Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2010, Article ID 205786, 21 pages
doi:10.1155/2010/205786

Research Article

Technology Integration Framework for Fast and Low Cost Handovers—Case Study: WiFi-WiMAX Network

Mohamed Kassab,[1] Jean-Marie Bonnin,[1] and Abdelfettah Belghith[2]

[1] *Telecom Institute/Telecom Bretagne/RSM Department, Université Européenne de Bretagne, 35510 Cesson Sevigné, France*
[2] *ENSI/CRISTAL Lab/HANA Research Group, University of Manouba, 2010 Manouba, Tunisia*

Correspondence should be addressed to Mohamed Kassab, mohamed.kassab@gmail.com

Received 1 October 2009; Revised 14 February 2010; Accepted 18 April 2010

Academic Editor: K. Daniel Wong

The Next Generation Wireless Networks (NGWNs) are seemed to be heterogeneous networks based on the integration of several wireless technologies. These networks are required to achieve performances equivalent to classic wireless networks by ensuring the continuity of communications and the homogeneity of network management during horizontal and vertical handovers. This task is even more important when management services, like security and quality of service (QoS), are deployed at access technology level. In this paper, we propose a framework for heterogeneous wireless technology integration based on network architecture skeleton and a handover management mechanism. This framework optimizes the layer-2 handover procedure to achieve performances required by sensitive applications while ensuring the minimization of signaling overhead required for operated networks. As an application example, we make use of this framework to propose a heterogeneous network based on WiFi and WiMAX technologies. We present an application example of the framework using the specification of a WiFi-WiMAX network. We propose several performance evaluations based on simulation tests based on this application. The latter confirm the efficiency of handover delay optimization and the minimization of management signaling costs.

1. Introduction

The growth of wireless communication has been, in a few years, important thanks to the advantages they offer such as deployment flexibility and user mobility during communications. Several wireless technologies have emerged. These technologies have been designed independently and intended to cover specific service types, user categories, and usability domains. Among these technologies, there is not one good and generic enough to replace all the others; each technology has its own merit, advantages, and development possibilities. For example, 3G technologies, for example, UMTS and CDMA2000, propose network access associated to telephony services. WMAN technologies, for example, WiMAX and HyperMAN, are used to deploy outdoor metropolitan networks. WLAN technologies, for example, WiFi, have been developed to be an extension of already existing wired LANs; they are also used to deploy local public wireless networks. In addition, user categories and usability domains have converged so that terminals and communication means have evolved to integrate multiple technologies.

The result of this evolution is a multitechnology environment that can be exploited to offer an enhanced connectivity to users. The Next Generation Wireless Networks (NGWNs) appear to be the integration of already existing and newly developed wireless technologies that offers a heterogeneous access to the same global core network. A multi-technology terminal will be able to change its access technology each time its environment changes. For example, it will be connected to a WiFi access point when it is in the mall; it will handover to the WiMAX when it will move to the street and it will use UMTS in the train. This could be a great advance depending on the adequate mechanisms which are available to ensure a seamless mobility.

On the other hand, wireless technologies are no longer limited to be a basic communication medium. They evaluate by integrating several management services such as user authentication, data exchange confidentiality, and QoS management. However, the integration of these services at the access technology level with specific designs will affect the handover performances in NGWNs. In fact, the change of the serving Point of Attachment (PoA) requires the renegotiation of management services between the terminal and the network in addition to the redirection of data traffic to the new terminal location. As a result, the HO execution time may increase significantly, which should induce significant latency to exchanged data and even the break of the ongoing session.

Public wireless networks have to guarantee a good level of service while insuring the transparency of management to users. The deployment of such networks using heterogeneous technologies will require a good connectivity during handovers, by reducing latency, and the homogeneity of management services such as authentication and QoS. This is possible by deploying anticipation mechanisms that reduce negotiation exchanges between the terminals and the network, such as context transfer and proactive negotiation [1], and accelerate the redirection data traffic during the execution of the HO.

Researchers have been interested in this problem and several papers have proposed models for efficient technology-integration solutions that deal with network access provider requirements. However, the mobility management offered by these solutions does not ensure yet seamless handovers during heterogeneous mobility. Indeed, most solutions offer roaming possibilities based on the sharing of user databases. At best, the integration architectures offer to graft one technology to another and to manage heterogeneous mobility based on Mobile IP and extensions. These solutions enable the optimization of the network reattachment (i.e., the layer-3 HO) by limiting the heterogeneous handover to the re-attachment to the new PoA (i.e., layer-2 HO). This does not solve the connectivity disruption due to the re-establishment of network services defined at the technology level. On the other hand, the structure of these technology-integration solutions is not suited to heterogeneous mobility. Indeed, the organization of the PoAs in the core network is based on the access technology they offer rather than the closeness of radio coverage while the executed HOs will be based on the latter closeness. As a consequence, the HO management mechanisms based on exchanges between heterogeneous entities will result in a nonnegligible overhead that could disrupt the network performances.

In this work, we propose a technology-integration framework that provides a new approach to deploy next generation wireless networks. This framework offers a heterogeneous access to a global network with optimized mobility performances regarding HO execution time and signaling cost. The idea is to optimize the layer-2 HO execution in a heterogeneous and homogeneous mobility and to adapt the network architecture so that this optimization yields to a minimum signaling surplus. The framework defines a network architecture skeleton and HO management mechanisms. They tend to optimize the layer-2 HO execution while ensuring the continuity of management services defined at the technology-level. In addition, we propose an application of this framework to an actual wireless network based on the WiFi and WiMAX technologies. We make use of this application to demonstrate the ability of the proposed framework to enable the enhancement of HO performances while ensuring a reduced signaling overhead.

This paper is organized as follows. In Section 2, we propose an overview of solutions adopted for wireless technology integration. In Section 3, we detail the specification of the technology-integration framework. We propose, in Section 4, the specification of wireless network based on the WiFi and WiMAX technologies. We demonstrate the advantages offered by this architecture based on performances evaluations in Section 5. We detail how the proposed framework can get along with layer-3 mobility management mechanisms in Section 6. We propose, in Section 7, a discussion about heterogeneous technology integration. We draw up main conclusions and propose future trends of our work in Section 8.

2. Technology Integration in the Literature

Heterogeneous-technology integration has been studied by several researches. Most studies focused on networks integrating UMTS and data wireless technologies, that is, WiFi [2–6] and WiMAX [7–9]. Two inter working architectures have been proposed: loosely and tightly coupled architectures [2, 10].

With loosely coupled architecture, the interconnected technologies are considered as independent networks concerning the handling of data traffic and the management of network services such as authentication and QoS. Each technology has a separate user subscription and profile management systems. Roaming privileges are assigned to subscriptions related to one network. This helps to minimize session disruption based on the cooperation of accounting entities. The tightly coupled architecture proposes the integration of wireless technologies in the same network architecture. This integration may be performed in different levels of the management architectures of the considered technologies. User subscriptions and profiles are management based on common centralized entities. In all cases, user mobility is managed using Mobile IP and its extensions [11].

The main advantage of loosely coupled architectures is the few modifications to technologies and their core network architectures. However, due to the high level of integration, the mobility management mechanisms are not able to optimize significantly the performance of layer-3 handover. Thus, the roaming mechanisms are not able to reduce sufficiently the session disruption to deal with requirements of sensitive applications.

The tightly coupled architectures propose integration at lower level of network architecture. The complexity of the implementation increases, and more modifications must be operated to technologies and core network architecture. Nevertheless, the lower level of integration ensures a very interesting enhancement of HO performances [4, 5]. This is due to the fact that the inter-working takes place at a point of the management architecture closer to the mobile terminal.

The tightly coupled architecture can significantly improve the performance of heterogeneous handovers. This can be even more enhanced by using the ConteXt Transfer Protocol (CXTP) [12] in addition to MIP. The CXTP proposes a protocol to transfer mobile terminal contexts between Access Routers managing the access control of a wireless network. CXTP has been designed as a generic protocol that can accommodate a wide range of services. The context transfer can be reactive, during the HO execution, or proactive from the serving AR to a possible target AR. CXTP can be useful if some network services such as user authentication and QoS are integrated to the layer-3 level in wireless networks [13]. Consequently, several management exchanges between a terminal and the Access Router (AR), which controls the access to the network, are required during the network entry. Thus, the CXTP enables the reduction of exchanged messages between mobile terminal and target AR during the HO execution.

However, the latter optimization limits only the effects of sub network change during terminal mobility (layer-3 HO optimization). Indeed, all the negotiation exchanges and the service establishment procedures defined at access-technology level must be performed during heterogeneous handover executions.

A solution could be the association of the tightly coupled architectures to an optimization of the terminal to technology association procedure. This optimization will take into account the possible resemblances between the definition of services and user profiles of technologies to prevent the execution of the negotiations and procedures during handover executions. This may be based on management mechanisms like context transfer or proactive execution of exchanges.

3. Technology-Integration Framework

This framework aims at defining an optimization of the handover performances as part of a heterogeneous mobility.

We consider an operator network that offers a reliable network access, to mobile terminals, based on several wireless technologies. Network services, such as user authentication, QoS management, and billing, have to work properly and seamlessly while terminals are moving over the network. We define the network architecture and the position of management entities that are involved in the handover management procedure.

The proposed framework specifies the skeleton of the network architecture, the definition of mobility context and the L2-HO management mechanisms. The latter proposes the enhancement of L2-HO performances based on mobility-context exchanges.

3.1. Network Architecture Skeleton. The global wireless network is organized into *access subnetworks*, each one gathering a set of PoAs. We do away with the classic organization of wireless networks that separates each technology in an autonomous network. PoAs can be gathered in access sub networks based on the closeness of their wireless coverage or based on common management requirements. It also remains possible to gather PoAs offering the same wireless access technology. We define new management entities: *the Layer 2 Access Managers (L2-Acc-Mgrs)* that manage terminal mobility over the network. To each access subnetwork is associated an L2-Acc-Mgr. Figure 1 shows this architecture.

The L2-Acc-Mgr integrates several functions to manage terminal mobility. It acts as a *service proxy* regarding exchanges between terminals and core network entities during the network entry procedure. For example, terminal authentication is supported by the L2-Acc-Mgr that acts as AAA-proxy between the terminal and the AAA server in the core network. At the end of this procedure, the L2-Acc-Mgr maintains the terminal authentication profile (authentication keys) to use it for future purposes.

The L2-Acc-Mgr supports the *Neighborhood management function* that maintains the PoAs' neighborhood. It provides a list of PoAs to which a terminal may move while being associated with a particular PoA.

The *L2-HO management function* integrates the intelligence related to the L2-HO management, that is, the triggering of HO management exchanges, the execution of exchanges and the management of terminal contexts.

3.2. L2-HO Management Mechanisms. During the network entry, a terminal associates itself with the network and activates a set of services and functionalities. The *terminal context* includes the parameters negotiated during the network entry and states related to network services used by the terminal [1]. The acceleration of the establishment of this context is required, at the time of handover, to reduce the delay that results from the HO execution phase. The establishment of the terminal context on the target PoA, based on already available information, is the solution.

The nature of information elements included in the terminal context defines how it can be exploited to perform a context re-establishment. This defines values of information elements to be established, when and how they will be established, and the network entities that have to manage these information elements [1]. Authors in [14] propose a study that define the latter points based on the characteristics of information elements and particularly:

(i) the scope of the information element,

(ii) the transferability of the information element,

(iii) and the stability of the information element value over the time.

In the following part, we identify the network entities that will manage the context establishment, the values to be established, the mechanisms that establish contexts, and finally when the establishment has to be performed (i.e., before, during, or after the HO execution), while taking into account the network architecture decided upon and the nature of information elements that may be included in terminal contexts.

3.2.1. Management of Terminal Contexts. Regarding the scope, a terminal context consists of *global session* and *local*

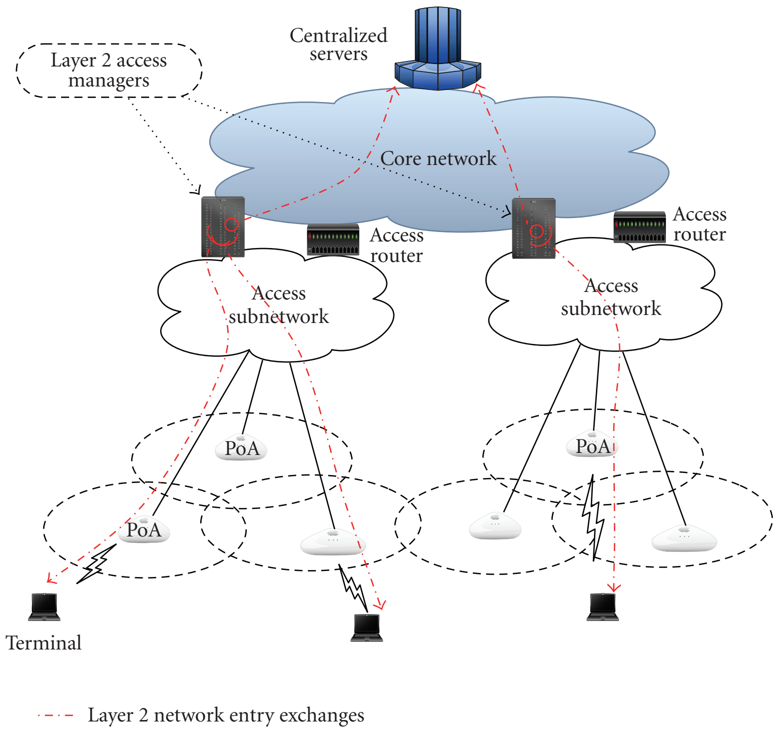


Figure 1: The L2-Acc-Mgr in the network architecture.

association information elements. The *global session* information elements are related to the association established between the terminal and the core network entities such as AAA servers. The *local association* information elements are related to the association established between the terminal and the serving PoA. When a terminal executes a HO without performing a new network entry, it maintains its *global session* while re-establishing the *local association* with the new serving PoA.

Then, a context information element is *transferable information* when it remains valid while the terminal changes its serving PoA. Such information element can be reused with target PoA to avoid renegotiation during HO execution. Other elements are *nontransferable context information*, their current value, associated to a serving PoA, cannot be exploited to avoid negotiations between the terminal and target PoA to establish a new association. This type of information has to be re-established through regular exchanges during the HO execution. Finally, an information element can be *conditionally transferable* if the value associated to the serving AP is not valid for transfer; however, it can be used to define a new value associated to target PoAs. It is possible to define *translation rules* for this specific set of information elements so as to enable their establishment while avoiding negotiations during HO execution.

Based on these two classifications we define the content of terminal contexts and the entities that have to manage these contexts, following the recommendation proposed in [1].

The L2-Acc-Mgr is the most entitled entity to manage the greater part of the terminal context. First, the global session information elements are held by the L2-Acc-Mgr thanks to the *service proxy function*. Second, local information elements that are conditionally transferable may require centralized information related to the neighbor PoAs or the terminal to be translated for re-establishment. The latter information is held by the L2-Acc-Mgr, so it is the better able to manage conditionally transferable local information elements. The *HO management function* of the L2-Acc-Mgr is responsible of managing the latter information elements, of the terminal context.

The *HO management function* defines the values for information elements to be established by the L2-Acc-Mgr. The latter values will be derived based on the ones used with the current association, cached information elements or terminal accounting profile. A *Translation function* is defined as a part of the *HO management function*. It is responsible of defining values to be established for information elements constituting the context terminal.

This case can be illustrated over a heterogeneous wireless network offering access to multi-technology terminals. A mobile terminal can switch between two PoAs offering heterogeneous technologies. In this case, QoS parameters can be transferred to re-establish the new association since the two wireless technologies do not necessarily use the same QoS representation. A QoS translation function can solve the conformity problem as most QoS management mechanisms have common bases.

The definition of new values for a context information element may result into a synchronization problem between the terminal and the network. Indeed, the terminal must be able to integrate the translation subfunction used by the

L2-Acc-Mgr to define the new information element value. Therefore, *the translation rules* are defined so that both the terminal and the L2-Acc-Mgr can compute a value that corresponds to the new association without performing any exchange.

The local information elements that have values valid for different local associations (transferable information), are managed by the PoAs. A serving PoA is responsible for redistributing them to target PoAs and caching them.

Finally, there is a set of information elements that current values cannot be exploited to avoid management exchanges between a mobile terminal and the network to establish a new association. We name this category: *non transferable context information*. This type of information has to be re-established through regular exchanges during the handover execution. We can mention connection parameters used with a terminal, for example, data rate. These parameters depend on the position of the terminal in the cell and the serving AP capacity, and so they have to be negotiated during the association.

3.2.2. Context Establishment Exchanges. Two options are available for context establishment: the context transfer and the proactive negotiation [1].

The context transfer is an adequate establishment solution for transferable information elements. It is performed between the entity managing the information element and one or a set of PoAs. In the same way, conditionally transferable information element re-establishment can be based on a context transfer mechanism. After being translated, an information element is transferred to target PoAs.

The context transfer is not the appropriate solution for the re-establishment of non-transferable information elements. An information element might require to be re-established over standard exchanges or the involvement of the terminal in the negotiation or generation process. It remains possible to establish non transferable information elements using *proactive negotiations*. The latter are based on the standard exchanges usually performed during the network entry procedure to generate information elements.

The adequate time to perform a context establishment depends on the stability of the information element value during the time. There are static information elements that values do not change during the local association and dynamic information elements that values change during a local association based on network conditions, terminal behaviors, accounting constraints, and so forth. Proactive context establishment can be performed with static information elements so that it will be available immediately at the HO execution. However, proactive establishment is not excluded with dynamic context. This depends on the frequency of information element update. If an information element is known not to be frequently updated, it remains possible to perform a *conditional proactive establishment*. The information element shall be associated to a *validity condition*. At the time of the handover, the information element is used only if the validity condition is verified. In other cases, the information element is established reactively during HO execution based on its last update.

3.2.3. HO Establishment Exchanges. Regarding our specification, the context transfer is suitable for information elements managed by the L2-Acc-Mgr. Proactive and reactive exchanges are combined to manage static and dynamic information elements. The exchange (a) of Figure 2 shows the proactive establishment procedure involving the L2-Acc-Mgr and two neighbor PoAs. The target PoA may execute a reactive exchange to obtain values related to dynamic information elements from the L2-Acc-Mgr as shown in Figure 2(b).

The establishment of local association information elements managed by serving PoA can be based on *context transfer* and/or *proactive negotiation*. These mechanisms may be combined to establish one or more information elements in the same procedure or used as alternatives for the same information element to define different procedures since they have different properties [1]. Figure 3 shows exchanges based on the two mechanisms.

The context transfer can be proactive and/or reactive. For the proactive one, the establishment exchanges are initiated by the serving PoA with a list of neighbor PoAs indicated by the L2-Acc-Mgr. During HO execution, a target PoA may require additional information elements from the serving PoA. As such, it can engage reactive context transfers with the previous serving PoA.

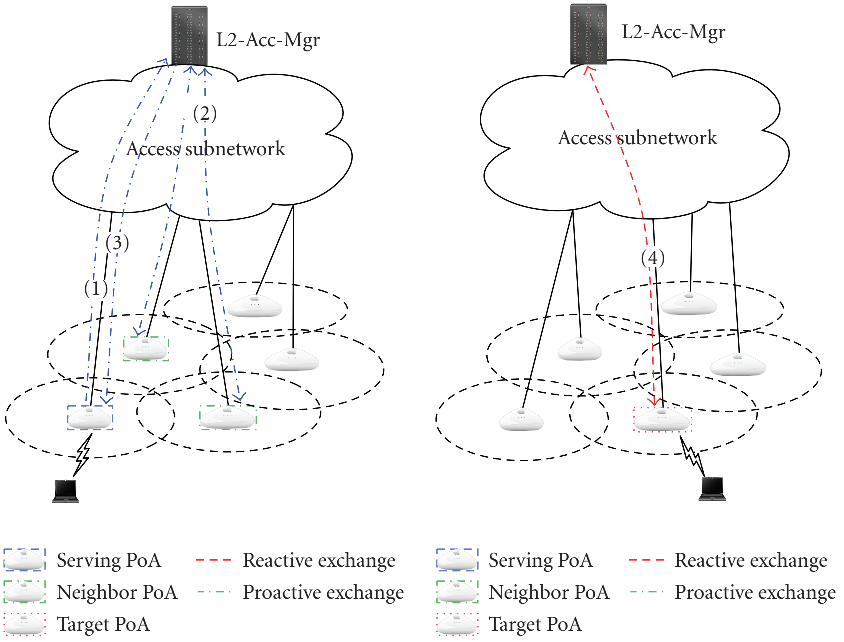
Proactive negotiations are engaged between the terminal and neighbor PoAs through the current association (established with the serving PoA). It is mostly used for information elements managed by PoAs that cannot be established through context transfer.

The L2-Acc-Mgr is responsible of managing L2-HO management exchanges with entities associated to its access subnetwork (i.e., PoAs and terminals) and L2-Acc-Mgrs from other access subnetworks. Consequently, the L2-HO management exchanges are limited to the access subnetwork during intrasubnet mobility. Intersubnetworks exchanges are relayed by L2-Acc-Mgrs during inter-subnetwork mobility. A target L2-Acc-Mgr converses with the serving L2-Acc-Mgr for centralized establishment exchanges as shown in Figure 4.

In a nonoptimized architecture, the HO management exchanges between PoAs are routed through the core network from one access subnetwork to another during intersubnet mobility. The HO management exchanges between PoAs and centralized entities, during an intra-subnet mobility event, are engaged through the core network while the terminal mobility is restricted to the access network. Thus, the use of L2-Acc-Mgrs restricts as much as possible the HO management operations to intra-access subnetwork exchanges. This may ensure the efficiency of these exchanges and reduce the signaling overhead over the core network.

4. WiFi-WiMAX Network

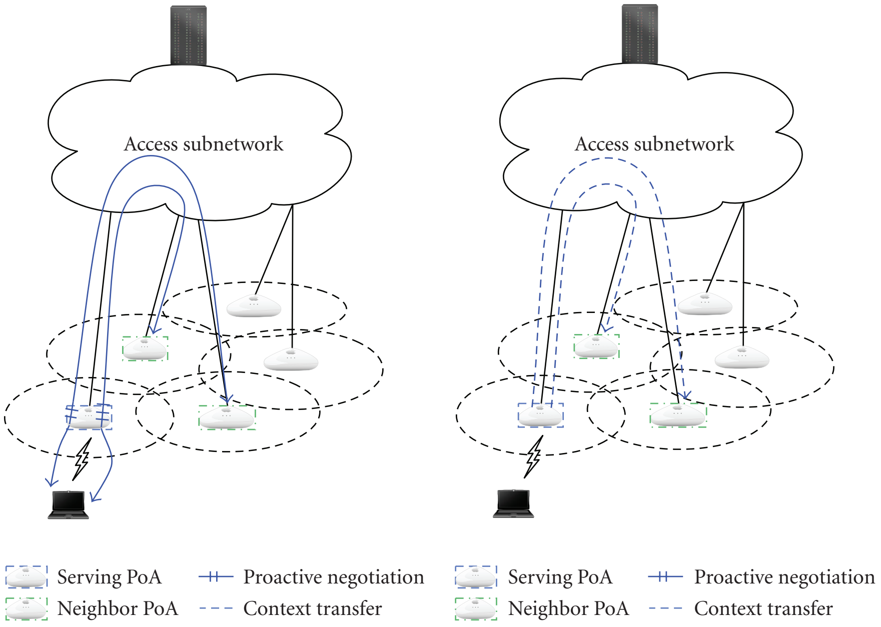
As an application of the technology-integration framework, we propose the integration of the WiFi and WiMAX



(a) proactive establishment

(b) reactive establishment

Figure 2: Centralized establishment.



(a) Proactive negociation

(b) Context Transfer

Figure 3: Distributed establishment.

technologies in a heterogeneous wireless network. This network offers to terminals a wireless connectivity adapted to their location. The WiMAX is deployed for an outdoor access and the WiFi in building for indoor access. Terminals will roam from one technology to another according to their movements while being attached to the same global network.

4.1. WiFi-WiMAX Integration in the Literature. Some researches were interested in the collaboration between WiFi and WiMAX technologies. Most of these researches have proposed to use the WiMAX technologies as backhaul support for WiFi hotspot [7, 15, 16]. Therefore, the designed networks did not fall within the category of 4G networks, and the two technologies do not cooperate to offer the wireless access to mobile users. More recent research studies were interested in the inter-working of the WiFi and the WiMAX as access technologies in the same heterogeneous network. However, the majority of these studies were limited to the enhancement of the HO decision mechanism between the two technologies and did not discuss the problems related to the integration and the collaboration of these technologies in the same network architecture [17–19].

In [20], authors were interested in inter-working of the WiFi and the WiMAX technologies. They proposed a solution to ensure a continuity of QoS management through the heterogeneous wireless access. The solution proposes a mapping between the QoS management parameters of each technology to ensure seamless change of technologies. To fix the context of their work, authors tried to define an interconnection architecture for the network. They proposed the interconnection of separate WiFi and WiMAX access networks through a core network and to manage the layer-3 HO using Mobile IP. However, no additional management arrangements were proposed (e.g., collaboration between QoS accounting, context transfer between BSs and APs) to enable the use of the QoS mapping through the deployed access network.

Thus, at the best of our knowledge, there is no serious work that offers a design of a heterogeneous network integrating the WiFi and the WiMAX technologies.

4.2. Technologies' Overview. We propose an overview of the WiFi [21] and WiMAX technologies [22]. We focus particularly on the network architecture and the layer-2 network service defined by each technology and the manners in which they interact with mobility management.

4.2.1. WiFi. The WiFi technology is based on the IEEE 802.11 standard that defines the PHY and MAC layers for the wireless medium. This standard has been completed by several extensions that define services such as the QoS management and user authentication. The proposed specification is limited to the management of these services through the wireless part of the network and has not defined operations that involve centralized entities.

User authentication is proposed by IEEE 802.11i extension [23] that defines a robust securing mechanism offering a privacy equivalent to wired network. It proposes a complete security framework defining the security architecture, the key hierarchy, and the cryptographic mechanisms. The 802.11i authentication is based on an authentication key hierarchy and key generation exchanges. They establish mutual authentication between peers and generate cryptographic suite to secure data exchanges.

The basic IEEE 802.11 standard offered only a best effort service to an application flow. The QoS management for the WiFi technology has been defined by the IEEE 802.11e extension [24]. Two operation modes have been defined:

(i) a per-packet QoS management, *the prioritized QoS*, based on priorities associated to transmission queues with different channel access priorities,

(ii) a per-flow QoS management, *the parameterized QoS*, based on QoS parameters associated to virtual traffic stream. The latter are a set of data packets to be transferred in accordance with the QoS requirements of an application flow.

Table 1: User priority to traffic class mapping.

User Priority	Traffic Type	Description
1	Background	Bulk transfers, games, etc.
2	Spare	
0	Best Effort	Ordinary LAN priority
3	Excellent Effort	Best Effort for important users
4	Controlled Load	Some important applications
5	Video	Less then 100 millisecond delay
6	Voice	less than 10 millisecond delay
7	Network Control	High requirements

The WiFi equipments and deployed networks are followed by particular evolution. Indeed, the QoS management proposed by IEEE 802.11e was not adopted in network deployments. The enhancements of the communication performances were based on the evolution of the PHY layer performances.

With the WiFi-WiMAX integration, the WiFi technology will coexist with the WiMAX technology, which offers a strong service differentiation between categories of data traffics based on user profiling (c.f. the next subsection). So as to offer a homogenous network access service to users over the network, we propose to adopt a QoS-enabled WiFi access in our specification. We consider the *Parameterized QoS* as it most closely matches the QoS management defined by WiMAX [25].

The Parameterized QoS proposes a QoS management based on virtual connections: the Traffic Streams (TSs). The latter are sets of data packets to be transferred in accordance with the QoS requirements of an application flow. A terminal specifies TS requirements to the Access Point (AP) using the admission control exchange. The requirements can be data rate, packet size, service interval, and so forth. An AP may accept or reject new Traffic Specification requests based on the network conditions, terminal profile, and so forth. The traffic differentiation is based on traffic specification (TSPEC) associated to TSs. The TSPEC element contains a set of QoS parameters that define the characteristics and the QoS expectations of a traffic flow. In addition User Priorities (UP) are used to indicate the traffic class of the TS. Table 1 presents the mapping between UP values and traffic class.

The WiFi technology was developed to be an extension of wired networks and not as an operator technology such as WiMAX or UMTS. Thus, the IEEE 802.11 standard and its extensions have not specified the core network architectures and mechanisms. The deployment of RSN security and parameterized QoS requires an AAA server that manages the identities and the profiles of authorized users.

The negotiations defined by the WiFi authentication and the parameterized QoS, during the network entry, require considerable time, which turns into a connection

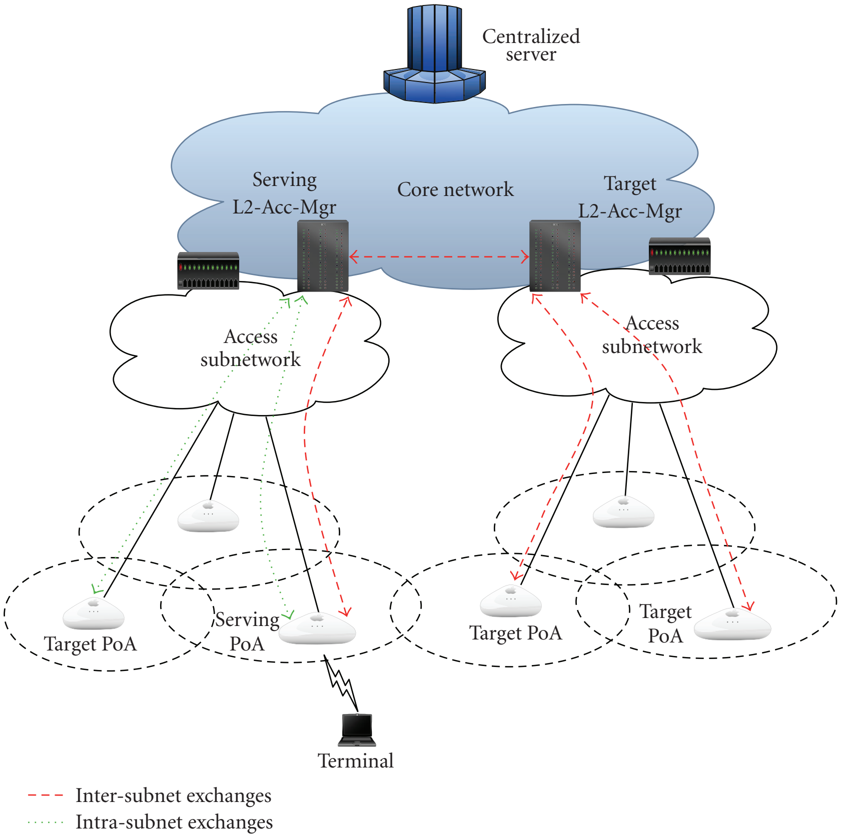


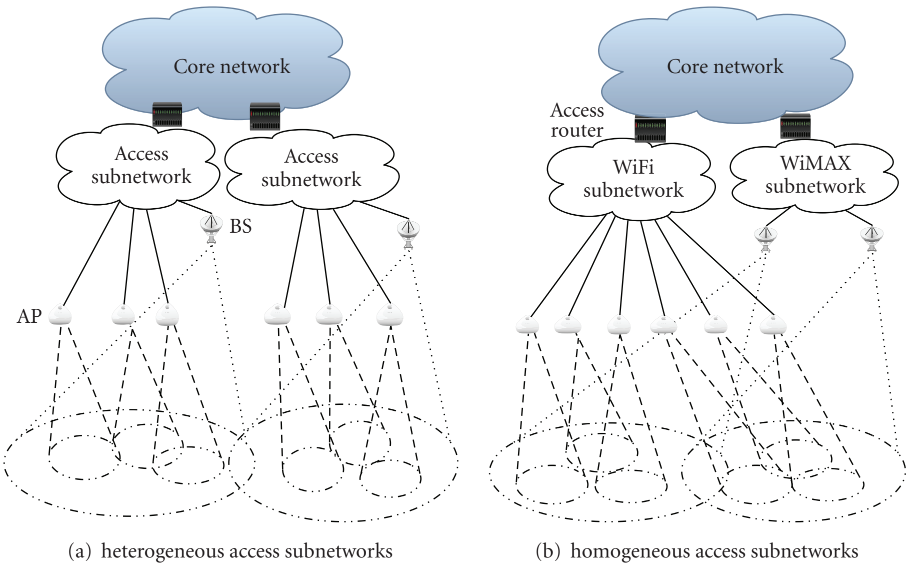
Figure 4: HO management exchanges.

interruption during a handover. The authentication process can last up to 1 s [26]. Several solutions are available to ensure reduced authentication delays during horizontal HO less than 25 milliseconds (ms) [27]. However, these solutions are not effective for a heterogeneous HO management, which will be the current architecture results to a new network entry for the target technology.

4.2.2. WiMAX. The WiMAX technology offers a last mile wireless broadband access as an alternative to cable and DSL. It defines the physical layer design and the wireless medium access mechanism and network services such as the QoS management, mobility management, user authentication, and accounting for wireless part of the network based on the IEEE 80216 standards [28, 29]. In addition, an end-to-end network specification is proposed by the WiMAX forum [30–33]. It includes the core network architecture reference models, protocols for end-to-end aspects, procedures for QoS management, and user authentication.

The reference model defines a logical modeling of the network architecture. The Access Service network (ASN) is defined as a set of network functions providing radio access to mobile stations. The Connectivity Service Network (CSN) is a set of network functions that provides IP connectivity services to Mobile Stations such as IP parameters allocation, Policy and Admission Control, and Inter-ASN mobility management. CSN includes network elements such as routers, AAA proxy/servers, and user databases. The QoS management is defined by the NWG specification [30–33] and the IEEE 802.16e-2005 standard [29]. It defines the data traffic differentiation mechanism over the wireless link and associated management functions included in the core network entities, that is, ANS-GWs and Authorization and Accounting servers.

A terminal is associated with a number of service flows characterized by QoS parameters. This information is provisioned in a subscriber management system or in a policy server, typically a AAA server. A service flow is a MAC transport service that provides unidirectional transport of packets (uplink or downlink). IEEE 802.16 specifies five Data Delivery services in order to meet the QoS requirement of multimedia applications: *Unsolicited Grant service (UGS)*, *Real-Time Polling Service (rtPS)*, *Non-Real Time Polling Service (nrtPS)*, *Extended Real-Time Variable Rate (ERT-VR) service*, and *Best Effort (BE)*. Each Data Delivery Service is associated with a predefined set of QoS-related service flow parameters. The QoS profile, which is a set resource-access authorizations and preprovisioned service flows, is downloaded from the AAA server to the ASN-GW at the network entry as a part of the authentication and authorization procedure. Service flows creation is initiated based on negotiation exchanges engaged by the terminal, the BS, and the ASN-GW.



(a) heterogeneous access subnetworks

(b) homogeneous access subnetworks

Figure 5: WiFi-WiMAX network.

Security in WiMAX network is based on Key management protocol (PKM). The latter defines mutual authentication exchanges between the terminal and the network entities, that is, the BSs and the ANS-GWs. These exchanges result in the generation of a hierarchical sequence of authentication keys. Each key is related to the authentication of the terminal with a level of the access network: BS, ASN-GW, and AAA server. After the authentication, the terminal negotiates with the serving BS a cryptographic suite for each provisioned service flows.

The WiMAX network entry procedure requires, as with WiFi, several exchanges for the authentication and the establishment of provisioned service flows. The technology defines an HO management mechanism based on proactive and reactive terminal context transfers from the ASN-GW and the serving BS to target BSs while attempting to ensure minimal delay and data loss during the HO procedure. The terminal context includes authentication parameters, service flow parameters (QoS information, cryptographic information, classification rules, etc.), and PHY capabilities of the terminal. Having these information elements, a target BS will be able to associate the terminal during the HO procedure with the minimum of negotiation exchanges. However, such as the HO management mechanism defined for the WiFi, this optimization is restricted to horizontal HOs.

4.3. WiFi-WiMAX Integration

4.3.1. Network Architecture. We propose a flexible deployment schema for the network architecture. The access subnetworks may offer a *homogeneous deployment* that gathers PoAs offering the same technology: WiMAX subnetworks including Base Stations (BSs) and WiFi subnetworks including Access Points (APs). It is also possible to offer a *heterogeneous deployment* that gathers PoAs according to the wireless coverage neighborhood apart from their technologies. In all types of deployment, a mobile terminal may execute vertical HOs (BS to AP and AP to BS) and horizontal HOs (AP to AP and BS to BS). Figure 5 shows the two deployments.

4.3.2. The L2-Acc-Mgr. L2-Acc-Mgrs, associated to access subnetworks, manage the L2-HO for both vertical and horizontal HOs. They support *WiFi and WiMAX specific functions* that manage authentication and accounting exchanges with terminals during network entries. An L2-Acc-Mgr acts as an ASN-GW for the WiMAX terminals and as an AAA proxy for the WiFi terminal during the network entries. These functions allow the L2-Acc-mgr to support *layer-2 service proxy* function.

This specification defines management exchanges between L2-Acc-Mgr and PoAs (APs and BSs), the intelligence related the triggering of exchanges, and the management of context information elements. We limit the description of the neighborhood management function to the definition of *Recommended PoA lists*. The actual content is to be defined by the network operator that can define the neighborhood management function based on wireless cell load, network topology, PoA geographic neighborhood, link status, and mobility behaviors.

The translation functions define the information element values to be established during HO procedures for both vertical and horizontal HOs. This specification considers the user authentication, the QoS management and WiMAX PHY layer enhancement as the services to be managed during the L2-HO preparation procedure. In the next subsection, we detail the specification of this function.

4.3.3. Terminal Context Translation. For horizontal HOs, the translation function provides context information elements based on the ones used during actual association. The

Table 2: QoS mapping between IEEE 802.11e and IEEE 802.16e-2005 classes.

802.16e-2005 Data Delivery service	802.11e UPs	Application
UGS	6,7	Voice
ERT-VR	5	Voice with silence suppression
RT-VR	4	Video
NRT-VR	3	FTP
BE	1,2,0	Email,Web

computation is based on what is defined by each technology for internal HO optimization.

When the context establishment is executed to prepare a vertical HO (serving PoA and target PoA with different technologies), the computation of values of context information elements is less obvious than with horizontal HOs. However, we have found a similitude between the QoS and authentication management of WiMAX and WiFi. Therefore, we define a mapping between the terminal context of the WiFi and WiMAX that enables the translation function to define values for WiFi context information-elements (resp., for WiMAX context information-elements) based on values related to a WiMAX association (resp., for WiFi association).

(a) QoS Information Elements. Regarding QoS management, the traffic differentiation defined by *IEEE 802.11e parameterized QoS* mechanism and the WiMAX QoS management are very similar, particularly *Traffic Stream* and *Service Flow* concepts.

We specify an association between User Priorities used in IEEE 802.11e and IEEE 802.16e-2005 Data Delivery services. These two types of information are used to characterize in each technology the class of the traffic flow. We suggest the static association between class of services of both technologies shown in Table 2. Classes are mapped according to the key QoS requirement for each Data Delivery Service. As shown in the mapping table, more than one User Priority correspond to UGS and BE data delivery service. Therefore, when the IEEE 802.16e-2005 is the serving technology, we propose to map Service Flows with data delivery service corresponding to UGS into TSs with UP equal to 6 and those with data delivery service corresponding to BE into TSs with UP equal to 1.

In addition, we propose a mapping between QoS parameters associated to each IEEE 802.16e-2005 Data Delivery service and IEEE 802.11e QoS parameters defined in the TSPEC information element. The IEEE 802.16e-2005 defines specific QoS parameters for each Data Delivery Service. However, IEEE 802.11e defines a list of parameters used for QoS characterization that may be more extensive than needed or available for any particular instance of parameterized traffic. The specification does not define a correspondence between traffic categories (defined using UPs) and possible lists of associated parameters. To be able to ensure a mapping between QoS parameters, we propose to consider the matching defined by the IEEE 802.16e-2005 between Scheduling services and QoS parameters as a reference in the translation procedure. The parameters associated to a traffic flow depend on the traffic class associated to it in both IEEE 802.11 and IEEE 802.16e-2005. We propose a static translation procedure between QoS parameters to be used by the Translation Function. The translation process depends on the QoS information related to the current terminal association, that is, the serving technology.

(i) *Terminal associated to a IEEE 802.11 PoA*: in this case, the Parameter Translation Function translates the TSPEC list into an SF info list.

Firstly, the UP related to the TS is translated into a Data Delivery Service in accordance to mapping proposed in Table 2. The retained Data Delivery Service indicates the IEEE 802.11e QoS parameters to be determined using the translation. Secondly, the Parameter Translation Function defines values related to the Data Delivery Service parameters based on the mapping in Table 3.

(ii) *Terminal associated to IEEE 802.16 PoA*: in this case, the Parameter Translation Function translates the SF info list into a TSPEC list.

SF info includes the Data Delivery Service and related QoS parameters. The Parameter Translation Function translates the Data Delivery Service into a UP based on mapping defined in Table 2. Then, it defines which parameters to be included in the TSPEC and their values.

Table 3 presents the mapping used to compute IEEE 802.16e-2005 QoS parameters based on the IEEE 802.11e parameters.

We now discuss some translation choices and difference with mapping used in the reverse translation (i.e., from 802.16e-2005 parameters to 802.11e ones).

(a) Unsolicited Grant Interval parameter indicates the nominal interval between successive grant opportunities for UGS and ERT-VR flows. Unsolicited Polling Interval parameter indicates the same QoS characteristic for RT-VR flows. These parameters do not have an equivalent in 802.11e QoS parameters. However, the TSPEC include Maximum Service Interval and Minimum Service Interval that defines, respectively, maximum and minimum of the interval between the start of two successive transmission opportunities. Thus, we use these two parameters to define a mean value corresponding to the IEEE 802.16e-2005 parameter: (*MinimumServiceInterval* + *MaximumServiceInterval*)/2. When the current serving technology is the 802.16e-2005, we may allocate the same value to Maximum and Minimum Service Interval 802.11 parameters. This value tallies to Unsolicited Grant Interval or Unsolicited Polling Interval value depending on Data Delivery Service.

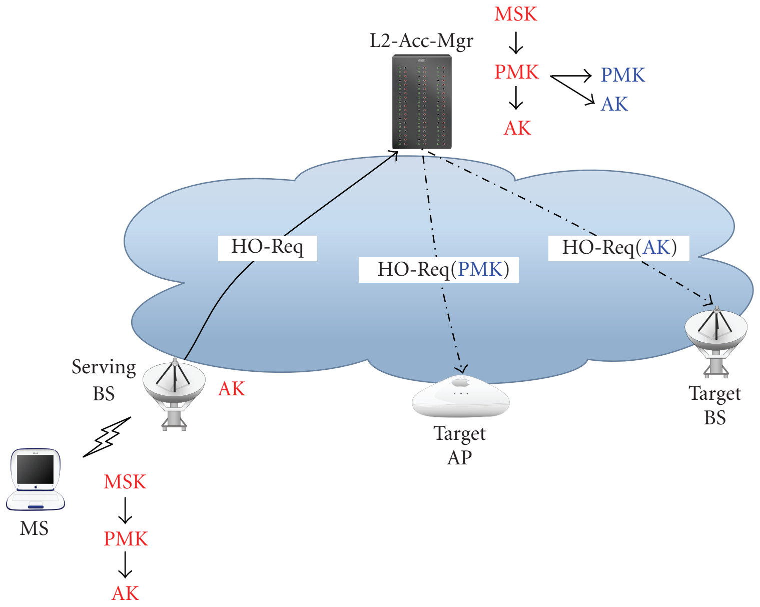


FIGURE 6: Proactive key distribution, Scenario 1.

(b) The correspondence between Traffic Priority and User Priority is defined only for mapping from 802.11 specification to the 802.16 one. In the reverse case, the value of the User Priority parameter is obtained based on the Data Delivery Service as previously indicated.

(c) The Tolerated Jitter parameter do not have an equivalent in 802.11e QoS specification. However, we propose to compute a corresponding value based on available parameters. The jitter value is defined as $J = \max(D) - \min(D)$ where D is the delay imposed to exchanged data packets. We have $D = D_l + D_n$, where D_l is local delay due to buffering and scheduling and D_n is the network delay due to the transmission of the packet. We suppose that D_l is negligible compared to D_n, and thus the latter equation will be $D = D_n$. Thus, $\max(D)$ corresponds to the *Delay Bound* 802.11 parameter. Additionally, $\min(D)$ can be computed based on the data rate perceived by the 802.11 station. The Parameter Translation Function can obtain a *Mean Data Rate* value based on information gathered by the L2-Acc-Mgr about mobile connectivity and cell states.

(b) Authentication Information Elements. The authentication procedures defined by the WiFi and the WiMAX are both based on negotiation exchanges that result to the generation of hierarchical sequences of authentication keys. The two key sequences are similar and have a common root key, the Master Session Key (MSK), negotiated between the AAA server, and the terminal for WiFi and WiMAX. Thus, it is possible to define a mapping between levels of two key sequences.

The WiMAX authentication procedure results to the establishment of the MSK transferred from the AAA server to the authenticator. The authenticator computes a Pairwise Master Key (PMK) and an Authorization Key (AK); it transfers the AK to the Base Station. A 3-way-handshake exchange is performed between the terminal and the BS based on the AK. The exchange results in the generation of Traffic Encryption Keys (TEK).

The IEEE 802.11i authentication results to an MSK negotiated between the terminal and the AAA server. The latter generates a PMK key, based on the identity of the serving AP, that it transfers to the AP. This key is used to perform the 4-way-handshake between the terminal and the serving AP. This exchange computes the Pairwise Transient Key (PTK) used to secure data transfer.

Conforming to the WiMAX specification, the AK is generated by the L2-Acc-Mgr, which acts as an ASN-GW, and delivered to the BS. Similarly, the 802.11 PMK is generated by the L2-Acc-Mgr (the 802.11 AAA proxy) and delivered to the AP. The 802.16 AK and the 802.11 PMK have the same functionality in authentication procedures. We consider these two keys as the starting point to define the inter technology translation for security parameters.

When the terminal is associated with a BS, it shares an 802.16 PMK with the L2-Acc-Mgr. This key is used to compute the AK that the L2-Acc-Mgr transfers to the BS. During the HO preparation procedure, the L2-Acc-Mgr uses the 802.16 PMK to generate keys for target PoAs. 802.16 AKs are generated for BSs, and 802.11 PMK are generated for APs. Figure 6 details related exchanges.

When the terminal is associated with an 802.11 AP, it shares an 802.11 PMK with the L2-Acc-Mg.During the HO preparation procedure, the L2-Acc-Mgr uses the 802.11 PMK to generate keys for target PoAs. 802.16 AKs are generated for BSs, and 802.11 PMK are generated for APs. Figure 7 details related exchanges.

Table 3: QoS mapping between IEEE 802.11e and IEEE 802.16e-2005 classes.

IEEE 802.16e-2005 parameter	IEEE 802.11e parameter	Description
Maximum Sustained Traffic Rate	Peak Data Rate	The peak information rate in bit per second
Maximum Latency	Delay Bound	The latency period starting at the arrival of a packet at the MAC till its successful transmission to the destination
Minimum reserved Traffic rate	Minimum Data Rate	The minimum data rate required by the traffic flow
Maximum Traffic Burst	Burst Size	The maximum continuous burst the system should accommodate for the traffic flow
SDU size	Nominal MSDU size	Number of bytes in a fixed size packet
Unsolicited Polling Interval	(**a**)	The maximum nominal interval between successive polling grant opportunities for the traffic flow
Unsolicited Grant Interval	(**a**)	The nominal interval between successive grant opportunities for the traffic flow
Traffic Priority	User Priority (**b**)	The priority among two IEEE 802.16e-2005 service flows identical in all QoS parameters.
Tolerated Jitter	(**c**)	The maximum delay variation (jitter) (in milliseconds)

(c) WiMAX PHY Information Elements. The WiMAX technology defines parameters related to PHY-layer capabilities of terminal. These parameters have no equivalent in the WiFi specification. Thus, we maintain a caching mechanism for PHY-layer capabilities managed by the translation function. PHY-layer capabilities of terminals are maintained during the ongoing session. When preparing an HO with target BSs, if a terminal has never been attached to a BS in previous associations, the L2-Acc-Mgr sends an HO-Req to target BSs without these parameters. Additionally, it indicates to the terminal, in the recommended Candidate PoA List, to execute proactive exchanges to negotiate these parameters with target BSs.

4.3.4. Context Establishment Procedure. The L2-HO optimization is based on the establishment of terminal contexts on target PoAs to avoid their re-negotiation and consequently reduce the HO delay. The context establishment procedure is mainly proactive. The neighborhood management function provides the *Recommended PoA List* to which the establishment is initiated. The QoS parameters, the authentication keys, and the WiMAX PHY profiles are established based on a context transfer managed by the L2-Acc-Mgr. The cryptographic suites are established based on a context transfer between the serving PoA and target PoAs (preparation of a horizontal HO) or proactive negotiation between the terminal and target PoAs (preparation of a vertical HO). The translation function computes values for the information elements to be established based on the available terminal context.

In addition to proactive establishment, the specification defines reactive establishment exchanges that may be engaged by the target PoA during the HO execution.

Figure 8 shows an example of the proactive phase of the context establishment procedure. The terminal is associated with a serving AP. The context establishment is performed with an AP and a BS. When a mobile terminal associates itself through an AP, the context establishment is started using an HO-Request, which includes QoS information elements sent by the serving AP to the L2-Acc-Mgr. The translation function builds the contexts related to PoAs in the *Recommended PoA List*. The HO management function initiates context transfer to PoAs using HO Request messages that includes terminal contexts. Based on target PoA responses, which indicates the support of terminal requirements, the HO management function builds the *PoA List* that is forwarded to the serving AP. The serving AP transfers the list to the terminal. The cryptographic suites are established, with available PoAs, using a context transfer with target APs and a proactive negotiation with the target BSs.

The previous example describes a preparation procedure performed with target PoAs in the same access network as the serving PoA. The HO messages are exchanged between PoAs, and the L2-Acc-Mgr managing the subnetwork and context messages are exchanged between involved PoAs. When a target PoA is located in an access network different from the serving PoA one, the HO management exchanges are relayed between the serving L2-Acc-Mgr and the target L2-Acc-Mgr to reach the involved entities. The serving L2-Acc-Mgr is the manager of the preparation procedure while the target L2-Acc-Mgr relays the messages between the latter entity and the target PoA. Figure 9 shows the exchange.

Regarding context transfers between PoAs and proactive negotiations between the terminal and the target PoAs, we make the choice not to execute these exchanges during the inter-subnet preparation procedure. Therefore, the preparation will be limited to centralized exchanges performed between the L2-Acc-Mgr and the PoAs. This is justified by results we have obtained in work related to HO preparation mechanisms proposed for the IEEE 802.11 networks regarding velocity support and signaling cost [34]. The evaluation has shown that exchanges performed between PoAs and particularly proactive negotiations are not adapted to inter-subnet mobility. In fact, they increase the signaling cost of the preparation procedure and reduce the HO performance in high mobility environments.

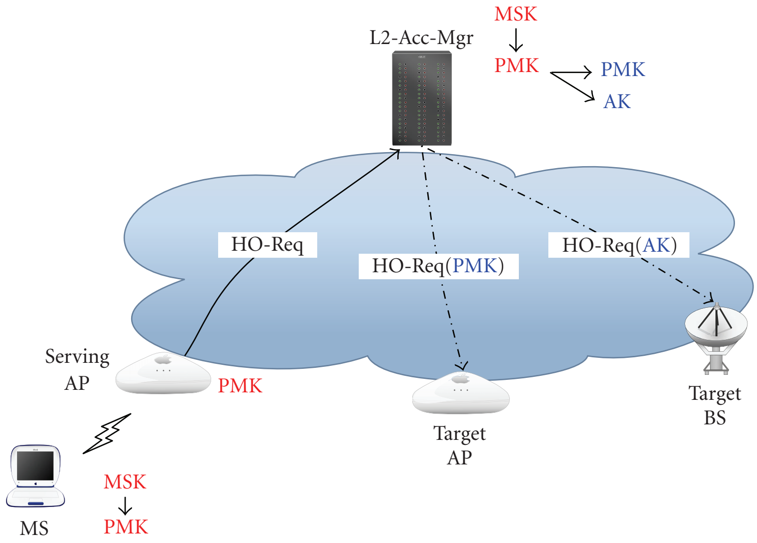


Figure 7: Proactive key distribution, Scenario 2.

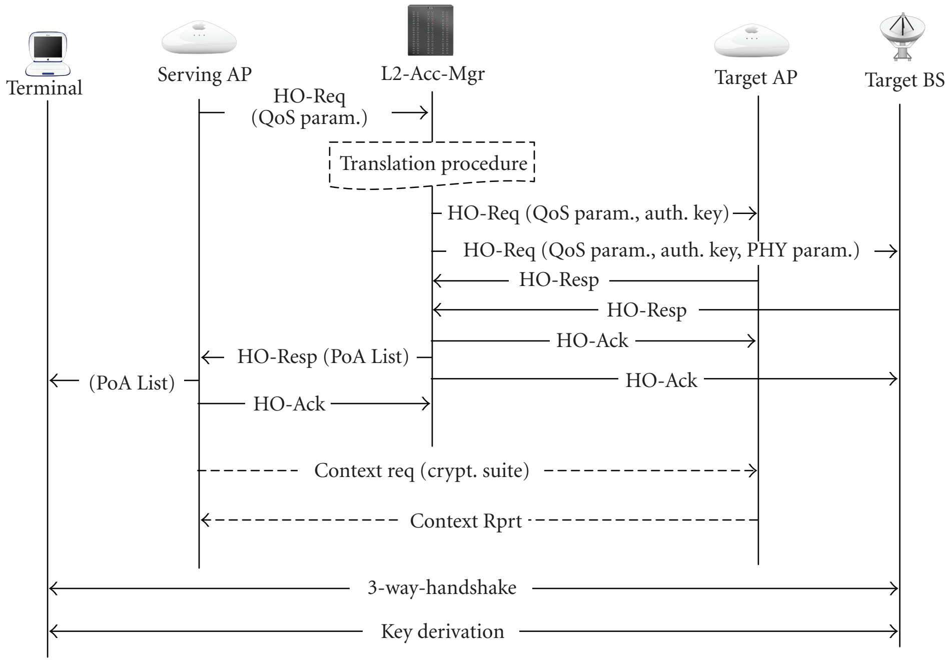


Figure 8: Example of context establishment.

4.3.5. HO Execution Optimization. The HO preparation procedure, presented in previous sections, establishes a set of context information elements and parameters in target PoAs. The exchanges engaged during the HO execution depend on the information elements that were established proactively during the HO preparation procedure or requested reactively during the HO execution. We present in the following paragraphs possible HO execution scenarios for both WiMAX and WiFi technologies. We consider optimal scenarios where target PoAs were able to acquire all context information elements.

The establishment of the terminal context results in an important optimization of the L2-HO execution procedure for both vertical and horizontal HOs. The terminal no longer needs to reauthenticate itself and to renegotiate QoS parameters and PHY profile (when the WiMAX is the target technology) during the L2-HO execution.

Figure 10 presents a regular WiFi network entry that may be executed during a first network association and an optimized reassociation procedure that may be executed during HO with an AP. In the first case, the terminal performs a regular 802.11i authentication (2, 3, 4, and 5),

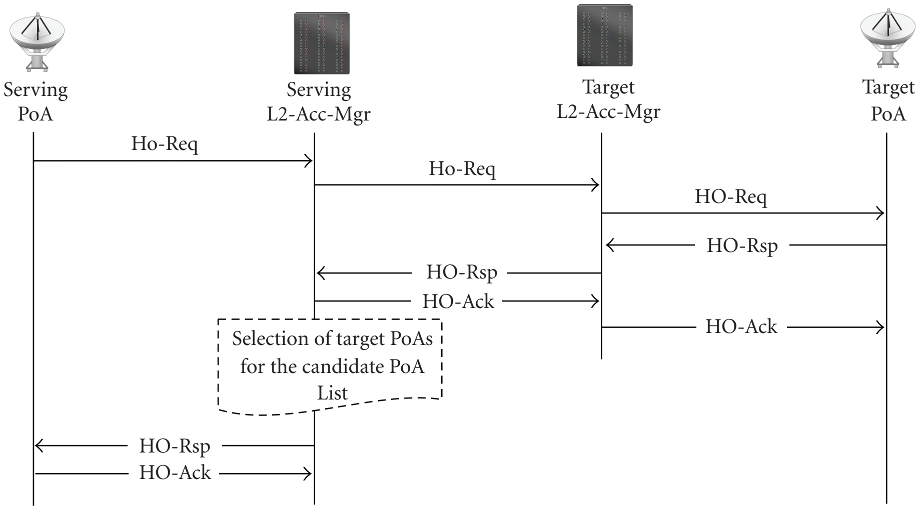


Figure 9: Inter-subnet HO preparation exchanges.

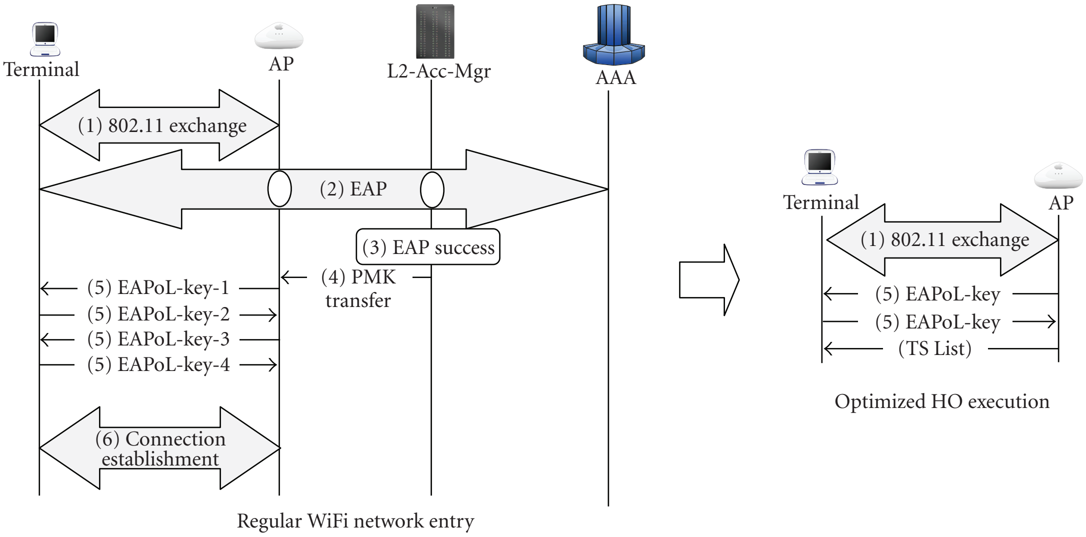


Figure 10: Association versus Re-association with a WiFi Access Point.

including exchanges with the AAA server, and the 802.11e traffic streams' establishment (6).

During a HO preparation, a target AP may acquire the Traffic Stream (TS) list and the PMK during the first phase of the procedure based on exchanges performed with the serving L2-Acc-Mgr. The target AP acquires also the PTK based on a context transfer or computes this key with a proactive negotiation performed with the AP. Therefore, in the second case of Figure 10, the terminal starts the HO execution with the legal IEEE 802.11 re-association and authentication. Over Authentication Req/Resp, the terminal and the target AP inform each other about the preestablished keys. Then, they engage a key-handshake to exchange the Group Temporal Key (GTK). If this part of the authentication exchange succeeds, the new serving AP sends to the terminal the TS List (including TSPECs), and the latter can start data exchange.

Figure 11 presents a regular WiMAX network entry that is executed during a first network association and an optimized re-association procedure that have to be executed during an HO with a BS. In the first case, the terminal performs all steps of regular WiMAX association: synchronization (1), ranging (2), basic capabilities negotiation (3), authentication (4,5, and 6), cryptographic key negotiation (7,8), and connection establishment (10,11) [29].

During handover preparation, a target BS may acquire proactively the authentication key AK, the encryption key list TEK list, the SF list, and the WiMAX PHY capabilities of the terminal. So in the second case of Figure 11, The HO execution starts with a Ranging exchange between the terminal and the target BS. The Ranging Response (RNG-Rsp) indicates the re-entry steps that are omitted thanks to the availability of terminal context information elements obtained during HO execution. Then, the target BS sends an

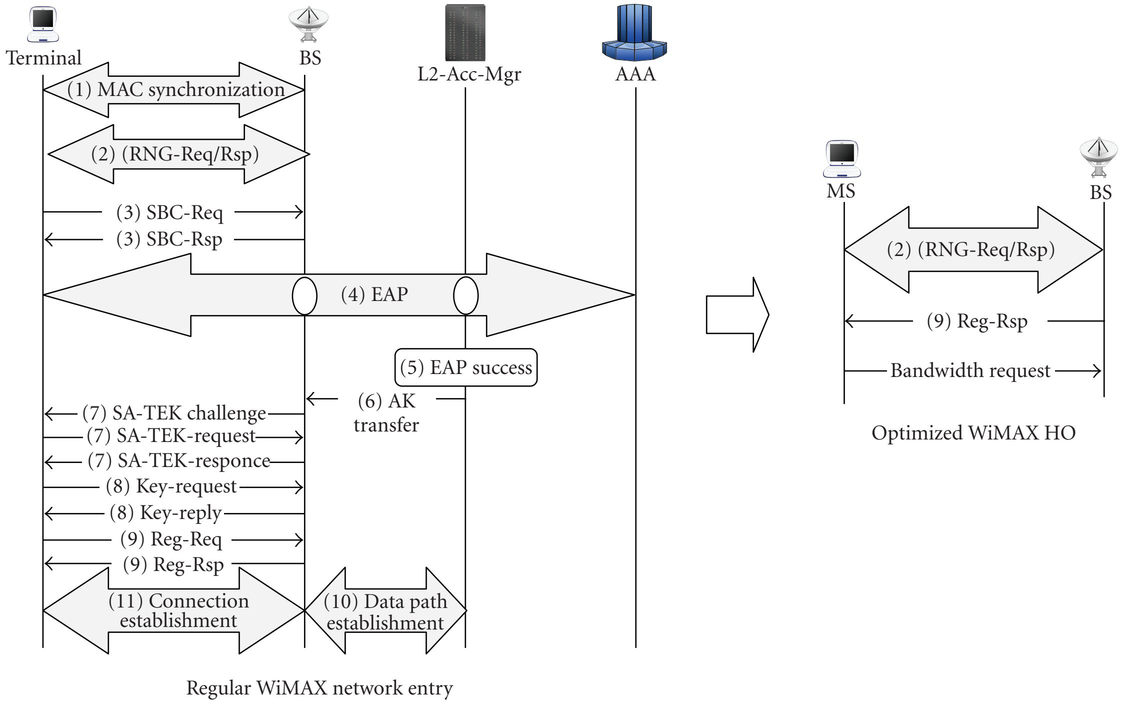


Figure 11: Association versus Re-association with a WiMAX Base station.

unsolicited Registration Response (REG-Rsp) that includes information about connections. Finally, the terminal sends a Bandwidth Request header with zero BR field to the target BS that regards this message as a confirmation of successful re-entry registration.

As shown in Figures 10 and 11, the handover execution is significantly reduced for both WiFi and WiMAX.

5. Performance Evaluation

In this section, we evaluate the performances of the L2-HO management for WiFi-WiMAX network. This evaluation requires the definition of parameters and metrics that will constitute the reference of the evaluation. The evaluation criteria will highlight both the contributions of new mechanisms and the limits of their application.

5.1. Handover Delay. The most obvious criterion that must be evaluated is the HO delay. The latter is defined as the time during which the station is not connected to any PoA. Therefore, the HO delay includes the time required to detect the need to perform a handover, to choose a target PoA, and to perform re-association exchanges.

We adopt the network simulator SimulX [35] that supports features that enable the design and the evaluation of future communication protocols like cross-layer interactions, multi-interface inter-working in terminals, and heterogeneous network environments. We have integrated to SimulX the IEEE 802.11 architecture [14] and the WiMAX architecture [36]. Both have been validated through simulation tests that result in well-known performances of both technologies. The WiFi-WiMAX architecture and the L2-HO optimization mechanism proposed in this researches have been implemented in the simulator based on the latter architectures [25].

Table 4: Handover delay.

Target technology	Opt. HO (ms)	Non-opt. HO (ms)
WiFi	24, 67	1000
WiMAX	23, 16	700

In the first scenario, we evaluate the HO delay performed when we use the L2-HO optimization mechanism. We consider a wireless network with a single access subnetwork that includes all the PoAs (two BSs and two APs). A terminal moves with a straight path to cross the wireless coverage of all PoAs of the network. We measure the delay involved by the executed L2-HOs. To show the contribution of L2-HO optimization mechanism, we can compare the inter-technology HO delay to the network entry delay of the WiFi and WiMAX technologies, which correspond to non-optimized HOs.

Table 4 lists HO delay values obtained with different types of HOs. The delay due to non-optimized HOs is evaluated to 700 ms when the WiMAX is the target technology and 1000 ms when the WiFi is the target technology. Let's note that the WiFi handover delay is larger than the WiMAX handover delay although that nonoptimization handover execution of WiMAX seems to engage even more exchanges than the WiFi handover execution (c.f. Figures 10 and 11). Actually, the detection and the search phases contribute largely to the delay induced to traffic during the handover procedure of WiFi. However, these phases are well optimized in handover procedure of WiMAX. For example, there is no search phase at the time of HO as the serving BS sends a recommended neighbor list to terminal. As a consequence, the overall HO delay of WiFi network entry during HO is larger that of the WiMAX.

The L2-HO management mechanisms ensure a uniform execution time for both intratechnology and intertechnology HOs limited to a mean value of 24,63 ms. This is obtained thanks to the context establishment mechanism that ensures the same optimization of the HO execution regardless of the target PoA type.

In a second phase of this evaluation, we study the effect of wireless cell conditions on the performances of the L2-HO optimization performances. We consider a network topology integrating six BSs with six APs in each WiMAX cell. The PoAs are attached to two access subnetworks: a WiFi subnetwork and a WiMAX subnetwork relayed through a core network, which hosts also the AAA server. A terminal moves with a straight path and a velocity of 10 m/s. We measure the HO delay for WiFi to WiMAX and WiMAX to WiMAX handovers.

In WiFi networks, the performance of terminal exchanges depends on the cell load because of the contention-based medium access [27]. In a previous research, we were interested in the evaluation of HO performances in WiFi networks. We showed that the wireless cell load has non-negligible effects on the HO execution performances. We evaluated a management mechanism that ensures the same optimization of HO execution for WiFi terminals. Results demonstrated that such optimization ensures a limited execution time (lower than 50 ms) even with high loads.

The performance of WiMAX wireless access is not sensitive to the cell load as the medium access is managed by the BS that allows transmission opportunities to the medium modeled by transmission frame [28]. However, two parameters can have an influence on the performances of HO execution: the IEEE 802.16 frame duration and the contention-based transmission period defined for network entry.

The duration of the IEEE 802.16 frame, which is configurable, has an effect on the delay between two transmission opportunities for one terminal, which impacts on the delays for exchange between the terminals and the BS. In a previous research, we have evaluated the variation of the regular WiMAX network entry as a function of the frame duration. Results have shown that the network entry duration vary from 700 ms to 1 s with frame duration that varies from 3 ms to 12 ms.

We evaluate the effect of the frame duration of the optimized WiMAX handover. Figure 12 plots the delay due to optimized WiMAX handover as a function of the 802.16 frame duration. This curve shows that the handover delay increases when the lEEE 802.16 frame duration increases. However, even with frame duration of 12 ms the handover delay remains reasonable and does not exceed the value of 50 ms (tolerable threshold of real-time applications).

The second parameter considered for WiMAX cells is the contention-based transmission period. It is used by a terminal that starts an HO procedure or an association procedure with a BS. This period has a limited duration during a single frame. The exchanges over it will be impeded by the number of terminals trying to communicate.

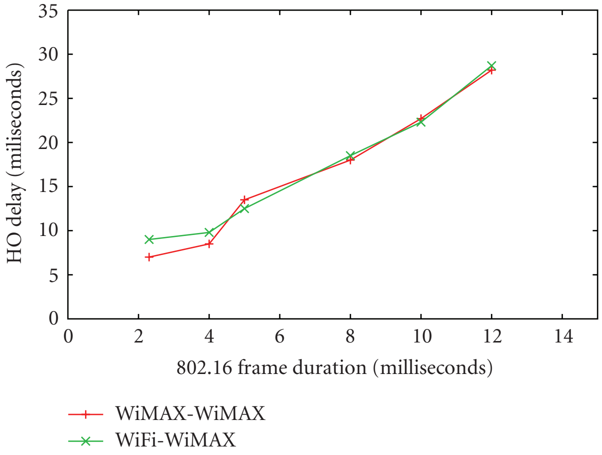


Figure 12: Effect of the 802.16 frame duration on optimized HO performances.

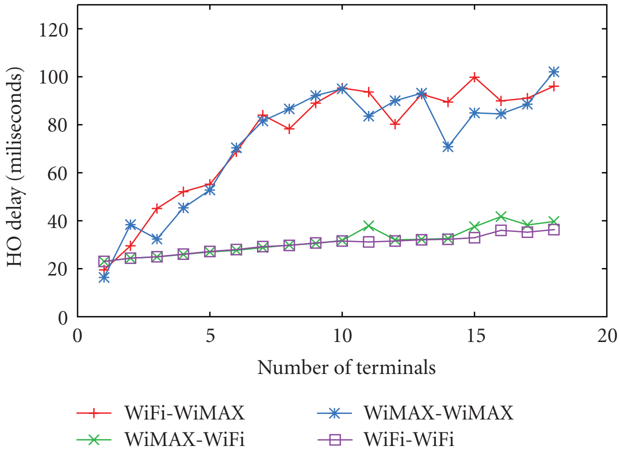


Figure 13: Effect of number of terminals on optimized HO performances.

To evaluate the effect of the number of terminals executing a network entry on the HO delay, we define a simulation scenario that varies the number of terminals executing HOs in the same contention-based transmission period of a cell, and we measure the average of HO delays. The simulation scenario defines a set of terminal moving at the same velocity, over similar trajectories, and neighbor starting points. The network topology includes six BSs with six APs in each WiMAX cell.

Figure 13 plots the evolution of the HO delay as a function of the number of terminals. The curves show an increase of the HO execution time (WiMAX to WiMAX HOs and WiFi to WiMAX HOs) with the increase of the number of terminals. This parameter exceeds 50 ms as soon as the number of terminals that try to associate exceeds 5.

5.2. Signaling Cost. We propose to evaluate the signaling overhead of the HO management mechanism associated to the WiFi-WiMAX integration network. This evaluation aims to compare the new architecture with alternative network deployments under the same conditions.

We consider a realistic deployment of the WiMAX and WiFi technologies over a city. The WiMAX is used to offer an outdoor access while the WiFi is used to offer indoor accesses. As shown in Figure 14, the WiMAX access is offered to user over a continuous coverage. The WiFi access is offered via scattered areas over the WiMAX coverage.

We compare the performances of the integration architecture (optimized architecture) to an architecture that does not integrate an L2-Acc-Mgr (non-optimized architecture). In the latter architecture, we suppose that the HO management functions, for example, neighborhood management and context establishment, are supported by centralized network servers. In addition, we evaluate the influence of the design of access subnetworks (*homogeneous deployment* versus *heterogeneous deployment*) on the HO management signaling cost performances. Four network architectures are considered: non-optimized architecture with homogeneous deployment, non-optimized architecture with heterogeneous deployment, optimized architecture with homogeneous deployment, and optimized architecture with heterogeneous deployment.

The signaling cost of a management mechanism is the transmission cost of management messages over the network links. We define a signaling cost formula that models the signaling overhead generated by one HO. This formula takes into account the proactive exchanges with neighbor PoAs during the HO preparation and the execution exchanges with a target PoA at the time of HO as shown in (1):

$$S_{\text{HO}} = S_{\text{HOpreparation}} + S_{\text{HOexecution}}. \tag{1}$$

We consider three types of network links: the local links (between entities in the same access subnetwork), the core network links, and the wireless links. To each link we associate a *weight* that models the cost of transmitting of one byte over this link. These weights allow to quantify link transmission costs relatively rather than define absolute values. A signaling cost formula is the sum of subformulas that are products of the messages' size into the crossed links' weight.

The sub-formula $S_{\text{HOpreparation}}$ of (1) (resp., $S_{\text{HOexecution}}$) is different as the HO preparation is engaged from a serving AP or a serving BS (resp., the HO execution is engaged with a target AP or a target BS).

We make use of the *VanetMobiSim* software to emulate the terminal mobility over the considered wireless deployment [37]. This software offers the list of executed HOs considering a wireless deployment and a mobility model. The combination of the signaling cost formulas and the mobility statistics allow us to evaluate the signaling cost average of the HO management over the considered deployment [25]. We assume a mix of three types of mobility model: walking users, slow cars, and fast cars. We consider one hop neighborhood definition. The Recommended PoA list integrates PoAs whose coverage areas are tangent to the serving PoA one.

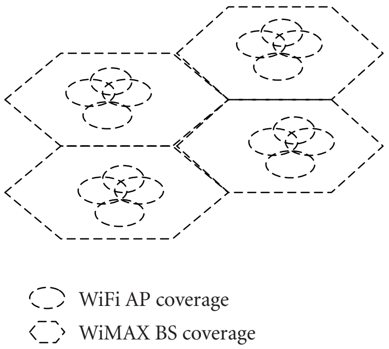


Figure 14: WiFi-WiMAX wireless coverage.

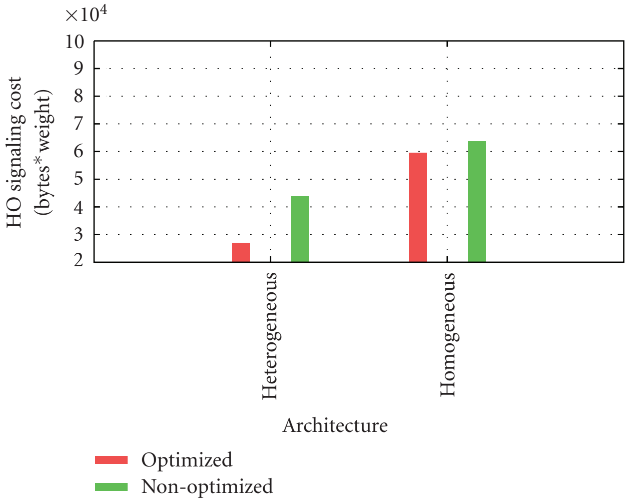


Figure 15: Basic configuration signaling cost.

In a first evaluation, we consider an arbitrary configuration with fixed value for link weight. These values indicate that the transmission cost of a management message over the core links is twice the transmission cost over the local links. The transmission cost over the wireless links is fourfold the transmission cost over local links. With this configuration, Figure 15 plots the measured HO signaling costs related to network architectures.

Both the optimized architecture and the heterogeneous deployment reduce the signaling cost of an HO. Particularly, a combination of these strategies in the same network offers a significant reduction of the HO signaling cost. The optimized architecture allows the confining of establishment exchanges at best to an access network and at worst to a connection between two L2-Acc-Mgrs. As a result, there is no more exchanges with centralized servers for HO management. On the other hand, the heterogeneous deployment allows to gather neighbor PoAs in the same access network. The use of the latter deployment with a non-optimized architecture enables to reduce inter-PoAs exchanges to the intra-access networks exchanges, which reduces significantly the HO management signaling cost. With an optimized architecture, the heterogeneous deployment enables, as well, to confine centralized exchanges to into one access network.

In a second step, we study the effect of architecture parameters on the HO management signaling cost. We consider the core-link weight and the neighborhood definition.

Figure 16 plots the evolution of the handover signaling cost as a function of the core-link weight. Both the optimized architecture and the heterogeneous deployment reduce the effect of core link cost on the HO signaling cost. The combination of an optimized architecture and a heterogeneous deployment offers the better optimization. These results confirm that the design of a network architecture based on this combination reduces the consumption of the core network resources by HO management signaling overhead. In fact, the signaling exchanges related to a mobile terminal will be enclosed in the wireless cells and access subnetworks in its mobility areas. Thus, the proposed designs ensure the enhancement of HO performances while reducing the core network resources.

The enlargement of neighborhood definition is important to ensure a better mobility support. Indeed, a multiple-hop neighborhood should ensure a good support of fast moving terminals. However, this neighborhood definition may result to an increase of the signaling cost of HOs. To study the effect of the neighbor list size, we assume a second neighborhood definition including PoAs that are reachable within two hops. The neighbors of an AP are the APs that surround within two hops and the BS that covers the area if it is reachable by a terminal on two hops. The neighbors of a BS are the APs on its coverage zone reachable at most with two hops and the BSs in its immediate wireless neighborhood.

We compare the HO signaling costs of this neighborhood definition to those obtained with the one-hop neighborhood definition proposed in the basic network configuration. The results are shown in Figure 17. Both the optimized architecture and the heterogeneous deployment reduce the effect of the growth of the neighbor-list size on the HO signaling cost. As in the previous evaluation, the combination of these network designs offers the better results regarding HO management signaling cost. This combination allows the operator to design wireless network with better mobility support without increasing the HO management signaling overhead.

6. Interaction with Layer-3 Handover Management Mechanisms

In this study, we are interested in optimization of HO performances in heterogeneous networks. Our proposals have been limited to the management of layer-2 handovers (L2-HO). Thus, it seemed interesting to study the interaction of this framework with additional HO management mechanisms, proposed in the literature, that may be deployed in heterogeneous networks. We consider in particular the mobility management based on FMIPv6 and the Media Independent Handover (MIH) mechanism proposed by the IEEE 802.21 standard to optimize vertical HOs.

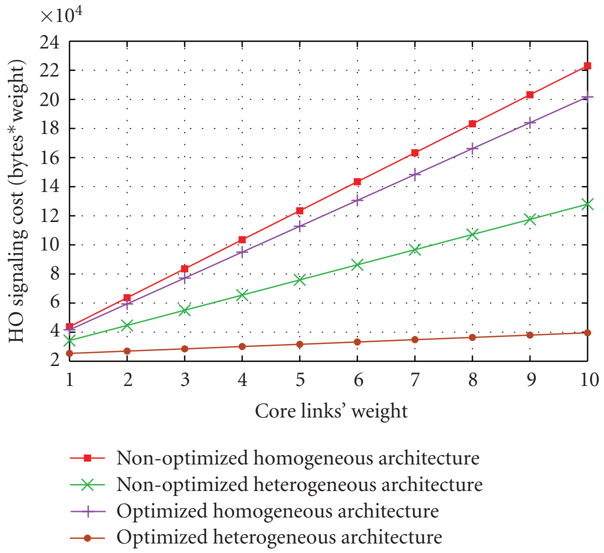


Figure 16: Core Link weight effect on HO signaling cost.

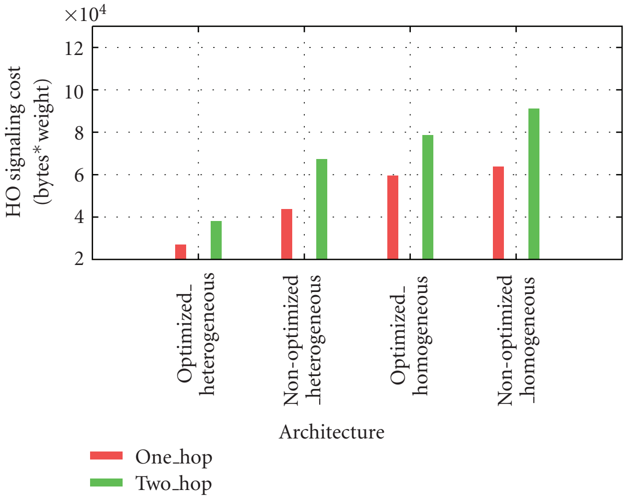


Figure 17: Neighborhood definition effect on HO signaling cost.

6.1. Collaboration with FMIP. The Fast handover for Mobile IPv6 (FMIPv6) [38] proposes an improvement to the MIPv6 that reduces the layer-3 handover latency. FMIPv6 defines a collaboration between access routers (ARs) to accelerate the acquisition of link configuration parameters and the forwarding of data traffic when a terminal executes a handover from a previous AR (PAR) to a new AR (NAR). It enables the mobile terminal to learn the IPv6 link configuration parameters (IP subnet) related to links, that it detects, before it starts effectively the HO execution. The terminal may request information, about all wireless links, to the current router. The reply can be received on the old link or on the new link (reactive HO). During the HO execution, the terminal sends a message to the NAR to inform it about the movement.

The framework, proposed in this research, enables two possible configurations regarding L3-HOs. In the first case, access subnetworks offers heterogeneous access technologies, which allow having several technologies on the same IP subnetwork (with the same prefix). This approach avoids the need to define a relation between the L2-HO mechanisms and a possible L3-HO, since the latter is no longer necessary. With the other possible configuration, each access subnetwork offers a single access technology, that is, WiFi access subnetworks and WiMAX access subnetworks. With this architecture, a vertical HO leads to a L2-HO associated to an L3-HO. Therefore, in addition to the L2-HO management mechanism we have defined, there is a need to ensure a management of the L3-HO. This can be possible by defining an interaction between the latter mechanism and FMIPv6. The L2-HO management mechanism defines the reception of neighboring PoAs list with which the HO preparation has been performed. This list may be used, by the FMIPv6 module, to engage the management procedure defined previously with ARs attached to PoAs in the list. Upon receiving an indication of the imminent HO execution, the terminal knows its next AR; so it can prepare the configuration of its interface with new IP parameters and wait for the indication of the L2-HO handover execution success. The latter HO execution is optimized thanks to the preparation procedure of the L2-HO management mechanism. The link availability indication may also be used to trigger the preparation of following handovers.

6.2. Collaboration with the MIH. The Media Independent Handover (MIH), proposed by the IEEE 802.21 [39], defines tools to manage multiple interfaces in the same terminal. Particularly, it manages exchange of information elements between the terminal and the network to enhance the decision and search phases of the handover procedure. It also helps the preparation of the HO execution between heterogeneous technologies. For example, the MIH provides to upper layers, link-layer triggers based on reactive and predictive local link state changes and network information (load balancing information, operator preferences) that enhance the HO detection. It also supports the transfer of global network information (list of available networks, neighbor maps and higher layer network services) from network servers to the terminal to help it on the HO preparation procedure. However, the handover execution optimization is not part of the MIH functions.

The mechanisms, proposed by the MIH, are complementary to the solution we have proposed. Indeed, it is possible to make use of the MIH with our solution. Its role will be to manage exchanges between the terminal and the network entities during the HO preparation procedure and to interact with heterogeneous interfaces for the optimization of HO execution based on context information elements established proactively.

In the integration example we have proposed in IV, we use mechanisms offered by WiFi and WiMAX to perform actions related to the heterogeneous HO management. The IEEE 802.21 proposes media-dependent interfaces and primitives to be used with the WiFi and the WiMAX technologies. This will make easier the integration of the MIH to the specification we have proposed. MIH functions can be used, for example to, transfer the Recommended PoA list to the terminal during HO preparation.

7. Discussions about Heterogeneous Technology Integration

It is obvious that the mobility management in the heterogeneous wireless networks is more complex than classic wireless networks. Indeed, the more we try to optimize the HO at a low level (to ensure better performances), the more proposed solutions are dependent on the specificities of technologies. This makes difficult the optimization of the L2-HO between heterogeneous technologies, particularly when their designs are based on different principles, for example, the network accesses (connected mode or shared access mode), core network organization, and so forth. In this research, we have been able, as well, to propose a layer-2 handover optimization solution based on general and technology-agnostic framework. This framework offers mechanisms that optimize the L2-HO delay independently of the engaged mobility type (homogeneous or heterogeneous), which is a novel idea.

Another interesting point related to this framework is the ability of the proposed architecture to facilitate the extension of heterogeneous networks based on additional technologies. In fact, the location of HO management functions at L2-Acc-Mgr allows avoiding the modification of technology specific network entities, for example, PoAs, and functions, for example, authentication and accounting during these possible extensions. Modifications are restricted to the adaptation of the L2-Acc-Mgr and their functions. Let us consider the extension of the WiFi-WiMAX network, we have proposed in Section 4, based on a UMTS access. This will require, first, to define the possible associations between the QoS and security parameters in UMTS, WiFi, and WiMAX to include adequate translation rules at the *Translation function*. Second, we have to define at UMTS core network entities that manage terminal active contexts, for example, Radio Network Controllers (RNCs) or Serving GPRS Support Node (SGNC), a context exchange with L2-Acc-Mgrs. Therefore, the latter will be able to execute translation rules and to engage context establishment over WiMAX BSs and/or WiFi AP.

Based on this framework, it is possible to propose a new organization of heterogeneous networks where heterogeneous PoAs are gathered in the same access subnetwork based on the neighbor of their wireless coverage. Although, this organization remains far from current deployments' organization, it is very interesting to consider these aspects for future network deployments as we have demonstrated that such a configuration enables optimized heterogeneous HOs with very low singling overhead, which is not the case with classic network configuration. At least, network providers have to retain that with the growth of heterogeneous mobility there is a need to consider wireless coverage neighborhood between heterogeneous PoAs to ensure a reasonable signaling overhead above the core network.

Finally, we return to the fact that the use of this framework remains interesting with classic architectures and that this configuration does not have as many constraints as is believed. In fact, we can use this framework to propose the interconnection of local and restricted wireless networks, for example, a WiFi hotspot or a private WLAN, to a larger network such as a WWAN or a WMAN. The L2-Acc-Mgrs will connect the hotspot to the core network router of the WWAN that manages PoAs with coverage close to the hotspot.

8. Conclusion

In this work, we have been interested in the integration of heterogeneous wireless technologies in the same network. We have defined a technology-integration framework that defines an optimization of both horizontal and vertical HOs based on context establishment mechanisms in heterogeneous environments. We have proposed an application of this general framework to the deployment of a WiFi-WiMAX network. This application demonstrates the utility of this framework based on a practical network deployment and enables the performance of evaluation tests. The latter shows an efficient optimization of handover delays associated to a minimization of management signaling costs.

We have shown the interest for network access providers to upside the conventional network architecture by merging the backbones of heterogeneous wireless access networks. Thus, PoAs will be gathered based on the closeness of wireless coverage, which ensures an efficient optimization of HO performances with minor signaling overhead. Such network deployments are more adapted to Next Generation Wireless Networks where vertical HOs will be more frequent and trivialized.

In future work, we are interested in proposing an application of this framework for the deployment of communication systems for transport context and especially rail transport. The latter are required to operate in extremely varied environments, such as urban and suburban environments, countryside, sparsely or very low populated, tunnels, and railway stations. In addition, transport systems have very high constraints regarding transmission delays, robustness, and reliability. On the other hand, the fact that trajectories are easily predictable offers interesting perspectives for the context management, which raises the interest of adapting our solution to this particular context.

References

[1] M. Kassab, J.-M. Bonnin, and A. Belghith, "General strategies for context re-establishment in IEEE 802.11 networks," in *Proceedings of the 8th International Conference on Intelligent Transport System Telecommunications (ITST '08)*, pp. 72–77, October 2008.

[2] G. Lampropoulos, N. Passas, L. Merakos, and A. Kaloxylos, "Handover management architectures in integrated wlan/cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 30–44, 2005.

[3] C. Makaya and S. Pierre, "An interworking architecture for heterogeneous ip wireless networks," in *Proceedings of the 3rd International Conference on Wireless and Mobile Communications (ICWMC '07)*, p. 16, March 2007.

[4] R. Samarasinghe, V. Friderikos, and A. Aghvami, "Analysis of Intersystem Handover: UMTS FDD & WLAN," Centre for Telecommunications Research.

[5] S.-L. Tsao and C.-C. Lin, "Design and evaluation of UMTS-WLAN interworking strategies," in *Proceedings of the 56th Vehicular Technology Conference*, vol. 2, pp. 777–781, September 2002.

[6] N. Vulic, I. Niemegeers, and S. H. De Groot, "Architectural options for the WLAN integration at the UMTS radio access level," in *Proceedings of the 59th IEEE Vehicular Technology Conference (VTC '04)*, vol. 5, pp. 3009–3013, May 2004.

[7] Y.-T. Chen, "Achieve user authentication and seamless connectivity on wifi and wimax interworked wireless city," in *IFIP International Conference on Wireless and Optical Communications Networks (WOCN '07)*, pp. 1–5, July 2007.

[8] S. Khan, S. Khan, S. A. Mahmud, and H. Al-Raweshidy, "Supplementary interworking architecture for hybrid data networks (UMTS-WiMAX)," in *International Multi-Conference on Computing in the Global Information Technology (ICCGI '06)*, August 2006.

[9] Q. Nguyen-Vuong, L. Fiat, and N. Agoulmine, "An architecture for umts-wimax interworking," in *Proceedings of the 1st International Workshop on Broadband Convergence Networks (BcN '06)*, pp. 1–10, April 2006.

[10] G. TS, "3GPP System to WLAN Interworking: System Description (Release6)," Tech. Rep., 3GPP TS, March 2004.

[11] C. Perkins, "IP Mobility Support for IPv4," IETF, August 2002.

[12] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, "Rfc context transfer protocol," *Internet Draft, draft-ietf-seamoby-ctp-11.txt*, February 2005.

[13] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)," Draft IETF (Work in progress), December 2006.

[14] M. Kassab, S. Hachana, J.-M. Bonnin, and A. Belghith, "High-mobility effects on WLAN fast re-authentication efficiency," in *FTDA-DN Workshop, Held in Conjunction with Qshine*, July 2008.

[15] K. Gakhar, A. Gravey, and A. Leroy, "IROISE: a new QoS architecture for IEEE 802.16 and IEEE 802.11e interworking," in *Proceedings of the 2nd International Conference on Broadband Networks (BROADNETS '05)*, pp. 607–612, October 2005.

[16] D. Niyato and E. Hossain, "Wireless broadband access: WiMax and beyond—integration of WiMAX and WiFi: optimal pricing for bandwidth sharing," *IEEE Communications Magazine*, vol. 45, no. 5, pp. 140–146, 2007.

[17] Z. Dai, R. Fracchia, J. Gosteau, P. Pellati, and G. Vivier, "Vertical handover criteria and algorithm in IEEE 802.11 and 802.16 hybrid networks," in *IEEE International Conference on Communications (ICC '08)*, pp. 2480–2484, May 2008.

[18] J. Nie, J. Wen, Q. Dong, and Z. Zhou, "A seamless handoff in IEEE 802.16a and IEEE 802.1 in hybrid networks," in *International Conference on Communications, Circuits and Systems*, pp. 383–387, May 2005.

[19] S.-F. Yang and J.-S. Wu, "Handoff management schemes across hybrid WiMAX^{TM} and Wi-Fi^{TM} networks," in *IEEE Region 10 Conference (TENCON '07)*, pp. 1–4, November 2007.

[20] T. Ali-Yahiya, K. Sethom, and G. Pujolle, "Seamless continuity of service across WLAN and WiMAN networks: challenges and performance evaluation," in *Proceedings of the 2nd IEEE/IFIP International Workshop on Broadband Convergence Networks (BcN '07)*, pp. 1–12, May 2007.

[21] "Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," EEE Computer Society, Standard, 1999.

[22] WiMAX Forum, "WiMAX Forum Web page," September 2008, http://www.wimaxforum.org/.

[23] LAN/MAN Standards Committee, "IEEE 802.11i: Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE Computer Society, Standard, April 2004.

[24] LAN/MAN Standards Committee, "IEEE 802.11e Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," IEEE Computer Society, Standard, November 2005.

[25] M. Kassab and J.-M. Bonnin, "Optimized layer-2 handover inWiFi-WiMAX networks," Research Report, Telecom Bretagne, 2009.

[26] M. Kassab, A. Belghith, J.-M. Bonnin, and S. Sassi, "Fast and secure hanfoffs for 802.11 infrastructures networks," *NetCon05 Lannion France*, november 2005.

[27] M. Kassab, A. Belghith, J.-M. Bonnin, and S. Sassi, "Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks," in *Proceedings of the 1st ACM International Workshop on Wireless Multimedia Networking and Performance Modeling (WMuNeP '05)*, pp. 46–53, October 2005.

[28] I. L. S. Committee, "Part 16: Air interface for fixed broadband wireless access systems," IEEE Computer Society, Standard, June 2004.

[29] I. L. S. Committee, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," IEEE Computer Society, Standard, February 2006.

[30] N. WG, "Wimax forum network architecture stage 2: architecture tenets, reference model and reference points, part 0," WiMAX Forum, Wimax End-to-End Network Systems Architecture, August 2007.

[31] N. WG, "Wimax forum network architecture stage 3: detailed protocols and procedures," WiMAX Forum, Wimax End-to-End Network Systems Architecture, March 2007.

[32] N. WG, "Wimax forum network architecture stage 2: architecture tenets, reference model and reference points, part 1," WiMAX Forum, Wimax End-to-End Network Systems Architecture, August 2007.

[33] N. WG, "Wimax forum network architecture stage 2: architecture tenets, reference model and reference points, part 2," WiMAX Forum, Wimax End-to-End Network Systems Architecture, August 2007.

[34] M. Kassab and J.-M. Bonnin, "HO preparation based on network-entry parameter pre-establishement: a signaling cost study," Research Report, Telecom Bretagne, October 2007.

[35] N. Montavont, J. Montavont, and S. Hachana, "Wireless IPv6 simulator: SimulX," in *Proceedings of the 40th Annual Simulation Symposium, Part of the Spring Simulation Multiconference*, Norfolk, Va, USA, March 2007.

[36] M. Kassab, J.-M. Bonnin, and M. Mahdi, "WiMAX Simulation module with management architecture and signaling exchanges," in *International Workshop on Network Simulation Tools (NSTOOLS)*, October 2009.

[37] M. Fiore, "Vanetmobisim," February 2007, http://vanet.eurecom.fr/.

[38] E. R. Koodli, "Mobile IPv6 Fast Handovers," IETF, RFC 5268, June 2008.

[39] LAN/MAN Standards Committee, "IEEE Standard for Local and Metropolitan Area Networks- Part 21: Media Independent Handover," *IEEE Std 802.21-2008*, pp. c1-301, January 2009.