of the frame, the CeAP encapsulates the PDCP PDU, including the adaptation sub-header, in a new Ethernet frame (i.e. 802.1q). The 802.11 the Destination Address (DA) and the Transmitter Address (TA) are copied in the destination and source address fields, respectively. The LLC protocol field is copied in the Ethernet EtherType as both have the same function. As seen in section 4.3.3, the VLAN value in the Ethernet 802.1q frame indicates the type of service, which corresponds to the cellular traffic in our case. It should be pre-configured in the RGW by the operator.

The DSLAM does not modify the address fields in the received frame. However, as the aggregation network uses a double tag frame, it should create a new Ethernet 802.1ad frame which includes these tags. Thus, the destination and source addresses, as well as the EtherType, are the same. The C_VLAN is proper to the customer line, while the S_VLAN indicates the type of traffic, which is cellular traffic in our case. The DLSAM assigns the value of the S_VLAN according to the VLAN on the received frame (i.e. from the RGW). Even though these two values have the same signification, i.e. indicate the service, they can be different. This depends on the operator configuration.

4.4.4 Messages

We defined different messages that are needed for the operation of Very Tight Coupling. These messages can either be sent over the LTE control plane or the WiFi Control plane.

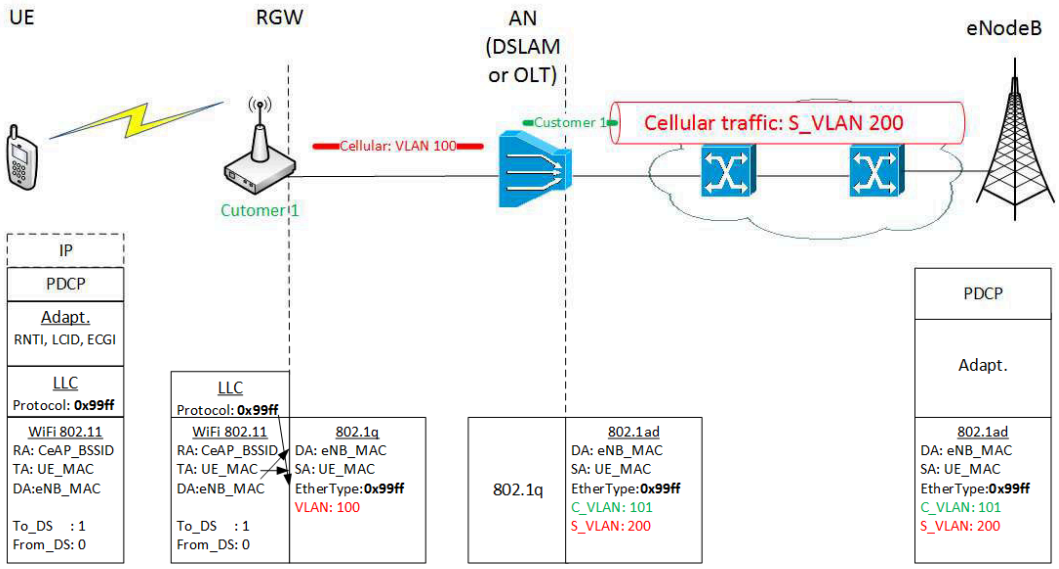


Figure 4.10: eNodeB/RGW interface protocol stack

CeAPList

The *CeAPList* is a new type of RRC message sent by the eNodeB to the UE (i.e. over LTE). It contains the information of different CeAPs, the eNodeB ECGI and MAC address, and a security random token. These information are summarized in the following:

- WiFi-CeAP-information:(WiFi network SSID,
  CeAP BSSID,
  CeAP priority) ;
- eNodeB-ECGI;
- eNodeB MAC address;
- Security-token;

The eNodeB MAC address is the destination address of all frames sent from the UE to the eNodeB through WiFi. The eNodeB ECGI is used in case of BBU hosteling to identify the destined eNodeB. The security token is generated randomly for each "WiFi initialization procedure". It is used to avoid a *TestMessage* to be replayed by an attacker, which would allow him to connect to the CeAP using the UE identity.

TestMessage

The *TestMessage* is sent by the UE to the eNodeB through WiFi. Its role is to make sure that the CeAP is not a rogue AP, and that it is really connected to the operator aggregation network. It contains the security-token received in the *CeAPList* message.

TestMessageAck

The *TestMessageAck* is an RRC message sent from the eNodeB to the UE through LTE. It is used first to acknowledge the reception of the *TestMessage*, which confirms the connection of the UE and changes it to the VTCo-mode. It is also used to communicate the new network policies to the UE.

PolicyUpdate

The *TestMessageAck* is an RRC message sent from the eNodeB to the UE on the LTE connection. It is used to update the current policy on the UE, to change the distribution of the traffic among the two networks for instance.

4.4.5 WiFi initialization procedure

The WiFi initialization procedure allows the UE to connect to a CeAP and thus to change from the LTE-mode to the VTCo-mode. The procedure is described in Fig.4.11.

Based on periodical measurements sent by the UE, the *Decision Engine* identifies the relevant CeAPs that can be used by the UE. The eNodeB sends a *CeAP_list* message over LTE that contains the information of the selected CeAPs, the eNodeB ECGI and/or MAC address and a one-usage random security token. Upon reception of this message, the UE tries to attach to the CeAP with the highest priority. Note that this is a simple association procedure that does not require any credentials. When the association to the CeAP is complete, the UE becomes in VTCo-mode. It sends a *test_message* to the eNodeB through WiFi containing the security token, i.e. through the CeAP. The eNodeB can detect false *test messages* by comparing the security token. Afterwards, the eNodeB computes new policies for the UE, updates the *User policy table* and sends a *test message ack* containing the new policies. Finally, the UE updates its policies and starts using the interfaces accordingly.

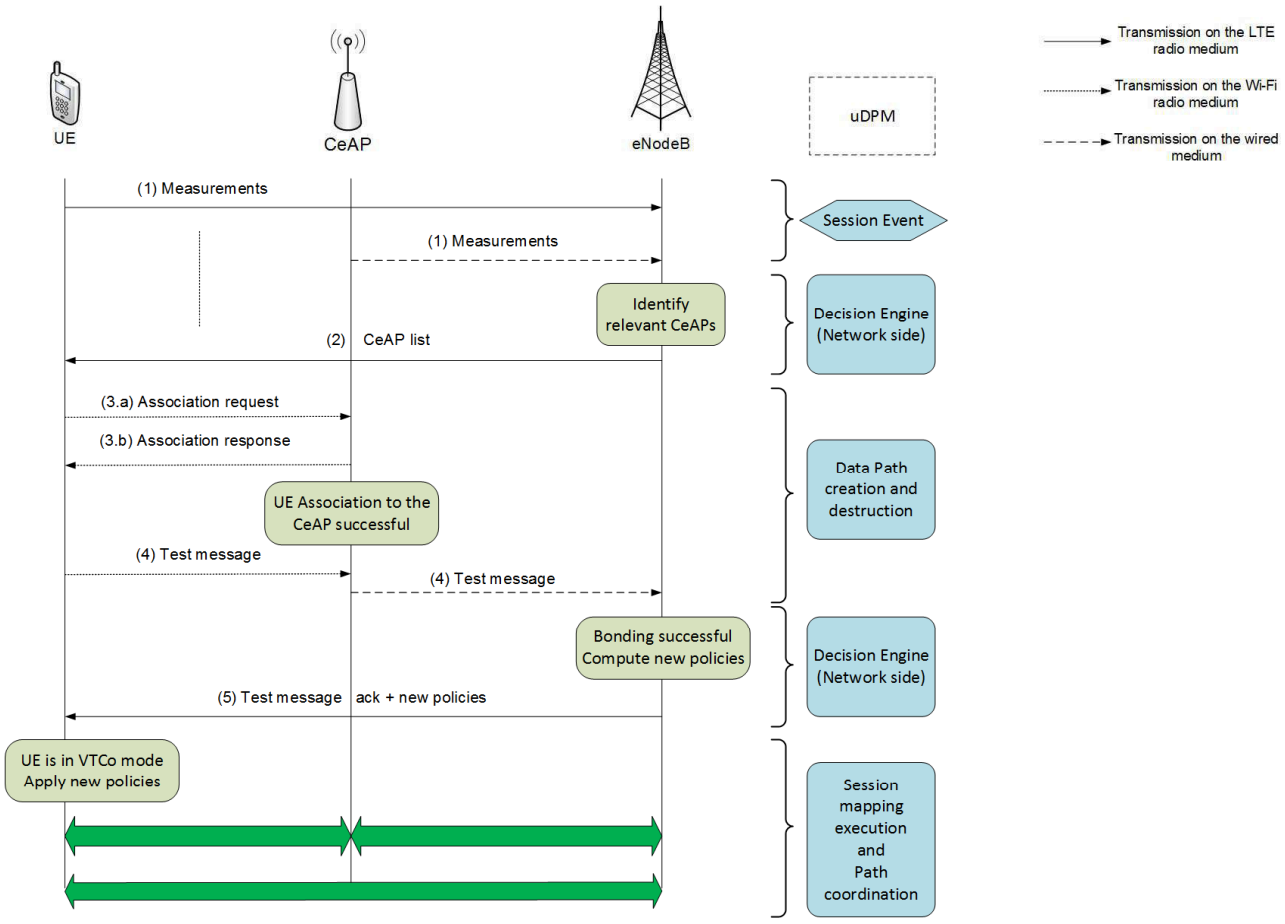


Figure 4.11: WiFi Initialization procedure

4.4.6 Mobility to another CeAP

The *decision engine* can detect, using LTE and WiFi measurements, that the UE is moving into another CeAP coverage that can be used. It sends the new CeAP information to the UE, which starts a new *WiFi initialization procedure* similar to the one described before.

4.4.7 Policy update

The policy update procedure is described in Fig.4.12. Using the measurements received from the UE and from the CeAP, the *decision engine* can decide change the current policy to a more appropriate one. For instance, if the current CeAP is becoming too loaded, it can decide to change the distribution traffic among the two access networks to have less traffic sent over WiFi. The new policy is sent to the UE on a *PolicyUpdate* message.

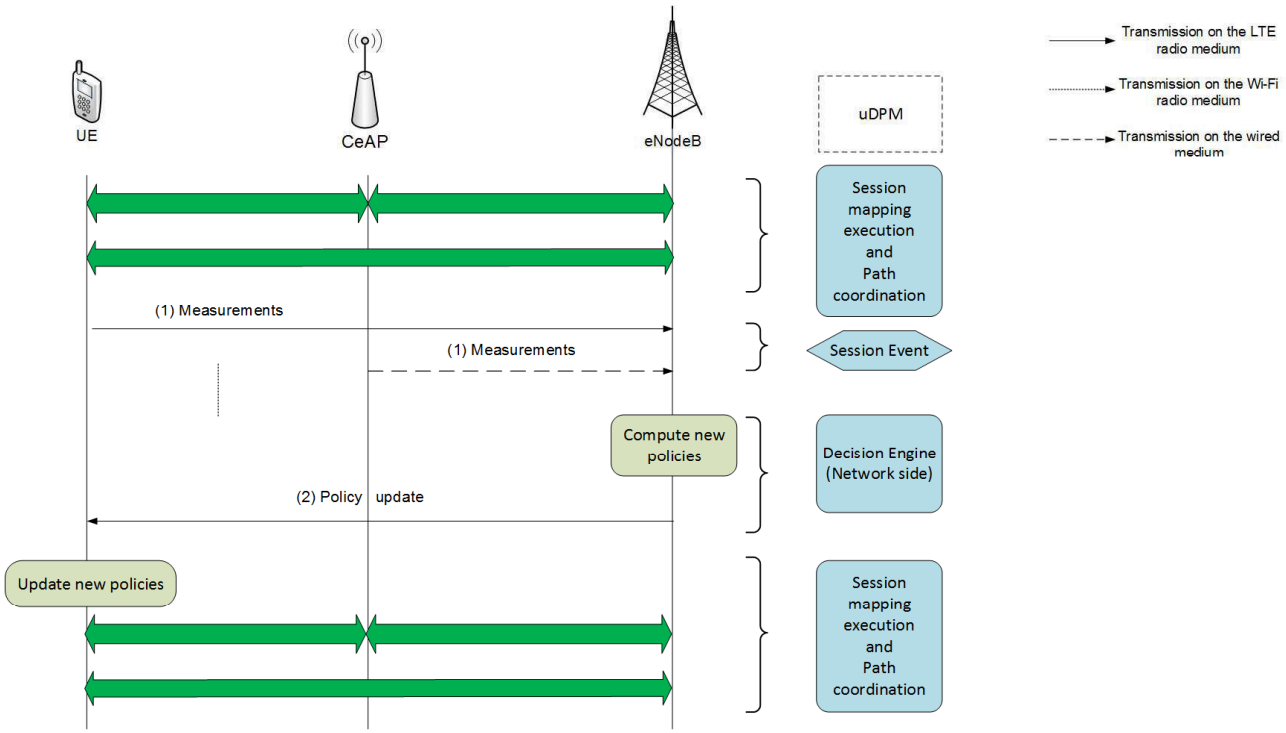


Figure 4.12: Policy update procedure

4.4.8 Measurement reports

The performance of Very Tight Coupling is mainly based on the interface decision and data path that are managed by the network and not the UE. In order to take optimized decisions, the network needs to have as much information as possible concerning the terminal and all nearby WiFi networks as well. There are thus two ways of obtaining these information: from the UE and from the CeAP itself.

UE measurement reports

The first possible measurements are transmitted by the UE to the eNodeB. This includes usual LTE measurements but should also include information about all nearby WiFi networks detected by the UE. These information contains all information that can be obtained over WiFi such as:

- WiFi SSID and CeAP BSSID: note that the UE may be configured to only report WiFi network with the operator SSID in order to avoid over-reporting of *non-very tight coupled* APs.
- Information about the WiFi network such as: the BSS load, CeAP channel, RSSI, channel utilization,...;

CeAP measurement reports

We propose to have a new protocol to allow the eNodeB to obtain *measurement reports* from a CeAP through the aggregation network. Typically, the eNodeB can have information such as the channel utilization and number of associated stations, which allows it to take decisions even if the UE is not yet in the range of the CeAP. Note that these information are the same that are already broadcast by every AP in beacon messages over WiFi.

4.5 Additional studies

We proposed an architecture of Very Tight Coupling that allows a deployment with a minimum modification of the current network architecture. In this section, we investigate its impact on other network aspects, and other requirements.

4.5.1 Impact on the aggregation network performance

We consider in our architecture RGWs acting like layer 2 bridges, which means that it only forwards frames to/from the UE/eNodeB without modifying address fields in the header. Thus, the traffic is transported over the aggregation network using UE and eNodeB mac addresses.

The aggregation network is a layer 2 network composed of interconnected switches. It can span over very large geographic area and over several cities. When a UE starts a transmission over WiFi, its address is not in the switch's forwarding tables. Thus, the frame is broadcast over all the switch interfaces and thus reaches the entire aggregation network. Broadcast is known to consume a lot of bandwidth and to force aggregation switches to save the MAC address of all UEs using a CeAP. This increases the switch's lookup time and decreases the global performance of the network.

One way of limiting the impact of broadcast in this architecture, is to use S_VLAN for isolation purpose. Indeed, the *cellular traffic* is only between the eNodeB and the RGW in its coverage, and should not go farther in the network. The operator can for instance configure an S_VLAN for each limited area of the aggregation network, e.g. for an area covered per main CO.

Note however that these issues can be limited by having BBU hostels installed at the main CO or in case of distributed UAG at main CO. As shown in section

2.2, in this architecture the IP core network is extended to the main CO and the aggregation network covers a smaller area.

4.5.2 Security issues

We first start by identifying the security issues and possible threats on the proposed architecture, and give insights on possible mitigation to these issues.

4.5.2.1 Non-authorized access

In very tight coupling, the CeAP does not use any WiFi security protocols. The reason of this is to avoid large delays induced by these protocols in the association between the UE and the CeAP. This actually does not have any impact on the user traffic security since it is ciphered between by PDCP between the UE and the eNodeB. However, the CeAP does not have any way to authenticate the user and any terminal can thus connect to the WiFi network without any credentials.

Scenario

A non-authorized terminal that is not connected to the LTE network associates to the CeAP without needing any credentials.

Threats

All the traffic sent to the CeAP is transported on the aggregation network over the *cellular traffic* S_VLAN, which includes only RGWs and eNodeBs in case of centralized architecture. However, the S_VLAN does not include the BRAS, which is the IP gateways that routes user traffic to outside IP networks, e.g. the Internet. Thus, traffic generated by the non-authorized user connected to the CeAP never reaches the BRAS and is confined within the operator aggregation network. The user does not have access to the Internet.

In case of distributed UAG architecture, the BBU-hostel as well as the BRAS are collocated in the main CO, where the S_VLAN terminates. However, the traffic on this VLAN is automatically forwarded to the BBU-hostel and not to the BRAS. This avoids the non-authorized user to have access outside networks.

However, a non-authorized access allows an attacker to perform other attacks that we detail in the following sections.

Mitigation

The CeAP should implement an authentication mechanism. Current WiFi security protocols (i.e. WEP, WPA) are time consuming. However, it is possible to implement simpler algorithms, for instance a three-part key system. Typically, a key is derived by the eNodeB and sent to the UE through LTE and to the CeAP through the eNodeB/RGW-interface. The key is then used for secure communication between the CeAP and the UE.[1]

4.5.2.2 Flooding

In the proposed architecture, the CeAP functional block is a layer 2 bridge that it only forwards layer 2 (i.e. Ethernet) frames between the UE and the eNodeB without modifying the address fields. This means that all communications between the UE and the eNodeB use the real eNodeB MAC address. We identified two possible attacks that can be conducted due to these issues.

Attack 1: Flooding the eNodeB or the UE

Scenario An attacker is listening on the WiFi network. It intercepts the frames between a an associated UE and the CeAP and gets the UE and eNodeB MAC addresses. The attacker generates random WiFi frames using these addresses (i.e. known as MAC address spoofing), and replays UE or eNodeB traffic, i.e. PDCP PDUs. The receiver, i.e. eNodeB or UE depending on the way of the attack, believes that the traffic is really coming from the other part (i.e. UE or eNodeB), it thus processes and decodes the PDU.

Threat This does not have any influence on the traffic as the eNodeB, or the UE, can detect that the frame is incorrect using the PDCP counter. However, this consumes processing and memory resources on the eNodeB, or the UE, as they have to process and decode each frame coming from the attacker.

Mitigation Although some propositions [82][83] have been made to solve MAC address spoofing in WiFi networks, there is no actual solutions in use in today WiFi APs. Cisco proposes to have a Wireless Intrusion Prevention system [84]. However, this would require too much deployment and modification of CeAPs. One other solution is for the eNodeB to detect messages replayed by the attacker and to disconnect the UE from the CeAP. As PDCP packets are ciphered, the attacker can

[1] This is what is proposed by 3GPP for the LWA solution [81]

not modify it. Thus, a PDCP with a duplicate sequence number means that this is a replayed frame.

Attack 2: MAC flooding

Scenario An attacker associated to the CeAP floods the network with generated traffic using random destination addresses. The switches in the aggregation networks receiving this traffic with unknown addresses automatically broadcasts it on all their ports.

Threat MAC flooding uses the broadcast nature of Ethernet-based networks, which consumes a lot bandwidth in the aggregation network and resources in the switches.

Mitigation The only way to face this issue is to prevent the attacker from connecting to the CeAP in the first place. The mitigation is thus the same as proposed for the non-authorized access issue. However, it is worth mentioning that most of today switches already implement security mechanisms to prevent flooding attacks, for e.g. the Cisco switchport-security [85].

4.5.2.3 disassociation attacks

This is actually a well known denial-of-service attack on WiFi networks. Its main objective is to block user traffic from reaching its destination.

Scenario A UE that is connected to the LTE network associates to the CeAP using the two-handshake procedure, and starts sending data. An attacker sends a *disassociation* request to the CeAP using UE MAC address. The CeAP removes the UE from the associated stations. Thus, when a new frame from the UE arrives at the CeAP, it is rejected and not forwarded. The UE can not reconnect to the CeAP because of the one usage token sent in the *test message*.

Threat This attack increases the loss rate over the WiFi network as all UE frames are rejected from the CeAP.

Requirement The eNodeB should rapidly detect the issue and modify the UE policy to use LTE only.

Mitigation One way for the eNodeB to detect the issue is from the *measurement reports* sent by the UE. The UE should send a report immediately after detecting a significant increase of the WiFi loss rate, including this data. The eNodeB can then take this information into consideration to modify the UE policy to avoid using WiFi.

4.5.3 Interface selection and policies

The main objective of Very Tight Coupling is to have fast handovers between WiFi and LTE, and to allow moving users to use WiFi even if they stay under the WiFi AP coverage only few seconds. This requires very fast and dynamic interface selection procedures. In very tight coupling, this function is in the network, and not in the terminal as done today.

Using the different input, i.e. LTE measurements, WiFi measurements from the UE and CeAP measurements, the network needs to choose which interface the UE has to use and if several ones are available, how to distribute the traffic among them. This is very challenging, as the objective of the operator is to offload its LTE network to WiFi, while providing always a good satisfying QoS. In the following, we identified problems that need to be solved to achieve these requirements.

Handover/Handoff trigger

Let us take the example of a user using WiFi and LTE simultaneously in a Very Tight Coupling architecture. Let us now assume that the UE is moving outside the AP coverage. In current WiFi networks, the UE measures the Received Signal Strength (RSS) to decide when to detach from the WiFi AP. However, for users moving at relatively high speed, the RSS may drop quickly depending on the user speed. This delays the time the UE detects that it is outside the WiFi AP coverage. In very tight coupling, it is possible to combine LTE and WiFi measures, as well as AP information, to optimize the decision to trigger a WiFi detachment.

Traffic distribution

One important aspect when using WiFi and LTE simultaneously, is to efficiently distribute the traffic among the two interfaces in order to maximize the offloaded capacity while ensuring a good QoS. Unlike current coupling mechanisms that use per-session interface selection, Very Tight Coupling performs per-packet interface selection, which means that for each outer packet, PDCP decides on interface to send it. This allows to have a more efficient distribution of the traffic, but also requires more sophisticated algorithms. Indeed, this depends on different parameters such as the instantaneous load and available capacity on the WiFi AP, as well as the user profile.

4.5.4 Reliability on WiFi

In Very Tight Coupling, the traffic needs to cross two networks: WiFi and the access/aggregation network. Even if the access/aggregation network is a managed by the operator and considered as reliable, this is not the case of the WiFi networks, which are usually subject to a high loss rate due to collisions. This can be an issue for downlink traffic, eNodeB to UE, as the eNodeB has no way to know if a frame has been correctly received by the UE. Even if PDCP includes sequence numbering, it does not have acknowledgement nor retransmission mechanisms. This is because this function is usually ensured by RLC for LTE transmissions, which is not used in Very Tight Coupling.

4.6 Conclusion

Very Tight Coupling between LTE and WiFi is a novel concept that proposes a low cost and efficient solution, which can be used by operator to offload the cellular network and to enhance its capacity as well. In this chapter, we proposed an architecture for Very Tight Coupling, in which we defined the different building blocks and procedures. We also discussed the impact of such an architecture on performance and security aspects.

The next stage is to analyze the performance of Very Tight Coupling to show its efficiency in terms of offloading and capacity enhancement.

Chapter 5

Mathematical analysis of Very Tight Coupling

5.1 Introduction

In this chapter, we study the performance of very tight coupling when APs are connected to one, two and more eNodeBs. UEs are generally connected to the Base Station (BS) from which they receive the strongest signal. For a given UE, the larger the distance to a base station is, the higher the path loss is. Hence, a UE is generally connected to the closest BS. However, due to the presence or absence of obstacles between the UE and BSs, propagation is affected by the well-known shadowing effect. The better BS is not always the closest one.

In very tight coupling, offloading is only possible if both the UE and the AP are connected to the same eNodeB. Due to shadowing, an AP connected to the closest BS is not always able to offload the traffic of all nearby UEs because some UEs can be served by a different BS (see Fig.5.1).

We consider three different scenarios. A *single-eNB coupling*, where WiFi APs are connected to the nearest eNodeB only. In the second scenario, we consider *double-eNB* coupling where APs are connected to the two nearest eNodeBs. In the last one, a *total-eNB coupling* is considered which is an ideal scenario where each AP is connected to all BSs, which means that offloading is always possible.

We first propose a mathematical model to analyze the performance of *single-eNB coupling* in case of two BSs in the network. We then extend the study for a larger number of BSs and use Monte Carlo simulations.

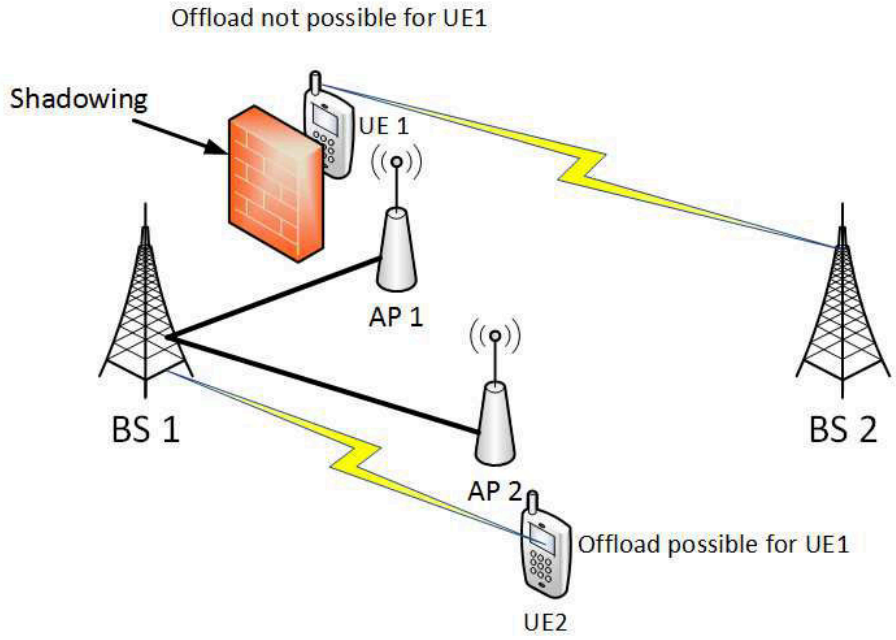


Figure 5.1: Offload possibility in presence and in absence of shadowing

5.2 The model

In this section, we present the model that we considered and the assumptions that we made about both the cellular and WiFi networks.

5.2.1 Cellular network

We consider an hexagonal cellular network. We assume that all BSs transmit at the same power P_t and on the same frequency, i.e. the frequency reuse factor is 1. The distance between two contiguous BSs is D and the cell radius is equal to $\frac{D}{\sqrt{3}}$.

For propagation, we consider a classical Okumura-Hata model, where the received power is:

$$P = P_t \left(\frac{r_0}{r}\right)^{\alpha} \tag{5.1}$$

where P_t is the transmission power, r is the distance between the UE and its serving BS, r_0 and α are propagation parameters. Equation (5.1) is equivalent to the more classical formula $P = P_t \frac{k}{r^{\alpha}}$ with $r_0 = \sqrt[\alpha]{k}$. This way of presentation is preferred to ease homogeneity checks.

In order to avoid very large received power when a UE is too close to a BS, we take:

$$P = P_t \min\left(1, \left(\frac{r_0}{r}\right)^{\alpha}\right). \tag{5.2}$$

We also take into account the shadowing effect and consider it as a standard normal random variable ξ with a standard deviation σ. Thus, the received power becomes:

$$P = P_t \min\left(1, \left(\frac{r_0}{r}\right)^{\alpha}\right) 10^{\xi\sigma/10}. \tag{5.3}$$

We assume that a US is served by the best BS, i.e the BS from which it receives the strongest signal. However, in presence of shadowing the best BS is not always the nearest one and the UE can be outside the hexagonal cell of its serving BS.

Shadowing effect

We consider a log normal shadowing effect represented by a log normal random variable (r.v). Let $\xi_{k,i}$ be the log normal r.v representing the shadowing effect between UE_i and BS_k, and σ its standard deviation. When correlation is taken into account, variable $\xi_{k,i}$ is written as:

$$10\log(\xi_{k,i}) = 10\log(\xi_{c,i}) + 10\log(\xi_{s,k,i}) \tag{5.4}$$

where $\xi_{c,i}$ is a log-normal r.v that represents the shadowing effect due to the obstacles close to UE i, which is common to all BSs, and $\xi_{s,k,i}$ is a log-normal r.v that represents the shadowing effect due to obstacles between UE i and BS k. Let σ_c and σ_s be the respective standard deviations of $\xi_{c,i}$ and $\xi_{s,k,i}$. The variable $\xi_{k,i}$ (in dB) is the sum of two log-normal r.v., it is then a log-normal r.v with a standard deviation σ:

$$\sigma^2 = \sigma_c^2 + \sigma_s^2 \tag{5.5}$$

and the correlation coefficient is $\rho = \frac{\sigma_c}{\sigma}$. Using (5.3) and (5.4), we deduce the SIR which is the ratio between the useful signal (received from BS_1) and the signals received from the interfering BSs (BS_k with $k > 1$):

$$\text{SIR} = \frac{P_{t,1} \min\left(1, \left(\frac{r_0}{r_1}\right)^{\alpha}\right) 10^{\frac{\xi_{c,1}\sigma_c}{10}} 10^{\frac{\xi_{s,1,1}\sigma_s}{10}}}{\sum_{k>1} P_{t,k} \min\left(1, \left(\frac{r_0}{r_k}\right)^{\alpha}\right) 10^{\frac{\xi_{c,1}\sigma_c}{10}} 10^{\frac{\xi_{s,k,1}\sigma_s}{10}}}. \tag{5.6}$$

Note that the terms involving $\xi_{c,1}\sigma_c$ can be simplified, and (5.6) can be written:

$$\text{SIR} = \frac{P_{t,1} \min\left(1, \left(\frac{r_0}{r_1}\right)^{\alpha}\right) 10^{\frac{\xi_{s,1,1}\sigma_s}{10}}}{\sum_{k>1} P_{t,k} \min\left(1, \left(\frac{r_0}{r_k}\right)^{\alpha}\right) 10^{\frac{\xi_{s,k,1}\sigma_s}{10}}}. \tag{5.7}$$

We can see in (5.7), that the SIR depends only on the "non-correlated part" of the shadowing, which is represented by a log-normal r.v with standard deviation $\sigma_s^2 = \sigma^2 - \rho\sigma^2$. It was found in [86] that the typical value for a site-to-site cross correlation is between 0.3 and 0.5. For the shadow standard deviation, typical values are in the range of 5dB to 12dB as mentioned in [87][88][89]. We thus take σ_s between 3dB to 10dB.

Bit rate model

The bit rate R for a given bandwidth W (in MHz) and an SINR γ is computed with the Shannon capacity formula $R = W \log_2(1+\gamma)$. In this study, we consider a UE running an application that generates a bit rate R. The required bandwidth is then:

$$W = \frac{R}{\log_2(1+\gamma)}. \tag{5.8}$$

5.2.2 WiFi network

The capacity of a WiFi AP depends on different parameters such as the number of users that are connected or to the environment (i.e. most WiFi APs are deployed inside buildings). In our study, we assume that WiFi networks have always enough capacity to offer the same bit rate as the LTE network. In other words, for any location of a UE in the cellular network, there is an AP that can deliver a bit rate at least equal to R (i.e. the bit rate required by the user). Note that the study can be easily extended by integrating a probability of coverage by an AP in the analysis. In very tight coupling, there is no need for WiFi specific security mechanisms. Hence, the attachment between the UE and the APs does not require any authentication key. We thus assume that the association time is negligible.

5.2.3 Approach of the analysis

The objective of the study is to compute the amount of resources that can be spared when a UE is served by a WiFi AP instead of the cellular network. Thus, we consider a UE at a given location and assume that a WiFi AP with enough capacity is close to the UE. The analysis is valid for both downlink and uplink.

We first compute the offload probability, which is the probability that the UE and the detected AP are connected to the same BS. Then we compute the SINR of a UE connected to the considered BS. We deduce the distribution of the SINR. After

that, we compute the mean saved bandwidth which is a function of the SINR. For any random variable X, we denote by $F_X(t)$ the cumulative distribution function (CDF) of X, by $\overline{F}_X(t)$ its complementary cumulative distribution function (CCDF), by $f_X(t)$ its probability distribution function (PDF) and by $E[X]$ its expectation.

5.3 Performance analysis

Without loss of generality, we study the zone between two contiguous cells formed by two transmitting BSs: BS 0 and BS 1. This zone is a diamond as shown in Fig.5.2. For the sake of simplicity, we suppose that all UEs on the shaded area receive the same power from all base stations when they are at the same distance from BS 0. Thus, we consider only the case of a UE located on the straight line between BS 0 and BS 1 (Fig.5.2). A similar approach was used in [90].

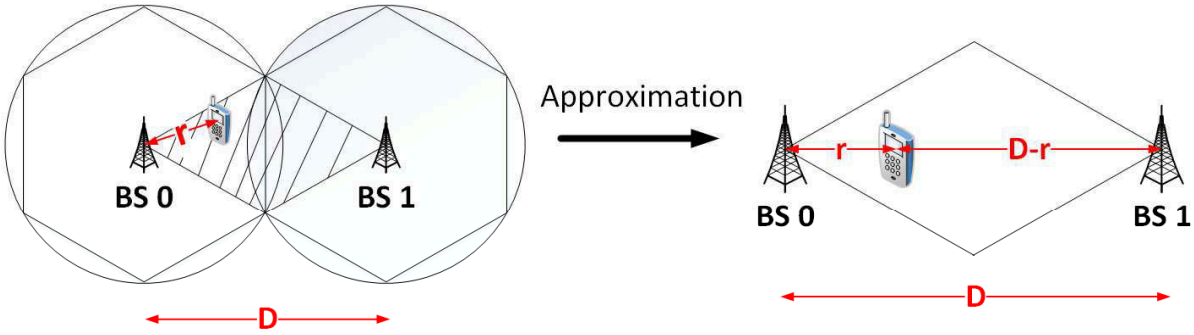


Figure 5.2: Hexagonal cellular network with only two Base Stations

5.3.1 Offload probability

We first compute the probability $p_0(r)$ that the data traffic generated by a UE at distance r from BS 0 can be offloaded. In very tight coupling, offload is only possible if both the UE and the AP are connected to the same BS. Since APs are connected to the nearest BS (e.g. BS 0), $p_0(r)$ is the probability that a UE at a distance r is connected to BS 0.

It is worth noting that in the *single-eNB coupling*, we are only interested about UEs located at $r < D/2$ as they are the only ones that can be offloaded. Since there are only two base stations in the analytical model, $p_0(r)$ for a given UE is the probability that this UE receives a signal from the nearest base station (i.e. BS 0) larger than the one received from the other base station (i.e. BS 1): $p_0(r) = \mathbb{P}(P_0 >$

P_1). This probability is given for $r_0 < r < D - r_0$ by:

$$p_0(r) = \mathbb{P}\left(\xi_0 - \xi_1 > \frac{10}{\sigma}\alpha \log_{10}\left(\frac{r}{D-r}\right)\right).$$

Note that $\xi_0 - \xi_1$ is a normal variable with a standard deviation equals to $\sqrt{2}$. Hence, $p_0(r)$ is equal to:

$$p_0(r) = \frac{1 + \text{erf}\left(\frac{10\alpha}{2\sigma \ln 10} \ln\left(\frac{D}{r} - 1\right)\right)}{2}. \tag{5.9}$$

When $r < r_0$ (i.e. the UE is very close to BS 0), the power received from BS 0 is equal to $P_t 10^{\xi_0 \sigma/10}$ according to (5.3) and $p_0(r)$ is computed in a similar way:

$$p_0(r) = \frac{1 + \text{erf}\left(\frac{10\alpha}{2\sigma \ln 10} \ln\left(\frac{D-r}{r_0}\right)\right)}{2}. \tag{5.10}$$

When $r > D - r_0$, $p_0(r)$ is:

$$p_0(r) = \frac{1 + \text{erf}\left(\frac{10\alpha}{2\sigma \ln 10} \ln\left(\frac{r_0}{r}\right)\right)}{2} \tag{5.11}$$

Finally, for all values of r, $p_0(r)$ is :

$$p_0(r) = \begin{cases} \frac{1}{2} + \frac{1}{2}\text{erf}\left(a\alpha \ln\left(\frac{D-r}{r_0}\right)\right) & \text{if } r < r_0 \\ \frac{1}{2} + \frac{1}{2}\text{erf}\left(a\alpha \ln\left(\frac{D}{r} - 1\right)\right) & \text{if } r_0 < r < D - r_0 \\ \frac{1}{2} + \frac{1}{2}\text{erf}\left(a\alpha \ln\left(\frac{r_0}{r}\right)\right) & \text{if } r > D - r_0 \end{cases} \tag{5.12}$$

with $a = \frac{5}{\sigma \ln(10)}$.

$$f_{W|r}(w) = \begin{cases} 0 & \text{if } w > R \\ K \frac{\exp\left(\frac{R \ln 2}{w}\right) \exp\left(-a^2(\alpha \ln(\frac{D-r}{r_0}) - \ln(\exp(\frac{R \ln 2}{w}) - 1))^2\right)}{w^2(\exp\left(\frac{R \ln 2}{w}\right) - 1))(1 + \text{erf}\left(a\alpha \ln(\frac{D-r}{r_0})\right))} & \text{if } w < R \text{ and } r < r_0 \\ K \frac{\exp\left(\frac{R \ln 2}{w}\right) \exp\left(-a^2(\alpha \ln(\frac{D-r}{r}) - \ln(\exp(\frac{R \ln 2}{w}) - 1))^2\right)}{w^2(\exp\left(\frac{R \ln 2}{w}\right) - 1))(1 + \text{erf}\left(a\alpha \ln(\frac{D-r}{r})\right))} & \text{if } w < R \text{ and } D - r_0 < r < r_0 \\ K \frac{\exp\left(\frac{R \ln 2}{w}\right) \exp\left(-a^2(\alpha \ln(\frac{r_0}{r}) - \ln(\exp(\frac{R \ln 2}{w}) - 1))^2\right)}{w^2(\exp\left(\frac{R \ln 2}{w}\right) - 1))(1 + \text{erf}\left(a\alpha \ln(\frac{r_0}{r})\right))} & \text{if } w < R \text{ and } r > D - r_0 \end{cases} \tag{5.13}$$

5.3.2 Distribution of the SINR at a given distance

Here, we compute the SINR of a UE at distance r that is connected to BS 0. We first assume that BS 1 is the most interfering base station; the BS that generates

the highest interference. Hence, the SINR of a UE connected to BS 0 is the ratio between the two powers received respectively from BS 0 and BS 1. Its CCDF $\overline{F}_{\gamma|r}(x)$ when $x \geq 1$ is:

$$\begin{aligned}\overline{F}_{\gamma|r}(x) &= \mathbb{P}(\gamma > x/P_0 > P_1) \\ &= \frac{\mathbb{P}(P_0 > P_1 x)}{\mathbb{P}(P_0 > P_1)}.\end{aligned}$$

Note that $\overline{F}_{\gamma|r}(x) = 1$ when $x < 1$. Since we already suppose that the UE is connected to BS 0, which is the best server, the power received from BS 0 is larger than the power received from BS 1. That means that the SINR is always bigger than 1.

We first compute the probability $\mathbb{P}(P_0 > P_1 x)$ when $r_0 < r < D - r_0$ and $x > 1$:

$$\begin{aligned}\mathbb{P}(P_0 > P_1 x) &= \mathbb{P}\left(P_t \left(\frac{r_0}{r}\right)^{\alpha} 10^{\xi_0 \sigma/10} > x P_t \left(\frac{r_0}{D-r}\right)^{\alpha} 10^{\xi_1 \sigma/10}\right) \\ &= \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{10}{2\sigma}\log_{10}\left(\frac{(D-r)^{\alpha}}{x r^{\alpha}}\right)\right)\right).\end{aligned}$$

Similarly, it is easy to show that when $r < r_0$:

$$\mathbb{P}(P_0 > P_1 x) = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{10}{2\sigma}\log_{10}\left(\frac{(D-r)^{\alpha}}{x r_0^{\alpha}}\right)\right)\right)$$

and when $r > D - r_0$, $\mathbb{P}(P_0 > P_1 x)$ is:

$$\mathbb{P}(P_0 > P_1 x) = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{10}{2\sigma}\log_{10}\left(\frac{r_0^{\alpha}}{x r^{\alpha}}\right)\right)\right).$$

5.3.3 Distribution of the bandwidth required for a given rate

The required bandwidth W to carry a traffic with a rate equal to R can be computed using (5.8). The CDF of W for a given rate R is thus:

$$\begin{aligned}F_{W|r}(w) &= \mathbb{P}\left(\frac{R}{\log_2(1+\gamma)} < w\right) \\ &= \mathbb{P}\left(\gamma > \exp\left(\frac{R \ln 2}{w}\right) - 1\right).\end{aligned}$$

Note that the bandwidth is an inverse function of the SINR. Thus, the CDF of W can be written using the CCDF of the SINR γ:

$$F_{W|r}(w) = \overline{F}_{\gamma|r}\left(\exp\left(\frac{R\ln 2}{w}\right) - 1\right). \tag{5.14}$$

Since the bandwidth is at most equal to the bit rate R, $F_{W|r}(w)$ is equal to 1 for values of w larger that R. Next, we can deduce the PDF of W for $w \leq R$:

$$\begin{aligned} f_{W|r}(w) &= \frac{dF_{W|r}(x)}{dw} \\ &= \left(\frac{R\ln(2)}{w^2}\right)\exp\left(\frac{R\ln(2)}{w}\right) f_{\gamma|r}\left(\exp\left(\frac{R\ln 2}{w}\right) - 1\right) \end{aligned}$$

$f_{W|r}(w)$ is given for all values of w and r in (5.13) with $K = \frac{2Ra\ln(2)}{\sqrt{\pi}}$.

5.3.4 Computation of the offloaded capacity

In this section, we compute how much capacity can be spared for single and *total-eNB coupling*. We consider the case of two contiguous BSs as shown in Fig.5.2. Note that in this case, a *double-eNB coupling* is equivalent to a *total-eNB coupling*.

5.3.4.1 Single-eNodeB coupling

In this scenario APs are only connected to the nearest BS. Thus, a UE can offload only if it is also connected to the nearest one, i.e the distance to its serving BS is lower than $D/2$. Thus, the mean saved bandwidth in the considered area is computed by introducing the offload probability that is given by (5.12) and a user density denoted by ρ.

$$E[W] = \int_{r=0}^{\frac{D}{2}}\int_{w=0}^{R}\int_{\theta=-\frac{\pi}{6}}^{\frac{\pi}{6}} \rho p_0(r) f_{W|r}(w) r w dr dw d\theta. \tag{5.15}$$

On the other hand, we also compute the mean number of users connected to BS_0 in the whole area (i.e the diamond in Fig.5.2):

$$E[N] = \int_{r=0}^{D}\int_{\theta=-\beta}^{\beta} \rho p_0(r) r dr d\theta \tag{5.16}$$

where β is a parameter that can easily be deduced (see Fig.5.3):

$$\beta = \begin{cases} \frac{\pi}{6} & \text{if } r < \frac{D}{\sqrt{3}} \\ \arcsin\left(\frac{\frac{D}{2}}{r}\right) - \frac{\pi}{6} & \text{if } r > \frac{D}{\sqrt{3}} \end{cases} \tag{5.17}$$

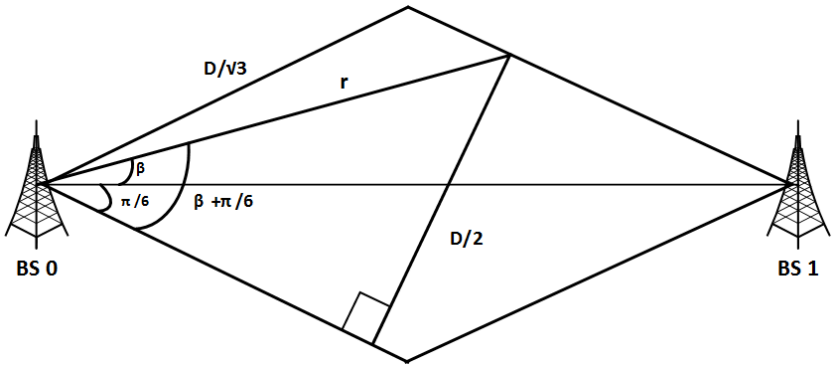


Figure 5.3: Computation of parameter beta

The mean saved bandwidth per user $E_N[W]$ is defined as the ratio of the mean saved bandwidth given by (5.15) and the mean number of users (5.16). It can be simplified as:

$$E_N[W] = \frac{\int_{r=0}^{\frac{D}{2}} \int_{w=0}^{R} p_0(r) f_{W|r}(w) r w dr dw}{\int_0^{\frac{D}{\sqrt{3}}} p_0(r) r dr + \int_{\frac{D}{\sqrt{3}}}^{D} (\frac{6}{\pi} \arcsin(\frac{D}{2r}) - 1) p_0(r) r dr}. \tag{5.18}$$

Note that $E_N[W]$ does not depend on the user density ρ.

5.3.4.2 Total-eNodeB coupling

This scenario assumes that APs are connected to all BSs and that the offload is always possible for an UE whatever its distance from its serving BS. Hence, the mean saved bandwidth is similar to the previous case but considers the mean bandwidth used in the whole area:

$$E[W] = \int_{r=0}^{D} \int_{w=0}^{R} \int_{\theta=-\beta}^{\beta} \rho p_0(r) f_{W|r}(w) r w dr dw d\theta. \tag{5.19}$$

The mean saved bandwidth per user is computed the same way as in (5.18).

5.4 Simulation methodology

We consider the same hexagonal model as described in section 5.2 composed of 31 base stations (i.e. 30 interfering BSs) and UEs uniformly distributed. Monte Carlo based simulation are performed for 10^5 snapshots. As for the mathematical model, we consider a classic Okumura-Hata model [88][91] for propagation where the path loss at a given location r ($L_u(r)$) is computed as follows:

$$L_u(r) = 69.55 + 26.16\log(f) - 13.82\log(h_b) - 3.2\left[\log(11.75h_m)\right]^2 - 4.97 + \left[44.9 - 6.55\log(h_b)\right]\log(r) \quad (5.20)$$

where f is the frequency in MHz, h_b is the height of the eNodeB antenna, h_m is the height of the UE antenna and r the distance between the UE and the eNodeB. Table (5.1) summarizes the simulation parameters. We choose $f = 900$MHz, $h_m = 1.5$m and $h_b = 32$m. We deduce α from (5.20) and take $r_0 = 3 \times 10^{-4}$ (r_0 is such that $L_u(r_0) = 0$). For each UE, the power of the signal received from each BS is computed and the SINR is deduced. Then, we compute the mean bandwidth for a given bit rate using the Shannon formula (5.8).

We compute the offload probability in *single-eNB coupling* as the number of UEs that are connected to the nearest BS divided by the total number of users. Similarly, in the *double-eNB coupling* scenario the offload probability is the ratio between the number of UEs that are either connected to the nearest BS or to the second nearest BS and the total number of UEs. For each scenario, we deduce the mean offload bandwidth using the probability computed.

5.5 Results

We present and discuss the results obtained with the mathematical model and by simulations.

5.5.1 Mathematical model

Fig.5.5 shows the mean saved bandwidth per user for different values of the shadowing standard deviation σ for the two studied scenarios. Fig.5.4 shows the ratio of the mean saved bandwidth when the APs are connected to only one BS. In the absence of shadowing (i.e. $\sigma = 0$dB), all the traffic can be offloaded in both cases and the same amount of bandwidth can be saved in the two scenarios. This can observed in

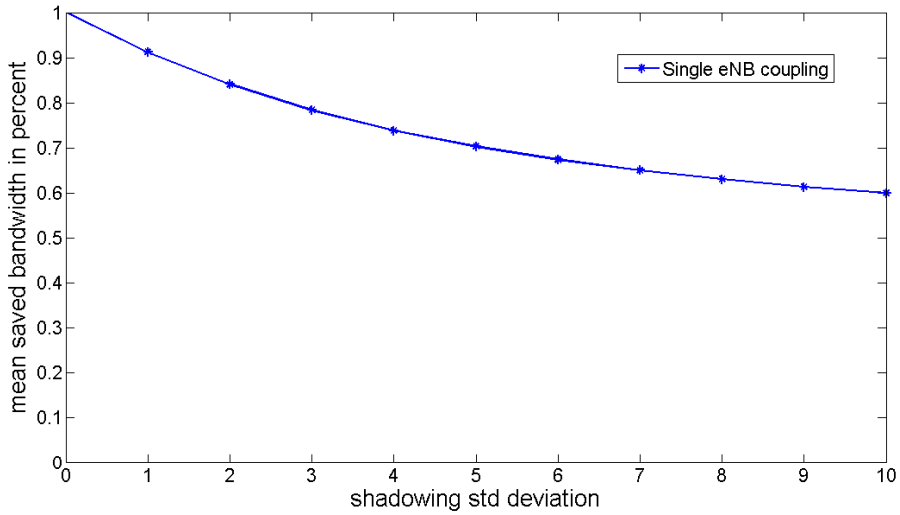


Figure 5.4: Reduction of the offload capacity when the APs are connected to a limited number of BSs (analytical model)

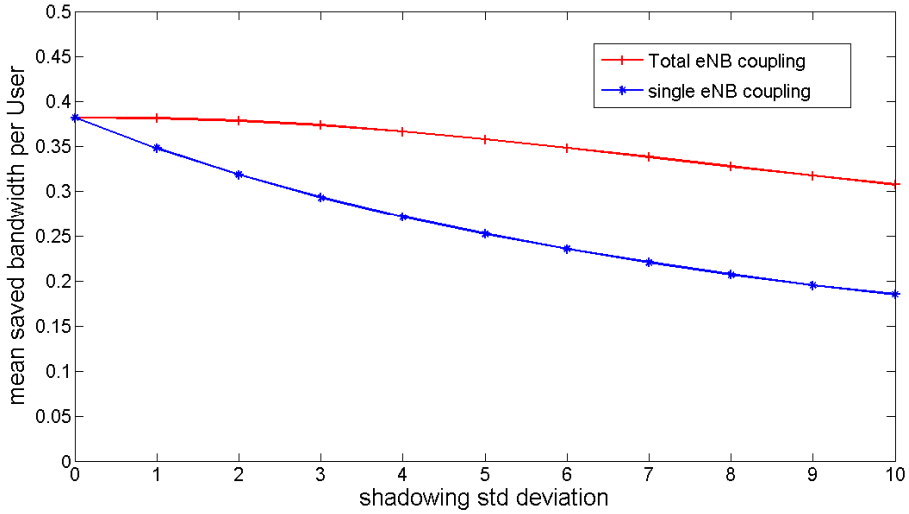


Figure 5.5: Mean saved bandwidth vs. shadowing std deviation (analytical model)

Fig.5.5. When the shadowing increases, UEs have less chances to be connected to the nearest BS and then less chances to be offloaded in a *single-eNB coupling* case. In *total-eNB coupling*, more bandwidth can be saved compared to the first scenario since even the UEs that are outside the hexagonal cell and connected to BS 0 can be offloaded. Besides, the farther a UE is from its serving BS the more bandwidth it consumes, which means that more capacity can be spared in the *total-eNB coupling* case.

We only considered here two BSs and only UEs that are present in the diamond

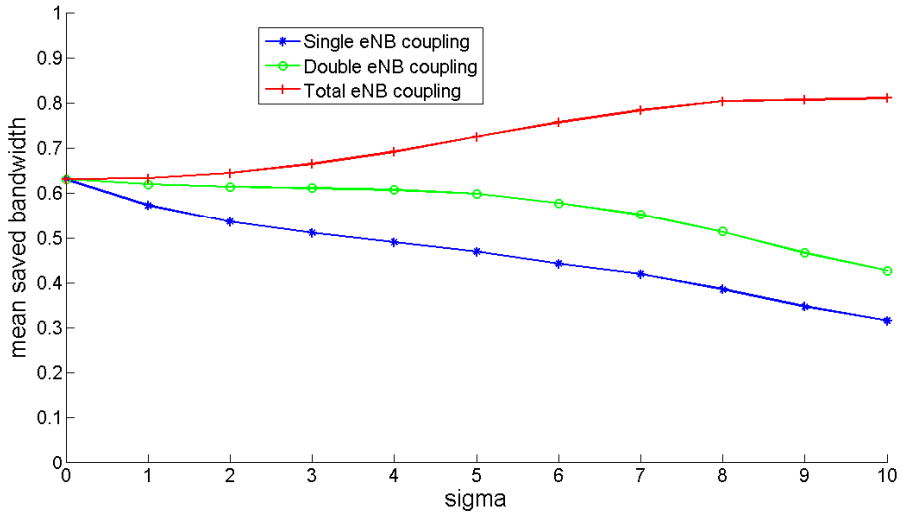


Figure 5.6: Mean saved bandwidth vs. shadowing std deviation (simulation)

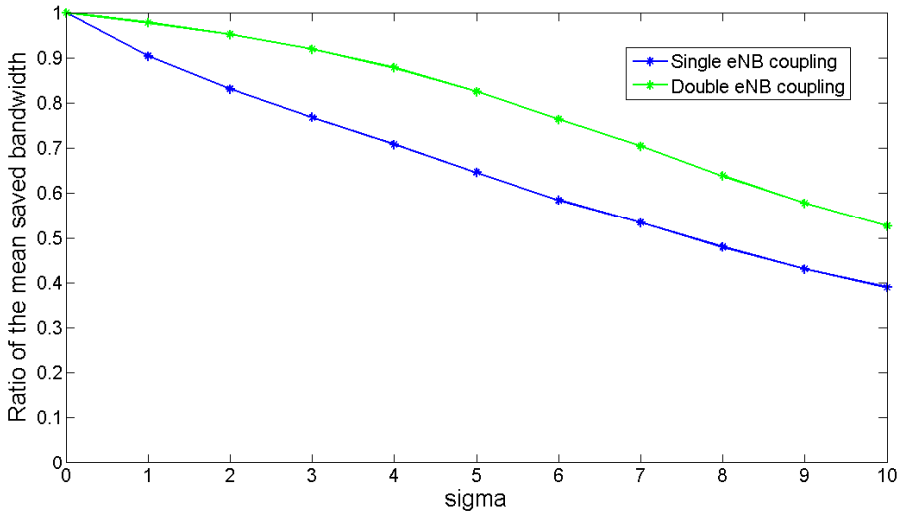


Figure 5.7: Reduction of the offload capacity when the APs are connected to a limited number of BSs (simulation)

area (Fig.5.2). However in a real scenario and in presence of a high shadowing, the UEs that are actually connected to BS 0 can be far outside the considered area, which involves an increase of the total consumed bandwidth. This explains the decrease of the saved capacity in the *total-eNB coupling* case instead of an increase.

5.5.2 Simulation

In this section, the results obtained by simulation are presented. Fig.5.6 illustrates the mean saved bandwidth as a function of the standard deviation of the shadowing effect for the three scenarios. Fig.5.7 shows the ratio of the mean saved bandwidth for single and *double-eNB coupling*. We first see on Fig.5.6 that for a very low

Parameter	values
nb of snapshots	10^5
nb of BSs	31
σ (dB)	$[0:10]$
Intersite distance D (km)	1
bit rate R (Mbps)	1
r_0 km	3×10^{-4}
α	3.5

Table 5.1: Monte Carlo simulation parameters

shadowing, the three scenarios give approximately the same results. In the absence of shadowing UEs are always connected to the nearest BS and the offloading is possible in the three scenarios. This is why about 100% of the bandwidth can be spared (see Fig.5.7). As shadowing increases, UEs have less chances to be connected to the nearest BS and then less chances to offload in the single and *double-eNB coupling* case. In *total-eNB coupling*, the saved bandwidth increases with the shadowing, which can be explained by looking at the SINR CDF (Fig.5.8).

The SINR CDF is plotted for two values of σ (3dB and 8dB). We can see that there are more users with a low SINR when the shadowing is high compared to UEs with a good SINR. For instance, only 5% of the users have an SINR equals to 2dB for a 3dB-shadowing while there are almost 7% for a 8dB-shadowing. This means that the higher is the shadowing, the more bandwidth-consuming UEs there are, which explains the increase in *total-eNB coupling* observed in Fig.5.6.

5.5.3 Analysis

Tab.5.2 shows the offloaded capacity for three typical values of the shadowing standard deviation in case of non-total coupling. When the shadowing is low (i.e. 3dB), a large amount of the capacity (i.e. 75%) can be spared in the case of *single-eNB coupling*. We can obtain the same performance with a *double-eNB coupling* for a 6dB-shadowing while only 57% of the bandwidth can be saved for the *single-eNB coupling* in this case. If the shadowing is high (i.e. 8dB) less then the half of the

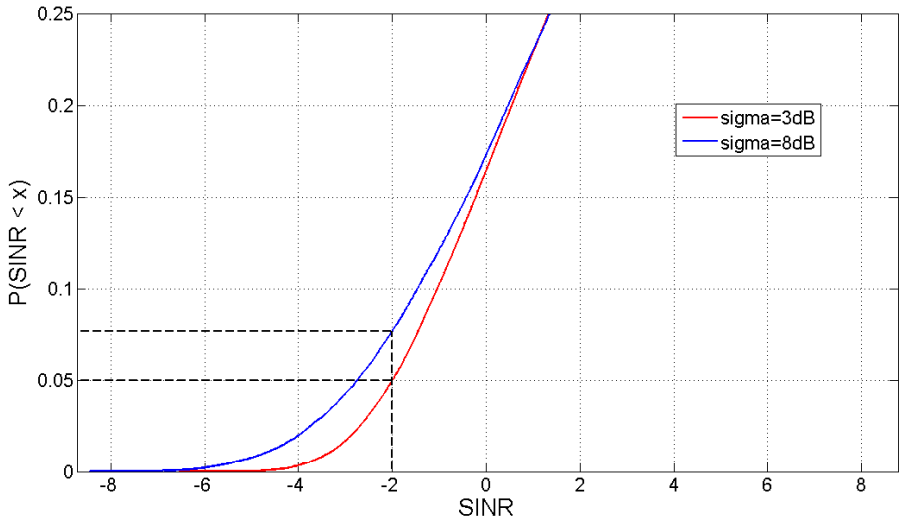


Figure 5.8: CDF of the SINR

bandwidth can be offloaded in *single-eNB coupling* and only 64% in *double-eNB coupling*.

	single-eNB coupling	double-eNB coupling
$\sigma = 3$dB	75%	92%
$\sigma = 6$dB	57%	75%
$\sigma = 8$dB	47%	64%

Table 5.2: Proportion of the offloaded capacity in case of non-total coupling for two values of shadowing

For a low shadowing, we consider that *single-eNB coupling* is sufficient and there is no need to connect all APs to more than one eNodeB. However, when shadowing is high, *a double-eNB coupling* is necessary. For instance, a high shadowing can be seen as a typical scenario where terminals are indoor and APs deployed inside buildings, WiFi can thus provide a better indoor coverage and a higher throughput than the LTE network. In this case, it is interesting for the operator to connect the APs to two eNodeBs covering that area in order to increase the offload probability and to spare more capacity.

5.6 Conclusion

In this chapter, we studied mathematically the performance of very tight coupling architecture between LTE and WiFi for offloading. We propose an analytical model

and compute the mean bandwidth that can be saved when WiFi is used instead of LTE in three scenarios:*single-eNB coupling*, *double-eNB coupling* and *total-eNB coupling*. We show, using Monte Carlo simulations, that for a low shadowing, connecting the APs to the nearest eNodeB, i.e. a *single-eNB coupling*, is enough and there is no need to for a *double-eNB coupling*.

In this study, we used mathematical tools to analyze the performance of Very Tight Coupling. However, Very Tight Coupling has never been implemented and deployed by operators, and it is still only a proposition. An interesting work would be to study the feasibility of Very Tight Coupling by proposing proof-of-concept. This would allow to have more thorough studies with real LTE and WiFi parameters.

Chapter 6

Experimental Evaluation

6.1 Introduction

In the last chapter, we performed a mathematical study of Very Tight Coupling in which we focused on the bandwidth that can be saved for different coupling schemes. The results were promising and showed that offloading to WiFi in Very Tight Coupling can be very helpful for operators to save capacity especially in case of high shadowing. In this chapter we go a bit further and demonstrate the feasibility of Very Tight Coupling. We implement the architecture on a platform with a real LTE radio-link and perform experiments to study the performance in a real-time environment. Typically, we study how link-layer protocol should be configured the and the impact of the delay on the WiFi and LTE radio links.

6.2 Presentation of the testbed

In this section, we describe the testbed on which we performed the different experiments. We chose to use Open Air Interface (OAI) framework as it has a real-time mode, which allows to do more realistic tests with a real radio interface. Moreover, OAI is open source and is thus the most suitable software to implement Very Tight Coupling on it. We first briefly introduce OAI and the different functions it offers, and then give details about our testbed .

6.2.1 Open Air Interface

Open Air Interface framework (OAI) [92] is an open source software developed by Eurecom that proposes a complete implementation of a release 10 LTE network

including the entire protocol stacks of the E-UTRAN and the LTE EPC.

One important aspect of OAI is that it can be used in a real-time mode with real LTE radio channel. Radio Frequency cards such as National Instruments/Ettus Universal Software Radio Peripheral (USRP) or Eurecom ExpressMimo are needed. OAI can also be used in a simulation mode. In this case, it can run either with a full physical layer and a simulated radio interface, or with the abstraction of the physical layer. In both cases, the full protocol stack is executed as it is in the real time mode.

In addition to the radio access part, OAI can run a complete LTE EPC network. This includes the different EPC entities: SGW, PGW and MME, and the HSS database. This provides an IP connectivity to the UE allowing it to access external IP networks normally.

We found OAI as the most suitable software to prototype and test Very Tight Coupling. On the one hand, OAI includes the entire LTE protocol stack of the E-UTRAN, including the PDCP layer, which is the most important block in Very Tight Coupling. On the other hand, OAI is open source and developed in a simple C language, which allows us to easily develop and integrate Very Tight Coupling code. Finally, the real-time mode of OAI allows us to experiment and see the behavior of Very Tight Coupling in a realistic environment.

6.2.2 Testbed

Our testbed consists of three nodes (see Fig.6.1) denoted by PC1, PC2 and PC3:

- PC 1 runs an OAI LTE UE using a USRP B210 radio card. It also include a WiFi network interface allowing a maximum bit rate of 150Mbps.
- PC 2 runs an OAI LTE eNodeB using a USRP B210 radio card.
- PC 3 is used as a CeAP. We emulate a real WiFi AP using the linux hostapd tool [93]. It broadcasts a specific SSID, and does not use any WiFi security mechanisms. The hostapd tool supports layer 2 bridging. Thus, in line with the architecture we defined in chapter 4, we configured the CeAP as a WiFi layer 2 bridge, connecting the WiFi network to the Ethernet network. Thus, the CeAP is totally transparent in the different communication between the UE and the eNodeB, which have the impression to be directly connected to each others over a layer 2 network. For the hardware, we use the same network interface as the one used for the UE.

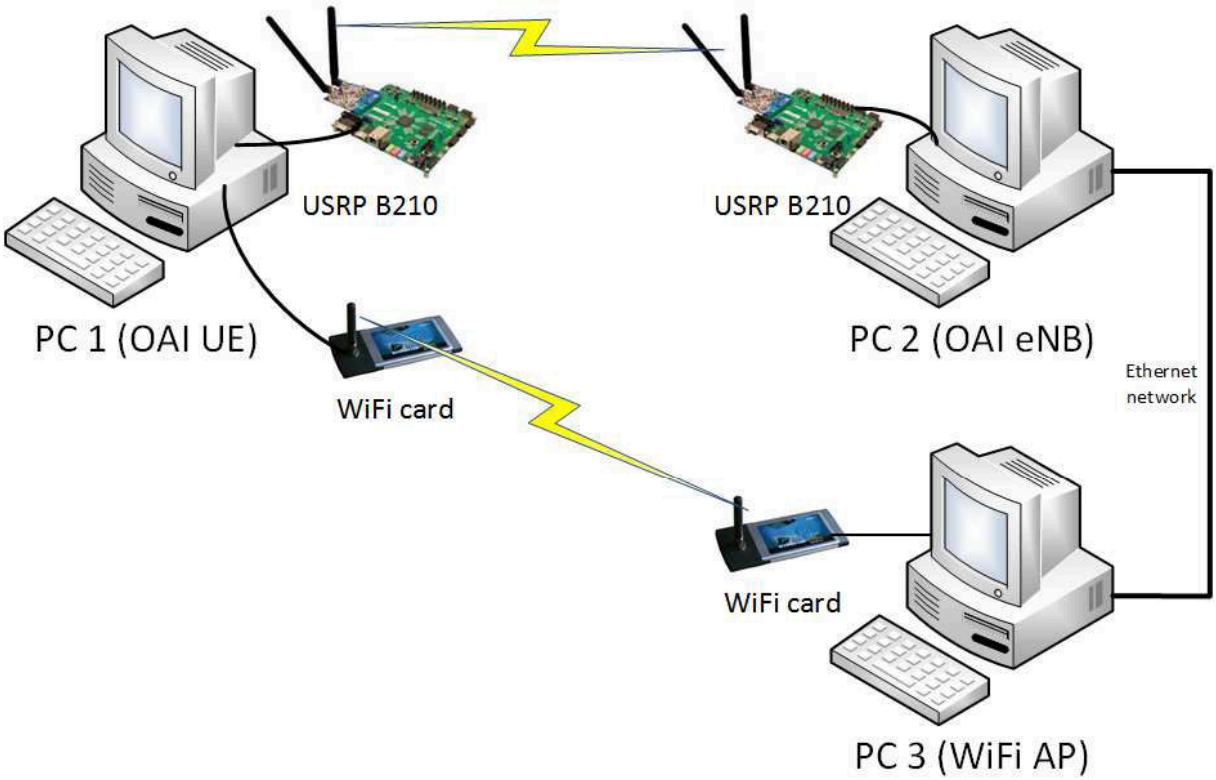


Figure 6.1: Testbed used for experimentation

Regarding LTE, we use FDD mode with 5MHz of bandwidth. At the RLC layer, we use the Unacknowledged Mode (UM) of RLC, which was the much stable in OAI compared to the Acknowledge Mode (AM). Hence, this may introduce some losses on LTE. As OAI is still under development, the achievable throughput on the LTE connection is limited. In our installation, we could reach 2Mbps on the downlink. Note that all these information concern an older OAI version compared to the one in use today. As OAI is always being enhanced, all these parameters are not necessary still the same. Finally, Very Tight Coupling concerns mostly the radio part, we thus don't use the OAI EPC. In this case, OAI attributes fixed IP addresses to both the eNodeB and the UE.

The Ethernet network connects the eNodeB to the CeAP and is thus considered as the aggregation network. It provides a 100Mbps bit rate and the delay to cross it is very low, i.e. less than 1ms. Thus, it does not have any impact on the obtained results. However, it is worth noting that the delay is higher in a real aggregation network depending on the distance and number of equipment to cross between the eNodeB and the CeAP.

As most of today applications are based on TCP, we chose this protocol for our

experiments. TCP is a reliable transport protocol, which relies on acknowledgement (ack) and retransmissions to ensure the good reception of all packets. It uses a transmitting window that indicates how much packets should be sent before waiting for an ack. The main idea of TCP is to continuously increase its bit rate, by increasing the size of the window until a congestion is detected, and to reduce it aggressively when this happens. TCP uses a Retransmit Timeout (RTO) to detect losses. Specifically, the RTO is started when a packet is sent and if no acknowledgement has been received after its expiration, the packet is considered as lost and is retransmitted. TCP has also a congestion control algorithm that is used to avoid network saturation when a congestion is detected. Typically, TCP considers the network as congested when a loss is detected, i.e. when the RTO expires. The RTO is computed using the past Round Trip Time (RTT) values. When it expires, the RT0 is increased to RT0∗2.

There are several versions of TCP that implement different congestion control algorithms. In our experiments, we use the default version provided with the linux kernel, which uses CUBIC congestion control algorithm [94] with Selective Acknowledgment (SACK) extension [95]. The idea of CUBIC is to aggressively the congestion control window when it is far from saturation point, and slowly when it get closer. This allows CUBIC to provide good performance for high bandwidth networks.

In the version of OAI that we used in our experiments, the uplink data channel is not stable, which induced a high loss rate. The uplink is only used for TCP acknowledgement. However, a lost packet would force TCP to reduce its bit rate, which does not reflects the real throughput of the network. We thus decided to always send acknowledgement over WiFi.

In our study, we are interested in the downlink performance. Thus, we install a TCP server waiting for connections in the UE using the iperf linux tool [96]. Then, we install a source at the eNodeB that connects to the UE and generates TCP traffic using iperf. We monitor the achieved throughput at the UE. Note that iperf works at the application layers and gives the goodput, i.e. throughput at the application.

6.2.3 Implementation of Very Tight Coupling

Our implementation of very tight coupling consists of different modules that we developed and integrated to the OAI source code. In the following, we present each module and show how it interacts with OAI code. We also speak about the features of Very Tight Coupling that we did not implement and that we did not consider in

our study.

WiFi Integration module

The *WiFi Integration module* is the main block of Very Tight Coupling that allows OAI to use the WiFi Interface. It includes the *wifi_rx_thread*, i.e. a process running in parallel with the main program, that listens continuously on the WiFi interface and which is responsible for receiving WiFi traffic. It also includes the *wifi_tx_thread*, which is responsible for transmitting the out-going frames to the WiFi network interface.

The module also includes the adaptation sub-header that is added to allow transportation of PDCP PDUs over WiFi. Moreover, it consists of different functions used to build and send WiFi 802.11 frames over the WiFi interface.

Interface selection module

The *interface selection module* is integrated to the PDCP layer. It allows it to choose for each outer PDCP PDU on which interface it should be sent, i.e. WiFi or LTE, according to the selected policy.

PDCP reordering module

We extend the PDCP reordering feature used for the bearer split scenario (see section 2.3.3) to the LTE/WiFi coupling case. The *PDCP reordering module* includes a buffer used to store inner PDUs, a reordering function and a timer.

When this module is activated, the reordering function checks for each in-coming PDU if it has the correct sequence number and that the previous one has been already received. If this condition is verified, the PDU is delivered to the upper layer, otherwise it is stored in the buffer. If the buffer is empty, a timer is started. When the timer expires, all PDUs in the buffer are delivered. This avoids to have PDUs stored indefinitely in case a PDU was lost. In our experiments, we calibrated the timer value as such to equal twice the mean RTT of the worst link (i.e. LTE).

Fixed parameters

There are some functions of Very Tight Coupling that we did not implement. These function are listed in the following:

WiFi Initialization procedure In Very Tight Coupling, the *WiFi initialization procedure* is the first for the UE to be able to use a CeAP. We did not implement

this procedure, and consider that the UE is always connected WiFi. However, in some cases the UE should use only LTE. Thus, we have a specific policy that indicates that the UE is in LTE-only mode and should not use the WiFi network.

Decision engine In Very Tight Coupling, the *decision engine* computes the policies using the different measurements it gets from the UE and CeAP. We did not implement it in our study, and use instead fixed policies.

Policies We consider in our experiments fixed policies. Typically, a variable is used to indicate to the *selection interface module* what is the current policy.

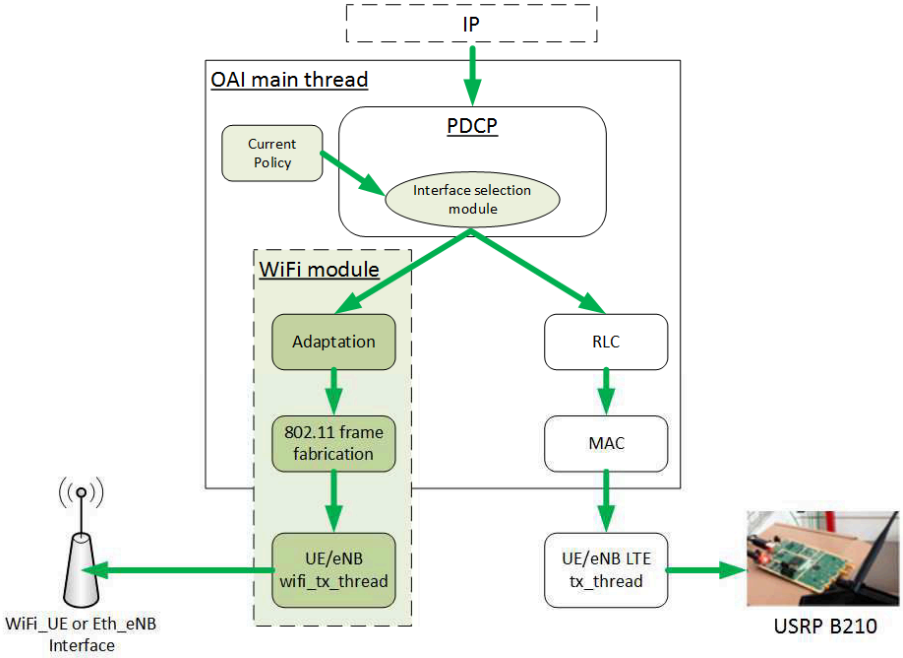
Interaction of Very Tight Coupling with OAI code

Fig.6.2 shows how the different modules interacts with each others and with OAI code. Very tight coupling specific modules are highlighted in a different color. In the transmission way (TX) (see Fig.6.2a), IP packets arriving at the OAI main thread, go first through standard PDCP processing (i.e. cyphering, adding header). Then, the *interface selection module* in PDCP selects on which interface to send the PDU, according to the current policy. When LTE is selected, the PDU is processed by OAI code and follows the usual LTE stack, i.e. RLC/MAC. It is then transmitted to the lte_tx_thread that is responsible for PHY procedures and transmission over the radio through the USRP B210 card. In case the *interface selection module* has selected the WiFi interface, the PDU is sent to the *WiFi module*, which adds the adaptation and the 802.11 header. The resulting frame is then transmitted to the *wifi_tx_thread* that is responsible for sending it to the WiFi interface.

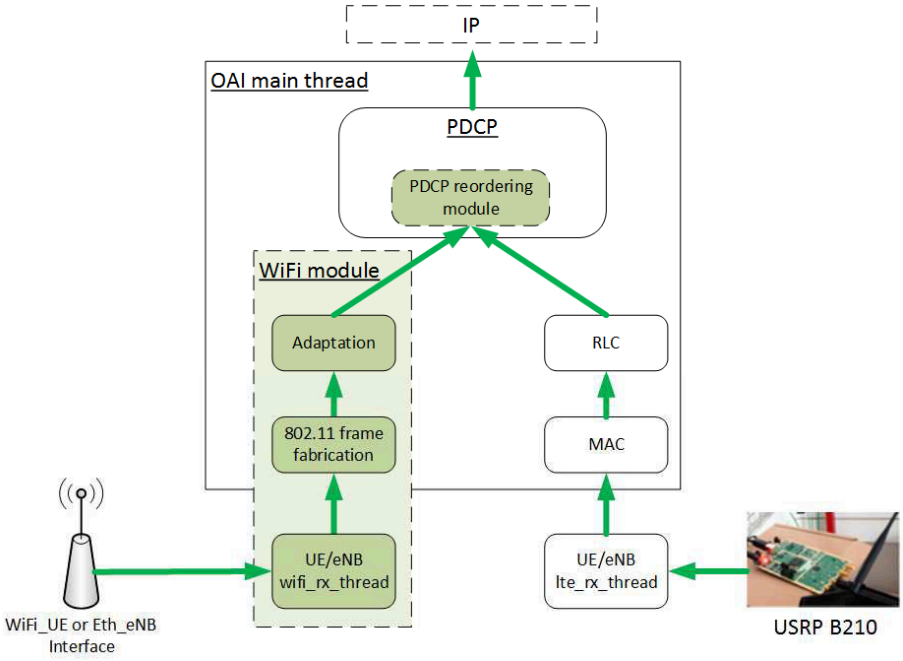
In the reception way (RX) (see Fig.6.2b), LTE processing is done by OAI, while WiFi received frames are processed by the *WiFi module*. In both cases, the received traffic terminates at PDCP. When activated, the *PDCP reordering module* processes the PDU before delivery to IP.

6.3 Experimental evaluation

In this section, we experimentally evaluate the performance of Very Tight Coupling. We first present the methodology that we followed in our experiments. We describe the different policies that we defined for the evaluation. Finally, we present and discuss the results obtained for each type of experiment.



(a) Transmission (TX)



(b) Reception (RX)

Figure 6.2: Very Tight Coupling modules interaction in OAI

6.3.1 Methodology

We assume that the UE is always under the eNB coverage and never looses LTE connectivity. Each experiment consists of series of 70 seconds over which the source

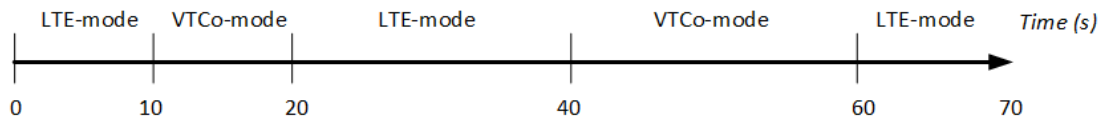


Figure 6.3: Very Tight Coupling: division of the experiment duration

eNodeB in the eNodeB first establish a TCP connection to the server that is installed in the UE, and starts generating traffic until the end of the experiment. We are interested to the case of moving users that are always connected to LTE and that stays only few seconds into a CeAP vicinity. We thus suppose that at two moments, the UE becomes in VTCo-mode for different duration, i.e. between second 10 and second 20, and between second 40 and second 60. During these periods, the traffic is sent over WiFi only or in parallel with LTE, depending on the selected policy. For the rest of the time, LTE is used normally. As defined in Very Tight Coupling, the control plane is always sent over LTE, and only the data plane is concerned by the policy changing. For the rest of this chapter, we call VTCo-periods the two periods the UE is in VTCo-mode, and call the others LTE-periods.

We define three main indicators that we use in the analysis:

- The mean global throughput in Mbps: corresponds to the throughput computed over the whole experiment (i.e. over the 70 seconds);
- The mean throughput when WiFi is activated: this is the achieved throughput during the two VTCo-periods, whatever the selected policy;
- The mean LTE throughput: this indicator corresponds to the throughput obtained over LTE only, i.e. the LTE-periods.

For each study, we first give the evolution of the achieved throughput in order to study the behavior of TCP. Then, we perform a series of 20 experiments. We compute on each experiment the mean of each indicator. Finally, we compute the mean and the standard deviation over the 20 experiments.

We defined two policies for our study. As we did not implement a dynamic modification of policies, we fix this parameter for each series of experiment. These policies are described in the following.

Full LTE-offload policy

In the *Full LTE-offload policy* corresponds to a scenario in which the network decides to completely offload the eNodeB to the CeAP. In this case, the data plane is sent

over WiFi during the two VTCo-periods, while the control plane is kept over LTE.

LTE/WiFi aggregation policy

In the *LTE/WiFi aggregation policy*, the data plane is split over LTE and WiFi during the VTCo-periods. In our experiments, we sent one PDU on two over WiFi. However, due to the LTE link instability and high loss rate, we only send over LTE if the RLC transmitting buffer is empty. This avoids having additional delays caused by the buffer. In practice, the average percentage of packets transmitted over WiFi is closer to 65%.

6.3.2 Impact of the delay

LTE and WiFi have very different characteristics in terms of delays and achievable throughputs. This is due to several aspects: for instance the resources are assigned by the network in LTE while they are competitively shared between users in WiFi. This might cause issues when one tries to use the two networks simultaneously, which is the case of the *LTE/WiFi aggregation policy*.

In this experiment, we study what would be the impact of a large difference between the delays on the WiFi and LTE links. We thus perform two sets of experiments: in the first one the delays on the two links are similar. In the second one, we throttle WiFi bandwidth to 4Mbps and introduce a delay of 200ms to the WiFi link, using the linux traffic control (tc) [97] and Network Emulator (netem) [98] tools. As we use the WiFi uplink for TCP acknowledgments, even for packets transmitted over LTE, we add only a delay on the downlink. Even if this results in delay asymmetric links for WiFi transmissions, that allows us to see the behavior of TCP in such a scenario. This is interesting as the 3GPP proposed to have only the downlink on WiFi and LTE, while the uplink is always on LTE. The link asymmetry can likely occur in this case.

This study is only interesting when using WiFi beside LTE, so we only do it with the *LTE/WiFi Aggregation policy*. However, we provide results obtained in the *Full LTE-offload* for sake of comparison.

Throughput achieved for the Full LTE-offload policy

This experiment shows the possibility of having all the data plane over WiFi while keeping the control plane over LTE. An increase of the throughput (see Fig.6.4) can be observed during the two VTCo-periods. Here the UE can enjoy the whole bit

Indicator	Full LTE-offload to WiFi	LTE/WiFi aggreg. and similar delays	LTE/WiFi aggreg. and 200ms in WiFi
Mean global throughput(Mbps)	2.7 ± 0.2	3.1 ± 0.2	2.0 ± 0.4
Mean throughput when WiFi is activated(Mbps)	3.9 ± 0.2	4.4 ± 0.9	2.3 ± 0.8
Mean LTE throughput(Mbps)	1.8 ± 0.2	2.1 ± 0.8	1.7 ± 0.3

Table 6.1: Indicators for the different scenarios (Delay impact experiment)

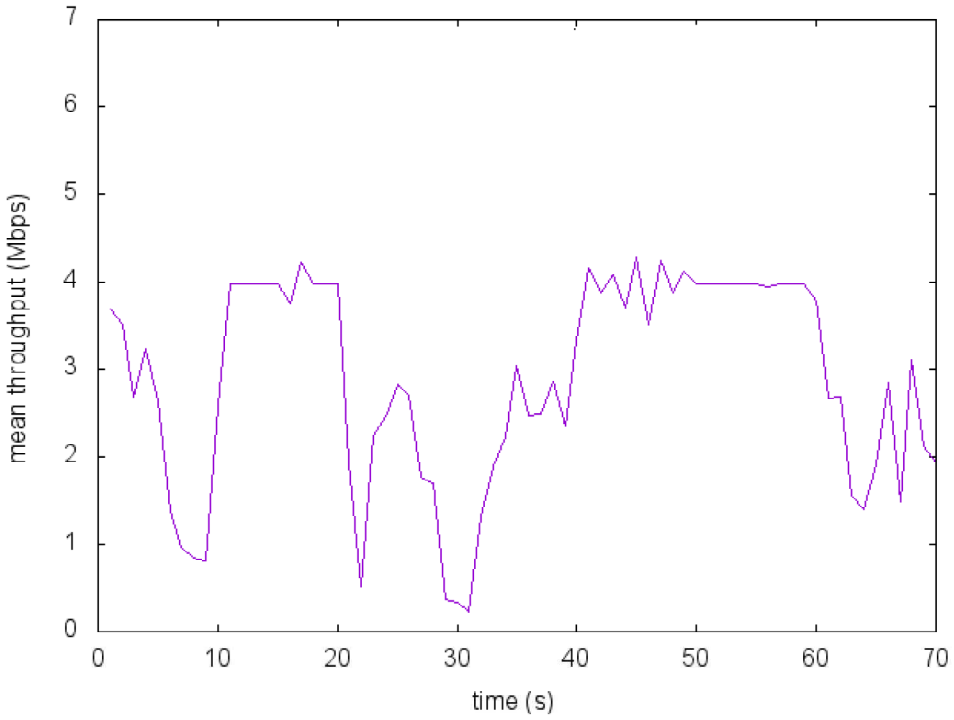


Figure 6.4: Achieved throughput for the Full LTE-offload

rate offered by the WiFi network while still being connected to the LTE network. We use the results of this experiment for comparison with further ones.

Throughput achieved for similar delays on the two links

We study here the performance of the *LTE/WiFi aggregation policy* when the delay on the two links are similar. Fig.6.5 shows the achieved throughput and Table.6.1 the indicators for this experiment.

In this case, the mean throughput when WiFi is used with LTE, is higher than the ones that can be achieved individually over the two links, i.e. 4Mbps over WiFi and 2Mbps over LTE. We can observe the same thing in Fig.6.5, where the throughput over the two *VTCo-periods* can reach more than 5Mbps. This is a typical example

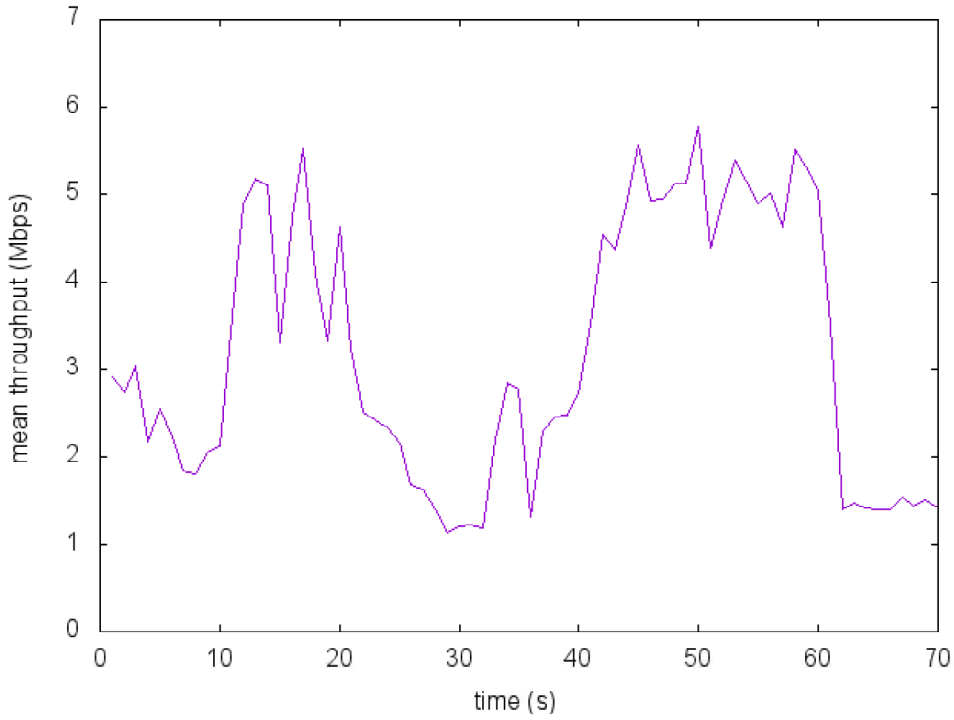


Figure 6.5: Achieved throughput for the LTE/WiFi aggregation when the delays on the two links are similar

of link-aggregation where the two bandwidths are aggregated. Due to the equal latency over the two links, they are seen as a single link from the TCP point of view.

Throughput achieved for different delays on the two links

In this experiment, we add a delay of 200ms to the WiFi link which is much higher than the mean latency over LTE, i.e. 25ms. The mean achievable throughput in this case is less than 2Mbps, which is less that the WiFi individual bit rate. This can be observed in case of a link with variable latency [99]. In our case, this occurs because packets sent over the low delay link need to be buffered by TCP and are only delivered when receiving the ones sent over the high delay link.

On the other hand, we can observe throughput fluctuations during the two *VTCo-periods* (see Fig.6.6). This is a typical example of the head-of-line blocking that occurs when using TCP over multi-paths with different latency, and even in multipath TCP (MPTCP) [100]. The head-of-line blocking occurs when packets sent over a low latency link are blocked in the buffer waiting for a late packet. These packets are delivered in burst to the upper layer when this late packet arrives, which

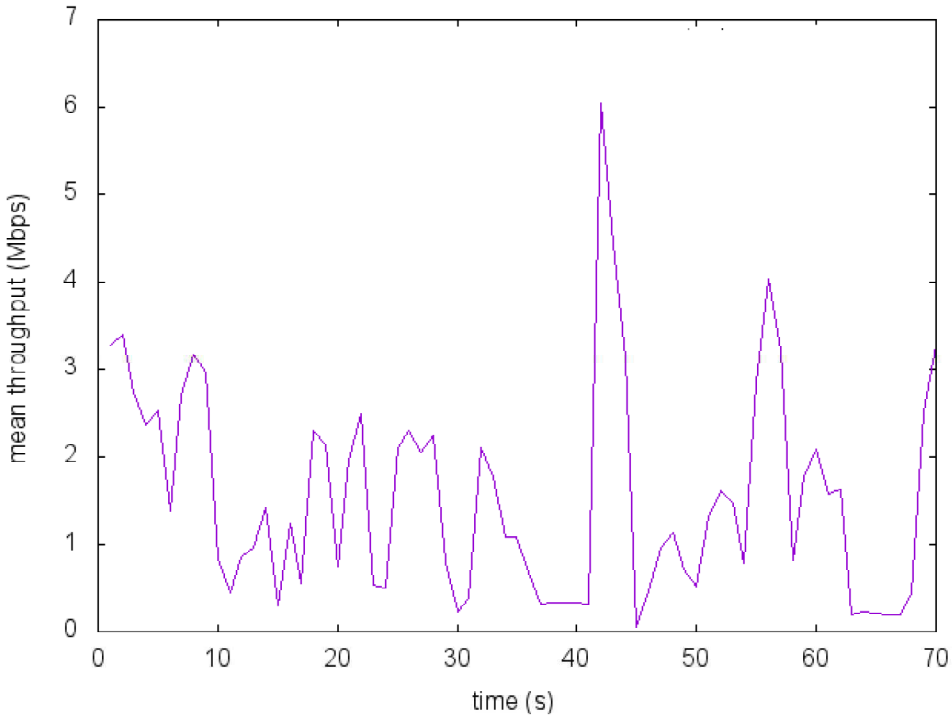


Figure 6.6: LTE/WiFi aggregation when the delays on the two links are different

explains the throughput picks.

Discussion

In these experiments, we studied the impact of the delay diversity on the two links. We first experimented a scenario where the two links have similar latency characteristics, and then introduced a delay in the WiFi link. We showed that when the delays are similar, it is possible to aggregate the two link bandwidth and thus improve the throughput. On the other hand, when the latency is too high on one link compared to the other, it is not possible to get the same result due to TCP reordering and congestion control algorithms.

6.3.3 Study of the link-layer configuration

We showed in the last experiment, the delay difference of the two links can have a very strong impact on the obtained performance. This is mainly due to TCP congestion control algorithms that adapt the throughput depending on the link quality. If for instance the WiFi link has a larger delay compared to LTE, PDUs sent over WiFi will arrive much later at the PDCP layer. Having a reordering function

Indicator	Full LTE-offload to WiFi	LTE/WiFi aggreg. and reordering	LTE/WiFi aggreg. and no reordering
Mean global throughput(Mbps)	3.1 ± 0.1	2.0 ± 0.3	3.1 ± 0.2
Mean throughput when WiFi is activated(Mbps)	5.2 ± 0.1	2.7 ± 0.6	4.7 ± 0.4
Mean LTE throughput(Mbps)	1.6 ± 0.2	1.6 ± 0.2	3.8 ± 0.4

Table 6.2: Indicators for the different scenarios

at the PDCP layer seems to be the natural solution to avoid TCP throughput degradation.

In this study, we perform two experiments on which we consider WiFi and LTE links with very different delays, i.e. delay on LTE is higher than in WiFi. In the first experiment, we activate the *PDCP reordering module*, which is responsible for delivering packets to the upper layer only is there are no missing ones. In the second experiment, the *PDCP reordering module* is not used and packets are delivered immediately to IP after reception by PDCP. Note that this experiment concerns only the *LTE/WiFi aggregation policy* in which both LTE and WiFi are used in parallel. However, we also provide results obtained for the *Full LTE-offload policy* for comparison purpose.

Due to a bad antenna installation, the LTE link was not stable inducing losses and high delays. On the other hand, the WiFi link was stable. This allowed us to study the scenario where the two links have different characteristics in terms of delay and loss rate.

Throughput achieved for the Full LTE-offload policy

In this experiment, we fix the policy to *Full LTE-offload*. We do not use the PDCP reordering as it is not necessary for this scenario. We plot the achieved throughput in Fig.6.7. WiFi provides a better bit rate compared to LTE, which explains the increase during the two VTCo-periods. It reaches 5.3 Mbps and remains stable during the whole period with a mean of 5.2 Mbps.

Throughput achieved for LTE/WiFi aggregation policy with PDCP reordering

In this experiment, we use the *LTE/WiFi aggregation policy* with the PDCP reordering function activated. Fig. 6 shows the achieved throughput in one series of this experiment. During the first VTCo-period, i.e. seconds 10 to 20, the bit

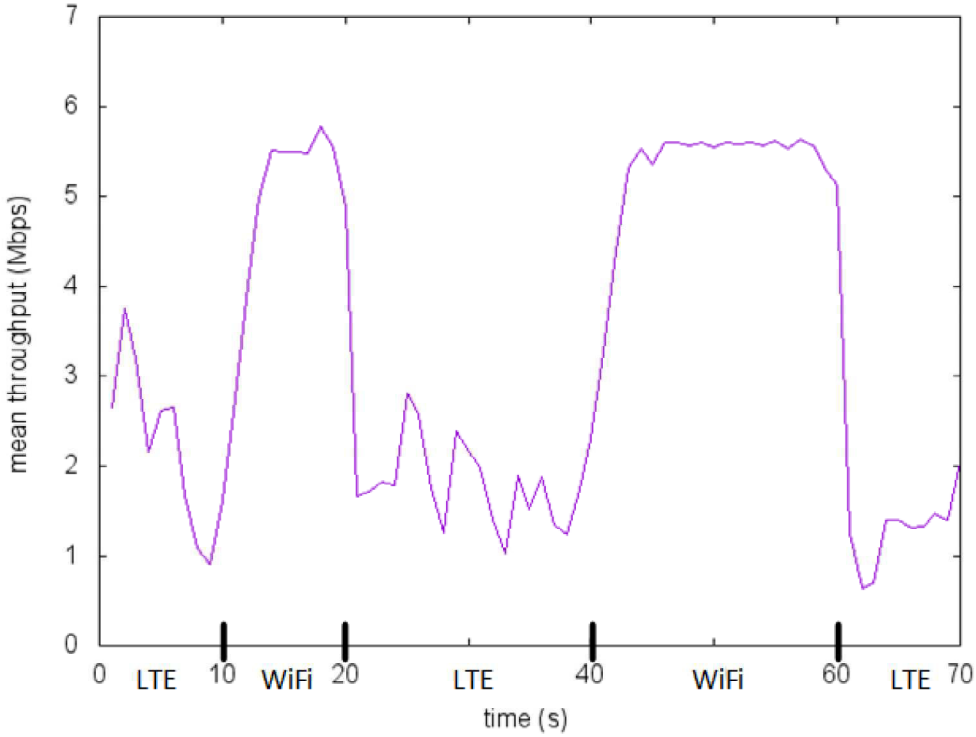


Figure 6.7: Full LTE-offload policy without PDCP reordering

rate is increasing while the UE starts using WiFi beside LTE and it reaches more than 5Mbps. In the second VTCo-period, the bit rate increases again at second 40 and reaches 4.8Mbps at 52. The mean throughput achieved during the two VTCo-periods is only 2.7Mbps and is limited to 2Mbps for the whole duration.

The delays on WiFi and LTE are different. In this case, PDUs sent over WiFi arrive much earlier than the ones sent over LTE. The *PDCP reordering module* detects a gap in the received sequence numbers, and thus stores the PDUs received over WiFi in the buffer. When a late PDU arrives, the buffer is already full and PDUs are delivered in burst to TCP. This explains the peaks in the throughput. This is the same issue observer in the last experiment that we explained by the *head-of-line* blocking. In our case, this happens when one missing or late PDCP PDU blocks the already received ones in the buffer from being delivered.

One other issue concerns the PDCP reordering timer. In our experiments, we fixed its value to twice the mean RTT, i.e. the mean RTO, of the worst link. However, the LTE connection is not stable and the RTT is thus variable. As the RTO is computed using the RTT, it is variable as well. When the RTT increases, the RTO becomes larger than the reordering timer. When the timer expires, the stored PDUs in the buffer are delivered before the expiration of the RTO. However,

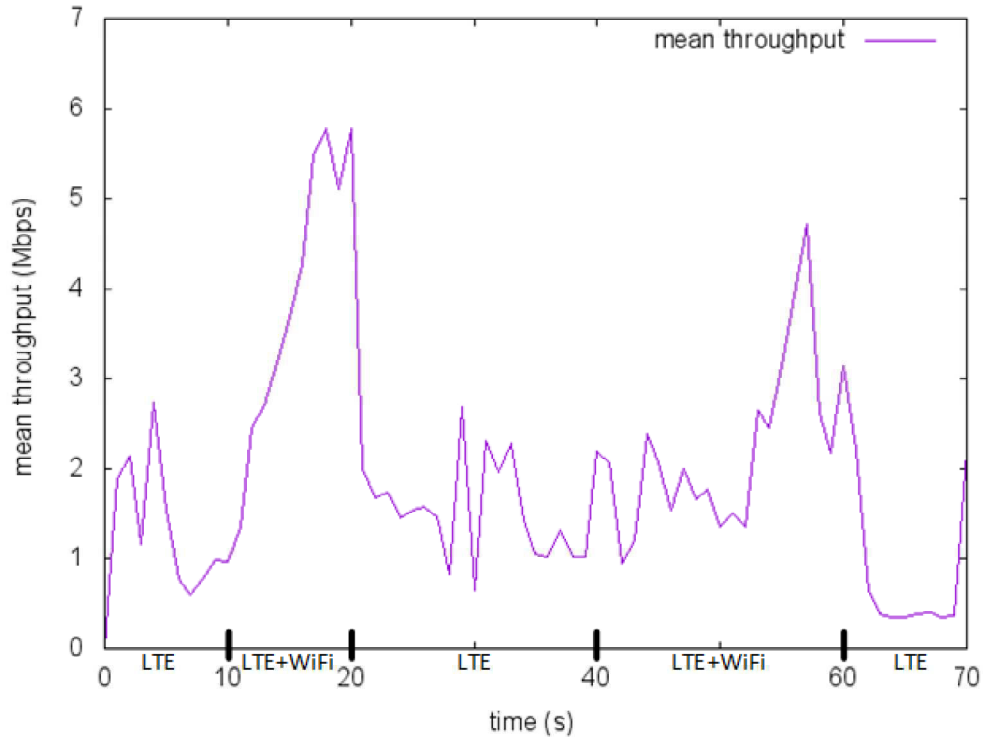


Figure 6.8: LTE/WiFi aggregation with PDCP reordering activated

this also means that if one late PDU arrives to PDCP with an old sequence number, it is considered as incorrect and is thus ignored. This forces TCP to re-transmit a PDU that was not actually lost. On the other hand, if the RTT decreases, the RTO becomes lower than the reordering timer. In this case, the reordering timer always expires after the RTO and PDUs in the buffer are thus always delivered after the expiration of the RTO. When this happens, TCP divides its bit rate, and is forced to re-transmit the segments that it considered are lost and that were actually just delivered after the RTO expiration.

Throughput achieved for the LTE/WiFi aggregation policy without PDCP reordering

We now deactivate the PDCP reordering function. Fig. 6 shows the obtained throughput for this experiment. In this case, the throughput during the two VTCo-periods is varying between 3.5Mbps and 6Mbps with an average of 4.7Mbps, . This confirms the observation on the first test, i.e. when PDCP reordering was activated, that we explained by the head-of-line blocking problem. Here PDCP immediately delivers received PDUs to TCP even if there are missing ones. The selective acknowl-

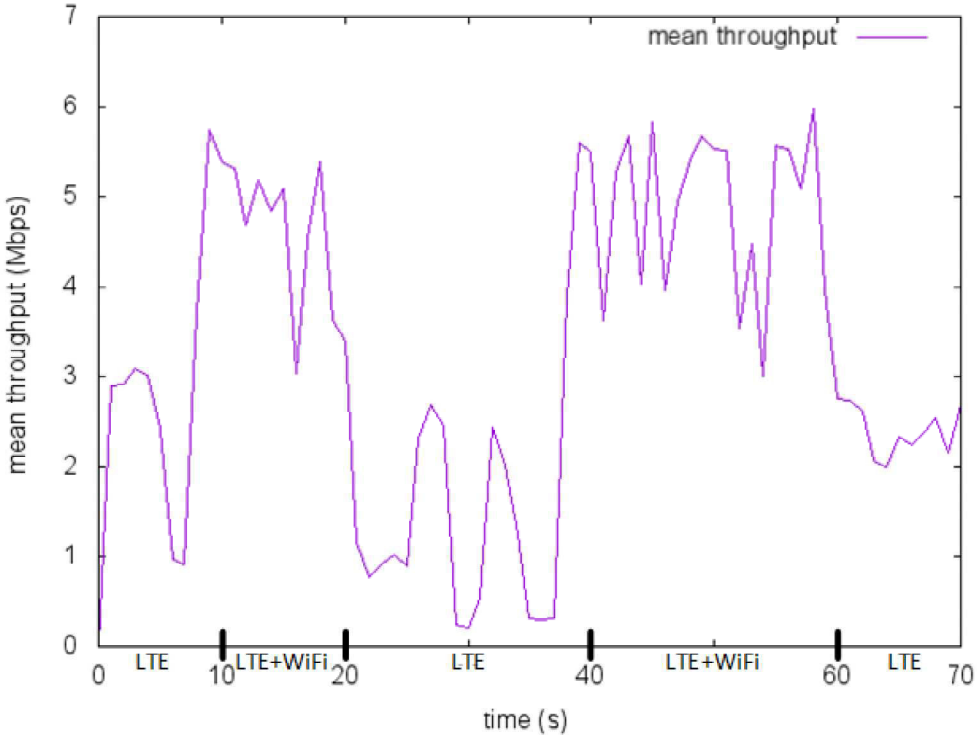


Figure 6.9: LTE/WiFi aggregation without PDCP reordering

edgement (SACK) allows TCP to only re-transmit missing segments. This avoids having useless retransmission as observed in the first experiment. The throughput drops that can be observed are the result of the RTT variation on the LTE link. When the RTT suddenly increases, segments are received after the expiration of the RTO which forces TCP to reduces its bit rate.

Discussion

In these experiments, we studied the use of a reordering function at the PDCP layer when WiFi is used in parallel with LTE, i.e. with the *LTE/WiFi aggregation policy*. We conclude that reordering PDUs at PDCP before delivery to TCP does not improve the throughput when the difference between the delays on the two links is too large. It actually disturbs higher layer such as TCP and causes head-of-line blocking. This leads TCP to decrease its bit rate and to uselessly re-transmit already received segments.

In the next experiments, we do not activate the reordering function.

6.3.4 Very Tight Coupling and Network coding

In this section, we study the use of network coding with Very Tight Coupling. We first give a brief introduction of the concept and explain how we intend to use it with Very Tight Coupling. We then present and discuss the obtained results in these experiments.

6.3.4.1 Network Coding: an overview

Network coding was introduced in [101]. The idea is to send, in addition to regular network packets (typically IP packets), the linear combination of these packets. Thus, even if the destination does not receive all packets, it can decode the missing ones using the encoded packet. A typical example is for a source to send packet p_1 and p_2 and their linear combination which corresponds to the XOR of the two: $p_{xor} = p_1 \oplus p_2$. Even if the destination receives only one packet, let us say p_2, it can decode the other one with a simple XOR using the encoded packet: $p_1 = p_{xor} \oplus p_2$.

Network coding can be used for redundancy. For instance, authors is [100] proposes to use it with MPTCP. A specific subflow is reserved to send coded segments of other subflows. Thus, if some segments are lost on one link, they can be recovered using the coded ones. We propose to use the same idea in Very Tight Coupling.

6.3.4.2 Introduction of Network Coding in Very Tight Coupling

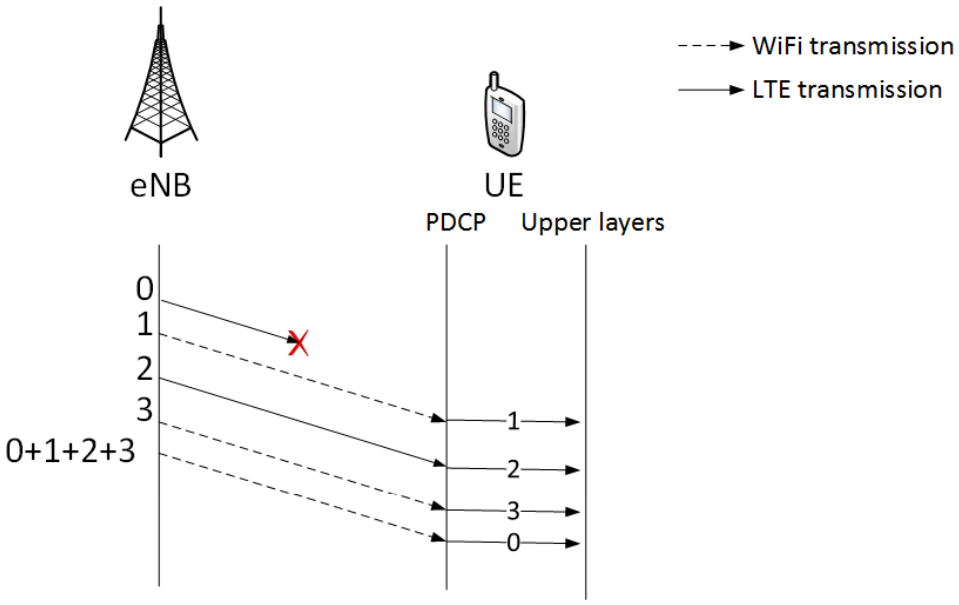


Figure 6.10: Network coding use in Very Tight Coupling

Network coding can be interesting for very tight coupling. When the UE is using WiFi and LTE in parallel, i.e. in the *LTE/WiFi aggregation policy*, the data plane is split between the two networks and a part of the traffic is sent over WiFi. As seen in the last study, when the delay on one link is too large compared to the other, delayed PDUs are considered as lost by TCP, which decreases its bit rate. To avoid this to happen, we propose to send every K PDCP PDUs the XOR combination of these PDUs on the most reliable link, i.e. WiFi in our case. The destination can retrieve a missing or even a late PDUs using the encoded PDU and the $K-1$ already received ones.

In the example shown in Fig.6.10, the eNB sends four PDUs and then sends a XOR of all these PDUs. It can then recover PDU 0, which is lost, with a simple XOR between PDU 1 to PDU 3 and the encoded PDU. This can also apply to the case of high delay links on which very late packets can be considered as lost by TCP.

Network coding module

We implemented a *network coding module* that we integrated to PDCP. Its role is to send each K PDUs the XOR combination of all these PDUs. We define a *coding set* as the set of K PDUs used in a XOR combination, and the *XORed PDU* as the resulting PDU.

The *XORed PDU* is sent in a special PDCP PDU. The sequence number is set to the last PDU of the *coding set*. We use one of the reserved bit in the PDCP header as a *xor indicator bit* to indicate that this is a *XORed PDU*.

The flowchart in Fig.6.11 shows the operation of the *network coding module* when a PDU is received. If the PDU is a regular one and not a *XORed PDU* (this can be known using the *xor indicator bit*), it is delivered to the upper layer and a copy is stored in a specific buffer.

When a *XORed PDU* is received, the *network coding module* checks whether all PDUs of the *coding set* have been received using the sequence number of the *XORed PDU* and parameter K. Specifically, it checks if all sequence numbers in [SN_XORed_PDU-K, SN_XORed_PDU] were received, where SN_XORed_PDU is the sequence number of the *XORed PDU*. If this the case, the *XORed PDU* is ignored and PDUs of the *coding set* are removed from the buffer. If one PDU only is missing, it is decoded by performing a XOR between the *XORed PDU* and the other K-1 PDUs of the *coding set*, and the retrieved PDU is delivered. In case more than one PDU is missing, the *XORed PDU* is stored until the reception of K-1 PDUs of the corresponding *coding set*.

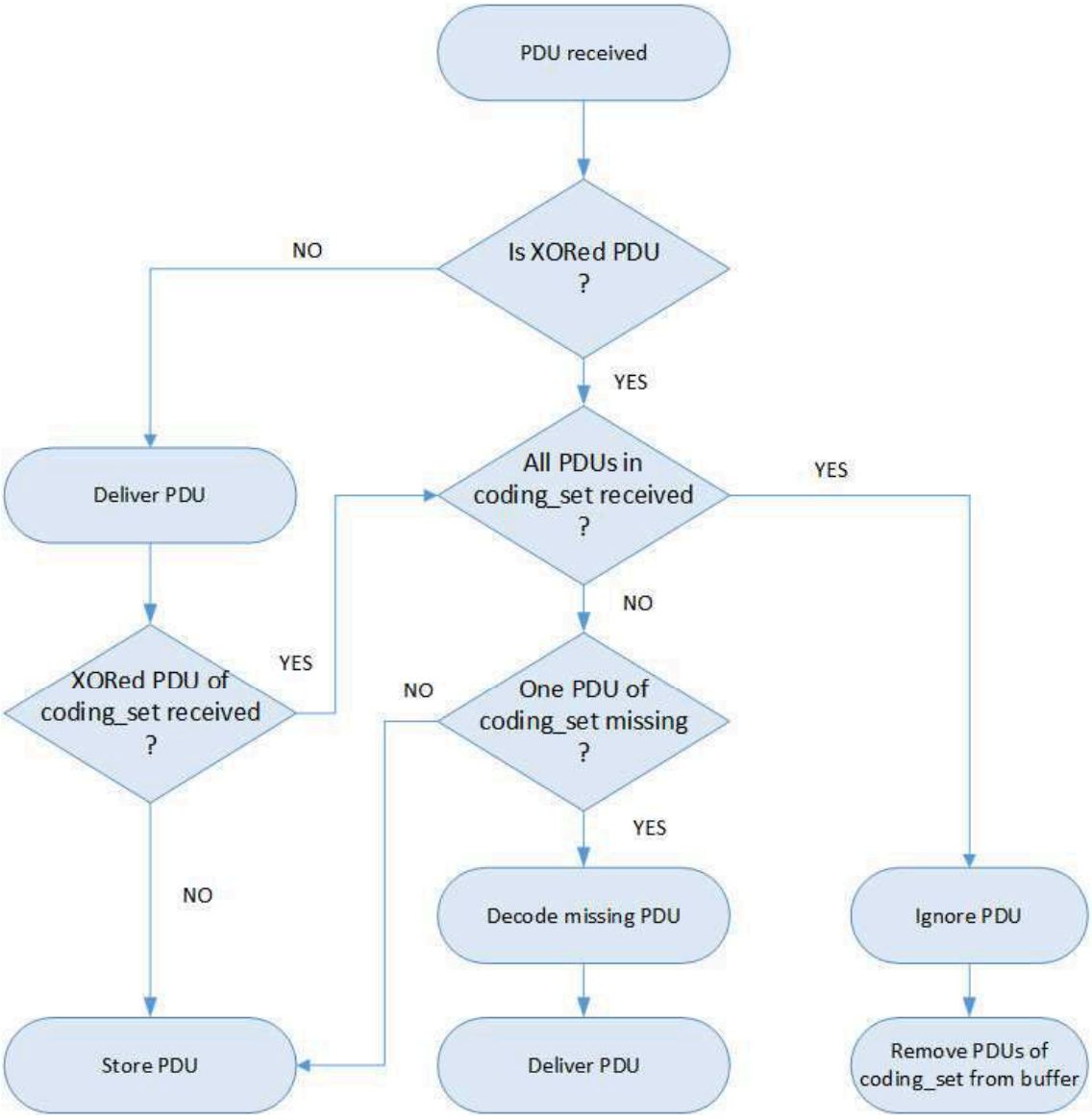


Figure 6.11: Network coding module operation

6.3.4.3 Network coding experiments

We performed three experiments in which we changed the value of K to 2, 4 and 8. We used the following indicators that we computed the same way as we did for the first experiment (see section 6.3.3):

- The mean throughput when WiFi is activated (in Mbps): this is the achieved throughput during the two VTCo-periods, whatever the selected policy;
- Mean ratio of recovered PDUs: this corresponds to the percentage of PDUs that were late or lost and that we could recover. It is equal to the total

Scheme	Mean throughput(Mbps) when WiFi is activated	Mean ratio of recovered PDUs
No coding	4.7 ± 0.4	-
K=2	3.5 ± 0.6	24%
K=4	5.0 ± 0.3	20%
K=8	5.0 ± 0.5	9%

Table 6.3: Mean throughput for the different coding schemes in case of LTE/WiFi aggregation

number of recovered PDUs over the total number of received ones. Since the network coding is only performed when WiFi is activated, this parameter is only computed over the two VTCo-periods.

In our experiments, the WiFi link is the most reliable one. We thus send systematically *XORed PDUs* over WiFi. One interesting parameter is how much bandwidth is consumed by redundant PDUs. We define B_r as the ratio of the bandwidth consumed by this traffic, which we compute using this simple formula:

$$B_r = \frac{R}{R+W} \tag{6.1}$$

where R is the overall ratio of the redundant traffic and is equal to $\frac{1}{K}$. For instance, for $K = 2$, a *XORed PDU* is sent every two PDUs which corresponds to $\frac{1}{3} = 33\%$ of the overall traffic. W is the average ratio of the traffic sent over WiFi.

In the following, we present the results obtained for each experiment.

Network coding with K=8

Fig.6.12 represents the throughput obtained when $K = 8$. Even if the mean throughput reaches 5Mbps (see Table 6.3), brutal drops can be observed. In this experiment, if the distance between two lost or delayed PDUs is lower than 7, non of them can be recovered. This is why the average rate of recovered PDUs is low, i.e. 9% (see table 6.3). Most of the time, late PDUs are considered as lost, which explains TCP throughput drops.

Network coding with K=4

Fig.6.13 shows the throughput when $K = 4$. In this scenario, the *XORed PDU* consists of the combination of 4 successive PDUs. Even though *XORed PDUs* correspond to 20% of the whole entire traffic (computed using 6.1), the mean achievable

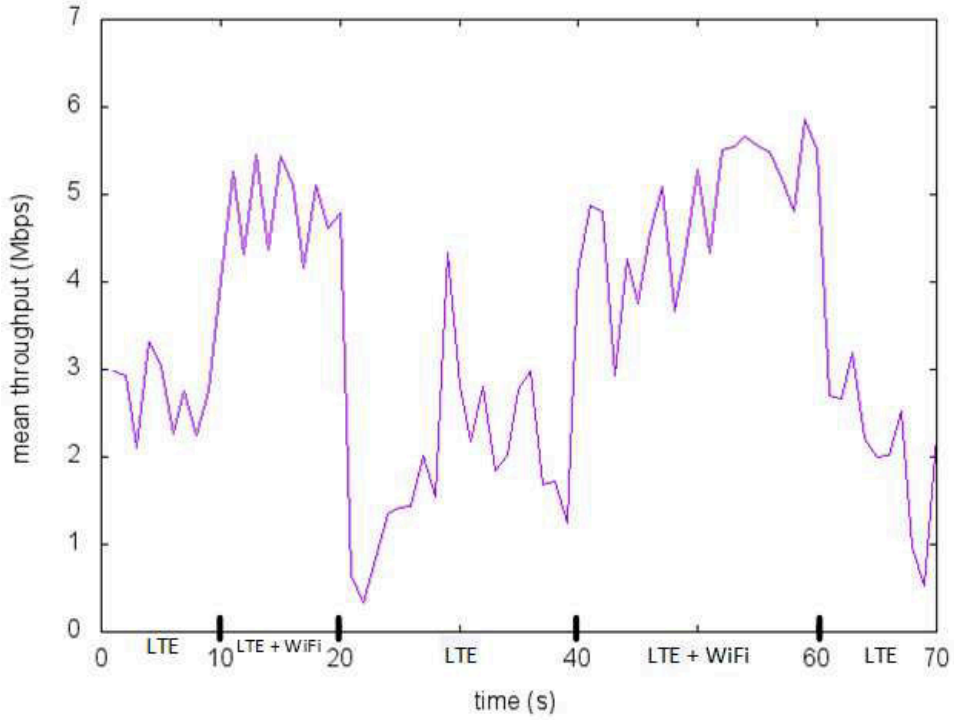


Figure 6.12: Network coding with K=8

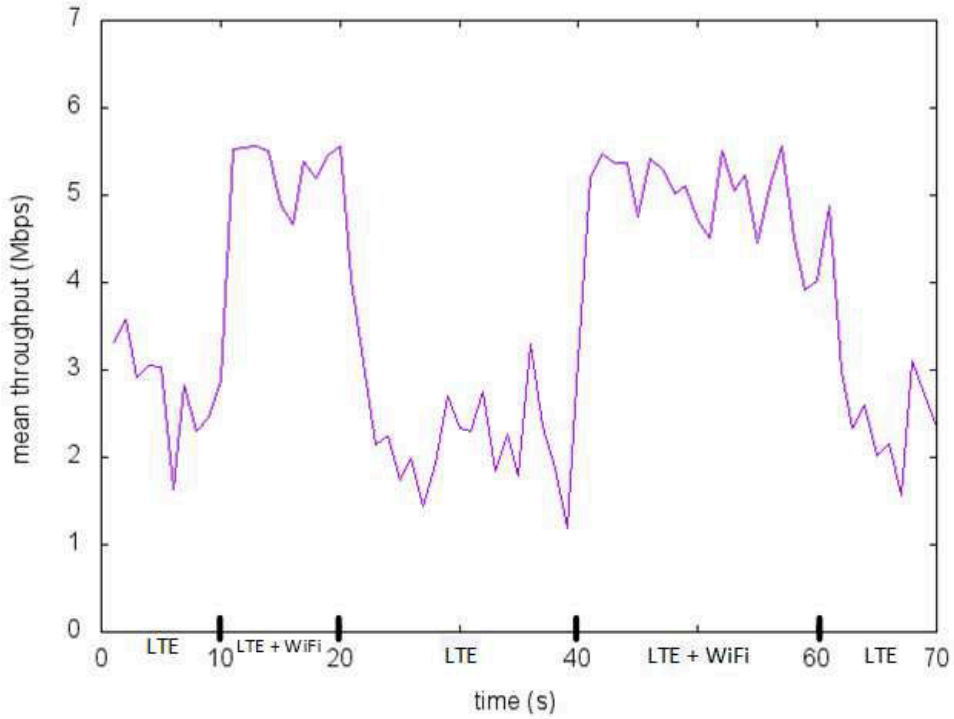


Figure 6.13: Network coding with K=4

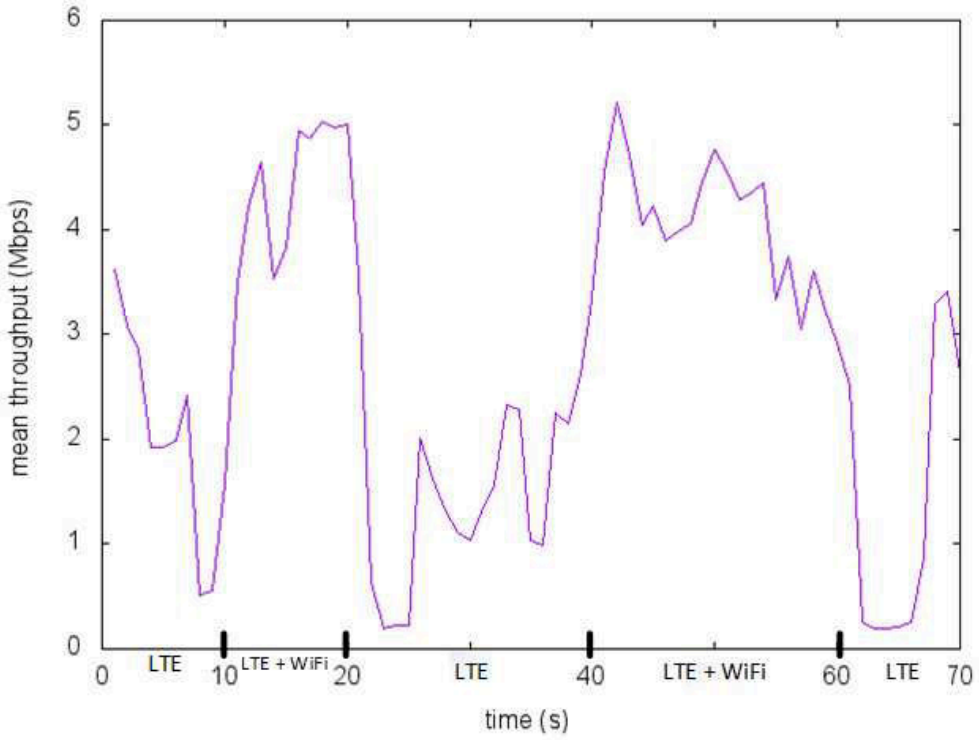


Figure 6.14: Network coding with K−2

bit rate can reach 5Mbps. However, we notice that the number of brutal throughput drops can be limited compared to the last case (i.e. K= 8). The reason is that it is possible to recover more PDUs as the minimum distance between the two is decreased. In this scheme, 20% of the traffic is actually recovered. This limits the number of losses and to have less likely TCP decreasing its bit rate.

Network coding with K=2

Fig. 6.14 plots the throughput obtained when $K = 2$. For the two VTCo-periods, the bit rate varies between 2Mbps and 4Mbps with an average of 3.5Mbps (see Table 6.3). With this coding scheme, the minimum tolerated distance between two lost or delayed PDUs is equal to two. This means that even if one PDU in two is lost, it can be recovered. This is why 24% of the received PDUs during the VTCo-periods correspond to decoded PDUs. On the other hand, using (6.1) and knowing that 65% of the whole traffic is sent over WiFi, we deduce that 33% of the WiFi bandwidth is used for the redundant traffic. This explains why the mean useful throughput is lower compared to the other schemes (i.e. $K = 4$ and $K = 8$), i.e. 3.5Mbps.

6.3.5 Discussion

In performed three experiments where we varied the number K, which corresponds to the number of PDUs combined together in a *XORed PDU* and also corresponds to the minimum distance between 2 successive losses to allow a PDU to be recovered. We tried three values of K, i.e. 2, 4 and 8.

Our conclusion is that a high redundancy rate, i.e. $K = 2$, is not preferred as it consumes too much bandwidth and thus limits the achievable throughput. On the other hand, having a high redundancy, i.e. $K = 8$, does not have much effect as this increases the minimum distance between two losses and limits the possibility of recovering a missing PDUs. In this case, we observed that TCP behavior is similar to the non-coding scenario with throughput drops.

We find that the most suitable redundancy rate is $K = 4$. The experiment has shown that it is possible to limit throughput drops since more lost or late PDUs can be recovered. Moreover, the consumed bandwidth is limited as the achievable throughput slightly less than the one obtained without network coding.

6.4 Conclusion

We presented a proof-of-concept of Very Tight Coupling that we implemented on a real-time platform based on the Open Air Interface framework. Our experimental analysis proved the feasibility and the potential of Very Tight Coupling. We performed several types of experiments and demonstrated that using WiFi and LTE simultaneously does not always increase the throughput, mainly due to the different characteristics of the two links. We show that even if the intuition is to reorder packets at the link-layer (i.e. PDCP) before delivering them to the upper layer, this actually disturbs delay sensitive higher protocols such as TCP and causes throughput drops.

Furthermore, we show that when using Network Coding in Very Tight Coupling, a trade-of has to be made between the mean achievable throughput and the acceptable throughput drops. Specifically, a high redundancy rate limits throughput drops caused by TCP congestion control but also consumes a lot of bandwidth. On the other hand, a low redundacy rate does not have much effect on the throughput and gives similar results to the ones obtained when no network coding is used at all.

Chapter 7

Conclusion and Future Work

In this chapter, we summarize our main contributions and give some insights for future possible works.

7.1 Main Contribution

One of the key enablers for 5G networks is the ability for users to use all available access networks simultaneously and to move seamlessly between these networks, and also to allow a separation of the user and control planes. Very Tight Coupling between LTE and WiFi was proposed with the same requirements and with the same goals.

In this thesis, we proposed an architecture for Very Tight Coupling between LTE and WiFi. This novel coupling solution gives a new possibility for operator to offload the cellular networks to WiFi with no additional deployment and minimum software modifications and configurations, and to provide a complementary access network to enhance the capacity.

Our work was achieved in four parts: design of the architecture, mathematical analysis, implementation of the architecture and an experimental evaluation. Hereafter, we give a summary of these contributions.

Architecture design

Before proposing the architecture, we first did an extended state-of-the-art of all existing solutions for multi-homing and mobility management. We did a qualitative analysis to identify the benefits and drawbacks of each solution. The conclusion was that most current solutions required modification of the protocol stack and/or the

network architecture, which is not interesting for an operator that wants to limit the costs. Moreover, in all solutions, the data path management is done by the terminal itself, which has limited or no knowledge about the network capacity and thus leads to non-optimized decisions. Very Tight Coupling was proposed to overcome these issues, by connecting WiFi APs to LTE eNodeBs. In this thesis, we proposed an architecture that can be integrated to the COMBO proposed converged network. We first detailed how to easily connect WiFi APs to eNodeBs. We then proposed a protocol stack and gave the specification of a new sub-header. We also described different procedures for the operation of Very Tight Coupling. Finally, we identified some issues and proposed some insights to solve them.

Mathematical analysis

In LTE, the UE is connected to the best eNodeB, i.e. from which it receives the strongest signal. However, due to the shadowing effect, the best eNodeB is not always the nearest one. In very tight coupling, the UE and the WiFi AP need to be connected to the same eNodeB to be able to use WiFi and LTE in parallel.

In this analysis, we studied the performance of Very Tight Coupling when the APs are connected: i) to the nearest eNodeB, ii) to the two nearest eNodeBs and iii) to all eNodeBs. We took into consideration the shadowing effect and how much capacity can be saved for different value of the shadowing.

Using Monte Carlo simulations, we found that for a low-shadowing, it is not necessary to connect WiFi APs to more than one eNodeB. On the other hand, connecting APs to more eNodeBs when the shadowing increases is required. This is a typical case of outdoor terminals and WiFi APs deployed inside buildings. It is interesting for the operator to connect APs to at least two eNodeBs covering that area in order to spare more capacity.

Implementation and Experimental Evaluation

After we designed and mathematically analyzed the performance of Very Tight Coupling, we setup a testbed based on the Open Air Interface framework, which offers a full implementation of an LTE network. We thus developed several modules that we integrated into OAI code. These modules allow to use WiFi in parallel to LTE and to send PDCP packets over WiFi. We also added a function to PDCP to reorder the packets received from LTE and WiFi before delivering them to the upper layer.

We tested the performance of the downlink for two coupling policies: i) a full-LTE offload and ii) an LTE/WiFi aggregation. In the full-LTE offload, all the data plane is sent over WiFi while the control plane is kept on LTE. With this scenario, we demonstrated the feasibility of Very Tight Coupling, and that it is possible to have the data plane over WiFi and the control plane over LTE. In the LTE/WiFi aggregation, the data plane is split between WiFi and LTE, while the control plane is on LTE. We first found that the fact that WiFi and LTE links have different delays impact strongly the performance and that using the two simultaneously does not increase the throughput. Moreover, we proved that reordering the packets at PDCP before delivering them to the upper layer does not solve the issue, it even disturbs higher protocols such as TCP.

To address the delay diversity over the two links, we proposed to use Network Coding. The idea is to send the XOR combination of several packets and to send it over the most reliable link, i.e. LTE. Herewith, if one packet is delayed, it can be easily retrieved using the coded packet and the already received ones. For this purpose, we developed a module for network coding operation and performed experimentation for three different coding schemes: i) two packets combinations where we send a coded packet each two packets, ii) 4 packets combinations and ii) 8 packets combinations. We showed that the first option avoids to have throughput drops that are due to delayed packets, but consumes also a lot of a bandwidth. On the other hand, the two other options have not the same efficiency, but avoids reducing too much the mean throughput.

7.2 Very Tight Coupling and 3GPP

In March 2016, an approach called LTE/WiFi link aggregation (LWA) was proposed by the 3GPP. Like Very Tight Coupling, the idea is to connect WiFi APs to eNodeBs and to reuse PDCP for WiFi communications. This was proposed at the end of this thesis, and we thus could not take it into consideration. In the following, we highlight the similarity and differences between LTE/WiFi aggregation and Very Tight Coupling.

In the Very Tight Coupling architecture that we proposed, WiFi APs functions are limited to layer 2 bridging and have no knowledge about LTE cellular traffic. In LWA, APs are aware of the process and thus include additional functions for bearer establishment with eNodeBs. Moreover, a new WiFi security protocol is proposed to

LWA, unlike Very Tight Coupling that uses only PDCP security. The convergence of fixed and cellular access networks allows Very Tight Coupling to be proposed with a simple implementation for the layer 2 interface between eNodeB and APs using VLANs. In opposite, LWA proposes an IP interface using GTP tunneling.

7.3 Future Work

This thesis was a first work on Very Tight Coupling between LTE and WiFi and it can be extended to other studies. We identify some of these studies in the following.

Mobility and shadowing

In our experiments, we consider fixed users with ideal LTE connectivity. However, Very Tight Coupling mainly targets moving users, and as we demonstrated in the mathematical analysis, it is more beneficial for high shadowing, e.g. indoor or cell-edge users. It would be interesting to extend the study to take all of these parameters into consideration.

Comparison with other coupling mechanisms

An interesting study would be to compare the performance of Very Tight Coupling with other coupling scenarios, especially loose-coupling such as MPTCP-based solutions. This can be done first by developing a mathematical model and then experimentally using the developed testbed.

Advanced network coding schemes

In our work, we experimented a simple coding based on the XOR combination of several frames. This scheme allows to only retrieve a single loss among the packets coded together. However, it is usual in WiFi networks to have bulk losses where this scheme is useless. An interesting work would be to have a more sophisticated coding scheme allowing to retrieve several consecutive losses. This can be performed for instance by coding packets over a sliding window. However, it is worth noting that there must be a trade-off between the number of packets to code together and the maximum tolerated delay. Indeed, we should wait for the last packet before being

able to retrieve the first lost one, which would be useless if the delay between the two packets is too large.

Interface selection and data path management

In very tight coupling, the data path management and how to distribute the traffic among the WiFi and LTE interfaces is done by the network, by providing the terminal with appropriate policies. These policies indicate to the terminal how much traffic should be sent over WiFi, which WiFi AP to use and at which moment of the day.

The decision has thus to be optimized and dynamic. To achieve this, the network should take into considerations all available information provided by the UE such as LTE measurements and the instantaneous load on each nearby WiFi APs. Using these information, the network should be able to select the best current access networks for each user. Note that the best network is not the same for all users as it depends on user requirements and applications. For instance, a user doing VoIP or cloud-gaming requires low latency while a user that is downloading needs high bit rate.

Moreover, Very Tight Coupling was proposed in a way to allow all kind of users to use WiFi in parallel to LTE. These users include moving users that, depending on their speed, may move under several WiFi APs coverage during a short period. The network should thus be able to move data flows between these networks seamlessly to the user. This is very challenging, as the network should take dynamic decisions but should also anticipate the user exit from the AP coverage to avoid any packet losses. The network should also be able to know the incoming APs that can be used, and know exactly when to use it. As the user may stay only few seconds under the AP coverage, losing 1 second because of a late decision results in unused capacity. On the other hand, a too early decision may result in users connected to a very far APs and inducing bad performance.

Appendix A

.1 Contexte de la thèse

Cette thèse a été effectué dans le cadre du projet Européen COMBO (COnvergence of Fixed and Mobile BrOadband access/aggregation networks). COMBO regroupe 15 partenaires de différents milieux. Des opérateurs participent au projet tels que: Deutsche Telekom AG (DTAG), Orange et Telefonica. Des partenaires industriels sont également impliqués: Ericsson, ADVA Optical Networking, AITIA International, Telnet, FON, Argela et JCP-connect. Le projet compte également des universités et instituts académiques: Telecom Bretagne, Lund University (ULUND), Centre Tecnologic de Telecomunicacions de Catalunya (CTTC), Politecnico di Milano (POLIMI) ainsi que la "Budapest University of Technology and Economics".

Le projet COMBO a comme objectif la proposition et conception de nouvelles architectures réseaux permettant la convergence des réseaux d'accès fixe et cellulaire, i.e. Fixed Mobile Convergence (FMC). Plusieurs travaux ont déjà traité de la convergence fixe/mobile, mais cette convergence était jusqu'à présent limité au niveau service, i.e. réseaux tout IP. COMBO se concentre plutôt sur la convergence de l'architecture réseau elle même. Ceci a pour but d'avoir une meilleure utilisation des équipements réseaux et de l'infrastructure, ce qui aura comme résultat une réduction des coôts, de meilleures performances et une expérience plus transparente pour l'utilisateur. Notre travail au sein de COMBO est de proposer une nouvelle méthode de couplage WiFi/LTE et de l'évaluer en utilisant des outils mathématiques et expérimentaux.

.2 Contributions

Il y a plusieurs problèmes lorsqu'un terminal utilise les réseau WiFi et LTE de façon simultané. Comme la plupart des applications se basent sur les adresses IP pour identifier les sessions, un changement dans l'adresse du terminal causera une rupture de ces sessions, ce qui arrive par exemple lorsque le terminal se déplace d'un réseau d'accès à un autre.

Ceci est du au fait que les réseaux fixes et cellulaires sont aujourd'hui séparés et interconnectés seulement grâce au réseau Internet. Le projet COMBO propose de nouvelles architectures de réseau convergent dans lesquelles les réseaux d'accès fixe et cellulaire partagent des parties du réseau, par exemple le réseau d'agrégation. Ce nouveau type de réseau offre de nouvelles possibilités de réseaux hétérogènes WiFi/LTE totalement intégrés. Dans cette thèse, nous étudions une nouvelle architecture de couplage WiFi/LTE, appelée "Very Tight Coupling entre WiFi/LTE", qui permet à l'utilisateur d'utiliser simultanément WiFi et LTE de façon transparente. Tout d'abord, nous proposons une architecture du Very Tight Coupling suivie par une analyse de performance en utilisant des outils mathématiques. Nous avons ensuite implémenté la solution sur une plateforme temps réel, sur laquelle nous avons effectué divers expérimentations.

.3 Présentation du Very Tight Coupling

L'idée générale du Very Tight Coupling est de connecter les points d'accès WiFi aux stations de bases LTE (i.e. eNodeBs). Ceci est notamment possible grace à la convergence proposée par COMBO. Cette connexion permet de réutiliser les procédures de sécurité LTE assurée par le protocole PDCP (Packet Data Convergence Protocol), ce qui évite d'avoir de mécanismes de sécurité spécifique à WiFi et réduisant par la même occasion le temps d'attachement d'un terminal à un point d'accès WiFi. Il est ainsi possible aux utilisateurs qui se déplacent et qui ne restent qu'un temps limité sous couverture WiFi de pouvoir utiliser ce point d'accès. Contrairement aux solutions de couplage proposées dans la littérature, seulement le plan utilisateur peut être déchargé vers WiFi en Very Tight Coupling, tandis que le plan contrôle (i.e. trafic de signalisation) est maintenu sur la voie LTE. L'intégration des deux technologies étant faite à un niveau bas (i.e. PDCP), le terminal n'obtient qu'une seule adresse, assurant nativement la continuité de session lors de déplacements entre les différents réseaux d'accès.

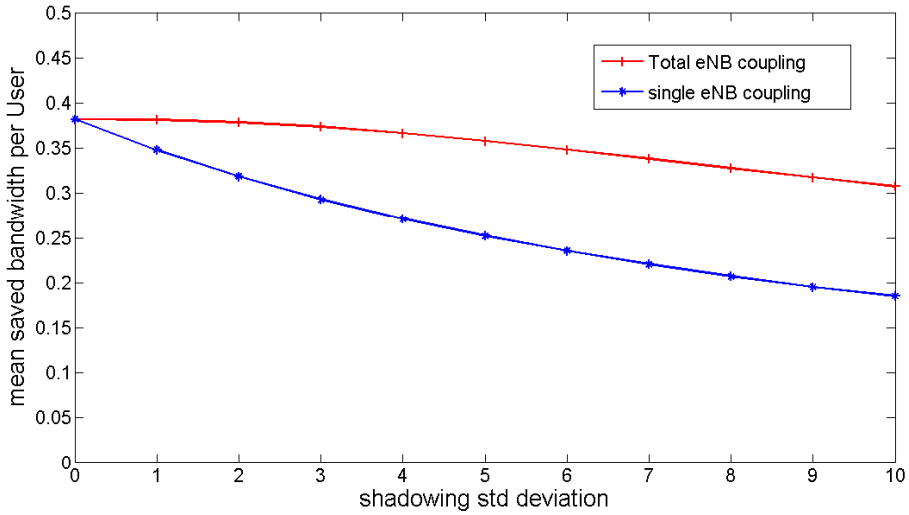


Figure 1: Capacité moyenne économisée vs. écart type de l'effet de masque (modèle analytique)

.4 Analyse de performance du Very Tight Coupling

Nous nous intéressons à la capacité pouvant être économisée dans une architecture Very Tight Coupling. D'une façon générale, un terminal est connecté à la station de base de laquelle il reçoit le signal le plus fort, qui est généralement la station la plus proche. Cependant, en présence d'obstacle entre le terminal et la station de base, la propagation du signal subit un effet de masque (i.e. shadowing). La meilleure station de base n'est pas systématiquement la plus proche. En Very Tight Coupling, l'utilisation de WiFi par le terminal n'est possible que si ce dernier et le point d'accès sont connectés à la même station de base.

Dans cette étude, nous considérons trois types de scénarios dans lesquels un point d'accès WiFi peut être connecté à 1) la station de base la plus proche (single eNB-coupling), 2) les 2 stations de bases les plus proches (double eNB-coupling) ou 3) toutes les stations de base du réseau (total eNB-coupling). Nous prenons également en compte l'effet de masque, et calculons la capacité moyenne qui peut être économisée lorsque le terminal utilise WiFi au lieu de LTE. Ci-dessous, les résultats obtenus mathématiquement sont tout d'abord exposés, puis ceux obtenus par simulation.

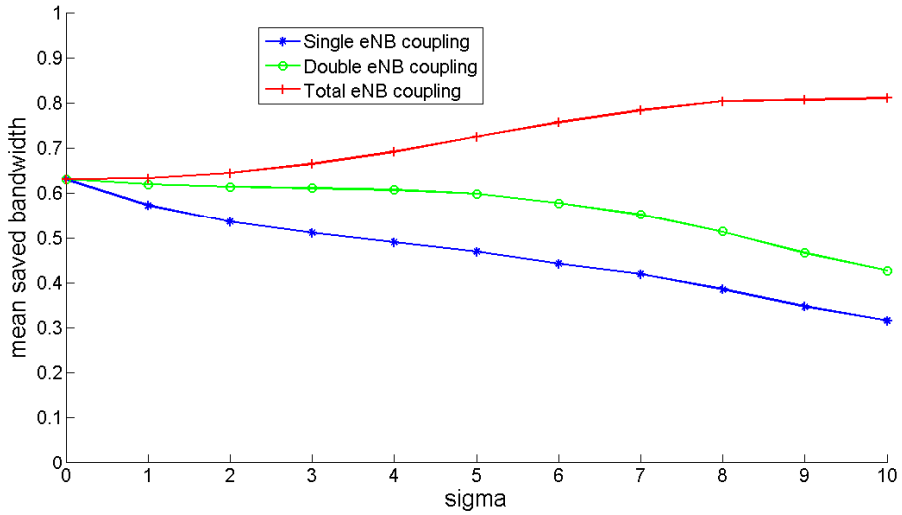


Figure 2: Capacité moyenne économisée vs. écart type de l'effet de masque(simulation)

.4.1 Résultats du modèle mathématique

La figure 1 montre la capacité moyenne économisée par utilisateur en fonction de l'écart type de l'effet de masque pour deux scénarios de déploiement possibles: 1) single-eNB coupling et 2) total eNB-coupling. En l'absence d'effet de masque (i.e. σ − 0dB), tous les utilisateurs peuvent être déchargés vers WiFi dans les deux scénarios. Plus l'effet de masque augmente, moins les terminaux ont de chance d'être connectés à la station de base la plus proche, et donc moins de chance d'être déchargés vers WiFi dans le cas d'un single-eNB coupling. Dans le cas du total-eNB coupling, plus de bande passante peut-être économisé comparé au cas précédent vu que même les terminaux qui sont à l'extérieur de la cellule que couvre la station de base auquel ils sont attachés peuvent être déchargés vers WiFi. Par ailleurs, plus un terminal est éloigné de sa station de base d'attache, plus de bande passante il consomme, et donc plus de bande passante peut être sauvegardée dans le cas du total-eNB coupling. Cependant, nous avons seulement considéré deux stations de base dans notre étude et les terminaux présents entre les deux, alors que dans un scénario plus réaliste et dans le cas d'effet de masque élevé, les terminaux attachés à BS 0 peuvent être très éloigné de la zone considérée, impliquant de ce fait une hausse de la bande passante et non une baisse comme observé dans la figure 1.

.4.2 Résultats de la simulation

La figure 2 montre la capacité moyenne sauvegardée par utilisateur en fonction de l'effet de masque pour trois scénarios de déploiement. Les résultats observés confirment ceux obtenus grâce au modèle mathématique. En l'absence de shadowing, les terminaux sont toujours connectés à la station de base la plus proche et peuvent toujours être déchargés vers WiFi et ce quelque soit le type de déploiement considéré. Ensuite, plus le shadowing augmente, moins les utilisateurs auront de chance à être connecté à la station de base la plus proche, causant une baisse de la capacité sauvegardée dans le cas du single et double-eNB coupling. Cependant, dans le cas du total-eNB coupling, nous observons une hausse de la bande passante économisée contrairement à la baisse observée dans le modèle mathématique. Ceci est du au fait que plus l'effet de masque est important, plus il y aura de terminaux consommant beaucoup de bande passante.

.4.3 Implémentation et expérimentations du Very Tight Coupling

Notre banc de testes est basée sur le framework open source développé par Eurecom: Open Air Interface (OAI). OAI permet de simuler/émuler un réseau LTE complet, i.e. réseau d'accès (RAN) ainsi que réseau coeur (EPC). Dans le cas d'une émulation, il est possible d'avoir une liaison LTE réelle en utilisant des cartes radio telles que les cartes Ettus USRP B210, ce que nous utilisons pour notre banc de testes.

Notre banc de test est composé de trois noeuds principaux:

- le PC 1 est utilisé comme un terminal LTE émulé grâce à OAI en utilisant une carte radio USRP B210. Il inclut également une interface WiFi offrant un débit max de 150Mbps.
- le PC 2 est utilisé comme eNodeB émulé également grâce à OAI et une carte radio USRP B210.
- le PC 3 est utilisé en tant que point d'accès WiFi. Nous utilisons pour cela l'utilitaire hostapd fournis sous linux. Le point d'accès diffuse un SSID spécifique et n'utilise aucun mécanisme de sécurité WiFi classique. Comme hostapd permet d'avoir du pontage WiFi de niveau 2, nous avons configuré le PC 3 pour connecter le terminal connecté en WiFi et l'eNB de façon totalement transparente.

Nous nous intéressons dans nos études aux performances, et plus précisément au débit, sur la voie descendante. Nous installons donc un client TCP au niveau de l'eNB qui va générer du trafic vers un serveur installé dans le terminal, et mesurer le débit à ce niveau là.

Nous définissons trois indicateurs que nous utiliserons pour notre étude de performance:

- Le débit moyen global: correspond au débit calculé sur toute la durée de l'expérimentation (70sec).
- Le débit moyen en période VTCo (activation du very tight coupling): calculé seulement sur les périodes VTCo.
- Le débit LTE moyen: calculé uniquement sur les période ou le terminal n'utilise que LTE.

Pour chaque étude, nous effectuons des séries de 20 expérimentations et calculons une moyenne des indicateurs définis précédemment. Nous exposons également les résultats obtenus pour une série afin d'étudier le comportement de TCP.

Impact du délai

Dans cette étude, nous nous intéressons à l'impact que peut avoir une différence de délais sur les liens WiFi et LTE. Pour cela, nous effectons deux séries d'experiences: une premiere dans laquelle les délais sont similaires sur WiFi et LTE, ainsi qu'une seconde série dans laquelle nous ajoutons artificiellement à la liaison WiFi un délai de 200ms et limitant le débit à 4Mbps en utilisant l'outil Linux Network Emulator (netem). Les résultats des deux séries sont exposées respectivement dans les figures 3 et 4.

Lorsque les délais sont similaires sur les deux liens, le débit obtenus, i.e. 4.4Mbps, lors de l'utilisation de WiFi et LTE simultanément (périodes VTCo) est supérieur aux débits individuels des deux liens. Ceci est un exemple d'agrégation de liens ou les bandes passantes ont pu être agrégées. D'un autre coté, dans le cas ou les délais sont différents, le débit atteint est inférieur à 2Mbps (inférieur au débit WiFi individuel). Ceci peut s'expliquer par le fait que les paquets envoyés sur le lien LTE arrivent plus rapidement que ceux envoyés sur le lien WiFi, causant un désordonnancement au niveau TCP les obligeant à être stockés. Des fluctuations de débit peuvent également être observées dans ce cas là qui sont un exemple typique

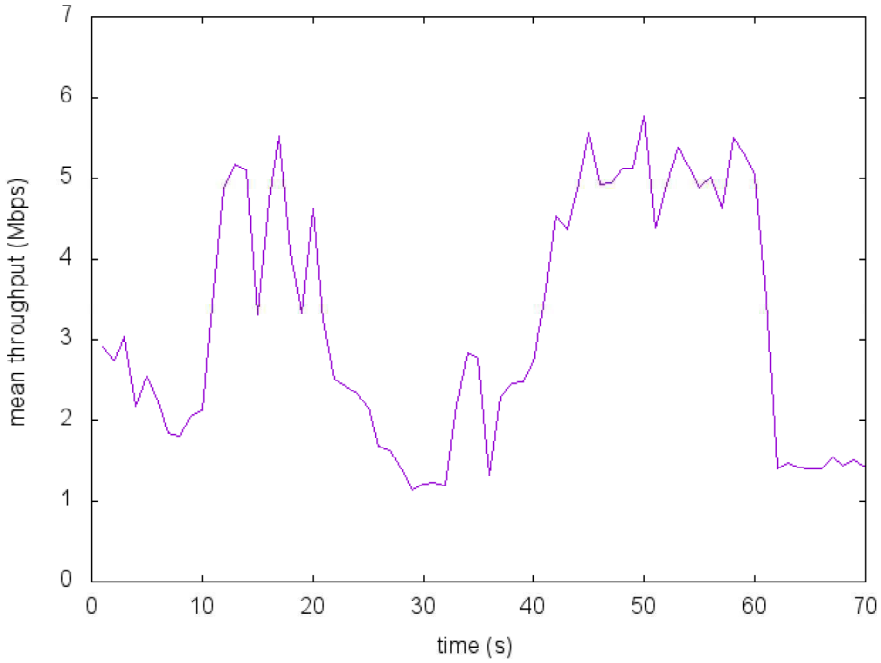


Figure 3: Débit moyen obtenus pour des délais similaires sur WiFi/LTE

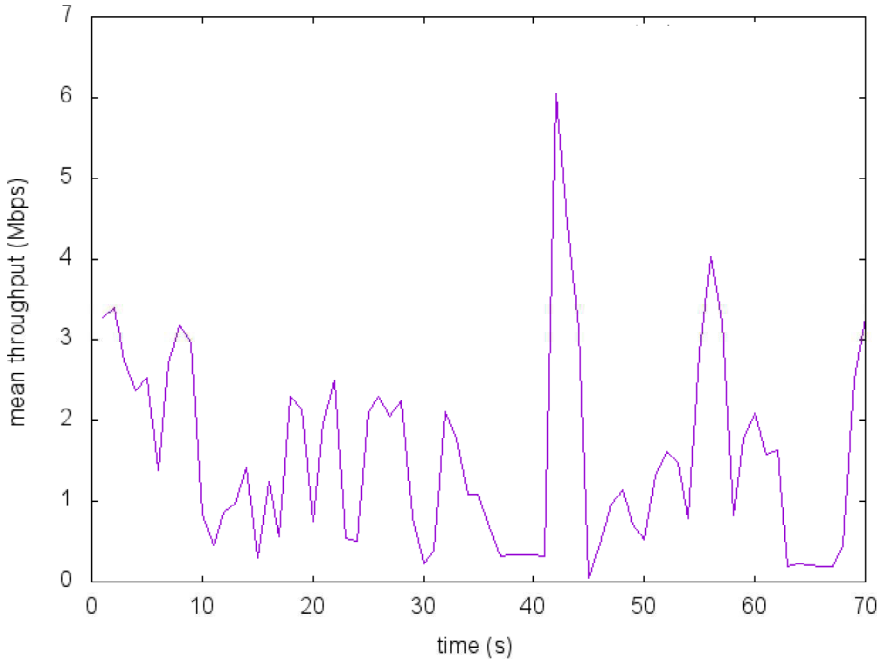


Figure 4: Délai moyen obtenus pour des délais différents

du problème de "head-of-line blocking" qui se produit lors l'utilisation de TCP pour des transmissions multi-chemins. Les pics de débit se produisent lorsque des paquets stockés dans le buffer sont délivrés en block à la couche supérieur lorsqu'un paquet

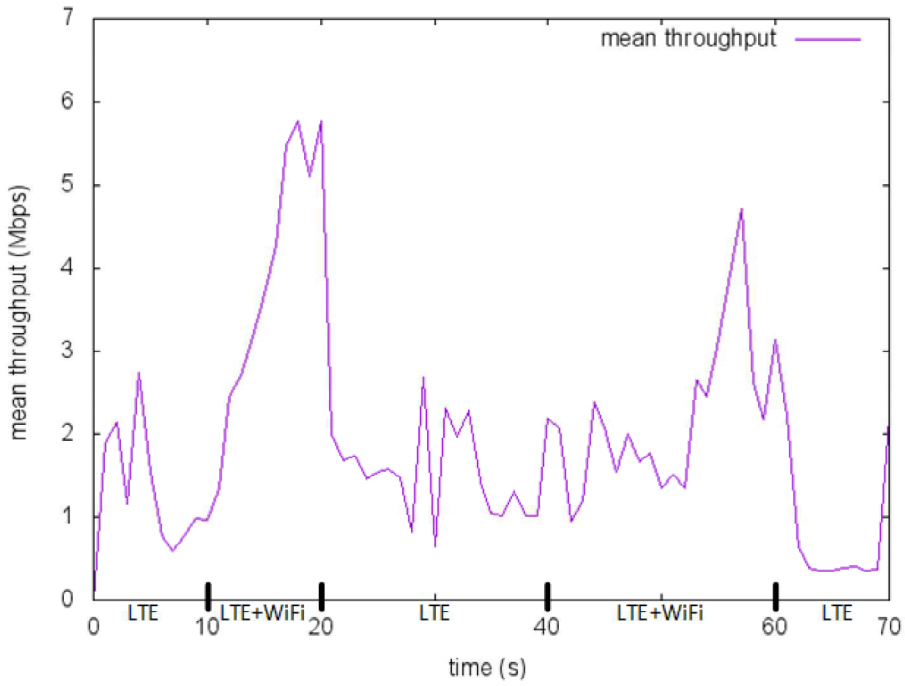


Figure 5: Débit moyen en utilisant le réordonnancement PDCP

en retard arrive.

Configuration de la couche liaison

Dans l'étude précédente, nous avons expérimenté l'utilisation de WiFi et LTE simultanément lorsque le délai sur un lien est largement supérieur au délai sur l'autre. Nous proposons d'avoir une fonction de réordonnancement de paquets au niveau de la couche PDCP ce qui assurera à TCP de recevoir toujours les paquets dans l'ordre. Nous comparons les résultats obtenus avec et sans la fonctionnement de réordonnancement. La figure 5 montre le débit moyen obtenu lorsque la fonction de réordonnancement est utilisée au niveau PDCP. Dans ce cas, les paquets envoyés sur le lien le plus rapide sont stockés et ne sont délivrés à la couche supérieur (TCP) seulement lorsque les paquets manquants envoyés sur l'autre lien sont reçus. Ce qui explique les pics de débits, comme observé dans l'expérimentation précédente, qui est un exemple typique de "head-of-line blocking". En revanche, lorsqu'aucun réordonnancement de paquet n'est effectué au niveau PDCP, le débit moyen est beaucoup plus élevé. Dans ce cas là, PDCP délivre immédiatement les paquets reçus à TCP même si des paquets sont manquants. Dans cette étude, nous avons prouvé qu'il est inutile d'ajouter une fonction de réordonnancement à la couche PDCP et qu'il est

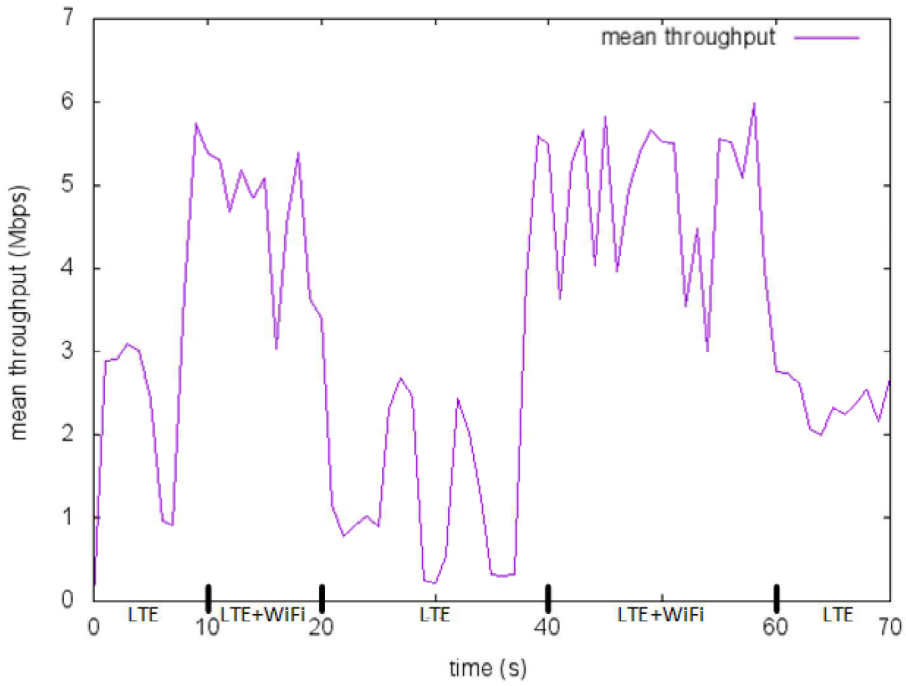


Figure 6: Débit moyen sans l'utilisation le réordonnancement PDCP

préférable de laisser TCP gérer seul les pertes et retards de paquets.

Codage réseau

Pour pallier les problèmes liés à la différence de délai sur les deux liens, nous proposons d'utiliser du codage réseau, ou "network coding". L'idée est d'envoyer après k paquets un paquet de redondance. Ce paquet est calculé en faisant l'addition logique (i.e. XOR) des k paquets. Si l'un de ces paquets est perdu, il peut être récupéré grâce au k-1 paquets reçu et au paquet de redondance. Nous avons étudié trois configurations possibles en faisant varier la valeur de k. Nous avons démontré qu'il est possible pour une petite valeur de k de limiter les chutes de débits brusques observées dans le cas de délais différents, mais que dans ce cas le débits consommés par la redondance est élevé. D'un autre coté, une grande valeur de k ne permet la récupération que de très peu de paquets perdus ou en retard, limitant son utilité.

.5 Conclusion

Dans cette thèse, nous avons défini une architecture pour le Very Tight Coupling entre WiFi et LTE. Après une étude de performance mathématique, nous avons

implémenté la solution sur une plateforme utilisant des liaisons LTE/WiFi réelles et avons effectué plusieurs types d'expérimentations. Nous avons étudié l'impact que peut avoir une grande différence de délai sur les deux liens, WiFi et LTE, et que les utiliser simultanément n'augmente pas nécessairement le débit. Nous avons également étudié la configuration de la couche de convergence (i.e. PDCP), et avons démontré que le fait d'ajouter une fonction de réordonnancement à ce niveau là est contre-productif. Finalement, nous avons proposé de faire du "codage réseau" (i.e. network coding) pour pallier le problème de la différence de délai sur les liens WiFi et LTE ; nous démontrons que dans ce cas il est nécessaire d'avoir un compromis entre taux de redondance et débit utile.

List of Publications

.6 Peer-reviewed International Conferences

1. Khadraoui, Y., and Lagrange, X. (2014). Virtual residential gateways: Architecture and performance. In EuCNC2014: 23rd European Conference on Networks and Communications.

2. Khadraoui, Y., Lagrange, X., and Gravey, A. (2014, May). A Survey of Available Features for Mobile Traffic Offload. In European Wireless 2014; 20th European Wireless Conference; Proceedings of (pp. 1-4). VDE.

3. Khadraoui, Y., Lagrange, X., HÃűst, S., and Monath, T. (2015, July). On connection Control and Traffic Optimisation in FMC Networks. In HPSR 2015: 16th International Conference on High Performance Switching and Routing.

4. Khadraoui, Y., Lagrange, X., and Gravey, A. (2016, May). Very Tight Coupling between LTE and WiFi: a Practical Analysis. In CoRes 2016.

5. Khadraoui, Y., Lagrange, X., and Gravey, A. (2016, January). Performance analysis of LTE-WiFi very tight coupling. In 2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC) (pp. 206-211). IEEE.

6. Khadraoui, Y., Lagrange, X., and Gravey, A. (2016, March). Very tight coupling between LTE and WiFi: From theory to practice. In 2016 Wireless Days (WD) (pp. 1-3). IEEE.

7. Khadraoui, Y., Lagrange, X., and Gravey, A. (2016, September). TCP performance for practical implementation of very tight coupling between LTE and WiFi. In 2016 Vehicular Technology Conference: VTC2016-Fall. IEEE.

.7 Deliverables

We contributed to the following deliverables:

1. DELIVERABLE, ICT-COMBO. D3.2 "Analysis of horizontal targets for functional convergence".

2. DELIVERABLE, ICT-COMBO. D3.5 "Assessment of candidate architectures for functional convergence".

References

[1] 3GPP. General packet radio service (gprs) enhancements for evolved universal terrestrial radio access network (e-utran). Technical report, Release 13, Technical specification TS 23.401, 2016. xiii, 15, 16, 18

[2] 3GPP. Packet data convergence protocol (pdcp) specification. Technical report, Release 12, TS 36.323 version 12.4.0, 2015. xiii, 19

[3] Stéphane Gosselin, Tahar Mamouni, Philippe Bertin, Jose Torrijos, Dirk Breuer, Erik Weis, and Jean-Charles Point. Converged fixed and mobile broadband networks based on next generation point of presence. In *Future Network and Mobile Summit (FutureNetworkSummit), 2013*, pages 1–9. IEEE, 2013. xiii, 21, 22

[4] COMBO. Analysis of horizontal targets for functional convergence. Technical report, Deliverable D3.2, 2015. xiii, 25

[5] Cisco Visual Networking Index. Global mobile data traffic forecast update, 2015-2020. Technical report, February. 2016. 1

[6] Ericsson. Mobility report. Technical report, June. 2016. 1

[7] Combo (convergence of fixed and mobile broadband access/aggregation networks), fp7 ict integrated project. URL `http://www.ict-combo.eu/`. 2, 20

[8] Xavier Lagrange. Very tight coupling between lte and wifi for advanced offloading procedures. In *WCNC Workshop, Interference and design issues for futur heterogeneous networks*. IEEE, 2014. 3, 55

[9] Younes Khadraoui, Xavier Lagrange, and Annie Gravey. Performance analysis of lte-wifi very tight coupling. In *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 206–211. IEEE, 2016. 3

[10] Younes Khadraoui, Xavier Lagrange, and Annie Gravey. Very tight coupling between lte and wifi: From theory to practice. In *2016 Wireless Days (WD)*, pages 1–3. IEEE, 2016. 4

[11] Younes Khadraoui, Xavier Lagrange, and Annie Gravey. Very tight coupling between lte and wifi: a practical analysis. In *CoRes 2016*, 2016. 4

[12] Younes Khadraoui, Xavier Lagrange, and Annie Gravey. Tcp performance for practical implementation of very tight coupling between lte and wifi. In *To be published in IEEE 84th Vehicular Technology Conference: VTC2016-Fall*, 2016. 4

[13] Wireless network mapping web site, all the networks. found by everyone. URL `https://wigle.net/`. 8

[14] Thenu Kittappa. Virtual access points: Performance impacts in an 802.11 environment and alternative solutions to overcome the problems. Technical report, Aruba White paper. 9

[15] IEEE Standards Association et al. Ieee 802.1 ad virtual bridged local area networks, amendment 4: Provider bridges. 12

[16] Amit Cohen and Ed Shrum. Migration to ethernet-based dsl aggregation. In *Broadband Forum TR-101*, 2006. 12

[17] IEEE Standards Association et al. Ieee 802.1 q virtual bridged local area networks, 2005. 13

[18] COMBO. Framework reference for fixed and mobile convergence. Technical report, Deliverable D2.1, 2013. 14

[19] 3GPP. Radio resource control (rrc) protocol specification. Technical report, Release 13, TS 36.331 version 13.1.0, 2016. 17

[20] 3GPP. Radio link control (rlc) protocol specification. Technical report, Release 13, TS 36.322 version 13.1.0, 2016. 17

[21] 3GPP. Medium access control (mac) protocol specification. Technical report, Release 13, TS 36.321 version 13.1.0, 2016. 17

[22] M Riegel et al. Mobile sctp. draft-riegel-tuexen-mobile-sctp-09. Technical report, txt, Internet draft, Internet Engineering Task Force, 2007. 17

[23] 3GPP. General packet radio system (gprs) tunnelling protocol user plane (gtpv1-u). Technical report, Release 13, TS 29.281 version 13.1.0, 2016. 18, 49

[24] Carsten Bormann and Mikael Degermark. Robust header compression (rohc): Framework and four profiles: Rtp, udp, esp, and uncompressed. 2001. 20

[25] China Mobile. C-ran: the road towards green ran. *White Paper, ver*, 2, 2011. 20

[26] Nicola Carapellese, Massimo Tornatore, and Achille Pattavina. Placement of base-band units (bbus) over fixed/mobile converged multi-stage wdm-pons. In *Optical Network Design and Modeling (ONDM), 2013 17th International Conference on*, pages 246–251. IEEE, 2013. 20

[27] COMBO-project. A universal access gateway for fixed and mobile network integration. Technical report, White paper, 2015. 22, 24

[28] CPRI Specification. V5.0 common public radio interface (cpri); interface specification, ericsson ab, huawei technologies co. *Ltd, NEC Corporation, Alcatel Lucent and Nokia Siemens Networks GmbH & Co. KG*, pages 1–119, 2011. 26

[29] Kin K Leung, Bruce McNair, Leonard J Cimini, and Jack H Winters. Outdoor ieee 802.11 cellular networks: Mac protocol design and performance. In *Communications, 2002. ICC 2002. IEEE International Conference on*, volume 1, pages 595–599. IEEE, 2002. 29, 32

[30] Elena Lopez-Aguilera, Jordi Casademont, and Josep Cotrina. Propagation delay influence in ieee 802.11 outdoor networks. *Wireless networks*, 16(4): 1123–1142, 2010. 32

[31] Giuseppe Bianchi. Performance analysis of the ieee 802.11 distributed coordination function. *IEEE Journal on selected areas in communications*, 18(3): 535–547, 2000. 33

[32] Alexander Gladisch, Robil Daher, and Djamshid Tavangarian. Survey on mobility and multihoming in future internet. *Wireless personal communications*, 74(1):45–81, 2014. 37

[33] IEEE. 802.3ad: Aggregation of multiple link segments, 2000. 40

[34] SysKonnect. Link aggregation according to ieee standard 802.3ad. Technical report, White paper, 2002. 40

[35] ITU-T Rec. G.998.2. Ethernet-based multi-pair bonding. Technical report, 2005. 40

[36] ITU-T Rec. G.998.1. Atm-based multi-pair bonding. Technical report, 2005. 40

[37] 3GPP. Study on small cells enhancements for e-utra and e-utran. Technical report, Release 12, Technical Report TR 36.842, 2013. 40, 55

[38] Hua Wang, Claudio Rosa, and Klaus I Pedersen. Dual connectivity for lte-advanced heterogeneous networks. *Wireless Networks*, 22(4):1315–1328, 2016. 40

[39] Jeffrey G Andrews. Seven ways that hetnets are a cellular paradigm shift. *Communications Magazine, IEEE*, 51(3):136–144, 2013. 515. 40

[40] Mehdi Bennis, Meryem Simsek, Walid Saad, Stefan Valentin, Merouane Debbah, and Andreas Czylwik. When cellular meets wifi in wireless small cell networks. *IEEE Communications Magazine*, 51(6), 2013. 41

[41] Miika Komu, Mohit Sethi, and Nicklas Beijar. A survey of identifier–locator split addressing architectures. *Computer Science Review*, 17:25–42, 2015. 42

[42] Dino Farinacci, Darrel Lewis, David Meyer, and Vince Fuller. The locator/id separation protocol (lisp). 2013. 42

[43] Chris White, Darrel Lewis, David Meyer, and Dino Farinacci. Lisp mobile node. 2016. 42

[44] Christian Vogt. Six/one router: a scalable and backwards compatible solution for provider-independent addressing. In *Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture*, pages 13–18. ACM, 2008. 42

[45] Anja Feldmann, Luca Cittadini, Wolfgang Mühlbauer, Randy Bush, and Olaf Maennel. Hair: Hierarchical architecture for internet routing. In *Proceedings of the 2009 workshop on Re-architecting the internet*, pages 43–48. ACM, 2009. 42

[46] Bengt Ahlgren, Jari Arkko, Lars Eggert, and Jarno Rajahalme. A node identity internetworking architecture. In *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pages 1–6. IEEE, 2006. 42

[47] RJ Atkinson and SN Bhatti. Identifier-locator network protocol (ilnp) architectural description. Technical report, 2012. 42

[48] Michael Menth, Matthias Hartmann, and Dominik Klein. Global locator, local locator, and identifier split (gli-split). *Future Internet*, 5(1):67–94, 2013. 43

[49] X Xu. Routing architecture for the next generation internet (rangi), draft-xu-rangi-04. txt, 2011. 43

[50] Xiaohu Xu and R Jain. Routing architecture for the next-generation internet (rangi), 2009. 43

[51] Amine Dhraief and Nicolas Montavont. Toward mobility and multihoming unification-the shim6 protocol: A case study. In *2008 IEEE Wireless Communications and Networking Conference*, pages 2840–2845. IEEE, 2008. 43

[52] Alberto García-Martínez, Marcelo Bagnulo, and Iljitsch Van Beijnum. The shim6 architecture for ipv6 multihoming. *IEEE Communications Magazine*, 48(9):152–157, 2010. 43

[53] Amine Dhraief. *Mobility and multihoming convergence*. PhD thesis, (Institut Mines-Télécom-Télécom Bretagne-UEB), 2009. 43

[54] Robert Moskowitz, Pekka Nikander, Petri Jokela, and Thomas Henderson. Host identity protocol. Technical report, 2008. 43

[55] Jianli Pan, Subharthi Paul, Raj Jain, and Mic Bowman. Milsa: a mobility and multihoming supporting identifier locator split architecture for naming in the next generation internet. In *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, pages 1–6. IEEE, 2008. 43

[56] Jianli Pan, Raj Jain, Subharthi Paul, and Chakchai So-In. Milsa: A new evolutionary architecture for scalability, mobility, and multihoming in the future internet. *IEEE journal on selected areas in communications*, 28(8):1344–1362, 2010. 43

[57] Dino Farinacci, Tony Li, Stan Hanks, David Meyer, and Paul Traina. Generic routing encapsulation (gre). Technical report, 2000. 43

[58] N Leymann, C Heidemann, M Wesserman, L Xue, and M Zhang. Gre notifications for hybrid access. draft-lhwxz-gre-notificationshybrid-access-01. Technical report, txt, Internet draft, Internet Engineering Task Force, 2014. 43

[59] Randall Stewart. Stream control transmission protocol. Technical report, 2007. 44

[60] Alan Ford, Costin Raiciu, Mark Handley, and Olivier Bonaventure. Tcp extensions for multipath operation with multiple addresses. Technical report, 2013. 44

[61] Sébastien Barré, Olivier Bonaventure, Costin Raiciu, and Mark Handley. Experimenting with multipath tcp. In *ACM SIGCOMM Computer Communication Review*, volume 40, pages 443–444. ACM, 2010. 45

[62] Christoph Paasch, Simone Ferlin, Ozgu Alay, and Olivier Bonaventure. Experimental evaluation of multipath tcp schedulers. In *Proceedings of the 2014 ACM SIGCOMM workshop on Capacity sharing workshop*, pages 27–32. ACM, 2014. 45

[63] Oh Chan Kwon, Yunmin Go, Yongseok Park, and Hwangjun Song. Mpmtp: Multipath multimedia transport protocol using systematic raptor codes over wireless networks. *IEEE Transactions on Mobile Computing*, 14(9):1903–1916, 2015. 45

[64] Juhoon Kim, Yung-Chih Chen, Ramin Khalili, Don Towsley, and Anja Feldmann. Multi-source multipath http (mhttp): a proposal. *ACM SIGMETRICS Performance Evaluation Review*, 42(1):583–584, 2014. 45

[65] Mike Belshe and Roberto Peon. Spdy protocol. 2012. 46

[66] R Hamilton, J Iyengar, I Swett, and A Wilk. Quic: A udp-based secure and reliable transport for http/2. *IETF, draft-tsvwg-quic-protocol-02*, 2016. 46

[67] Gaetano Carlucci, Luca De Cicco, and Saverio Mascolo. Http over udp: an experimental investigation of quic. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, pages 609–614. ACM, 2015. 46

[68] R Stewart, Q Xie, M Tuexen, S Maruyama, and M Kozuka. Sctp dynamic address reconfiguration. *IETF RFC5061. Sep*, 2007. 46

[69] Seok J Koh, Mee Jeong Lee, Maximilian Riegel, Mary Li Ma, and Michael Tuexen. Mobile sctp for transport layer mobility. *draftreigel-sjkoh-sctp-mobility-04. txt, Internet draft, IETF*, 2004. 46

[70] Charles Perkins. Ip mobility support for ipv4. Technical report, 2002. 47

[71] Charles E Perkins. Mobile ip. *IEEE communications Magazine*, 35(5):84–99, 1997. 47

[72] D Johnson, C Perkins, and J Arkko. Rfc 3775: Mobility support in ipv6. *IETF, June*, 2004. 48

[73] George Tsirtsis, V Park, and H Soliman. Dual-stack mobile ipv4. Technical report, 2009. 48

[74] Sri Gundavelli, Kent Leung, Vijay Devarapalli, Kuntal Chowdhury, and Basavaraj Patil. Proxy mobile ipv6. Technical report, 2008. 48

[75] 3GPP. Ip flow mobility and seamless wireless local (wlan) area network offload. Technical report, Release 10, Technical Report TS 22.261. 48

[76] Antonio De la Oliva, Carlos Jesus Bernardos, Maria Calderon, Telemaco Melia, and Juan Carlos Zuniga. Ip flow mobility: smart traffic offload for future wireless networks. *Communications Magazine, IEEE*, 49(10):124–132, 2011. 48

[77] Jonathan Rosenberg, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley, and Eve Schooler. Sip: session initiation protocol. Technical report, 2002. 49

[78] 3GPP. Architecture enhancements for non-3gpp accesses. Technical report, Release 10, Technical specification TS 23.402, 2012. 57

[79] 3GPP. Access network discovery and selection function (andsf) management object (mo). Technical report, Release 13, Technical specification TS 24.312, 2016. 57

[80] Alcatel-Lucent. Wifi roaming-building on andsf and hotspot 2.0. Technical report, White paper, 2012. 57

[81] 3GPP. Evolved universal terrestrial radio access (e-utra) and evolved universal terrestrial radio access network. Technical report, Release 13, TS 36.300, 2016-04. 74

[82] Fanglu Guo and Tzi-cker Chiueh. Sequence number-based mac address spoof detection. In *International Workshop on Recent Advances in Intrusion Detection*, pages 309–329. Springer, 2005. 74

[83] Bandar Alotaibi and Khaled Elleithy. A new mac address spoofing detection technique based on random forests. *Sensors*, 16(3):281, 2016. 74

[84] Cisco. Cisco adaptive wireless intrusion prevention system. Technical report, White paper, 2009. 74

[85] Cisco. Configuring port security. Technical report, White paper, 2006. 75

[86] Rubén Fraile et al. Mobile radio bi-dimensional large-scale fading modelling with site-to-site cross-correlation. *European transactions on telecommunications*, 19(1):101–106, 2008. 82

[87] William C Jakes and Donald C Cox. *Microwave mobile communications*. Wiley-IEEE Press, 1994. 82

[88] John David Parsons. *The mobile radio propagation channel*, volume 2. John Wiley New York, 2000. 82, 88

[89] Gordon L Stüber. *Principles of mobile communication*. Springer, 2011. 82

[90] Andrew J Viterbi et al. Soft handoff extends cdma cell coverage and increases reverse link capacity. *IEEE Journal onSelected Areas in Communications*, 12 (8):1281–1288, 1994. 83

[91] 3GPP. Radio network planning aspects. Technical report, Release 1999, Technical Report TR 03.30, 2005. 88

[92] Open air interface. URL `http://www.openairinterface.org`. 95

[93] Jouni Malinen. hostapd: Ieee 802.11 ap, ieee 802.1 x/wpa/wpa2/eap/radius authenticator. *Hostapd: IEEE 802.11 AP, IEEE 802.1 X/WFA/WFA2/EAP/RADIUS Authenticator*, 2013. 96

[94] Sangtae Ha, Injong Rhee, and Lisong Xu. Cubic: a new tcp-friendly high-speed tcp variant. *ACM SIGOPS Operating Systems Review*, 42(5):64–74, 2008. 98

[95] S Floyd, J Mahdavi, M Mathis, and A Romanow. Tcp selective acknowledgment options. 1996. 98

[96] Ajay Tirumala, Feng Qin, Jon Dugan, Jim Ferguson, and Kevin Gibbs. Iperf: The tcp/udp bandwidth measurement tool. *htt p://dast. nlanr. net/Projects*, 2005. 98

[97] Alexey N. Kuznetsov. Linux traffic control tool. *http://linux.die.net/man/8/tc*. 103

[98] Stephen Hemminger. Netem-emulating real networks in the lab. In *Proceedings of the 2005 Linux Conference Australia, Canberra, Australia*, 2005. 103

[99] Mun Choon Chan and Ramachandran Ramjee. Tcp/ip performance over 3g wireless links with rate and delay variation. *Wireless Networks*, 11(1-2):81–97, 2005. 105

[100] Ming Li, Andrey Lukyanenko, and Yong Cui. Network coding based multipath tcp. In *Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on*, pages 25–30. IEEE, 2012. 105, 111

[101] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li, and Raymond W Yeung. Network information flow. *Information Theory, IEEE Transactions on*, 46(4): 1204–1216, 2000. 111

Résumé

Le trafic de données mobiles augmente de façon permanente. Afin d'éviter une saturation, les opérateurs doivent décharger le réseau cellulaire vers des réseaux d'accès alternatifs. WiFi se trouve être une bonne solution qui permet à l'opérateur de tirer parti de bandes de fréquence sans licence ainsi que du très grand nombre de points d'accès déjà déployés.

Dans cette thèse, nous présentons tout d'abord un état de l'art des différentes solutions de couplage entre LTE et WiFi. Nous montrons que la plupart de ces solutions ne garantissent pas la continuité de session ou sont sujettes à une duplication des procédures de sécurité. Ceci a conduit à la proposition du Very Tight Coupling entre LTE et WiFi. Dans ce type d'architecture, les points d'accès WiFi sont connectés à une station de base LTE et les mécanismes de sécurité LTE sont réutilisées afin de permettre un accès rapide au réseau WiFi. Ceci permet également d'avoir une double connectivité et de garder le trafic de signalisation sur le réseau LTE, ce qui donne la possibilité d'avoir des procédures de sélection optimisées.

Nous étudions comment le Very Tight Coupling peut être implémenté et comment les points d'accès WiFi intégrés dans les passerelles résidentielles peuvent être connectées aux stations de base LTE dans le cas d'un réseau fixe/cellulaire convergent. Nous évaluons ensuite par des outils mathématiques, les performances de différents schémas de couplage et calculons le taux de capacité pouvant être économisée. Ensuite, nous présentons une implémentation du Very Tight Coupling sur une plateforme utilisant une interface radio LTE réelle basée sur Open Air Interface. Nous effectuons plusieurs expérimentations afin de trouver la meilleure configuration du protocole de la couche liaison de données. Nous démontrons que le fait d'utiliser WiFi et LTE en parallèle n'augmente pas systématiquement le débit.

Mots-clés : LTE, WiFi, Réseaux hétérogènes

Abstract

The mobile data traffic has been continuously increasing. To avoid saturation of cellular network, operators need to use alternative access networks for offloading purpose. WiFi is a good solution as the operator can take advantage of its unlicensed spectrum as well as the large number of deployed WiFi access points.

In this thesis, we first provide a state-of-the-art of the different coupling solutions between LTE and WiFi. We show that most solutions cannot guarantee session continuity or duplicate the security procedures. This leads to propose «Very Tight Coupling» between LTE and WiFi. In this architecture, WiFi access points are connected to the LTE base stations and the security mechanisms of LTE are reused to ensure fast access to WiFi. It allows dual connectivity and to keep control signalling in the LTE network, which gives the possibility to have optimized interface selection procedures.

We study how very tight coupling can be implemented and how WiFi APs that integrated in customer residential gateways can be connected to LTE base stations in a converged fixed/cellular network. We then mathematically evaluate the performance of different deployment schemes and compute how much capacity can be saved on the LTE network.

Furthermore, we implement the solution on a platform with a real LTE radio interface based on the Open Air Interface framework as a proof-of-concept. We perform several experiments to find the configuration of the link-layer protocols that gives the highest bit rate. In particular, we show that using WiFi and LTE simultaneously does not always increase the bit rate.

Keywords : LTE, WiFi, Heterogeneous networks

TELECOM Bretagne

n° d'ordre : 2016telb0411
Télécom Bretagne
Technopôle Brest-Iroise - CS 83818 - 29238 Brest Cedex 3
Tél : + 33(0) 29 00 11 11 - Fax : + 33(0) 29 00 10 00